Declaration

The work in this thesis is my own except where otherwise stated.

[Signature]

Charles Hempel
Acknowledgements

It is with great pleasure that I thank Dr. L. G. Kovács for his encouragement and generous supervision. Not only has he devoted much of his time to proof reading this work, but many results in this thesis such as Lemmas 5.2, parts of 1.1 and 3.3 are his.

I would also like to thank Dr B. Höfling for his help with number theory and GAP, Professor M. F. Newman for his help with metacyclic 2-groups and for making his and Professor M. Xu's classification available, Dr P. J. Cossey for answering my numerous questions on general group theory, Professor B. H. Neumann for his ideas about how my work can be extended and all of the above people for their general guidance.

I would like to acknowledge the generous support provided by an Australian National University Scholarship, and I would like to thank everyone in the School of Mathematical Sciences where I was located.

Finally, I would like to thank Manami Aoi and my parents for their love and support.
Abstract

A group $G$ is metacyclic if it contains a cyclic, normal subgroup $N$ such that $G/N$ is also cyclic. The first five chapters of this thesis are almost entirely devoted to the proof of Theorem 5.3 in which finite metacyclic groups are classified up to isomorphism in terms of presentations. Those groups which are split are then identified. A GAP program to determine the canonical presentation afforded by Theorem 5.3 of any finite metacyclic group is listed in Chapter 6. Infinite metacyclic groups, the structure of which is by comparison much easier understand, are classified in similar terms in Chapter 7.
List of notation

$G/N$ the quotient group of $G$ modulo $N$

$H \leq G$ $H$ is a subgroup of $G$

$N \trianglelefteq G$ $N$ is a normal subgroup of $G$

$m \mid n$ $m$ divides $n$.

$p^m \mid n$ $p^m$ exactly divides $n$.

$\psi(n, p)$ integer $m$ such that $p^m \mid n$

$n_\pi$ the $\pi$ component of $n$

$G_\pi$ the Hall $\pi$-subgroup of a finite nilpotent group $G$

$(m \mid n)$ smallest $i$ such that $i \equiv m_{(p)} \mod n_{(p)}$ for all $p \in \pi(n)$

$J(n)$ the prime residue group modulo $n$

$\text{ord}_n m$ the order of $m$ modulo $n$

$m_n^{-1}$ the inverse of $m$ mod $n$ in $J(n)$

$\varpi(G)$ the set of primes which divide the order of $G$

$\pi(m/n)$ $\{ p \mid p$ is a prime divisor of $m \}, (m/n \text{ nonzero rational in lowest form})$

$J(m, n)$ the set $\{ \kappa \in J(n) \mid \kappa^m = 1 \}$

$T(n)$ the set $\{ \kappa \in J(n) \mid \text{if} \text{ord}_n \kappa^s = \text{ord}_n \kappa, \text{then} \kappa^s \mod n \geq \kappa \}$
\( T(m, n) \) the set \( T(n) \cap J(m, n) \)

\( O(G) \) the set of orders of elements of \( G \)

\( \Gamma \) the set \( \{ (n, H) \mid n \in \mathbb{N}, n \geq 1, H \leq J(n) \} \)

\( \mathbb{N} \) the set of natural numbers 0, 1, 2, ...

\( \mathbb{Z} \) the set of integers

\( \mathbb{Q} \) the set of rational numbers

\([G : H]\) index of \( H \) in \( G \)

\( N \cong M \) \( N \) is isomorphic to \( M \)

\( N \approx M \) \( N \) is characteristically conjugate to \( M \)

\( Q_n \) quaternion group of order \( n \)

\( C(G) \) \( \{ H \mid H \leq G, H \) contains a kernel of \( G \} \)

\( \text{Aut} G \) group of automorphisms of \( G \)

\( \exp G \) the exponent of \( G \)

\( N_{\text{Aut} G}(S) \) normaliser of \( S \) in \( \text{Aut} G \)

\( C_{\text{Aut} G}(S) \) centraliser of \( S \) in \( \text{Aut} G \)

\( N_{G/C} \) subgroup of \( \text{Aut}(G/C) \) induced by a subgroup \( N \) of \( N_{\text{Aut} G}(C) \)

\( V(P) \) the set \( \{ g^2 \mid g \in P \} \)

\( \delta(m, n) \) the Kronecker delta function

\( \zeta(G) \) the centre of \( G \)

\( G' \) the derived subgroup of \( G \)

\([x, y]\) the commutator \( x^{-1}y^{-1}xy \) of \( x \) and \( y \)

\( \mathbb{Q}_\pi(G) \) the largest normal \( \pi \)-subgroup of \( G \)
# Contents

Abstract iv

1 Background 1
   1.1 Introduction ........................................................ 1
   1.2 Notation and basic facts ........................................ 3

2 Standard Hall-decompositions and $p$-groups of odd order 8

3 Metacyclic 2-groups 12

4 Expressions for induced automorphism groups of quotients of $p$-groups 24

5 Finite metacyclic groups 43

6 The GAP program 59

7 Infinite metacyclic groups 73

Bibliography 76
Chapter 1

Background

1.1 Introduction

A group $G$ is metacyclic if it contains a cyclic, normal subgroup $N$ such that $G/N$ is also cyclic. Such a subgroup $N$ will be called a kernel of $G$, and we hope that the reader will accept this restricted use of the term. It is easy to see that a metacyclic group can be written $G = SN$ with $S \leq G$, $N \leq G$ and both $S$ and $N$ cyclic. Such a product is a metacyclic factorisation of $G$. If $G$ has a metacyclic factorisation $SN$ with $S \cap N = 1$, then $G$ is split.

It was already known to Hölder (see Theorem 7.21 in Zassenhaus [21]) that finite metacyclic groups can be presented on two generators and three defining relations as in Lemma 1.1.

Certain classes of metacyclic groups have been given much attention. In [21], Zassenhaus discussed metacyclic groups with cyclic commutator quotient, as did
1.1. Introduction

M. Hall in [7]. There are several classifications of metacyclic $p$-groups in the literature especially those of odd order (see Beyl [2], King [9], Liedahl [11], [12], Newman and Xu [15], Rédei [16] and Lindenberg [13]).

Significant progress was made in 1994 when Hyo-Seob Sim proved in [20] that every finite metacyclic group decomposes canonically as a semidirect product of two Hall subgroups. The normal semidirect factor is chosen as the smallest normal Hall subgroup with nilpotent quotient; it was shown that it is always a split metacyclic group of odd order. The other semidirect factor is nilpotent. By breaking the problem into two simpler problems, Sim proceeded to classify metacyclic groups of odd order. In Chapter 2 we recall some of his key contributions. Sim produced a detailed list of other classes of metacyclic groups which have been studied in his thesis (see [20]) and everything in his introduction is relevant to this thesis as well.

The difficulty in generalising from groups of odd order to arbitrary groups lies in the metacyclic 2-groups. First they needed to be classified up to isomorphism. In chapter 3, we present a variant of a classification taken from unpublished work of Newman and Xu [15] done in 1988. Although metacyclic 2-groups have been classified, little of their automorphism groups was known. It is with the classification of chapter 3 that we proceed to calculate a type of automorphism group of 2-groups in Chapter 4. We note that we may have used a classification which was only published recently by Liedahl in [12]. This has attractive features and may well be worth examining more closely to see whether it simplifies the argument given here. Using the material in Chapter 4, finite metacyclic groups can be classified in Theorem 5.3.
1.2 Notation and basic facts

It is easy to see that subgroups and homomorphic images of metacyclic groups are metacyclic.

Much of the terminology that we assemble here will not be needed until Chapter 5. Enough of it is given here for the convenience of those readers who want to skip ahead to the statements in that chapter to see where we are going. Let $m$ and $n$ be two positive integers and $p$ be a prime. Let $\psi(n,p)$ denote the largest integer $i$ such that $p^i \mid n$, and we define $\psi(0,p) = 0$. For any set of primes $\pi$ the $\pi$ component of $n$, that is $\prod_{p \in \pi} p^{\psi(n,p)}$, is denoted by $n_\pi$, and the unique Hall $\pi$-subgroup of a finite nilpotent group $G$ by $G_\pi$. We use $(m \mid n)$ to denote the smallest natural number $t$ such that $t \equiv m_{\{p\}} \pmod{n_{\{p\}}}$ for all primes $p$ such that $p \mid n$. The set of natural numbers less than $n$ and relatively prime to $n$ form a group under multiplication modulo $n$, the group of reduced residues modulo $n$, denoted by $J(n)$. As usual, $m \mod n$ will denote the least nonnegative remainder on dividing $m$ by $n$. The order of $\alpha \in J(n)$ is the order of $\alpha$ modulo $n$ and is denoted by $\text{ord}_n \alpha$ and not $|\alpha|$ so as to avoid confusion with the absolute value of a number. If $m \mod n = \alpha \in J(n)$, $m_n^{-1}$ shall denote the inverse of $\alpha$ in $J(n)$, the inverse of $m$ modulo $n$. The set of primes dividing the order of a finite group $G$ will be denoted by $\varpi(G)$. If $0 \neq r \in \mathbb{Q}$ and $r = m/n$ with $\gcd(m,n) = 1$, then we define $\varpi(r)$ to be the set $\{ p \mid p$ is a prime divisor of $m \}$. It is easy to see that

$J(m) \rightarrow \prod_{p \in \varpi(m)} J(m_{\{p\}})$  \quad \varpi \mapsto \prod_{p \in \varpi(m)} (\varpi \mod p^{\psi(n,p)})$

is a homomorphism. By the constructive version of the Chinese Remainder Theorem
1.2. Notation and basic facts

(see Theorem 3.12 in Rosen [18]), the map is bijective, and its inverse may be written as

\[
\lambda_m : \prod_{p \in \omega(m)} J(m_{(p)}) \to J(m), \quad \prod_{p \in \omega(m)} l_p \mapsto \sum_{p \in \omega(m)} m_{p'}(m_{p'})^{-1} l_p \mod m
\]

where we write \( \prod_{p \in \omega(m)} l_p \) for the element of the external direct product

\[
\prod_{p \in \omega(m)} J(m_{(p)})
\]

whose component in the direct factor \( J(m_{(p)}) \) is \( l_p \). Let \( J(m, n) \) denote the subgroup of \( J(n) \) consisting of all elements with order dividing \( m \). Let \( T(n) \) denote the set

\[
\{ \kappa \in J(n) \mid \text{if } \text{ord}_n \kappa^* = \text{ord}_n \kappa, \text{then } \kappa^* \mod n \geq \kappa \}
\]

and let \( T(m, n) = T(n) \cap J(m, n) \). Thus \( T(m, n) \) consists of one number for each cyclic subgroup of order dividing \( m \) in \( J(n) \), namely the smallest number that generates this subgroup in \( J(n) \).

For any finite group \( G \), let \( O(G) \) denote the set of orders of elements of \( G \). Let \( \Gamma = \{ (n, G) \mid n \in \mathbb{N}, n \geq 1, G \leq J(n) \} \) and let \( (n, G) \in \Gamma \). Suppose \( \phi : O(G) \to \Gamma, \lambda \mapsto (\lambda \phi', \lambda \phi'') \) is a function such that for each \( \lambda \in O(G), \lambda \mid \lambda \phi' \).

We may define an equivalence relation, \( \sim \), on \( G \) as follows:

\[
a_1 \sim a_2 \iff (a_1 = a_2^\beta, \text{ for some } \beta \in |a_1|\phi'').
\]

We define \( T(\phi, G) \) to be the set of smallest representatives of the resulting equivalence classes in \( G \).

Let \( G \) be a group and \( C \trianglelefteq G \). A subgroup \( N \) of \( N_{\text{Aut} \ G}(C) \) induces a subgroup of \( \text{Aut} \ G/C \) in a natural way. This subgroup is denoted by \( N_{\downarrow G/C} \).
The main result in this thesis is Theorem 5.3, in which we classify finite metacyclic groups. The definitions given above cover all the terms in the statement of that theorem.

The first paragraph of following lemma is attributed to Hölder in III §7 of Zassenhaus [21]. The last two statements are observations of Kovacs.

**Lemma 1.1.** A group $G$ is metacyclic with a kernel of order $m$ and of index $k$ if and only if it has a presentation of the form

$$\langle x, y \mid x^k = y^l, y^m = 1, y^n = y^n \rangle$$

where $k, l, m$ and $n$ are positive integers such that $m | (n^k - 1)$ and $m | l(n - 1)$.

In this case, we have $G' = \langle y^{n-1} \rangle$, $\zeta G = (\zeta G \cap \langle x \rangle)(\zeta G \cap \langle y \rangle)$. Replacing $y$ by a suitable power of itself, we may assume that $l | m$. With such an $l$, we have $\exp G = \lcm(km/l, m)$.

Moreover, $N_{\Aut G}(\langle y \rangle) \leq C_{\Aut G}(G/C(y))$ and

$$(N_{\Aut G}(\langle y \rangle))_{G/(y)} = C_{\Aut(G/(y))}(G/C(y)).$$

**Proof.** All statements but the last two are relatively straightforward. We have $\lcm(km/l, m) = \lcm(|x|, |y|)$, and this common multiple divides $\exp G$. Let $p$ be the smallest prime divisor of $G$, and $t = \psi(\lcm(km/l, m), p)$. As $\langle x \rangle \langle y \rangle$ is a metacyclic factorisation of $G$, $\langle x \rangle_p \langle y \rangle_p$ is a metacyclic factorisation of a Sylow $p$-subgroup $P$ of $G$. Since $G$ is supersoluble, $G = PN$ for some normal $p'$-subgroup $N$ (see 5.4.8 in [17]). Then $P^p = \langle x \rangle_p \langle y \rangle_p$ because $P' \leq \langle y \rangle_p$, and by induction $P^{p^t} = 1$. Therefore $G^{p^t} \leq N$. Continuing the process for progressively larger primes, we find
that $G^{\text{lcm}(km/l,m)} \leq N^{\text{lcm}(km/l,m)/p} \leq \cdots \leq 1$ and hence $(\exp G)|\text{lcm}(km/l,m)$. Thus

$$\exp G = \text{lcm}(km/l,m).$$

Let $\alpha \in \text{NAut}_G(\langle y \rangle)$. Then $(y\alpha)^s = y$ for some integer $s$, and so

$$y^{\alpha s} = ((y\alpha)^s)^{x\alpha} = ((y\alpha)^{x\alpha})^s = (y^n\alpha)^s = (y\alpha)^{ns} = ((y\alpha)^s)^n = y^n = y^s.$$

Therefore $x\alpha x^{-1} \in C_G(y)$ and $\alpha \in \text{CAut}_G(G/C_G(y))$ and it follows that

$$\text{NAut}_G(\langle y \rangle) \leq \text{CAut}_G(G/C_G(y))$$

and

$$(\text{NAut}_G(\langle y \rangle))_{G/(y)} \leq \text{CAut}_G(G/(C_G(y))).$$

Conversely, let $\beta \in \text{CAut}_G(G/C_G(y))$. Then for some integer $r$ such that $\gcd(r, km_{(r')}) = 1$ and $x^r \equiv x \mod C_G(y),$

$$(g\langle y \rangle)\beta = (g\langle y \rangle)^r$$

for all $g \in G$. Set $u = r + km_{(r')}$, then clearly $(x^u)^k = (y^u)^l$ and $(y^u)^m = 1$. Also, $[G : C_G(y)] | km_{(r')}$, and so $y^{x^u} = y^{x^r} = y^s = y^n$, whence

$$(y^n)^{x^u} = (y^{x^u})^u = y^{nu} = (y^u)^n.$$

By von Dyck's Theorem (see 2.2.1 in Robinson [17]), there is an endomorphism of $G$ such that $x \mapsto x^u$, $y \mapsto y^u$. Since

$$\gcd(r, km_{(r')}) = 1,$$

we have $\gcd([G], u) = 1$, and so $x^u$ and $y^u$ generate $G$ and so this is an automorphism. Moreover, since $[G : \langle y \rangle] | km_{(r')}$, this automorphism induces $\beta$. This shows that $(\text{NAut}_G(\langle y \rangle))_{G/(y)} \geq \text{CAut}_G(G/(C_G(y))),$ and the last result follows. \qed
A finite metacyclic group may have kernels of different orders; even with $k$ and $m$ fixed, different choices of $l$ and $n$ may still lead to isomorphic groups. The main problem addressed in this thesis is to choose one parameter string $k, l, m, n$ for each isomorphism class of metacyclic groups.
Chapter 2

Standard Hall-decompositions and $p$-groups of odd order

In this chapter we recall some of the important work of Sim [20] on finite metacyclic groups and some basic facts on metacyclic $p$-groups for odd $p$. This will form the basis for the proof of Theorem 5.3. The following result is Lemma 5.3 in [20]:

**Lemma 2.1.** Let $G$ be a finite group with a metacyclic factorisation $G = SK$. To each set $\pi$ of primes, the subgroup $H = S_{\pi}K_{\pi}$ is the unique Hall $\pi$-subgroup of $G$ such that $S_{\pi} = S \cap H$ and $K_{\pi} = K \cap H$, so $H = (S \cap H)(K \cap H)$.

**Definition 2.1.** Let $G$ be a finite metacyclic group and let

$$\pi = \{ p \in \wp(G) \mid G \text{ has a normal Hall } p'\text{-subgroup } \}.$$ 

For a given metacyclic factorisation $G = SK$ let

$$H = S_{\pi}K_{\pi} \text{ and } N = S_{\pi'}K_{\pi'}.$$
Then $G = HN$ is a semidirect decomposition called the standard Hall-decomposition for the metacyclic factorisation $G = SK$.

As we already noted in the proof of Lemma 1.1, the smallest prime divisor of $|G|$ always lies in $\pi(H)$. Hence $|N|$ must be odd. As shown in Lemma 5.5 of [20], the subgroup $H$ in a standard Hall-decomposition $G = HN$ is nilpotent. The following deep result is Theorem 5.7 in [20] and is also fundamental for our Theorem 5.3:

**Theorem 2.2.** Let $G$ be a finite metacyclic group with a metacyclic factorisation $G = SK$ and $HN$ the corresponding standard Hall-decomposition. Then $N = (S \cap N)(K \cap N)$ is a split metacyclic factorisation with $S \cap N \leq C_N(H)$. The subgroup $K \cap N$ and the conjugacy class of $S \cap N$ are independent of the choice of the factorisation $G = SK$. 

$\square$
The independence of the conjugacy class of $S \cap N$ seems to depend on the conjugacy of Sylow systems in soluble groups (see for example 9.2.3 in [17]). For completeness, we detail the relevant argument here, writing $\pi = \omega(H)$ for the moment.

**Proof.** Let $S^*K^*$ and $S'K'$ be two metacyclic factorisations of $G$ with standard Hall-decompositions $HN$ and $H'S'$, respectively. For any subset $\varpi$ of $\pi'$, let $N_{\varpi} = S_{\varpi}K_{\varpi}$ and $N'_{\varpi} = S'_{\varpi}K'_{\varpi}$. Let $\hat{\varpi} = \{ p \in \pi' \mid p < q \}$ and $\hat{\varpi}' = \{ p \in \pi' \mid p > q \}$.

For any $q \in \pi'$, we have $HN_qN_q \leq G$, since $N_q$ is normal in $G$ and $HN_q \leq G$. Clearly it is a Hall $\varpi'$-subgroup. For any $p \in \pi'$, we have $HN_p \cap \bigcap_{p \leq q \in \pi'} (HN_q)^g$. A similar argument shows that $H'S'_{\varpi'} = \bigcap_{p \leq q \in \pi'} (H'S'_{\varpi})^g$. By 9.2.3 in [17], there is a $g \in G$ such that $H'S'_{\varpi} = (HN_q)^g$, for all $q \in \pi'$. Then

$$S^* \cap N = \prod_{p \in \pi'} C_{N_p}(H'^*N'^*_{\varpi})$$

by Lemma 5.6 (ii) of [20]

$$= \prod_{p \in \pi'} C_{N_p}(\bigcap_{p \leq q \in \pi'} (H'^*N'^*_{\varpi}N'_{\varpi}))$$

$$= \prod_{p \in \pi'} C_{N_p}(\bigcap_{p \leq q \in \pi'} (HN_qN_q)^g)$$

$$= \prod_{p \in \pi'} C_{N_p}(\bigcap_{p \leq q \in \pi'} (HN_qN_q)^g)$$

$$= \prod_{p \in \pi'} C_{N_p}(HN_p)^g$$

$$= \prod_{p \in \pi'} (C_{N_p}(HN_p))^g$$

$$= (\prod_{p \in \pi'} C_{N_p}(HN_p))^g$$

$$= (S \cap N)^g$$

by Lemma 5.6 of [20]. □

This theorem breaks up the problem into three components: investigating $H$, $N$ and the ways in which they can form a metacyclic semidirect product.
Definition 2.2. Let $C$ be a subgroup of a finite metacyclic $p$-group $P$. A metacyclic factorisation $SN$ of $P$ is $C$-standard if $|S| = \exp P$ and $N$ is a smallest kernel of $P$ contained in $C$.

It was proved in [20] (see the sentence preceding Lemma 3.4) that if $p$ is odd and subgroup $C$ of a metacyclic $p$-group $P$ contains a kernel, then $P$ has a $C$-standard factorization. We shall use the following generalisation of this:

**Lemma 2.3.** If $G$ is a nilpotent metacyclic group of odd order and $C$ is a subgroup containing at least one kernel, then $G$ has a $C$-standard factorisation.

**Proof.** This easily follows from Corollary 3.2 of [20]. □

The following result is Lemma 3.4 in [20]:

**Lemma 2.4.** Let $P$ be a finite $p$-group for an odd prime $p$, and $P = SN$ a metacyclic factorisation. Define $\alpha$, $\beta$, $\gamma$ and $\delta$ by $p^\alpha = [S : S \cap N]$, $p^\beta = [N : S \cap N]$, $p^\gamma = |N|$ and $p^\delta = [N : P']$. Then $\gamma \geq \beta$; $\beta + \delta \geq \gamma \geq \delta$; $\delta = 0$; implies $\beta = 0$; $P$ is presented by

$$\langle x, y \mid x^{p^\alpha} = y^{p^\beta}, y^{p^\gamma} = 1, y^p = y^{1+p^\delta} \rangle.$$

Suppose that $C \leq P$, $[P : C] = p^\kappa$ and $SN$ is a $C$-standard factorisation of $P$. Then $\alpha \geq \beta$, and $\beta < \delta$ implies $\alpha - \kappa < \beta$. □
Chapter 3

Metacyclic 2-groups

This chapter is concerned with classification of finite metacyclic 2-groups. There are several such classifications in the literature (see for example Beyl [2], King [9], Lindenberg [13], Rédei [16] and the recent Liedahl [11], [12]). We find most convenient an unpublished classification by Newman and Xu which they foreshadowed in [15]. Professor Newman has kindly made available the relevant pages of a book draft written by Professor Xu. I only claim to have filled some of the gaps in the exposition, as most of the work in this chapter is taken from that source. Their result has been modified slightly to Theorem 3.6, which is more applicable to Theorem 5.3. A group with a presentation given by item (n) in a statement like that of Theorem 3.6 below will loosely be referred to as a “group of type (n)” or simply a “type (n) group” where n = i, ii, ..., viii.

Lemma 3.1. If m and n are positive integers, then

\[ \langle a, b \mid a^{2m} = b^{2n+1} = 1, b^a = b^{-1} \rangle \not\cong \langle a, b \mid a^{2m} = b^{2n+1} = 1, b^a = b^{-1+2n} \rangle. \]
3. Metacyclic 2-groups

Proof. Let $P_1$ be the first group and $P_2$ the second. At $m = 1$, if $n = 1$, then $P_1$ is nonabelian and $P_2$ is abelian, while if $n > 1$, then $P_1$ is dihedral and $P_2$ is semidihedral. Thus we may assume that $m \geq 2$ and then argue as follows. By Lemma 1.1, $|P_i| = 2^{m+n+1}$ for $i = 1$ and 2. Consider the sets $V(P_i)$ defined by

$$V(P_i) = \{ g^2 \mid g \in P_i \}.$$ 

In $P_1$, for any integers $i$ and $j$, we have

$$(a^i b^j)^2 = \begin{cases} a^{2i} b^{2j} & \text{if } 2 \mid i, \\ a^{2i} & \text{otherwise,} \end{cases}$$

and so $|V(P_1)| = 2^{m+n-2} + 2^{m-2}$. In $P_2$, we have

$$(a^i b^j)^2 = \begin{cases} a^{2i} b^{2j} & \text{if } 2 \mid i, \\ a^{2i} & \text{if } 2 \nmid i \text{ and } 2 \mid j, \\ a^{2i} b^{2n} & \text{otherwise,} \end{cases}$$

and so $|V(P_2)| = 2^{m+n-2} + 2^{m-2} + 2^{m-2} > |V(P_1)|$. This shows that $P_1 \not\cong P_2$. □

The following result is due to Kummer (see pp 507–508 in [10] or Exercise 5.36 in [6]):

**Lemma 3.2.** If $m$ and $n$ are natural numbers, then the exponent in the highest power of $p$ to divide $\binom{m+n}{n}$ is the number of carries that occur when $m$ is added to $n$ in base-$p$ arithmetic.

**Lemma 3.3.** If $a$, $b$ and $c$ are natural numbers, $a \geq 1$ and $p$ is a prime, then
3. Metacyclic 2-groups

\[(\pm 1 + p^{a})^{p^{b}c}
\equiv (\pm 1)^{p^{b}c} + (\pm 1)^{p^{b}c-1}p^{a+b}c + (\pm 1)^{p^{b}c}\delta(p, 2)(1 - \delta(b, 0))p^{2a+b-1}c \mod p^{2a+b}\]

where $\delta$ is the Kronecker delta function.

**Proof.** It suffices to show that if $d \geq 3$ then $\binom{p^{b}c}{d}p^{ad}$ is divisible by $p^{2a+b}$; for $\binom{p^{b}c}{2}p^{2a} = p^{2a+b}c(p^{b}c-1)/2$ which is congruent to $\delta(p, 2)(1 - \delta(b, 0))p^{2a+b-1}c$ modulo $p^{2a+b}$.

In turn, this will follow once we show that $\binom{p^{b}c}{d}$ is divisible by $p^{b+2-d}$ whenever that makes sense, that is, whenever $b + 2 - d \geq 0$ (and $d \geq 3$). Let $e$ be the largest integer such that $p^{e} \leq d$. If $b + 2 - d \geq 0$, then $e \leq b$, and so by Kummer's Theorem $\binom{p^{b}c}{d}$ is divisible by $p^{b-e}$, and that is good enough because $b + 2 - d \leq b - e$. \square

**Corollary 3.4.** If $m \geq n \geq 1$, $p$ is a prime, $n + p \geq 4$ and $r \geq 1$, then each of the statements

\[(1 + p^{n})^{p^{r}} \equiv 1 \mod p^{m}\]

and

\[(-1 + 2^{n})^{2^{r}} \equiv 1 \mod 2^{m}\]

is equivalent to

\[r \geq m - n.\]

**Corollary 3.5.** If $P$ is the group presented by

\[\langle x, y \mid x^{p^{k}} = y^{p^{i}}, y^{p^{m}} = 1, y^{z} = y^{1+p^{n}} \rangle\]
3. Metacyclic 2-groups

where \( m - n \leq l \leq m, \ 1 \leq n \leq m \) and \( m - n \leq k \), then \( \zeta P = \langle x^{p^{m-n}}, y^{p^{m-n}} \rangle \). If \( P \) is the group presented by

\[
\langle x, y \mid x^2 = y^{x^n} = 1, y^x = y^{-1+2n} \rangle
\]

where \( m - 1 \leq l \leq m, \ 2 \leq n \leq m \) and \( m - n \leq k \), then \( \zeta P = \langle x^l, y^{2m-1} \rangle \) when \( m = n \) and \( \langle x^{2m-n}, y^{2m-1} \rangle \) otherwise.

Proof. This follows easily from Lemma 1.1 and Corollary 3.4. \( \square \)

**Theorem 3.6.** Every metacyclic 2-group has one of the following eight types of presentation, in which the parameters \( r, s, t, u, v \) and \( w \) are natural numbers:

(i) \( \langle a \mid a^{2r} = 1 \rangle \) with \( r \geq 0 \),

(ii) \( \langle a, b \mid a^{2r} = b^2 = 1, b^a = b \rangle \) with \( r \geq 1 \),

(iii) \( \langle a, b \mid a^2 = b^{2r} = 1, b^a = b^{-1} \rangle \) with \( r \geq 2 \),

(iv) \( \langle a, b \mid a^{2r} = b^2, b^{2r+1} = 1, b^a = b^{-1} \rangle \) with \( r \geq 1 \),

(v) \( \langle a, b \mid a^{2r+1} = 1, b^a = b^{1+2r} \rangle \) with \( r \geq 2 \),

(vi) \( \langle a, b \mid a^{2r+1} = 1, b^a = b^{-1+2r} \rangle \) with \( r \geq 2 \),

(vii) \( \langle a, b \mid a^{2r} = b^2, b^{2s+1} = 1, b^a = b^{1+2u} \rangle \) with \( r \geq s \geq u \geq 2 \) and \( u \geq t \),

(viii) \( \langle a, b \mid a^{2r+t+u} = b^{2r+u+t+u}, b^{2r+u+t+u+u} = 1, b^a = b^{-1+2r+u} \rangle \) where \( r \geq 2, v \leq r, w \leq 1, su = tu = tv = 0 \), and if \( v \geq r - 1 \), then \( w = 0 \).

Groups of different types or of the same type but with different parameters are not isomorphic.

Groups of type (i), (ii), (iii), (v) and (vi) are split; a type (iv) group is not split; a type (vii) group is split if and only if either \( r = s \) or \( s = u \) or \( t = 0 \); a type (viii) group is split if and only if \( w = 0 \).
Proof. Let $P$ be a metacyclic 2-group. Then of course $P$ is finite. Suppose first that $P$ has a cyclic maximal subgroup. By 5.3.4 in [17], $P$ is isomorphic to one of the first six types listed.

Suppose next that $P$ has no cyclic maximal subgroup. By Lemma 1.1, this $P$ has a presentation of the form (1.2) with $l | m$, so that $k$, $l$ and $m$ are now powers of 2. A further change in the generators of $\langle x \rangle$ and $\langle y \rangle$ can achieve that $n$ is of the form $\pm 1 + 2^\lambda$, for some $\lambda$. Using also the assumption that $P$ has no cyclic maximal subgroup, we conclude that $P$ has a presentation of the form

$$\langle x, y \mid x^{2^k} = y^{2^l}, y^{2^m} = 1, y^x = y^{\epsilon + 2^n} \rangle$$

where $\epsilon = \pm 1$, $m \geq n \geq 2$, $k \geq 2$, $m \geq l \geq 2$, $2^m | (\epsilon + 2^n - 1)2^l$, $2^m | (\epsilon + 2^n)^{2^k} - 1$ and $|P| = 2^k + m$. Note that the first divisibility condition amounts to

$$l \geq \begin{cases} m - n & \text{if } \epsilon = 1, \\ m - 1 & \text{if } \epsilon = -1 \end{cases}$$

and by Lemma 3.3 the second amounts to $k + n \geq m$.

Suppose first that $\epsilon = 1$. Then by Theorem 6.3 of [8], for example, we may show that

$$(x^iy^i)^{2^m - n} = x^{i2^{m-n}}y^{2^{m-n}}y^{ij2^m} = \begin{cases} x^{i2^{m-n}}y^{2^{m-n}} & \text{if } ij \text{ is even,} \\ x^{i2^{m-n}}y^{2^{m-n}}y^{2^m} = x^{i2^{m-n}}y^{2^{m-n}(1+2^{n-1})} & \text{if } ij \text{ is odd.} \end{cases} \tag{3.2}$$

This will be very useful in calculations that follow, only the first of which is detailed.

We distinguish the four cases: $k \geq l \geq n$, $l > k \geq n$, $l > k < n$ and $k \geq l < n$. 
In the first case, $P$ is clearly of type (vii). In the second case, we see that the two elements, $a = xy^{1-2^{k-l}}$ and $b = \begin{cases} \ y^{1+2^{m-1}} & \text{if } k = m - n, \\ \ y & \text{if } k > m - n \end{cases}$ generate $G$. If $k > m - n$, then
\[
2^{k} = (xy^{1-2^{l-2}})^{2^{k}} = (xy^{1-2^{k}})^{2^{k}(m-n)2^{m-n}} = (x^{2^{k}(m-n)}y^{(1-2^{l-2})2^{k}(m-n)+2^{m-n}})^{2^{m-n}} \quad \text{for some integer } d, \text{ since } G' = \langle y^{2^{n}} \rangle \text{ by (3.2)}
\]
\[
= x^{2^{k}y^{(1-2^{l-2})2^{k}}} = x^{2^{k}y^{2^{k}-2^{l}}} = y^{2^{k}} = b^{2^{k}}.
\]
If $k = m - n$, a direct application of (3.2) yields the same conclusion. In both subcases, we also have $b^{2^{m}} = 1$ and $b^{a} = b^{1+2^{n}}$. Therefore $P$ is a homomorphic image of the group defined by the presentation $\langle a, b \mid a^{2^{k}} = b^{2^{k}}, b^{2^{m}} = 1, b^{a} = b^{1+2^{n}} \rangle$. Since the group so defined has order at most $2^{k+m}$, it must be isomorphic to $P$, and so $P$ is of type (vii). If $l > k < n$, then in a similar way we may show that with $a = y^{-1}$ and $b = x^{-1}y^{(2^{l-k}-2^{n-k})(1-2^{n})}$ we have
\[
P \cong \langle a, b \mid a^{2^{n}} = b^{2^{k}}, b^{2^{m+k-n}} = 1, b^{a} = b^{1+2^{k}} \rangle,
\]
also a type (vii) group. If $k \geq l < n$, then $P$ is nilpotent of class at most two, and so the identity $(uv)^{m} = u^{m}v^{m}[v, u]^{(m)}$ holds (see 5.3.5 in [17]). With $a = x^{2^{k-l}}y^{-1}$ and
$b = x$ we see that

$$P \cong \langle a, b \mid a^{2^t} = b^{2^{k-l-1}}, b^{2^{k-l+m}} = 1, b^a = b^{1+2^{k-l+n}} \rangle$$

where

$$t = \begin{cases} 
1 & \text{if } k + n = m, \\
0 & \text{if } k + n > m.
\end{cases}$$

This takes us back to one of the three cases we have just considered. We have shown that when $\epsilon = 1$, $P$ is of type $(\text{vii})$.

Let us now turn to $\epsilon = -1$, in which case $l = m$ or $m - 1$. First suppose that $l = m$. Then (3.1) can readily be converted to a type $(\text{viii})$ presentation with $a = x$ and $b = y$: all one has to do is to show that the simultaneous equations

$$r + s + t = k,$$

$$r + s + u + v = r + s + u + v + w = m,$$

$$r + u = n,$$

have a solution that satisfies the conditions $(\text{viii})$ imposes on the parameters. Of course, in all solutions, $w = 0$. Then

$$(r, s, t, u, v) = \begin{cases} 
(n, \min(k, m) - n, k - \min(k, m), 0, m - \min(k, m)) & \text{if } n \leq k, \\
(k, 0, 0, n - k, m - n) & \text{otherwise}
\end{cases}$$

is such a solution. The discussion for $l = m$ is, therefore complete.

Hence we may suppose that $l = m - 1$. We have $m = l + 1 \geq 3$. First suppose that $n < m$. We may also assume that $k + n > m$, for otherwise with $x_1 = xy$,

$$P \cong \langle x_1, y \mid x_1^{2^k} = y^{2^m} = 1, y^{x_1} = y^{-1+2^n} \rangle,$$
a case considered in the previous paragraph. When \( k + n > m > l \geq 2 \), (3.1) can readily be converted to a type (viii) presentation with \( a = x \) and \( b = y \): all one has to do is to show that the simultaneous equations

\[
\begin{align*}
  r + s + t &= k, \\
  r + s + u + v &= r + s + u + v + w - 1 = m - 1, \\
  r + u &= n,
\end{align*}
\]

have a solution that satisfies the conditions (viii) imposes on the parameters. This is handled in a similar way to that used in the previous paragraph, as the reader can verify.

Next suppose that \( m = n \). Then \( y^x = y^{-1} \), and so \( x^2 \) is central, whence it is easy to see that, with \( y_1 = x^{2k-1} \),

\[
P \cong \langle x, y_1 \mid x^{2k} = y_1^{2^{m-1}}, y_1^{2^m} = 1, y_1^x = y_1^{x^{-1}+2^{m-1}} \rangle,
\]

a case handled in the previous paragraph. This proves that every metacyclic 2-group has a presentation listed in the statement.

It is clear that no group having one of the first six types is also of another of the first six types and that the parameters in these groups are invariants. Since such groups have cyclic maximal subgroups, \(|P|/\exp G \leq 2\).

Suppose that \( P \) is a type (vii) group. Lemma 1.1 shows that \(|P| = 2^{r+s+t}, \exp P = 2^{r+t} \) and \( P' = \langle b^{2^s} \rangle \). Clearly \( P/P' \cong C_2 \times C_{2^u} \). For such a group, it follows that \( r + s + t, r + t, r \) and \( u \) are invariants and therefore so are \( s \) and \( t \). Since \(|P|/\exp P = 2^r > 2\) in such a \( P \), no type (vii) group is of any of the first six types.
3. Metacyclic 2-groups

Note also that $C_4 \times C_4$ is a homomorphic image of $P$.

Suppose now that $P$ is of type (viii). By Corollary 3.5,

$$\zeta P = \begin{cases} 
\langle a^2, b^{2r+s+u+v+2w} \rangle & \text{if } s + v + w = 0, \\
\langle a^{2^{r+s+u+v+w}}, b^{2r+s+u+v+2w} \rangle & \text{otherwise,}
\end{cases}$$

which is cyclic of order greater than 2 if $w = 1$, cyclic of order 2 if $w = 0$ and $v = r$, and noncyclic otherwise. This proves that $w$ is an invariant for $P$. Further, $P' = \langle b^2 \rangle$, and so $P/P' \cong C_2 \times C_{2r+s+t}$. In particular, it follows that $C_4 \times C_4$ is not a homomorphic image of $P$, and so no type (vii) group is of type (viii). We have $|P|/\exp P = 2^{2r+2s+4u+4v+4w}/\max\{2^{r+s+t+w}, 2^{r+s+u+v+w}\} \geq 2^r > 2$, and so no type (viii) group is of any of the first six types.

Suppose that $w = 0$ for a type (viii) group $P$. Then, since $\exp P/P' = 2^{r+s+t}$, the following three statements are true:

(a) $\exp P = \exp P/P' = |P|^{1/2}$ if and only if $t = u = v = 0$;
(b) $\exp P = \exp P/P' > |P|^{1/2}$ if and only if $t > 0$ and $u = v = 0$;
(c) $\exp P > \exp P/P'$ if and only if $t = 0$ and $u + v > 0$.

In case (a), we have $P \cong \langle a, b \mid a^{2^{r+s}} = b^{2^{r+s}} = 1, b^s = b^{-1+2^r} \rangle$ where $r \geq 2$ and $s \geq 0$. In this case,

$$\zeta P \cong \begin{cases} 
C_2 \times C_{2r-1} & \text{if } s = 0, \\
C_2 \times C_{2r} & \text{otherwise,}
\end{cases}$$

and $P/P' \cong C_2 \times C_{2r+s}$, and so $|P/P'|/|\zeta P| = 2^{\max\{1, s\}}$. If $|P/P'|/|\zeta P| > 2$, we may conclude that the parameters are invariants. When $|P/P'|/|\zeta P| = 2$, it remains
to distinguish the two groups obtained by setting \((r, s)\) to \((q, 1)\) or \((q+1, 0)\), for any \(q\) with \(q \geq 2\), but, by Lemma 3.1,

\[
\left\langle a, b \mid a^{2^{q+1}} = b^{2^{q+1}} = 1, b^a = b^{-1} \right\rangle \neq \left\langle a, b \mid a^{2^{q+1}} = b^{2^{q+1}} = 1, b^a = b^{-1+2^q} \right\rangle.
\]

In case (b), we have \(P \cong \left\langle a, b \mid a^{2^{r+s+t}} = b^{2^{r+s}} = 1, b^a = b^{-1+2^r} \right\rangle\) where \(r \geq 2, s \geq 0\) and \(t \geq 1\). In this case,

\[
\zeta P \cong \begin{cases} 
C_2 \times C_{2^{r-t}} & \text{if } s = 0, \\
C_2 \times C_{2^{r+t}} & \text{otherwise},
\end{cases}
\]

and \(P/P' \cong C_2 \times C_{2^{r+s+t}}\). Firstly, \((\exp P)^2/|P| = 2^t\), and so \(t\) is an invariant of \(P\). Secondly, \(|P/P'|/|\zeta P| = 2^{\max\{1,s\}}\). If \(|P/P'|/|\zeta P| > 2\), we may conclude that the parameters are invariants. When \(|P/P'|/|\zeta P| = 2\), it remains to distinguish the two groups obtained by setting \((r, s)\) to \((q, 1)\) or \((q+1, 0)\), for any \(q\) with \(q \geq 2\), but, by Lemma 3.1,

\[
\left\langle a, b \mid a^{2^{q+1}} = b^{2^{q+1}} = 1, b^a = b^{-1} \right\rangle \neq \left\langle a, b \mid a^{2^{q+1}} = b^{2^{q+1}} = 1, b^a = b^{-1+2^q} \right\rangle.
\]

In case (c), we have \(P \cong \left\langle a, b \mid a^{2^{r+s+v}} = b^{2^{r+s+v}} = 1, b^a = b^{-1+2^{r+v}} \right\rangle\) where \(r \geq 2, v \leq r, su = 0\) and \(u + v > 0\). In this case,

\[
\zeta P \cong \begin{cases} 
C_2 \times C_{2^{r-1}} & \text{if } s = v = 0, \\
C_2 \times C_{2^{r-v}} & \text{otherwise},
\end{cases}
\]

and \(P/P' \cong C_2 \times C_{2^{r+s}}\). We also have \(|P/P'|/|\zeta P| = 2^{\max\{1, s+v\}}\). Since, in this case, \(\exp P = 2^{r+s+u+v}\), it follows that \(r + s, u + v\) and \(\max\{1, s + v\}\) are invariants of \(P\).
If \( s + v > 1 \), then \( s + v \) is an invariant, and so \( us = 0 \) yields that each of \( r \), \( s \), \( u \) and \( v \) are invariants of \( P \). Suppose that \( s + v \leq 1 \). Then \( s = 0 \) and either \( u > v = 0 \) or \( v = 1 \). It remains to distinguish the groups obtained by setting \((u,v)\) to \((q+1,0)\) and \((q,1)\) for any \( q \geq 2 \), but, by Lemma 3.1,

\[
\langle a, b \mid a^{2r} = b^{2r+s+1} = 1, b^{a_0} = b^{-1} \rangle \cong \langle a, b \mid a^{2r} = b^{2r+s} = 1, b^{a} = b^{-1+2r+s} \rangle.
\]

If \( w = 1 \), then \( P/(b^{r+s+u+v}) \) is of type (viii) with \( w = 0 \) and the arguments used in the previous paragraph can be used to show that the other parameters are invariant. Thus groups of different types or of the same type but with different parameters are not isomorphic.

It is easy to see that type (i), (ii), (iii), (v) and (vi) groups are split and that a type (iv) group is not split.

Let \( P \) be a type (vii) group. If \( r = s \), then

\[
P \cong \langle a, b \mid a^{2r} = b^{2r}, b^{2r+t} = 1, b^{a} = b^{1+2s} \rangle
\]

with \( r \geq u \geq 2 \) and \( u \geq t \). If \( u > t \), then \( \langle ab^{-1} \rangle \langle b \rangle \) is a split factorisation. If \( u = t \), then it follows that \( b^{2r+t} = 1 = (ab^{2u-1})^{2r} \) and that \( \langle ab^{2u-1} \rangle \langle b \rangle \) is a split factorisation. If \( s = u \), then

\[
P \cong \langle a, b \mid a^{2r} = b^{2r}, b^{2r+t} = 1, b^{a} = b^{1+2s} \rangle
\]

with \( r \geq s \geq 2 \) and \( s \geq t \). If \( r > s \) or \( s > t \) then \( \langle a^{b^{-1}b^{-1}} \rangle \langle a \rangle \) is a split factorisation, while if \( r = s = t \), then \( a^{2r} = (a^{2r-1}b^{-1})^{2r} = 1 \) and \( \langle a^{2r-1}b^{-1} \rangle \langle a \rangle \) is a split factorisation. If \( t = 0 \), then \( P \) is clearly split. Conversely suppose that \( r \neq s \), \( s \neq u \)
and that $P = \langle x \rangle \langle y \rangle$ is a split metacyclic factorisation. Since $\exp P = \max\{|x|, |y|\}$, we have $(|x|, |y|) = (2^r, 2^{r+t})$ or $(2^{r+t}, 2^r)$. Since $|P'| = 2^{r+t-s}$ and $P' \leq \langle y \rangle$, we have that $P/P'$ has invariants $(2^{r-s}, 2^r)$ or $(2^{t-s}, 2^{r+t})$. Since we know that $P/P'$ has invariants $2^r$ and $2^n$, only the second pair is possible and so $t = 0$. The statement about type (vii) groups being split has now been proved.

A type (viii) group with $w = 0$ is clearly split. Conversely, a split type (viii) group would have a presentation given by (3.1) with $l = m$. In that presentation, we could not have $\varepsilon = 1$, for then, as we have argued above, $P$ would be of type (vii) and therefore not of type (viii). We have also seen that $\varepsilon = -1$ and $l = m$ would lead to a type (viii) presentation with $w = 0$. Thus the statements about $P$ being split are true.

**Lemma 3.7.** Let $P = \langle a, b \mid a^2 = b^{2^{r+1}} = 1, b^r = b^{1+2^r} \rangle$ with $r \geq 2$. Then

$P \cong \langle x, y \mid x^{2^r} = y^2, y^4 = 1, y^x = y^{-1} \rangle$.

*Proof.* This follows easily using the substitutions $x = b$ and $y = ab^{2^{r-1}}$. □

**Theorem 3.8.** Every nonabelian metacyclic $p$-group has a presentation which is either of the form

$$\langle x, y \mid x^p = y^p, y^m = 1, y^x = y^{1+p} \rangle$$

where $m \geq n \geq 1$, $m \geq l \geq m - n$, $k \geq l \geq n$ and $n + p \geq 4$, or of the form

$$\langle x, y \mid x^k = y^k, y^m = 1, y^x = y^{1+2^m} \rangle$$

where $m \geq n \geq 2$, $k + n \geq m$ and $m \geq l \geq m - 1$.

*Proof.* This follows easily from Lemma 2.4, Theorem 3.6 and Lemma 3.7. □
Chapter 4

Expressions for induced automorphism groups of quotients of $p$-groups

In Theorem 3.6, we presented a classification of metacyclic 2-groups. In this chapter, we derive much further information about metacyclic $p$-groups which will be critical for Theorem 5.3. In particular, we need to calculate $N_{\text{Aut} P}(C)_{|P/C}$ as defined in the introduction where $C$ is a subgroup of such a group $P$ and $C$ contains a kernel.

**Definition 4.1.** For a metacyclic group $G$, we set

$$C(G) = \{ C \mid C \leq G, C \text{ contains a kernel of } G \}.$$

Note that $\text{Aut} G$ acts on the set of all subgroups of $G$ in a natural way, as it does on
4. Expressions for induced automorphism groups of quotients of $p$-groups

$C(G)$. We define an equivalence relation, $\approx$, on these sets by

$$A \approx B \iff A \text{ and } B \text{ lie in the same orbit under } \text{Aut } G.$$  

If $A \approx B$, then we shall simply say that $A$ and $B$ are equivalent.

It seems sensible to first find the kernels of $P$ and we shall see that this can be done by first finding all kernels of $P/P'$, and then inspecting their complete inverse images in $P$. We then list some explicit automorphisms $\alpha$ of $P$, enough to see in Corollary 4.8, that apart from one family of exceptions, any two kernels of equal order must be equivalent. We find that the exceptions are the 2-groups of the form

$$\langle x, y \mid x^{2^k} = y^{2^l}, y^{2^{l+1}} = 1, y^z = y^{-1} \rangle$$

with $k \geq 2$, $l \geq 2$, where $\langle y \rangle$ and $\langle x^{2^k-1} y \rangle$ are inequivalent kernels of the same order $2^{l+1}$. It is then easy to list all the elements of $C(G)$ and partition it into $(\text{Aut } P)$-orbits. One feature of our conclusions is that $N_{\text{Aut } P} \downarrow_{P/C}$ is either $\text{Aut}(P/C)$ itself or it consists of all automorphisms of the form $gC \mapsto (gC)^r$ with $r \equiv 1 \mod p$ modulo some fixed power of $p$. (That is, $r \equiv -1 \mod 4$ is only allowed when $N_{\text{Aut } P} \downarrow_{P/C} = \text{Aut}(P/C)$). The first step towards this conclusion, and in the calculation of the relevant power of $p$, has already been taken in Lemma 1.1: an element of $\text{Aut}(P/N)$ lies in $N_{\text{Aut } P} \downarrow_{P/N}$ if and only if it induces the trivial automorphism on the centraliser quotient $P/C_P(N)$. As all subgroups of the cyclic group $P/N$ are characteristic, if $C \geq N$ then $N_P(N) \leq N_P(C)$: so there is a subgroup $N_{\text{Aut } P} \downarrow_{P/C}$ in $N_{\text{Aut } P} \downarrow_{P/C}$, and we can readily obtain this subgroup. The second step is to select those $\alpha$ (from the list we used in sorting the kernels $N$ into orbits, and in
which we should include the identity) for which \( N\alpha \leq C \). These all lie in \( N_p(C) \); if \( \beta \in N_{\text{Aut}}(C) \), then \( N\alpha = N\beta \) for one of these \( \alpha \); thus the \( \alpha \downarrow_{P/C} \) obtained from the selected \( \alpha \) represent all the cosets of \( N_{\text{Aut}}(C) \downarrow_{P/C} \) modulo \( N_{\text{Aut}}(N) \downarrow_{P/C} \). We shall have to take care, though: the same coset may be represented several times. For example, an \( \alpha \) which does not normalise \( N \) may still normalise \( C_p(N) \) and act trivially on \( P/C_p(N) \).

Analogues of these results for metacyclic \( p \)-groups with odd \( p \) were, of course, needed and proved by Sim in his Corollary 4.7, though the analogues of the statements italicised above were not made explicit there. The arguments we present cover the odd case as well, so we need not rely on Sim for these details. Continuing the above discussion in that generality and using the presentation of \( P \) given in Theorem 3.8, we see from the orbits of the kernels \( N \) that \( N \) can almost always be chosen (within its orbit) so that \( P = \langle x \rangle N \), and then, as is easily seen from Corollary 3.5, we always have \( C_p(N) = \langle x^{p^{m-n}} \rangle N \). In the exceptional case we can take \( N = \langle x \rangle \), and then \( C_p(N) = \langle y^{p^{m-n}} \rangle N \), so in all cases \( P/C_p(N) \) is cyclic of order \( p^{m-n} \). This proves that, as long as \( P \) is nonabelian, \( N_{\text{Aut}}(N) \downarrow_{P/C} \) always consists of the \( gC \mapsto (gC)^r \) with \( r \equiv 1 \pmod{p^{m-n}} \). It is only in the listing of the relevant \( \alpha \) that case distinctions become really relevant; the precise conclusions are stated in Theorems 4.5 and 4.7.

**Lemma 4.1.** Let \( P \) be a metacyclic \( p \)-group. If \( N \) is a kernel of \( P \), then \( N \geq P' \) and \( N/P' \) is a kernel of \( P/P' \). Let \( M/P' \) be a kernel of \( P/P' \) and write \( M = \langle g \rangle P' \) for some \( g \in P \). The subgroup \( M \) is a kernel of \( P \) if and only if \( \langle g \rangle \geq P' \), in which case \( M = \langle g \rangle \). \( \square \)
Theorem 4.2. Let $P = X \times Y$ with $X = \langle x \rangle \cong C_{p^m}$, $Y = \langle y \rangle \cong C_{p^n}$, $p$ a prime and $m \geq n \geq 1$. Then the kernels of $P$ are the following:

(i) $\langle x^{p^{m-n} c} y \rangle$ with $0 < c < p^n$,
(ii) $\langle x^{p^d c} y \rangle$ with $1 \leq d < m - n$, $1 \leq c \leq p^n$ and $p \nmid c$,
(iii) $\langle xy^c \rangle$ where $0 \leq c < p^n$ and $p | c p^{m-n}$.

Subgroups of different types, or of the same type but with different parameters, are distinct.

Proof. Let $X \geq X_1 \geq X_2$ and $Y \geq Y_1 \geq Y_2$, and suppose that $\theta : X_1/X_2 \to Y_1/Y_2$ is an isomorphism. By Goursat's Theorem (see pp 42–48 in [5] or Theorem 1.6.1 in [19]),

$$\{ x_1 y_1 \mid (x_1 X_2)\theta = y_1 Y_2, x_1 \in X_1, y_1 \in Y_1 \}$$

is a subgroup $N$ of $P$ such that $X \cap N = X_2$, $Y \cap N = Y_2$ and $X_1 N = X_1 Y_1 = N Y_1$. Therefore $P/N$ is cyclic if and only if $X_1 = X$ or $Y_1 = Y$, and $N$ is cyclic if and only if $X_2 = 1$ or $Y_2 = 1$. Using also that $m \geq n$, we see that $N$ is a kernel if and only if $(X_2, Y_1) = (1, Y)$, or $(Y_1, Y_2) = (Y, 1)$ and $X_1 \neq X$ and $X_2 \neq 1$, or $(X_1, Y_2) = (X, 1)$ and $X_2 \neq 1$. The first, second and third cases correspond to $N$ being a kernel of the first, second and third types, respectively, in the statement of the theorem.

The second statement follows from the fact that, also by Goursat's Theorem, the map we have used from the set of all such 5-tuples $(X_1, X_2, Y_1, Y_2, \theta)$ to the set of all subgroups of $P$ is a bijection. \hfill \Box

Lemma 4.3. Let $\langle x, y \rangle$ be a metacyclic $p$-group $P$. If $g, h \in P'$, then $x \mapsto xg$, $y \mapsto yh$ defines an automorphism of $P$. 

Proof. The claim is equivalent to $|C_{\text{Aut}}(P/P')| = |P|^2$. For the same reason it is also equivalent to the statement with $(x, y)$ any other generating pair for $P$, for example, with $x$ and $y$ as in a presentation of Theorem 3.8, that is, either

$$\langle x, y \mid x^p = y, y^n = 1, y^x = y^{1+p} \rangle$$

where $m - n \leq l \leq m$, $1 \leq n \leq m$ and $m - n \leq k$, or

$$\langle x, y \mid x^k = y^2, y^m = 1, y^x = y^{-1+2n} \rangle$$

where $m - 1 \leq l \leq m$, $2 \leq n \leq m$ and $m - n \leq k$. Suppose $P$ has a presentation of the first type. Then $g = y^{ip}$ for some $i$, and $h = y^{jp}$ for some $j$. Therefore $yx^g = y^x = y^{1+p}$. Moreover,

$$(xg)^{pk} = (xy^{ip})^{pk}$$

$$= x^{pk} y^{ip} (x^{k-1} + \cdots + x+1)$$

$$= y^{ip} + ip (x^{k-1} + \cdots + x+1)$$

$$= y^{ip} + ip (1 + \cdots + 1 + (1+p)) + 1)$$

$$= y^{ip} + i (1 + \cdots + 1 + (1+p)) + 1)$$

$$= y^{ip}$$

by Lemma 3.3, since $k + n \geq m$.

It follows that $x \mapsto xg$, $y \mapsto y$ defines an endomorphism of $P$. Since $xg$ and $y$ generate $P$, this is an automorphism of $P$. Now $(yh)^x = y^{(1+ip)n} = (yh)^{1+p}$. Moreover, $x^{pk} = y^{pl} = y^{pl+ipn+1}$ since $n + l \geq m$, and so $x^{pk} = (yh)^{pl}$. Also, $(yh)^p = 1$. As before, it follows that $x \mapsto x$, $y \mapsto yh$ defines an automorphism of $P$. The composition of these two automorphisms is the required automorphism.
4. Expressions for induced automorphism groups of quotients of $p$-groups

The argument is similar if $P$ has a presentation of the second type. □

The following result is a strengthening of Lemma 4.1 (ii) of [20] and follows easily by an obvious adaptation of its proof.

**Lemma 4.4.** Let $SN$ be a metacyclic factorisation of a $p$-group $P$ and let $N \leq C \leq P$.

Then

$$N_{\text{Aut}}P(C) = C_{\text{Aut}}P(P/N)[N_{\text{Aut}}P(S) \cap N_{\text{Aut}}P(C)].$$

**Theorem 4.5.** Let $P = \langle x, y \mid x^{p^k} = y^{p^l}, y^{p^m} = 1, y^x = y^{1+p^n} \rangle$ with $p$ a prime, $m \geq n \geq 1$, $m \geq l \geq m - n$, $k \geq l \geq n$ and $n + p \geq 4$; let $\langle b \rangle$ be a kernel of $P$. Then $P$ has an element $a$ such that $a$ and $b$ satisfy the defining relations in a presentation of $P$ given by

$$\langle a, b \mid a^{p^r} = b^{p^s}, b^{p^{s+t}} = 1, b^a = b^{1+p^u} \rangle$$

where $r, s, t$ and $u$ are natural numbers with $r \geq s \geq 2$, $u \geq t$. Let $\langle b \rangle \leq C \leq P$, and let

$$v = \min \{ \max \{ s - \log_p[C : \langle b \rangle], s - u, 0 \}, s + t - u, \log_p[P : C] \}.$$

Then

$$N_{\text{Aut}}P(C)'_{P/C} = \begin{cases} \text{Aut}(P/C) & \text{if } v = 0, \\ \{ (gC \mapsto (gC)^{1+ip^r}) \mid i \in \mathbb{Z} \} & \text{otherwise.} \end{cases}$$
4. Expressions for induced automorphism groups of quotients of $p$-groups

$$\langle x, y \mid x^{16} = y^8, y^{16} = 1, y^x = y^5 \rangle \quad \langle x, y \mid x^{16} = y^4, y^8 = 1, y^x = y^5 \rangle$$

Figure 4.1: Subgroup lattices showing kernels in circles.

**Proof.** We first determine the kernels of $P$, and for each kernel find an $a$ with the given property. Note that $P' = \langle y^{p^n} \rangle$ and so $P/P' = \langle xP' \rangle \times \langle yP' \rangle \cong C_{p^n} \times C_{p^n}$. By Theorem 4.2, the kernels of $P/P'$ are

(i) $\langle x^{cp^{k-n}}y \rangle P'/P'$ with $0 \leq c < p^n$,

(ii) $\langle x^{cp^d}y \rangle P'/P'$ with $1 \leq d < k - n$, $1 \leq c \leq p^n$, and $p \nmid c$,

(iii) $\langle xy^c \rangle P'/P'$ with $0 \leq c < p^n$ and $p \nmid cp^{k-n}$.

By Lemma 4.1, $\langle x^{cp^{k-n}}y \rangle P'$ is a kernel if and only if

$$\langle y^{p^n} \rangle \leq \langle (x^{cp^{k-n}}y)^{p^n/c(p)} \rangle$$

Modulo $\langle y^{p^{n+1}} \rangle$, the element $z = y^{p^n}$ is a central element of order $p$, and so $(y^c)^{x^i} \equiv y^c z^i \mod \langle y^{p^{n+1}} \rangle$. Thus
\[(x^{cp^k-n}y)^{p^n/c(p)} = x^{cp^k/c(p)}y^{x^{cp^k-n}(p^n/c(p))-1} + y^{1^n/c(p)}\]

\[\equiv y^{cp^l/c(p)}y^{x^{cp^k-n}(p^n/c(p))-1} \ldots y^{1^n/c(p)}\]

\[= y^{cp^l/c(p)+p^n/c(p)}x^{cp^k-n}(p^n/c(p)-1+\ldots+1)\]

\[\equiv y^{cp^l/c(p)+p^n/c(p)} \mod (y^{p^n+1}).\]

From this we see that subgroups of the form \((x^{cp^k-n}y)\) listed are kernels if and only if \(p \nmid (1 + cp^l-n)\). Let

\[(4.1)\]

\[a = \begin{cases} 
  x^{1+c2^l-n(1+2^{n-1}+2^{k-l}+n-1)} & \text{if } p = 2 \text{ and } l + n = m, \\
  x^{1+cp^l-n} & \text{otherwise},
\end{cases}\]

and \(b = x^{cp^k-n}y\). Suppose that \(p = 2\) and \(l + n = m\). Now \(c2^l-n\) is even, so the elements \(x^{1+c2^l-n(1+2^{n-1}+2^{k-l}+n-1)}\) and \(x^{c2^k-n}y\) generate \(P\). By Lemma 3.3, we have

\[(1 + 2^n)c2^k-n(2^n-1) + \cdots + (1 + 2^n)c2^k-n + 1\]

\[\equiv (1 + c2^k(2^n - 1) + c2^{k+n-1}(2^n - 1)) + \cdots + (1 + c2^k + c2^{k+n-1}) + 1\]

\[= (1 + \cdots + 1) + c2^k(2^n - 1 + \cdots + 1) + c2^{k+n-1}(2^n - 1 + \cdots + 1)\]

\[\equiv 2^n + c2^{k+n-1} \mod 2^{k+n}.
\]

Therefore

\[(x^{c2^k-n}y)^{2^n} = x^{c2^k}y^{2^n+c2^{k+n-1}} = y^{c2^l+2^n+c2^{k+n-1}},\]

and so
4. Expressions for induced automorphism groups of quotients of $p$-groups

$$(x^{c_2^{k-n}}y)^{2^l} = (x^{c_2^{k-n}}y)^{2^{n^{2l-n}}}$$

$$= y(c_2^{l+2n}+c_2^{k+n-1})^{2^l-n}$$

$$= y^{c_2^{2l-n}+2^l+c_2^{k+l-1}}$$

$$= (x^{1+c_2^{l-n}(1+2^{n-1}+2^{k-l+n-1})})^{2^k},$$

and similarly $(x^{c_2^{k-n}}y)^{2^m} = 1$. We have

$$(1+2^n)^{1+c_2^{l-n}(1+2^{n-1}+2^{k-l+n-1})}$$

$$= (1+2^n)(1+2^n)^{c_2^{l-n}(1+2^{n-1}+2^{k-l+n-1})}$$

$$\equiv (1+2^n)(1+c_2^l(1+2^{n-1}+2^{k-l+n-1}) + c_2^{l+n-1}) \quad \text{by Lemma 3.3}$$

$$\equiv 1 + c_2^l(1+2^{n-1}+2^{k-l+n-1}) + c_2^{l+n-1} + 2^n$$

$$\equiv 1 + c_2^l + 2^n + c_2^{k+n-1} \mod 2^{l+n}.$$

Therefore the conjugate of $x^{c_2^{k-n}}y$ by $x^{1+c_2^{l-n}(1+2^{n-1}+2^{k-l+n-1})}$ is

$$x^{c_2^{k-n}}y^{1+c_2^{l-n}+2^n+c_2^{k+n-1}} = (x^{c_2^{k-n}}y)^{1+2^n}.$$

It follows that

(4.2) \quad $P \cong \langle a, b \mid a^{p^l} = b^p, b^m = 1, b^a = b^{1+p^n} \rangle$

and this presentation is clearly of the required form. The argument is similar when $p \neq 2$ or $l+n > m$.

Similarly, we may argue that $(x^{c_2^{p}}y)^{P'}$ is a kernel if and only if

$$\langle y^{p^n} \rangle \leq \langle (x^{c_2^{p}}y)^{p^{k-n}} \rangle.$$
Now with \( z = y^{p^n} \) as before,

\[
(x^{cp^d} y^{p^k-d})^{p^k-d} = x^{cp^k} y^{x^{cp^d(p^k-d-1)} + \ldots + 1} \\
= y^{cp^l} y^{zp^d(p^k-d-1)} \ldots y \\
= y^{cp^l+p^k-d} y^{zp^d(p^k-d-1)} y^{zp^d(p^k-d-1+\ldots+1)} \\
= y^{cp^l} \mod (y^{p^{n+1}}).
\]

It follows that the \((x^{cp^d} y)^P\) listed are kernels if and only if \( l = n \). Then it is easy to see that, with \( a = x^{cp^{k-n-d}} \) and \( b = x^{cp^d} \), \( P \) has a presentation given by

\[
\langle a, b | a^{p^{n+d}} = b^{p^n}, b^{p^k+m-n-d} = 1, b^a = b^{1+p^k-d} \rangle.
\]

With \( r = n + d \), \( s = n \), \( t = k + m - 2n - d \) and \( u = k - d \), we see that this presentation is also of the required kind.

Similarly, subgroups of the form \((xyc)^P\) are kernels if and only if \( (y^{p^n}) \leq (xyc) \).

The order of \( xyc \) modulo \( y \) is \( p^k \), so \( (xyc) \cap (y) = ((xyc)^p)^k \). Therefore \((xyc)^P\) is a kernel if and only if \( (y^{p^n}) \leq ((xyc)^p)^k \). Now

\[
(xyc)^p^k \equiv x^{p^k} (y^c)^x^{p^k-1} (y^c)^x^{p^k-2} \ldots (y^c)^x y^c \\
= x^{p^k} y^c z^{c(p^k-1)} y^c z^{c(p^k-2)} \ldots y^c z^{c-1} y^c \\
= x^{p^k} y^{cp^k} z^{c(p^k-1)} y^{cp^k-2+\ldots+1} \\
= y^{cp^l} y^{cp^k} y^{cp^k-2} y^{cp^k-3} \ldots y y^{cp^k-2} = y^{p^l+cp^k} \mod (y^{p^{n+1}}).
\]

It follows that if \( l > n \), then no \((xyc)^c\) is a kernel, and that if \( l = n \) then all relevant \((xyc)^c\) are kernels. Suppose that \( l = n \), and let \( a = y^{-1-cp^{k-l}} \) and \( b = (xyc)^{-1} \). Since
Expressions for induced automorphism groups of quotients of p-groups

$p | cp^{k-l}$, these elements generate $P$. Furthermore,

$$((xyC^{-1})^{p^k} = ((xyC)^{p^k})^{-1} = (x^{p^k}y^{cp^k})^{-1} = (y^{p^l}y^{cp^k})^{-1} = (y^{-1-cp^k-l})^{p^l},$$

$$((xyC^{-1})^{p^k+m-l} = 1,$$

and

$$((xyC^{-1})^{p^k+l-cp^k-l})^{-1} = (xyC^{p^k+l-cp^k-l})^{-1} = (xyC^{p^k+l-cp^k-l+c})^{-1} = (xyC(y^{1+cp^k-l})p^l)^{-1} = ((xyC)^{1+p^k})^{-1} = ((xyC)^{-1})^{1+p^k}.$$
is an automorphism $\alpha$ such that

$$
x \alpha = \begin{cases} 
  x^{1+c_{p^r}^{s-u}(1+2^{n-1}+2^{-r+s+u-1})} & \text{if } p = 2 \text{ and } u = t, \\
  x^{1+c_{p^r}^{s-u}} & \text{otherwise},
\end{cases}
$$

Since $p^w$ is the largest power of $p$ to divide $c_{p^r}^{s-u}$ for all relevant $c$, the largest power of $p$ which divides $c_{p^r}^{s-u}$ for all relevant $c$ is

$$
p^{\max\{w-r+u,0\}} = p^{\max\{s-r+w,s-u\}} = p^{\max\{s-log_p[C;(b)],s-u,0\}}.
$$

Next suppose that $\langle b \rangle$ is of the second type. Then we may suppose that $b = x^d y$ for some $d$ such that $1 \leq d < k - n$. In this case,

$$(r, s, t, u) = (n + d, n, k + m - 2n - d, k - d)$$

and equivalent kernels to $\langle b \rangle$ in $C$ are of the form $\langle x^d y \rangle = \langle x^{(c-1)p^d} b \rangle = \langle a^{c'} y^d b \rangle$ for some $c'$ such that $p^w | c' p^d$. Then with $a = x^{l+1+p^{-r-s-1}}$, it is easy to see that $a \mapsto a^{1+c'}$, $b \mapsto a^{c'} y^d b$ defines an automorphism in $N_{\text{Aut}_P}(C)$. Since $p^w$ is the largest power of $p$ dividing $c' p^d$ for all relevant $c'$, the largest power of $p$ which divides $c'$ for all relevant $c'$ is

$$
p^{\max\{w-d,0\}} = p^{\max\{s-log_p[C;(b)],s-u,0\}}.
$$

Finally suppose that $\langle b \rangle$ is of the third type. Then we may suppose that $b = x^{-1}$. In this case,

$$(r, s, t, u) = (l, k, m - l, k),$$

and, since $C < P$, the kernels equivalent to $\langle b \rangle$ in $C$ are of the form $\langle a^c b \rangle$ for some $c$ such that $p^w | c$. Since $r \geq s$, we have $k = l = r = s$. Then with $a = y^{-1}$, $a \mapsto a^{1+c}$, 


4. Expressions for induced automorphism groups of quotients of $p$-groups
4. Expressions for induced automorphism groups of quotients of \( p \)-groups

\( b \mapsto a^c b \) defines an automorphism in \( \text{NAut}_p(C) \). Then the largest power of \( p \) which divides \( c \) for all relevant \( c \) is \( p^w = p^{s-(s-u)} = p^{\max\{s-\log \left[C:(b)\right],s-u,0\}} \).

We have shown that for any kernel \( \langle b' \rangle \) equivalent to \( \langle b \rangle \) in \( C \), there is an \( \alpha \in \text{NAut}_p(C) \) such that \( b \alpha = b' \) and \( a \alpha = a^{1+e} \) where the largest power of \( p \) dividing all such \( e \) is \( p^{\max\{s-\log \left[C:(b)\right],s-u,0\}} \). It is easy to see that \( \text{NAut}_p(C) \) acts transitively on the set of subgroups equivalent to \( \langle b \rangle \) in \( C \). Therefore any element of \( \text{NAut}_p(C) \) is of the form \( \alpha \gamma \) where \( \gamma \in \text{CAut}_P(P/C_P(b)) \). By Dedekind's Law and Corollary 3.5,

\[
\text{C}_P(b) = \text{C}_{(a)}(b)(b) = (\zeta P \cap \langle a \rangle)(b) = \langle a^{p^{s+t-u}} \rangle \langle b \rangle,
\]

and so \( (gC)\gamma = (gC)^{1+jp^{s+t-u}} \) for some \( j \). Therefore \( (gC)\alpha \gamma = (gC)^{1+jp^w} \) where \( i \in \mathbb{Z} \) and \( v = \min\{\max\{s-\log \left[P:C\right],s-u,0\},s+t-u,\log \left[P:C\right]\} \). Of course, if \( v = 0 \), then the only restriction is that \( p \nmid 1 + i \) and \( \text{NAut}_p(C)\downarrow_{P/C} = \text{Aut}(P/C) \).

The statement about \( \text{NAut}_p(C)\downarrow_{P/C} \) now follows. \( \square \)

The second paragraph in Lemma 2.4 can now be generalised (see Definition 2.2 for a definition of \( C \)-standard).

**Lemma 4.6.** Let \( p \) be any prime and \( P = \langle x,y \mid x^{p^k} = y^{p^l}, y^{p^m} = 1, y^x = y^{1+p^n} \rangle \) with \( m \geq n \geq 2, k \geq 2, k + n \geq m \) and \( m \geq l \geq m - n \). Suppose that \( C \leq P \), \( [P:C] = p^w \), and \( \langle x \rangle \langle y \rangle \) is a \( C \)-standard metacyclic factorisation of \( P \). Then \( k \geq l \), and \( l < n \) implies \( k - w < l \). \( \square \)

**Theorem 4.7.** Let \( P = \langle x,y \mid x^{2^k} = y^{2^l}, y^{2^m} = 1, y^x = y^{-1+2^n} \rangle \) with \( m \geq n \geq 2, k + n \geq m \) and \( m \geq l \geq m - 1 \). Let \( C \in \text{C}(P) \).
If $k > 1$ and $l > 1$, then $C(P) = \{ \langle x^{2^{k-1}} y \rangle \} \cup \{ \langle x^{2^w}, y \rangle \mid 0 \leq w \leq k \}$, all orbits in $C(P)$ under $\text{Aut} \, P$ are singletons except that $\langle x^{2^{k-1}} y \rangle \cong \langle y \rangle$ when $l = m$ or $n < m - 1$, and $\text{N}_{\text{Aut} \, P}(C) \downarrow_{P/C}$ consists of all $(x \mapsto (xC)^r)$ with

$$r \equiv 1 \text{ mod }\begin{cases} 2 & \text{if } n \geq m - 1, \\ 2^{m-n-1} & \text{if } n < m - 1, \quad [P : C] < 2^k, \quad 2^m \nmid (2^{k+n-1} + 2^l), \\ 2^{m-n} & \text{otherwise}. \end{cases}$$

If $k = 1$ and $l > 1$, then $C(P) = \{ P, \langle y \rangle \}$, and

$$\text{N}_{\text{Aut} \, P}(C) \downarrow_{P/C} = 1.$$

If $k > 1$ and $l = 1$, then

$$C(P) = \{ \langle x \rangle \} \cup \{ \langle x^{2^t} y \rangle \mid 0 \leq t < k - 1 \} \cup \{ \langle x^{2^w}, y \rangle \mid 0 \leq w \leq k \},$$

all orbits in $C(P)$ under $\text{Aut} \, P$ are singletons except that $\langle x \rangle \cong \langle xy \rangle$, and

$$\text{N}_{\text{Aut} \, P}(C) \downarrow_{P/C} = \text{Aut}(P/C).$$

If $k = l = 1$, then the orbits in $C(P)$ under $\text{Aut} \, P$ are $\{ P \}$ and $\{ \langle x \rangle, \langle xy \rangle, \langle y \rangle \}$, and $\text{N}_{\text{Aut} \, P}(C) \downarrow_{P/C} = 1$.

Proof. Since $P' = \langle y^2 \rangle$ and since $k \geq 1$ in all cases considered, we always have $P/P' = \langle xP' \rangle \times \langle yP' \rangle \cong C_{2^k} \times C_2$ with kernels $\langle x \rangle P'/P'$ and the $\langle x^{2^t} y \rangle P'/P'$ with $0 \leq t \leq k$. By the Lemma 4.1, $\langle x \rangle P'$ is a kernel of $P$ if and only if $\langle y^2 \rangle \leq \langle x \rangle$, which is the case if and only if $l = 1$. Also by Lemma 4.1, $\langle x^{2^t} y \rangle P'$ is a kernel if and only if $\langle y^2 \rangle \leq \langle x^{2^t} y \rangle$. The order of $x^{2^t} y$ modulo $\langle y \rangle$ is $2^{k-t}$, so $\langle x^{2^t} y \rangle \cap \langle y \rangle = \langle (x^{2^t} y)^{2^{k-t}} \rangle$. 


Thus \( \langle x^2y \rangle P' \) is a kernel if and only if \( \langle y^2 \rangle \leq \langle (x^2y)^{2^{k-t}} \rangle \). We shall use that \( y^x \equiv y^{-1} \text{ mod } \langle y^4 \rangle \). If \( t > 0 \), then
\[
(x^2y)^{2^{k-t}} \equiv x^ky^{2^{k-t}} \equiv y^{2t+2^{k-t}} \text{ mod } \langle y^4 \rangle,
\]
and if \( t = 0 \) then
\[
(x^2y)^{2^{k-t}} = (xy)^{2k} \equiv x^{2k} \equiv y^{2t} \text{ mod } \langle y^4 \rangle.
\]

Therefore if \( k > 1 \) and \( l > 1 \), then \( \langle x^2y \rangle P' \) is a kernel if and only if \( t = k - 1 \) or \( k \).

If \( k = 1 \) and \( l > 1 \), then \( \langle x^2y \rangle P' \) is a kernel if and only if \( t = 1 \), in which case, \( \langle x^2y \rangle P' = \langle y \rangle \). If \( k > 1 \) and \( l = 1 \), then \( \langle x^2y \rangle P' \) is a kernel for all \( t \) such that

4. Expressions for induced automorphism groups of quotients of p-groups

Figure 4.2: Subgroup lattices showing kernels in circles.
Suppose that \( k > 1 \) and \( l > 1 \). It follows that

\[
C(P) = \{ (x^{2^{k-1}}y) \} \cup \{ (x^{2^w}, y) \mid 0 \leq w \leq k \}.
\]

Now \( (x^{2^{k-1}}y) \approx \langle y \rangle \) if and only if there an automorphism \( \alpha \) with \( y\alpha \in \langle x^{2^{k-1}}y \rangle \). By Lemma 4.4 we may assume that \( \alpha \in \text{N}_{\text{Aut}^p}((x)) \) and so \( x\alpha = x^r \) for some odd \( r \).

By Lemma 4.3, we may also assume that \( y\alpha = x^{2^{k-1}}y \). We have

\[
(x^{2^{k-1}}y)^{2^n} = (x^{2^{k-1}}y)^{2^{2n-1}}
\]

\[
= (x^{2^k}y^{1+(-1+2n)^{2^{k-1}}})^{2^{n-1}}
\]

(4.3) \[
= y^{(2^l+1+1-2^k+n-1)^{2^{n-1}}} \quad \text{by Lemma 3.3, since } k + 2n - 2 \geq m
\]

\[
= y^{(2^l+2)^{2^{n-1}}} \quad \text{since } k + 2n - 2 \geq k + n \geq m
\]

\[
= y^{2^n} \quad \text{since } l + n - 1 \geq l + 1 \geq m.
\]

Since \( r \) is odd, \( x^r \) and \( x^{2^{k-1}}y \) generate \( P \), and by (4.3), \( (x^{2^{k-1}}y)^{2^n} = 1 \). Further,

\[
(x^r)^{2^k} = x^{2^kr} = y^{2^l} = y^{2l}.
\]

It follows that \( \langle x^{2^{k-1}}y \rangle \approx \langle y \rangle \) if and only if there is an odd integer \( r \) such that the first of the following statements is true. It is easy to see that, for any given \( r \), each of these statements is equivalent to the next.
4. Expressions for induced automorphism groups of quotients of $p$-groups

\[(x^{2^k-1} y)^r = (x^{2^k-1} y)^{-1+2^n};\]
\[x^{2^k-1} y^{(-1+2^n)r} = y^{-1} x^{-2^k-1} (x^{2^k-1} y)^2^n;\]
\[x^{2^k} y^{(-1+2^n)r} = x^{2^{k-1}} y^{-1} x^{-2^{k-1}} (x^{2^{k-1}} y)^2^n;\]
\[y^{2^l+(-1+2^n)r} = y^{(-1+2^n)^{2^{k-1}} y^{2^n}};\]
\[y^{2^l+(-1+2^n)r+(-1+2^n)^{2^{k-1}}-2^n} = 1;\]
\[y^{2^l+(-1+2^n)r+1+2^n+(-1+2^n)^{2^{k-1}}-2^n} = 1;\]
\[y^{2^n+1+2^l+((2^n-1)^{r-1})-1} = 1.\]

It follows that $\langle y \rangle \approx \langle x^{2^k-1} y \rangle$ if and only if $l = m$ or $n < m - 1$; for when $l = m - 1$ and $n \geq m - 1$, clearly no such $r$ exists, and otherwise

\begin{equation*}
(4.4) \\
r = \begin{cases} 
1 + 2^{m-n-1} & \text{if } n < m - 1 \text{ and } 2^m \not| (2^{k+n-1} + 2^l), \\
1 & \text{otherwise}
\end{cases}
\end{equation*}

is a possible choice for $r$. If $w \neq \bar{w}$, $0 \leq w \leq k$ and $0 \leq \bar{w} \leq k$, then $|\langle x^{2^w}, y \rangle| \neq |\langle x^{2\bar{w}}, y \rangle|$ and it follows that all orbits in $C(P)$ under $\text{Aut} P$ are singletons, except that $\langle x^{2^k-1} y \rangle \approx \langle y \rangle$ when $l = m$ or $n < m - 1$.

By Dedekind’s Law and Corollary 3.5,

\[C_P(y) = C_{\langle x \rangle}(y) \langle y \rangle \]
\[= (\zeta P \cap \langle x \rangle) \langle y \rangle \]
\[= \begin{cases} 
\langle x^2 \rangle \langle y \rangle & \text{if } m = n, \\
\langle x^{2^{m-n}} \rangle \langle y \rangle & \text{otherwise.}
\end{cases}
\]
4. Expressions for induced automorphism groups of quotients of $p$-groups

When $n \geq m - 1$, this shows that $(x \mapsto x^r, y \mapsto y) \in \text{Aut} P$ for all odd $r$ and Lemma 1.1 shows that

$$\text{Aut}(P/C) = (\text{C}_{\text{Aut}(P/\langle y \rangle)}(P/C_P(\langle y \rangle)))_{\downarrow P/C} = \text{N}_{\text{Aut} P}(\langle y \rangle)_{\downarrow P/C} \leq \text{N}_{\text{Aut} P}(C)_{\downarrow P/C},$$

and so $\text{N}_{\text{Aut} P}(C)_{\downarrow P/C} = \text{Aut}(P/C)$. Henceforth suppose that $n < m - 1$. Note that $C$ contains either $\langle y \rangle$ or $\langle x^{2^{k-1}} y \rangle$, since these are the only kernels of $P$. Suppose that $[P : C] < 2^k$. Then $C$ contains both $\langle y \rangle$ and $\langle x^{2^{k-1}} y \rangle$. Therefore by Lemma 4.4 any $\alpha \in \text{N}_{\text{Aut} P}(C)$ is in a coset of $\text{N}_{\text{Aut} P}(\langle y \rangle)$ containing either the automorphism such that

$$x \mapsto \begin{cases} x^{1+2^m-2} - 1 & \text{if } 2^m \mid (2^{k+n-1} + 2^l), \\ x & \text{otherwise}, \end{cases} \quad y \mapsto x^{2^{k-1}} y$$

or $1$. Then

$$\text{N}_{\text{Aut} P}(C)_{\downarrow P/C} = \begin{cases} \{ xC \mapsto (xC)^{1+2^m-2n} \mid i \in \mathbb{Z} \} & \text{if } 2^m \mid (2^{k+n-1} + 2^l), \\ \{ xC \mapsto (xC)^{1+2^m-2n-1} \mid i \in \mathbb{Z} \} & \text{otherwise}. \end{cases}$$

Finally, suppose that $[P : C] = 2^k$. Then

$$\text{N}_{\text{Aut} P}(C)_{\downarrow P/C} = \text{N}_{\text{Aut} P}(\langle y \rangle)_{\downarrow P/C} = \text{C}_{\text{Aut}(P/\langle y \rangle)}(P/C_P(\langle y \rangle)) = \{ (xC \mapsto (xC)^{1+2^m-2n} ) \mid i \in \mathbb{Z} \}.$$

The statement regarding $\text{N}_{\text{Aut} P}(C)_{\downarrow P/C}$ is therefore true.

If $k = 1$ and $l > 1$, then $C(P) = \{ P, \langle xy \rangle, \langle y \rangle \}$, and so $[P : C] \leq 2$ for any $C \in C(P)$. It follows that $\text{N}_{\text{Aut} P}(C)_{\downarrow P/C} = \text{Aut}(P/C)$. 
If $k > 1$ and $l = 1$, then $n = m = 2$ and the statement about $C(P)$ follows. Further $x \mapsto xy$, $y \mapsto y$ defines an automorphism of $P$, since $xy$ and $y$ generate $P$, $(xy)^{2^k} = y^2$ and $y^{2^m} = y^{-1+2^n}$. If $[P : C] > 2$, then a kernel $K$ of minimal order contained in $C$ is of the form $(y)$ or $(x^{2^l}y)$ with $1 \leq t < k-1$. In the first case $x \mapsto x^r$, $y \mapsto y$ defines an automorphism for any odd $r$. In the second case, with $a = x^{1+2^k-t-1}$ and $b = x^{2^l}y$, we see that $P \cong \langle a, b \mid a^{2^l+1} = b^2, b^{2^k-t+1} = 1, b^a = b^{1+2^k-t} \rangle$. Again $a \mapsto a^r$, $b \mapsto b$ defines an automorphism for any odd $r$. In any case, $\mathbf{N}_{\text{Aut}}(P/K)_{\downarrow P/K} = \text{Aut}(P/K)$ and hence $\mathbf{N}_{\text{Aut}}(P/C)_{\downarrow P/C} = \text{Aut}(P/C)$.

The statements regarding the case when $k = l = 1$ follow from the fact that in that case $P \cong Q_8$. □

**Corollary 4.8.** Let $G$ be a $p$-group. Then kernels of $G$ of the same order are equivalent if and only if $G$ is not of the form

$$\langle x, y \mid x^{2^k} = y^{2^l}, y^{2^{l+1}} = 1, y^x = y^{-1} \rangle$$

with $k \geq 2$, $l \geq 2$. 
Chapter 5

Finite metacyclic groups

We are now in a position to classify finite metacyclic groups. We begin with a Lemma which shows that one of Sim's conditions defining a standard presentation was redundant.

Lemma 5.1. If $\alpha$, $\zeta$ and $\theta$ are integers, $\zeta$ is odd, $\gcd(\alpha, \zeta) = 1$, $\theta^\alpha \equiv 1 \mod \zeta$ and $\mu = \text{lcm}\{ q - 1 \mid q \in \varpi(\zeta) \}$, then $\theta^\mu \equiv 1 \mod \zeta$. □

Proof. Suppose $q \in \varpi(\zeta)$. Then $q \nmid \alpha$ because $\gcd(\alpha, \zeta) = 1$. Therefore $q \nmid \text{ord}_\zeta \theta$ since $(\text{ord}_\zeta \theta) | \alpha$, and so $q \nmid \text{ord}_\zeta \theta$. Since $|J(\zeta_q)|_{q'} = q - 1$, $(\text{ord}_\zeta \theta) | (q - 1)$. But $(q - 1) | \mu$, so $\theta^\mu \equiv 1 \mod \zeta_q$, and the result follows. □

The following observation made by Kovacs simplifies the classification in Theorem 5.3:

Lemma 5.2. If $\phi : O(J(\epsilon, \zeta)) \to \Gamma$ is the constant function $\lambda \phi' = \epsilon$, $\lambda \phi'' = J(\epsilon)$, then $T(\phi, J(\epsilon, \zeta)) = T(\epsilon, \zeta)$.
Proof. It is clear that $T(\phi, J(\epsilon, \zeta)) \supseteq T(\epsilon, \zeta)$. Suppose that $\kappa \in T(\phi, J(\epsilon, \zeta))$ and $s$ is an integer such that $\text{ord}_\zeta \kappa^s = \text{ord}_\zeta \kappa = \rho$, say. Then, since $\gcd(s, \in(\mathfrak{s}, \mathfrak{v}(s)) = 1$, $s + \in(\mathfrak{s}, \mathfrak{v}(s)) \mod \epsilon$ is an element, $w$ say, of $J(\epsilon)$. Moreover, since $\rho | \in(\mathfrak{s}, \mathfrak{v}(s))$, 

$$\kappa^w \equiv \kappa^s \mod \zeta.$$ 

Therefore $\kappa^s \mod \zeta = \kappa^w \mod \zeta \geq \kappa \mod \zeta$, by the definition of $T(\zeta, J(\epsilon), \phi)$. Thus $\kappa \in T(\zeta)$ and hence in $T(\epsilon, \zeta)$. □

In the following definition, $\lambda_\omega$ is the map given in equation (1.1).

**Definition 5.1.** We define $\Omega$ to be the set of 8-tuples of odd positive integers 

$$(\alpha, \beta, \gamma, \delta, \epsilon, \zeta, \theta, \kappa)$$

such that the following eleven conditions hold:

(i) $\beta | \alpha$,

(ii) $\beta | \gamma$,

(iii) $\in(\alpha) \subseteq \in(\zeta)$

(iv) $\in(\alpha \gamma) \cap \in(\zeta) = \emptyset$,

(v) $\delta | \gamma$,

(vi) $\gamma | \beta \delta$,

(vii) $\in(\beta) \subseteq \in(\delta)$

(viii) $\theta \in T(\phi_2, J(\alpha, \zeta))$ where $\phi_2 : O(J(\alpha, \zeta)) \to \Gamma$ is given by

$$\omega \phi'_2 = \omega, \quad \omega \phi''_2 = \left( \prod_{p \in \in(\omega)} L_p \right) \lambda_\omega$$
where

\[ \lambda(\omega, p) = \min\{\max\{\psi(\beta, p) - \psi(\delta, p), \psi(\beta, p) - \psi(\alpha, p) + \psi(\omega, p)\}, \psi(\gamma, p) - \psi(\delta, p), \psi(\omega, p)\} \]

and

\[ L_p = \begin{cases} J(\omega_{[p]}) & \text{if } \lambda(\omega, p) \leq 0, \\ (1 + p^{\lambda(\omega, p)}) & \text{otherwise.} \end{cases} \]

(ix) \( \kappa \in T(\epsilon, \zeta) \).

(x) \( \varpi(\delta/\beta) \subseteq \varpi(\beta(\text{ord}_\zeta \theta)/\alpha) \).

(xi) \( \gcd(\theta \kappa - 1, \zeta) = 1 \).

If \( m \) and \( n \) are natural numbers, the Chinese Remainder Theorem tells us that the smallest natural number \( c \) such that

\[ c \equiv n \mod 2^m, \]
\[ c \equiv 1 + (\delta \mid \gamma) \mod \gamma, \]
\[ c \equiv \eta \theta \kappa \mod \zeta \]

is

\[ (5.1) \quad c = (n \gamma \zeta(\gamma \zeta)_{2^m}^{-1} + (1 + (\delta \mid \gamma))2^m \zeta(2^m \zeta)_{\gamma}^{-1} + \eta \theta \kappa 2^m \gamma(2^m \gamma)_{\zeta}^{-1}) \mod 2^m \gamma \zeta \]

We are now ready for the main theorem.
Theorem 5.3. Each finite, metacyclic group has precisely one presentation of the form
\[
\langle x, y \mid x^{2^k \alpha} = y^{2^l \beta}, y^{2^m \gamma} = 1, y^z = y^\zeta \rangle
\]
where \((\alpha, \beta, \gamma, \delta, \epsilon, \zeta, \theta, \kappa) \in \Omega, c\) is given by (5.1), and one of the following five sets of conditions hold. In each of them \(\eta \in T(\phi_1, J(2^k, \zeta))\) where \(\phi_1 : O(J(2^k, \zeta)) \to \Gamma\) and \(\phi_1' : 2^\xi \mapsto 2^\xi\).

(a) \(k \geq l \leq m; l \leq 1; n = 1; 2^\xi \phi_1'' = J(2^\xi); l = m\) when \(2^{k-l} \geq \text{ord}_{\zeta} \eta\).

(b) \(k = 1;\) there exist natural numbers \(s, t, u\) with \(u \leq 1, t \leq 1, ut = 0\) and \(u + s > 0\) such that \(l = s + t + 1, m = s + t + u + 1\) and \(n = -1 + 2^{s+u+1}; 2^\xi \phi_1'' = 1\).

(c) \(k + m \geq 4;\) \(k \geq 1; m \geq 2; l = 1; n = 1 + 2^m - 1; 2^\xi \phi_1'' = J(2^\xi); m = 2\) when \(2^{k-l} \geq \text{ord}_{\zeta} \eta\).

(d) \(k \geq l \geq 2; l \leq m; n = 1 + 2^u\) with \(u \geq m - l\);

\[
2^\xi \phi_1'' = \begin{cases} 
J(2^\xi) & \text{if } v = 0, \\
(1 + 2^v) & \text{otherwise}
\end{cases}
\]
with \(v = \min\{\max\{l - k + \xi, l - u\}, m - u, \xi\}; l \geq n\) when \(k \geq l + \log_2(\text{ord}_{\zeta} \eta)\).

(e) There exist natural numbers \(r, s, t, u, v\) and \(w\) with \(r \geq 2, v \leq r, w \leq 1, su = tu = tv = 0,\) and \(w = 0\) when \(v \geq r - 1\) such that \(k = r + s + t, l = r + s + u + v, m = r + s + u + v + w\) and \(n = -1 + 2^r + u;\)

\[
2^\xi \phi_1'' = \begin{cases} 
J(2^\xi) & \text{if } s + v + w \leq 1, \\
(1 + 2^{s+v+w-1}) & \text{if } s + v + w > 1, 2^\xi < 2^{s+t+v+w} \text{ and } 2^{v+w} \nmid (2^{r+u-1} + 2^v), \\
(1 + 2^{s+v+w}) & \text{otherwise}.
\end{cases}
\]
5. Finite metacyclic groups

By 'precisely one presentation' we mean that the parameters $\alpha$, $\beta$, $\gamma$, $\varepsilon$, $\zeta$, $k$, $l$, $m$ and $c$ subject to the conditions described are invariants.

**Proof Theorem 5.3.** Let $G$ be a finite metacyclic group and $HN$ the standard Hall-decomposition for a metacyclic factorisation $G = SK$. Then $H \geq S_2K_2 = H_2$ and $G = H_2H_2'N$ where $H_2'N$ is a normal metacyclic subgroup of $G$ of odd order. Let $\varepsilon = |N \cap S|$, $\zeta = |N \cap K|$ and $q \in \varpi(N)$. If $K_q = 1$, then $S_qK$ is a normal Hall $q'$-subgroup of $G$. This would imply that $q \notin \varpi(N)$. Thus $\varpi(\varepsilon) \subseteq \varpi(\zeta)$. Note that $\Omega_{\varpi(H_2')}(G) \leq H_2'$. Since $H_2' \cap K$ is characteristic in $K$, it is a subgroup of $\Omega_{\varpi(H_2')}(G)$.

Since it is a kernel of $H_2'$, Lemma 2.3 shows that $H_2'$ has an $\Omega_{\varpi(H_2')}(G)$-standard factorisation, $XY$ say. Let $\alpha = [X : X \cap Y]$, $\beta = [Y : X \cap Y]$, $\gamma = |Y|$ and $\delta = [Y : H_2']$. Then $\alpha$, $\beta$, $\gamma$, $\delta$, $\varepsilon$, $\zeta$ are odd positive integers. By Lemma 2.4 of this thesis and Lemma 5.10 of [20], $\beta | \alpha$, $\beta | \gamma$, $\delta | \gamma$, $\gamma | \beta \delta$ and $\varpi(\beta) \subseteq \varpi(\delta)$.

By Lemma 2.4, for any $p \in \varpi(H_2')$, the Sylow $p$-subgroup of $H_2'$ has the following presentation:

$$\langle x_p, y_p \mid x_p^{\alpha} = y_p^{\beta}, y_p^{\gamma} = 1, y_p^{x_p} = y_p^{1+\delta(p)} \rangle.$$

Let $\overline{x} = \prod_{p \in \varpi(H_2')} x_p$ and $\overline{y} = \prod_{p \in \varpi(H_2')} y_p^{\alpha(p)\beta(p)}\gamma^{-1}$. A routine calculation shows that $\overline{x}^\alpha = \overline{y}^\beta$, $\overline{y}^\gamma = 1$ and $\overline{y}^{\overline{x}} = \overline{y}^{1+\delta(\gamma)}$. By the definition of $H$, $\varpi(\alpha \gamma) \cap \varpi(\zeta) = \emptyset$. Let $N \cap S = \langle u \rangle$, and $N \cap K = \langle v \rangle$ and $\kappa$ be the smallest positive integer such that $v^u = v^\kappa$. Then $\kappa \in J(\varepsilon, \zeta)$. Suppose that $s \in J(\varepsilon)$ such that $\kappa^s \mod \zeta$ is minimal in $J(\zeta)$. Then if $\phi : O(J(\varepsilon, \zeta)) \to \Gamma$ is the constant function $\lambda \phi' = \varepsilon$, $\lambda \phi'' = J(\varepsilon)$, then Lemma 5.2 shows that $T(\varepsilon, \zeta) = T(\phi, J(\varepsilon, \zeta))$ which contains $\kappa^s \mod \zeta$. Replacing $u$ by $u^s$, we may assume that $\kappa \in T(\varepsilon, \zeta)$. Let $\theta$ be the smallest positive integer such
that \( v^x = v^y \). Then \( \theta \in J(\alpha, \zeta) \) such that, by Lemma 2.4, \( \varphi(\delta/\beta) \subseteq \varphi(\beta(\text{ord}_p \theta)/\alpha) \) since the factorisation \( \langle x_p \rangle \langle y_p \rangle \) is \( \mathcal{O}_p(G) \)-standard for every \( p \in \varphi(H_{2'}) \). If \( G \) is nilpotent, then \( N = 1 \), and so \( \zeta = 1 \). Otherwise, there is a prime, \( q \in \varphi(N) \). Since the Hall \( q' \)-subgroups are not normal in \( G \), \( S_{q'} \) acts nontrivially on \( K_q \). By 10.1.6 in [17], \( S_{q'} \) must act nontrivially on \( \Omega_1(K_q) \). It follows that \( \gcd(\theta \kappa - 1, q) = 1 \) and, as in the nilpotent case, that \( \gcd(\theta \kappa - 1, \zeta) = 1 \). By the definition of \( T(\phi_2, J(\alpha, \zeta)) \), there is a \( \theta_1 \in T(\phi_2, J(\alpha, \zeta)) \) such that \( \theta_1 \equiv \theta t \mod \zeta \) for some \( t \in (\text{ord}_p \theta)^{\phi_2'}(\mathcal{O}_p(G)) \).

Then \( t = \sum_{p \in \varphi(\alpha)} l_p (\text{ord}_p \theta)^{\phi_p'}((\text{ord}_p \theta)^{\phi_p'}(\mathcal{O}_p(G))) \mod (\text{ord}_p \theta) \) with \( l_p \in L_p \) for all \( p \in \varphi(H_{2'}) \). By Theorem 4.5 and the definition of \( L_p \), for each \( p \in \varphi(H_{2'}) \), there is an element of \( \mathcal{N}_{\mathcal{A}ut H_p}(\mathcal{O}_p(G)) \) which maps \( x_p \) to \( x_p^{l_p} h_p \) with \( h_p \in \mathcal{O}_p(G) \). Forming the composite of the natural extensions of these automorphisms, we see that there is an element of \( \mathcal{N}_{\mathcal{A}ut H_{2'}}(\mathcal{O}_{2'}(G)) \) which maps \( x = \prod_{p \in \varphi(H_{2'})} x_p \) to \( \prod_{p \in \varphi(H_{2'})} x_p^{l_p} h = \bar{x}^t h \) with \( h \in \mathcal{O}_{2'}(G) \). Replacing \( \bar{x} \) and \( \bar{y} \) by their respective images under this composite, it follows that we may assume that \( \theta \in T(\phi_2, J(\alpha, \zeta)) \).

By Theorem 3.6, \( H_2 \) has exactly one of the following kinds of presentation:

(i) \( \langle a \mid a^{2^r} = 1 \rangle \), with \( r \geq 0 \).

(ii) \( \langle a, b \mid a^{2^r} = b^2 = 1, b^a = b \rangle \) with \( r \geq 1 \),

(iii) \( \langle a, b \mid a^2 = b^{2^r} = 1, b^a = b^{-1} \rangle \) with \( r \geq 2 \),

(iv) \( \langle a, b \mid a^2 = b^{2^r}, b^{2^r+1} = 1, b^a = b^{-1} \rangle \) with \( r \geq 1 \),

(v) \( \langle a, b \mid a^2 = b^{2^r+1} = 1, b^a = b^{1+2^r} \rangle \) with \( r \geq 2 \),

(vi) \( \langle a, b \mid a^2 = b^{2^r+1} = 1, b^a = b^{-1+2^r} \rangle \) with \( r \geq 2 \),

(vii) \( \langle a, b \mid a^{2^s} = b^2, b^{2^s+1} = 1, b^a = b^{1+2^u} \rangle \) with \( r \geq s \geq u \geq 2 \) and \( u \geq t \),
(viii) \( \langle a, b \mid a^{2^r s t + t} = b^{2^{r+s+t} w}, b^{2^{r+s+t} w} = 1, b^a = b^{-1+2^{r+s}} \rangle \) with \( r \geq 2, v \leq r, w \leq 1, su = tu = tv = 0, \) and if \( v \geq r - 1, \) then \( w = 0. \)

\( K_2 \) is a kernel of \( H_2 \) and is in \( \mathfrak{O}_2(G), \) since it is characteristic in the normal subgroup \( K. \) Let \( \langle b' \rangle \) be of minimal order among the kernels of \( H_2 \) that are contained in \( \mathfrak{O}_2(G). \) Define \( \xi \) by \( 2^\xi = [H_2 : \mathfrak{O}_2(G)]. \) Then \( \text{ord}_2 \eta = 2^\xi. \) Exactly one of the following five cases may arise:

(a) \( H_2 \) is of type (i) or (ii). It therefore has a presentation of the form

\[ \langle a, b \mid a^{2r} = b^{2^s} = 1, b^a = b \rangle \]

with \( r \geq s \) and \( s \leq 1. \) Then either \( \langle b' \rangle \approx \langle a^{2^t} b^s \rangle \) with \( 0 \leq t \leq r - 1, \) or \( \langle b' \rangle \approx 1 \) when \( s = 0, \) and so there is an \( a' \) in \( H_2 \) such that

\[ H_2 = \langle a', b' \mid a^{2^r s t} = b^{2^s}, b^{2^r s^{-1}} = 1, b^{a'} = b' \rangle \]

where \( r, s \) and \( t \) are natural numbers with \( r \geq s + t \) and \( s \leq 1. \) Then

\[ H_2 = \langle a', b' \mid a^{2^r k l} = b^{2^l}, b^{2^m} = 1, b^{a'} = b' \rangle \]

where \( k, l \) and \( m \) are natural numbers with \( k \geq l \leq m \) and \( l \leq 1. \) Suppose that \( 2^{k-1} \geq \text{ord}_2 \eta. \) Since \( b' = a^{-2^{k-l}} a^{2^l} b', \) \( \langle b' \rangle \) is a smallest kernel of \( H_2 \) which lies in \( \mathfrak{O}_2(G). \) By the definition of \( b', \) \( 2^l = |b| = |b'| = 2^m, \) and so \( l = m. \) In this case, we have \( N_{\text{Aut} H_2(\mathfrak{O}_2(G))} = H_2/\mathfrak{O}_2(G) = \text{Aut}(H_2/\mathfrak{O}_2(G)). \)

(b) \( H_2 \) is of type (iii), (iv) or (vi). By the cases \( k = 1 \) of Theorem 4.7, \( \langle b' \rangle \approx \langle b \rangle. \)

It is easy to see that there is an \( a' \in H_2 \) such that

\[ H_2 = \langle a', b' \mid a^{2^{r+s+t+1}} = b^{2^{r+t+s+1}}, b^{2^{r+t+s+1}} = 1, b^{a'} = b'^{-1+2^{r+s+t+1}} \rangle \]
for some natural numbers $s, t$ and $u$ such that $u \leq 1$, $t \leq 1$, $tu = 0$ and $s + u \neq 0$.

By Theorem 4.7, we have $N_{\text{Aut}H_2}(O_2(G))_{H_2/O_2(G)} = 1$.

(c) $H_2$ is of type (v). By Lemma 3.7, we have

$$H_2 = \langle x, y \mid x^{2^r} = y^2, y^4 = 1, y^x = y^{-1} \rangle.$$ 

Then $\langle b' \rangle \cong \langle x^{2^r} y \rangle$ with $0 \leq t \leq r - 2$ or $\langle b' \rangle \cong \langle y \rangle$, and so there is an $a' \in H_2$ such that

$$H_2 = \langle a', b' \mid a'^{2^{t+1}} = b'^2, b'^{2^{r-t+1}} = 1, b'^{a'} = b'^{1+2^{r-t}} \rangle$$

with $r \geq 2$ and $0 \leq t \leq r - 1$. Then

$$H_2 = \langle a', b' \mid a'^{2^k} = b'^2, b'^{2^m} = 1, b'^{a'} = b'^n \rangle$$

with $k + m \geq 4$, $k \geq 1$, $m \geq 2$ and $n = 1 + 2^{m-1}$. Suppose that $2^{k-1} \geq \text{ord}_x \eta$. Since $y = x^{-2^{k-1}} x^{2^t} y$, $\langle y \rangle$ is a smallest kernel of $H_2$ which lies in $O_2(G)$. By the definition of $b'$, $2^2 = |y| = |b'| = 2^m$, and so $m = 2$. By Theorem 4.7, we have $N_{\text{Aut}H_2}(O_2(G))_{H_2/O_2(G)} = \text{Aut}(H_2/O_2(G))$.

(d) $H_2$ is of type (vii). Theorem 4.5 shows that there is an $a' \in H_2$ such that

$$H_2 = \langle a', b' \mid a'^{2^r} = b'^2, b'^{2^s+t} = 1, b'^{a'} = b'^{1+2^n} \rangle$$

where $r, s, t$ and $u$ are natural numbers with $r \geq s \geq 2$, $u \geq t$. Then

$$H_2 = \langle a', b' \mid a'^{2^k} = b'^2, b'^{2^l} = 1, b'^{a'} = b'^{1+2^n} \rangle$$

where $k, l, m$ and $n$ are natural numbers with $k \geq l \geq 2$, $l \leq m$ and $n \geq m - l$. 
Theorem 4.5 also shows that
\[
N_{\text{Aut}} H_2(\mathbb{O}_2(G)) \downarrow_{H_2/O_2(G)} = \begin{cases} 
\text{Aut}(H_2/O_2(G)) & \text{if } v = 0, \\
\{ \theta \mid (a'O_2(G))^{i\theta} = (a'O_2(G))^{1+ip}, i \in \mathbb{Z} \} & \text{otherwise}
\end{cases}
\]
where
\[
v = \min \{ \max \{ s - r + \xi, s - u \}, s + t - u, \xi \}.
\]
Lemma 4.6 shows that \( l \geq n \) when \( r \geq l + \log_2(\text{ord}_\eta) \).

(e) \( H_2 \) is of type (viii). Irrespective of whether \( \langle b' \rangle = \langle b \rangle \) or \( \langle b' \rangle = \langle a^{2r+t+1}b \rangle \), we see that there is an \( a' \in H_2 \) such that
\[
H_2 = \langle a', b' \mid a^{2r+t+1} = b^{2^{r+s+t+1}}, b^{2^{r+s+t+1}+1} = 1, b^{a'} = b^{-1+2^{r+w}} \rangle
\]
where \( r, s, t, u, v \) and \( w \) are natural numbers with \( r \geq 2, v \leq r, w \leq 1, su = tu = tv = 0 \), and \( w = 0 \) when \( v \geq r - 1 \). By Theorem 4.7,
\[
N_{\text{Aut}} H_2(\mathbb{O}_2(G)) \downarrow_{H_2/O_2(G)}
\]
consists of all \((xC \mapsto (xC)^r)\) with
\[
2 \text{ if } s + v + w \leq 1, \\
r \equiv 1 \mod 2^{s+v+w-1} \text{ if } s + v + w > 1, \text{ord}_\eta < 2^{r+s+t} \text{ and } 2^{v+w} \mid (2^{r+t-1} + 2^v), \\
2^{s+v+w} \text{ otherwise.}
\]
In the nth case,
\[
H_2 = \langle a', b' \mid a^{2^k} = b^{2^l}, b^{2^m} = 1, b^{\alpha'} = b^m \rangle
\]
where \(k, l, m\) and \(n\) are specified in the \(n\)th type in the statement and

\[
N_{Aut H_2(O_2(G))} H_2/O_2(G)
\]

consists of all \((a' O_2(G) \mapsto a''^m O_2(G))\) where \(m \in 2^{k} \phi''_1\) and \(\phi_1\) is specified in the \(n\)th type in the statement for \(n = (a), (b), (c), (d)\) and \((e)\). By the definition of \(T(\phi_1, J(2^k, \zeta))\), there is an \(\eta_1 \in T(\phi_1, J(2^k, \zeta))\) such that \(\eta_1 \equiv \eta^m \mod \zeta\) for some \(m \in 2^k \phi''_1\). By the above, there is an element of \(N_{Aut H_2(O_2(G))}\) which maps \(a'\) to \(\bar{a} \in a''^m O_2(G)\). Then \(v\bar{a} = v_{a''^m} = v_{\eta^m} = v_{\eta_1}\), and we see that replacing \(a'\) and \(b'\) by their images under this automorphism, we may suppose \(\eta \in T(\phi_1, J(2^k, \zeta))\).

Further, \(x := a'xu\) and \(y := b'^{a_\alpha b_\alpha 2^m \zeta_\gamma^{-1} y^{a_\kappa e_\zeta^{-1}} \zeta_\gamma^{-1} v^{2^k a_\alpha (2^k) \zeta_\gamma^{-1} \beta_\gamma^{-1}}\) satisfy the relations

\[
x^{2^k \alpha \epsilon} = y^{2^k \beta \epsilon}, \quad y^{2^m \alpha \gamma} = 1, \quad \text{and}
\]

\[
y^x = b'^{a_\alpha b_\alpha 2^m \zeta_\gamma^{-1} y^{a_\kappa e_\zeta^{-1}} \zeta_\gamma^{-1} v^{2^k a_\alpha (2^k) \zeta_\gamma^{-1} \beta_\gamma^{-1}}}
\]

\[
= b'^{a_\alpha b_\alpha 2^m \zeta_\gamma^{-1} y^{1 + (\delta \gamma)} 2^{k e_\zeta^{-1}} \zeta_\gamma^{-1} v^{\eta \theta n 2^k a_\alpha (2^k) \zeta_\gamma^{-1} \beta_\gamma^{-1}}}
\]

\[
= y^c
\]

where \(c\) is the smallest natural number such that

\[
c \equiv n \mod 2^m,
\]

\[
c \equiv 1 + (\delta \mid \gamma) \mod \gamma,
\]

\[
c \equiv \eta \theta \kappa \mod \zeta.
\]

As we saw before,

\[
c = (n \gamma \zeta (\gamma \zeta)^{-1} + (1 + (\delta \mid \gamma)) 2^m \zeta (2^m \zeta)^{-1} + \eta \theta \kappa 2^m \gamma (2^m \gamma)^{-1}) \mod 2^m \gamma \zeta.
\]
Therefore $G$ has a presentation as described.

We now show that the parameters are invariant. Suppose that $G$ is of type (a) in the statement. That $k$, $l$, $m$ and $n$ are invariants of $G$ follows from the fact that the smallest kernel of $H_2$ contained in $\mathcal{O}_2(G)$ has index $2^k$ in $H_2$ and order $2^m$ and that $H_2$ is cyclic if and only if $l = 0$. If $G$ is of type (b), then $u$ and $t$ are invariants since Theorem 3.6 shows that two 2-groups of different types out of (ii), (iv) and (vi) are not isomorphic, and consideration of the order of $H_2$ shows that $s$ is an invariant.

Suppose that $G$ is of type (c) in the statement. That $k$ and $m$ are invariants of $G$ follows from the fact that the smallest kernel of $H_2$ contained in $\mathcal{O}_2(G)$ has index $2^k$ in $H_2$ and order $2^m$. Suppose that $G$ is of type (iv) in the statement. Since $2^l = |H_2|/\exp(H_2)$, $l$ is an invariant of $G$. Since $2^k$ is the index of a smallest kernel of $H_2$ contained in $\mathcal{O}_2(G)$, $k$ is an invariant of $G$. Since $|H_2/H_2'| = 2^{k+n}$, $u$ is an invariant of $G$. Finally, since $|H_2| = 2^{k+m}$, $m$ is also an invariant of $G$. If $G$ is of type (e) in the statement, then Theorem 3.6 shows that $r$, $s$, $t$, $u$, $v$ and $w$ are invariant. It follows that $k$, $l$, $m$ and $n$ are invariants of $G$ in each case.

We observe that $\beta = |H_2|/\exp(H_2'$), and so $\beta$ is an invariant of $G$. For every $p \in \varpi(H_2')$, we define $e_p = \exp(H_p/H_2')$, $f_p = |H_p|/\exp\mathcal{O}_p(G)$ and $g_p = p^{\alpha(p) + \alpha(\text{ord}_c \delta,p)}$. It follows that $e_p = \max\{\alpha(p), \alpha(p)\delta(p)/\beta(p)\}$ and $f_p = \min\{\alpha(p), \beta(p)(\text{ord}_c \theta)(p)\}$.

Let $\pi^* = \{p \in \varpi(H_2') \mid f_p = g_p\}$. If $f_p = g_p$ then $\alpha(p) \geq \beta(p)(\text{ord}_c \theta)(p)$ and hence $\beta(p) \geq \delta(p)$, so $e_p = \alpha(p)$. Otherwise $f_p < g_p$ and $\alpha(p) < \beta(p)(\text{ord}_c \theta)(p)$ and hence $f_p = \alpha(p)$. Therefore $\alpha = \prod_{p \in \pi^*} e_p \prod_{p \in \varpi(H_2') \backslash \pi^*} f_p$ is an invariant of $G$. Since
\[ \alpha \gamma = |H_2|, \gamma \text{ is an invariant, and since } \alpha \delta = |H_2|/|H_2|, \delta \text{ is an invariant of } G. \] We know from Theorem 5.7 in [20] that \( \varepsilon = |S \cap N| \) and \( \zeta = |K \cap N| \), are invariants. Suppose that \( G \) has a presentation with \( \theta \) replaced by \( \theta_1 \in T(\phi_2, J(\alpha, \zeta)) \). Then \( G \) has an element \( h \in H_2\gamma \) where \( H_2\gamma \cong H_2\gamma \) via an isomorphism mapping \( h \) onto \( \bar{x} \). Since \( H_2\gamma = H_2\gamma \) for some \( g \in \langle v \rangle \) we have \( h^g \phi_\theta(G) = \bar{x}\phi_\theta(G) \) for some integer \( s_1 \). Since the composite of the conjugation with the isomorphism is an element of \( \mathbb{N}_{\text{Aut}} H_2\phi_\theta(G) \), the integer \( s_1 \) is in \( (\text{ord}_\zeta \theta)\phi'' \). Moreover \( v^{s_1} = v^h = v^{s_1} = v^{s_1} \) and so \( \theta_1 = \theta^{s_1} \). By the definition of \( T(\phi_2, J(\alpha, \zeta)) \), \( s_1 = 1 \), and so \( \theta \) is an invariant of \( G \). Suppose that \( G \) has a presentation with \( \kappa \) replaced by \( \kappa_1 \in T(\zeta, \varepsilon) \). Theorem 2.2 shows that the conjugacy class of \( S \cap N \) is independent of the factorisation. It follows that \( N \) contains an element \( u_1 \) such that \( v^{s_1} = v^{s_1} \) and \( u_1^{s_2} = v^{s_2} \) for some integer \( s_2 \) and some \( v' \in \langle v \rangle \). Then \( v^{s_1} = v^{s_1} = v^{s_2} = v^{s_2} = v^{s_2} \) and so \( \kappa_1 = \kappa^{s_2} \mod \zeta \). By Lemma 5.2, \( s_2 = 1 \) and so \( \kappa \) is an invariant of \( G \). A similar argument to that used for \( \theta \) shows that \( \eta \) is also an invariant, and consequently \( c \) is too.

**Theorem 5.4.** Using the classification in Theorem 5.3,

- a type (a) group is split if and only if the following two conditions hold: (i) \( k = l \) or \( l = m \) or \( \eta = 1 \), (ii) for every \( p \in \varpi(H_2) \) either \( \text{ord}_\zeta \theta = 1 \) and \( \delta(p) = \beta(p) \) or \( \beta(p) = \gamma(p) \) or \( \alpha(p) = \beta(p) \);

- a type (b) group is split if and only if the following two conditions hold: (i) \( l = m \), (ii) for every \( p \in \varpi(H_2) \) either \( \text{ord}_\zeta \theta = 1 \) and \( \delta(p) = \beta(p) \) or \( \beta(p) = \gamma(p) \) or \( \alpha(p) = \beta(p) \).
a type (c) group is split if and only if the following two conditions hold: (i) $k = 1$ or $\eta = 1$, (ii) for every $p \in \varpi(H_{2'})$ either $\text{ord}_\zeta \theta = 1$ and $\delta_{(p)} = \beta_{(p)}$ or $\beta_{(p)} = \gamma_{(p)}$ or $\alpha_{(p)} = \beta_{(p)}$;

a type (d) group is split if and only if the following two conditions hold: (i) either $\eta = 1$ and $l = n$ or $k = l$ or $l = m$, (ii) for every $p \in \varpi(H_{2'})$ either $\text{ord}_\zeta \theta = 1$ and $\delta_{(p)} = \beta_{(p)}$ or $\beta_{(p)} = \gamma_{(p)}$ or $\alpha_{(p)} = \beta_{(p)}$;

a type (e) group is split if and only if the following two conditions hold: (i) $l = m$, (ii) for every $p \in \varpi(H_{2'})$ either $\text{ord}_\zeta \theta = 1$ and $\delta_{(p)} = \beta_{(p)}$ or $\beta_{(p)} = \gamma_{(p)}$ or $\alpha_{(p)} = \beta_{(p)}$.

Proof. Suppose $G$ has split factorisation $SK$. Then the subgroup $H$ in the corresponding Hall-decomposition $HN$ has a split factorisation $XY$ such that $Y \leq \mathcal{O}_\pi(H)(G)$. Conversely, suppose that $H = XY$ is a split factorisation of $H$ such that $Y \leq \mathcal{O}_\pi(H)(G)$. Then clearly $X \leq N_H(K \cap N)$, $Y \leq C_H(N)$ and by Lemma 5.6 in [20], $S \cap N \leq C_N(H)$. By Lemma 5.1 in [20], $(XU)(YV)$ is a metacyclic factorisation of $G$, and clearly this is split. It follows that $G$ is split if and only if $H$ has a split factorisation $XY$ with $Y \leq \mathcal{O}_\pi(H)(G)$, and this is the case if and only if $H_p$ has a split factorisation $\langle a \rangle \langle b \rangle$ with $\langle b \rangle \leq \mathcal{O}_p(G)$ for all $p \in \varpi(H)$.

Suppose $p \in \varpi(H_{2'})$. By the proof of Theorem 5.3 and Lemma 2.4,

$$H_p \cong \langle x_p, y_p \mid x_p^{\alpha_{(p)}} = y_p^{\beta_{(p)}}, y_p^{\gamma_{(p)}} = 1, y_p^{x_p} = y_p^{1+\delta_{(p)}} \rangle$$

where $\langle x_p \rangle \langle y_p \rangle$ is $\mathcal{O}_p(G)$-standard, $\alpha_{(p)} \geq \beta_{(p)}$ and $\beta_{(p)} < \delta_{(p)}$ implies

$$\alpha_{(p)} / \kappa_{(p)} < \beta_{(p)}.$$
If $\beta(p) = \gamma(p)$, then $\langle x_p, y_p \rangle$ is a split factorisation with $\langle y_p \rangle \leq \Omega_p(G)$. If $\alpha(p) = \beta(p)$, then $\langle x_p, y_p^{-1} \rangle$ is a split factorisation and $\langle y_p \rangle \leq \Omega_p(G)$. If $\text{ord}_\zeta \theta = 1$ and $\delta(p) = \beta(p)$ then $\langle x_p^{\alpha(p)/\beta(p)} y_p \rangle \langle x_p \rangle$ is a split factorisation and $\langle x_p \rangle \leq \Omega_p(G)$. Conversely suppose that $\alpha(p) \neq \beta(p)$, $\beta(p) \neq \gamma(p)$ and $\langle a \rangle \langle b \rangle$ is a split factorisation with $\langle b \rangle \leq \Omega_p(G)$. Then $\max\{|a|, |b|\} = \exp H_p = \alpha(p) \gamma(p)/\beta(p)$. If $|a| = \exp H_p$ then $|b| = |H_p|/\exp H_p = \beta(p)$, but $\langle y_p \rangle$ is a kernel of $H_p$ of minimal order $\gamma(p) > \beta(p)$ in $\Omega_p(G)$. Thus $|b| = \alpha(p) \gamma(p)/\beta(p)$ and so $b = x_p^r y_p^s$ for some integers $r$ and $s$ such that $p \nmid r$. Therefore $\Omega_p(G) \geq \langle x_p, y_p \rangle = H_p$, and so $\text{ord}_\zeta \theta = 1$, and $\delta(p) = \beta(p)$ since $\langle b \rangle = \langle x_p^r y_p^s \rangle \geq y_p^{\delta(p)}$. It follows that $H_p$ has a split factorisation $\langle a \rangle \langle b \rangle$ with $\langle b \rangle \leq \Omega_p(G)$ if and only if $\beta(p) = \gamma(p)$, $\alpha(p) = \beta(p)$, or $\text{ord}_\zeta \theta = 1$ and $\delta(p) = \beta(p)$.

If $G$ is of type (a), then $H_2$ has a presentation of the form

$$H_2 = \langle a', b' \mid a'^2 = b'^2, b'^{2m} = 1, b'^{a'} = b' \rangle$$

where $k, l$ and $m$ are natural numbers with $k \geq l \leq m$ and $l \leq 1$, and $\langle b' \rangle$ is a kernel of $H_2$ of minimal order in $\Omega_2(G)$. If $k = l$ or $l = m$, then $H_2$ clearly has a split factorisation $\langle a \rangle \langle b \rangle$ with $\langle b \rangle \leq \Omega_2(G)$. Also if $\eta = 1$, then $\langle a'^{2k-1} b'^{-1} \rangle \langle a' \rangle$ is such a factorisation. Conversely, suppose $k \neq l$, $l \neq m$ and $H_2$ has a split factorisation $\langle a \rangle \langle b \rangle$ with $\langle b \rangle \leq \Omega_2(G)$. Then a similar argument to that used above shows that $\eta = 1$. Thus $H_2$ has a split factorisation $\langle a \rangle \langle b \rangle$ with $\langle b \rangle \leq \Omega_2(G)$ if and only if $k = l$, $l = m$, or $\eta = 1$.

If $G$ is of type (b), then $H_2$ has a presentation of the form

$$H_2 = \langle a', b' \mid a'^2 = b'^{2st+1}, b'^{2st+u+1} = 1, b'^{a'} = b'^{-1+2st+u+1} \rangle$$

for some natural numbers $s, t$ and $u$ such that $u \leq 1, t \leq 1, tu = 0$ and $s + u \neq 0$. 

5. Finite metacyclic groups

If $\beta(p) = \gamma(p)$, then $\langle x_p, y_p \rangle$ is a split factorisation with $\langle y_p \rangle \leq \Omega_p(G)$. If $\alpha(p) = \beta(p)$, then $\langle x_p, y_p^{-1} \rangle$ is a split factorisation and $\langle y_p \rangle \leq \Omega_p(G)$. If $\text{ord}_\zeta \theta = 1$ and $\delta(p) = \beta(p)$ then $\langle x_p^{\alpha(p)/\beta(p)} y_p \rangle \langle x_p \rangle$ is a split factorisation and $\langle x_p \rangle \leq \Omega_p(G)$. Conversely suppose that $\alpha(p) \neq \beta(p)$, $\beta(p) \neq \gamma(p)$ and $\langle a \rangle \langle b \rangle$ is a split factorisation with $\langle b \rangle \leq \Omega_p(G)$. Then $\max\{|a|, |b|\} = \exp H_p = \alpha(p) \gamma(p)/\beta(p)$. If $|a| = \exp H_p$ then $|b| = |H_p|/\exp H_p = \beta(p)$, but $\langle y_p \rangle$ is a kernel of $H_p$ of minimal order $\gamma(p) > \beta(p)$ in $\Omega_p(G)$. Thus $|b| = \alpha(p) \gamma(p)/\beta(p)$ and so $b = x_p^r y_p^s$ for some integers $r$ and $s$ such that $p \nmid r$. Therefore $\Omega_p(G) \geq \langle x_p, y_p \rangle = H_p$, and so $\text{ord}_\zeta \theta = 1$, and $\delta(p) = \beta(p)$ since $\langle b \rangle = \langle x_p^r y_p^s \rangle \geq y_p^{\delta(p)}$. It follows that $H_p$ has a split factorisation $\langle a \rangle \langle b \rangle$ with $\langle b \rangle \leq \Omega_p(G)$ if and only if $\beta(p) = \gamma(p)$, $\alpha(p) = \beta(p)$, or $\text{ord}_\zeta \theta = 1$ and $\delta(p) = \beta(p)$.

If $G$ is of type (a), then $H_2$ has a presentation of the form

$$H_2 = \langle a', b' \mid a'^2 = b'^2, b'^{2m} = 1, b'^{a'} = b' \rangle$$

where $k, l$ and $m$ are natural numbers with $k \geq l \leq m$ and $l \leq 1$, and $\langle b' \rangle$ is a kernel of $H_2$ of minimal order in $\Omega_2(G)$. If $k = l$ or $l = m$, then $H_2$ clearly has a split factorisation $\langle a \rangle \langle b \rangle$ with $\langle b \rangle \leq \Omega_2(G)$. Also if $\eta = 1$, then $\langle a'^{2k-1} b'^{-1} \rangle \langle a' \rangle$ is such a factorisation. Conversely, suppose $k \neq l$, $l \neq m$ and $H_2$ has a split factorisation $\langle a \rangle \langle b \rangle$ with $\langle b \rangle \leq \Omega_2(G)$. Then a similar argument to that used above shows that $\eta = 1$. Thus $H_2$ has a split factorisation $\langle a \rangle \langle b \rangle$ with $\langle b \rangle \leq \Omega_2(G)$ if and only if $k = l$, $l = m$, or $\eta = 1$.

If $G$ is of type (b), then $H_2$ has a presentation of the form

$$H_2 = \langle a', b' \mid a'^2 = b'^{2st+1}, b'^{2st+u+1} = 1, b'^{a'} = b'^{-1+2st+u+1} \rangle$$

for some natural numbers $s, t$ and $u$ such that $u \leq 1, t \leq 1, tu = 0$ and $s + u \neq 0$. 

5. Finite metacyclic groups
and \( \langle b' \rangle \) a kernel of \( H_2 \) of minimal order in \( O_2(G) \). Then \( \langle b' \rangle \) is the only kernel of \( H_2 \). Moreover, \( H_2 \) has a split factorisation \( \langle a \rangle \langle b \rangle \) with \( \langle b \rangle \leq O_2(G) \) if and only if \( u = 0 \); for then it is dihedral or semidihedral, and when \( u = 1 \) it is generalised quaternion and therefore not split.

If \( G \) is of type (c), then \( H_2 \) has a presentation of the form

\[
H_2 = \langle a', b' \mid a'^{2k} = b'^2, b'^{2m} = 1, b'^{a'} = b'^n \rangle
\]

with \( k + m \geq 4, k \geq 1, m \geq 2, n = 1 + 2^{m-1} \) and \( m = 2 \) when \( 2^{k-1} \geq \text{ord} \eta \). Then \( \langle b' \rangle \) is a kernel of \( H_2 \) of minimal order in \( O_2(G) \). If \( k = 1 \), then \( m \geq 3 \) and \( \langle a'b'^{-1}b'^{2m-2} \rangle \) \( \langle b' \rangle \) is a split factorisation with \( \langle b' \rangle \leq O_2(G) \). If \( \eta = 1 \) and \( k \neq 1 \), then \( \langle a'^{2k-1}b \rangle \langle a' \rangle \) is a split factorisation with \( \langle a' \rangle \leq O_2(G) \). Conversely suppose that \( k \neq 1 \) and \( \langle a \rangle \langle b \rangle \) is a split factorisation of \( H_2 \) with \( \langle b \rangle \leq O_2(G) \). Then \( \langle b \rangle \geq H'_2 = \langle b'^{2m-1} \rangle \) and so \( |b| = \exp H_2 = 2^{k+1} \). Therefore \( \langle b \rangle = \langle a'b^s \rangle \) for some integer \( s \), and so \( O_2(G) \geq \langle a', b' \rangle = H_2 \) and \( \eta = 1 \). It follows that \( H_2 \) has a split factorisation \( \langle a \rangle \langle b \rangle \) with \( \langle b \rangle \leq O_2(G) \) if and only if \( k = 1 \) or \( \eta = 1 \).

If \( G \) is of type (d), then \( H_2 \) has a presentation of the form

\[
H_2 = \langle a', b' \mid a'^{2k} = b'^{2l}, b'^{2m} = 1, b'^{a'} = b'^{1+2n} \rangle
\]

where \( k, l, m \) and \( n \) are natural numbers with \( k \geq l \geq 2, l \leq m \) and \( n \geq m - l \), and \( \langle b' \rangle \) is a kernel of \( H_2 \) of minimal order in \( O_2(G) \). A similar argument to that used for the case \( p \in \omega(H_2') \) above shows that \( H_2 \) has a split factorisation \( \langle a \rangle \langle b \rangle \) with \( \langle b \rangle \leq O_2(G) \) if and only if \( k = l, l = m, \) or \( \eta = 1 \) and \( l = n \).

If \( G \) is of type (e), then \( H_2 \) has a presentation of the form

\[
H_2 = \langle a', b' \mid a'^{2r+u} = b'^{2r+v+u}, b'^{2r+v+u+w+u} = 1, b'^{a'} = b'^{-1+2r+v} \rangle
\]
where $r, s, t, u, v$ and $w$ are natural numbers with $r \geq 2$, $v \leq r$, $w \leq 1$, $su = tu = tv = 0$, and $w = 0$ when $v \geq r - 1$, and $\langle b' \rangle$ a kernel of $H_2$ of minimal order in $O_2(G)$. Moreover, it has a split factorisation $\langle a \rangle \langle b \rangle$ with $\langle b \rangle \leq O_2(G)$ if and only if $w = 0$, that is $l = m$. The theorem now follows. □
Chapter 6

The GAP program

The program below written in the GAP programming language computes the canonical presentation afforded in Theorem 5.3 of the group

\[(6.1) \quad \langle x, y \mid x^{1080} = y^{21960}, y^{26352} = 1, y^x = y^{22771} \rangle.\]

The canonical presentation of an arbitrary finite metacyclic group can be computed by twigging the first four lines accordingly. This program is available at the following URL:


\[
k := 8*27*5; \quad \# k := 1080
\]

\[
l := 5*8*9*61; \quad \# l := 21960
\]

\[
m := 16*27*61; \quad \# m := 26352
\]

\[
n := \text{ChineseRem}([16, 27, 61], [3, 10, 40*34]); \quad \# n := 22771
\]
6. The GAP program

```gap
60

g := FreeGroup(2);

\text{g} := g/[g.1^k/g.2^l,g.2^l/g.1^k,g.2^n,g.2^m];

\text{g} := \text{AgGroupFpGroup}(\text{g});

\text{g} := \text{RefinedAgSeries}(\text{g});

m := \text{Gcd}(l*(n-1),n^k-l,m);

n := \text{RemInt}(n,m);

a := g.1;

lk := \text{FactorsInt}(k);

b := g.\text{generators}[\text{Length}(lk)+1]^(1/\text{Gcd}(l,m));

1 := \text{Gcd}(l,m);

ox := k*m/l;

ls := \text{FactorsInt}(ox);

ll := \text{FactorsInt}(l);

lm := \text{FactorsInt}(m);

PR := \text{function}(n) \# \text{return list of positive integers prime}
\# to positive n.

\text{if n=1 then}

    return [];

\text{else}

    return \text{PrimeResidues}(n);

\text{fi};

end;;
```
6. The GAP program

ppsi:=function(n,p) #returns $n_{\{p\}}$ for positive $n$
return Product(Filtered(FactorsInt(n),r->r=p));
end;

p:=0;; np1:=0;; mp:=0;; xp:=0;; yp:=0;; np:=0;; th:=0;; oxpp:=0;; z:=0;;
standardise:=function() #if yp^xp=yp^np1 with
#np1=\pml+delta*np, then xp, yp, np1 and th will change
#so that xp and yp still generate the same group but np1=\pml+np.
local delta,deltap;
if p=2 and npl mod 4=3 then
np:=ppsi(np1+1,p);
delta:=(np1+1)/np;
deltap:=(np1+1)/np;
deltap:=delta^((OrderMod(delta,mp)-1));
np1:=np-1;
elif np1<>1 then
np:=ppsi(np1-1,p);
delta:=(np1-1)/np;
deltap:=(np1-1)/np;
deltap:=delta^((OrderMod(delta,mp)-1) mod mp);
np1:=np+1;
fi;
if np1<>1 then
xp:=xp^deltap;
yp:=yp^deltap;
th := th*n^(oxpp*(deltap-1)) mod z;
fi;
end;

inhpps := function(p) # returns true iff g has a normal Hall p'-subgroup.
    return n^(ppsi(ox,p)) mod ppsi(m,p) = 1;
end;

ei := function(u) # expresses agword u as list [i,j] where u = a^i*b^j.
    local ua, ub, lnk, lnm, eu, n;
    ua := 0;
    ub := 0;
    lnk := Length(lk);
    lnm := Length(lm);
    eu := ExponentsAgWord(u);
    for n in [1..lnk] do
        ua := ua*lk[lnk-n+1]+eu[lnk-n+1];
        od;
    for n in [1..lnm] do
        ub := ub*lm[lnm-n+1]+eu[lnk+lnm-n+1];
        od;
    return [ua, ub];
end;
lspi := Filtered(ls, r -> inhpps(r));
6. The GAP program

\[ \text{spi} := \text{Product}(\text{lspi});; \]
\[ \text{lmpi} := \text{Filtered}(\text{lm}, r \rightarrow \text{inhpps}(r));; \]
\[ \text{z} := \text{Product}(\text{Filtered}(\text{lm}, r \rightarrow \text{not } r \text{ in lmpi}));; \]
\[ \text{e} := \text{Product}(\text{Filtered}(\text{ls}, r \rightarrow \text{not } r \text{ in lspi}));; \]
\[ \text{pi} := \text{Set}(\text{Concatenation}(\text{lspi}, \text{lmpi}));; \]
\[ \text{th} := \text{Product}(\text{List}(\text{pi}, p \rightarrow n^{(\text{ox/ppsi(ox,p)})}) \text{ mod } z);; \]
\[ \text{ka} := n^{\text{spi}} \text{ mod } z;; \]
\[ \text{xi} := \text{OrderMod}(\text{th}, \text{z});; \]
\[ \text{u} := a^{(\text{Product}(\text{lspi}));; \]
\[ \text{v} := b^{(\text{Product}(\text{lmpi}));; \]
\[ \text{p} := 0;; \]
\[ \text{lxp} := \[];; \]
\[ \text{lyp} := \[];; \]
\[ \text{lkp} := \[];; \]
\[ \text{llp} := \[];; \]
\[ \text{lmp} := \[];; \]
\[ \text{lmp1} := \[];; \]
\[ \text{lxip} := \[];; \]
\[ \text{lambda} := 0;; \]
\[ \text{sjxp} := 0;; \]
\[ \text{xip} := 0;; \]
\[ \text{sjx} := \text{PR(xi});; \]
for p in pi do
   oxpp:=ox/psii(ox,p);
   xp:=a^oxpp;
   mp:=psii(m,p);
   yp:=b^(m/mp);
   kp:=psii(k,p);
   lp:=psii(l,p);
   lmpimp:=Product(Filtered(lmpi,r->not r=p));
   np1:=n^oxpp mod mp;
   xip:=psii(xi,p);
   sjxp:=PR(xip);
   standardise();
   if p=2 and (kp<=p or lp<=p) then
      if np1=1 then
         if lp>kp then
            xp:=xp*yp;
            lp:=kp;
            yp:=yp^(1+lp/kp);
         fi;
         if kp/xip>=lp then
            yp:=xp^(-kp/lp)*yp;
            kp:=kp*mp/lp;
         fi;
      fi;
   fi;
end;

6. The GAP program
mp:=lp;
fi;
else
if kp>lp and kp>xip and np>lp then
    yp:=xp^(kp/p)*yp;
    kp:=kp*mp/lp/p;
    mp:=4;
    np1:=mp-1;
elif np1=mp/p-1 and lp<>mp then
    xp:=xp*yp;
    lp:=mp;
elif np1=mp/p+1 and lp<>mp and mp>=8 then
    xp:=xp*yp^(lp/p*(mp/4-1));
    lp:=mp;
fi;
fi;
elif p=2 and np1 mod 4=3 then
    if lp<>mp then
        if mp=np then
            yp:=xp^(kp/p)*yp;
            np:=mp/p;
            np1:=np-1;
        else
            if kp>lp and kp>xip and np>lp then
                yp:=xp^(kp/p)*yp;
                kp:=kp*mp/lp/p;
                mp:=4;
                np1:=mp-1;
            endif;
        endif;
    endif;
endif;
fi;
if np<mp and kp*np=mp then
    xp:=xp*yp;
    lp:=mp;
fi;
if np<mp/p then
    if xip<kp and mp in DivisorsInt(kp*np/p+lp) then
        lambda:=mp/np;
    else
        lambda:=mp/np/p;
    fi;
    if lambda<>1 then
        sjxp:=Filtered(sjxp,r->r mod lambda=1);
    fi;
fi;
else
    if lp>kp then
        xp:=xp*yp;
        yp:=yp^(1+lp/kp);
        lp:=kp;
    fi;
6. The GAP program

if kp>=xip*lp and np>lp then
    yp:=xp^(-kp/lp)*yp;
    kp:=kp*np/lp;
    mp:=mp*lp/np;
    np1:=lp+1;
fi;

lambda:=Minimum(Maximum(lp/kp*xip,lp/np),mp/np,xip);

if lambda<>1 then
    sjxp:=Filtered(sjxp,r->r mod lambda=1);
fi;
fi;

Add(lxp,xp);
Add(lyp,yp);
Add(lkp,kp);
Add(llp,lp);
Add(imp,mp);
Add(lnpl,npl);
Add(lxip,xip);

if xip<>1 then
    sjx:=Filtered(sjx,t->t mod xip in sjxp);
fi;

od;
ltt:=List(sjx,t->th^t mod z);;
if ltt<>[] then
    th:=Minimum(ltt);
    t:=sjx[Position(ltt,th)];
    for p in pi do
        pp:=Position(pi,p);
        tp:=t mod lxip[pp];
        if tp=0 then
            tp:=1;
        fi;
        tmp:=lxp[pp];
        lxp[pp]:=lxp[pp]^tp;
        if p=2 and (lkp[pp]<p or llp[pp]<p) then
            lyp[pp]:=lyp[pp]^tp;
        elif p=2 and lnpl[pp] mod 4=3 then
            pmmn:=lmp[pp]/(lnpl[pp]+1);
            if pmmn<>1 and tp mod pmmn<>1 then
                lyp[pp]:=(tmp^Int(lkp[pp]/p))*lyp[pp];
            fi;
        else
            pmmn:=lmp[pp]/(lnpl[pp]-1);
            if pmmn<>1 and tp mod pmmn<>1 then
                lyp[pp]:=(tmp^Int(lkp[pp]/p))*lyp[pp];
            fi;
        fi;
    fi;
fi;
if \( l1p[pp] \geq lnp1[pp] - 1 \) then

if \( p=2 \) and \( l1p[pp] \times (lnp1[pp] - 1) = lmp[pp] \) then

\[
t := 1 + 2^\lambda (lnp1[pp] - 1) + 2^\lambda (lkp[pp] - l1p[pp] + lnp1[pp] - 1);
\]

\[
lyp[pp] := tmp^\lambda \int \left( (tp-1) \times lkp[pp] / l1p[pp] \times t^\lambda \mod(t, p^\lambda (k+m-n)-1) \right) \times lyp[pp];
\]

else

\[
lyp[pp] := tmp^\lambda \int \left( (tp-1) \times lkp[pp] / l1p[pp] \right) \times lyp[pp];
\]

fi;

else

\[
lyp[pp] := tmp^\lambda (tp-1) \times lyp[pp];
\]

fi;

fi;

fi;

od;

fi;

kpi := Product(lkp);

lpi := Product(l1p);

le := List(PR(e), s -> ka \times s \mod z);

if le<>[] then

ka := Minimum(le);

t := PR(e)[Position(le, ka)];

else
6. The GAP program

\begin{verbatim}
t:=1;
fi;
u:=u^t;
Add(1xp,u);
x:=Product(1xp);
lkpp:=List(lkp,t->(kpi/t));;
llpp:=List(lip,t->(lpi/t));;
pwyp:=function(t) #returns power of element of lyp used to
  #calculate y.
    local pt;
    pt:=Position(lyp,t);
    return t^(lkpp[pt]*e*
      (llpp[pt]^(OrderMod(llpp[pt],lmp[pt])-1)mod lmp[pt]))*
      z^(OrderMod(z,lmp[pt])-1)mod lmp[pt]);
end;;
y:=Product(List(lyp,pwyp))*v^(kpi*lpi^(OrderMod(lpi,z)-1));
Add(lmp,z);
Add(lnp1,th*ka mod z);
ei(x);
ei(y);
k:=kpi*e;
l:=lpi*z;
\end{verbatim}
\textbf{6. The GAP program}

\begin{verbatim}
m:=Product(lmp);
n:=ChineseRem(lmp,lnp1);

The output from redirecting standard input to GAP from a file containing the above
would look similar to the following:

gap> gap> gap> gap> gap> gap> gap> gap>
gap> #W  AgGroupFpGroup: composite index, use 'RefinedAgSeries'
gap> gap> gap> gap> gap> gap> gap> gap> gap> gap> gap> gap> gap> gap>
gap> [ 1039, 0 ]
gap> [ 540, 22889 ]
gap> 1080
gap> 4392
gap> 26352
gap> 5923
\end{verbatim}
The last six lines show that with \( x = a^{1039} \) and \( y = a^{540}b^{22889} \), the canonical presentation of the group given by (6.1) is

\[
\langle x, y \mid x^{1080} = y^{4392}, y^{26352} = 1, y^x = y^{5923} \rangle.
\]
Chapter 7

Infinite metacyclic groups

In this chapter, we classify infinite metacyclic groups. This is much simpler than the classification of their finite counterparts.

Recall that if \( m \) is a positive integer, then \( J(m) \) denotes the group of reduced residues modulo \( m \), and that \( n^{-1} \) is the inverse of \( n \) modulo \( m \).

**Theorem 7.1.** A group is infinite and metacyclic if and only if it has one of the following presentations:

(i) \( \langle x, y \mid y^x = y^n \rangle \) with \( n = \pm 1 \).

(ii) \( \langle x, y \mid y^m = 1, y^x = y^n \rangle \) with \( m \) a positive integer and \( n \in J(m) \) and \( n \leq n_m^{-1} \).

(iii) \( \langle x, y \mid x^{2k} = 1, y^x = y^{-1} \rangle \) with \( k \) a positive integer.

Groups of different types or of the same type but with different parameters are not isomorphic.

**Proof.** Surely these presentations give infinite metacyclic groups so let \( \langle x \rangle \langle y \rangle \) be a
metacyclic factorisation of an infinite group $G$ while we prove the necessity of the first statement.

Suppose that both $[G : \langle y \rangle]$ and $\langle y \rangle$ are infinite. Then $\langle x \rangle \cap \langle y \rangle = 1$ and $y^n = x$, with $n = \pm 1$ since $y^n$ must generate $\langle y \rangle$. It follows that $G$ has a presentation of the first type, realised by a semidirect product of two infinite cyclic groups.

Next suppose that $[G : \langle y \rangle]$ is infinite and that $\langle y \rangle$ is finite, of order $m$, say. Then $y^n = x$, for some $n \in J(m)$. With $x = x^{-1}$, we see that $G$ also has a presentation $\langle \bar{x}, y \mid y = y^n \rangle$, and so we may assume that $n \leq n^{-1}$. Thus $G$ has a presentation of the second type.

Next suppose that $[G : \langle y \rangle]$ is finite of order $k$, say. Then $\langle y \rangle$ is infinite, and so $y^n = x$ with $n = \pm 1$. If $n = 1$, then $G$ has a presentation of the second type with $n = 1$, so suppose that $n = -1$. Now for some integer $l$, $x^k = y^l \in \zeta$. If $k$ is odd, then $y = y^{-1} = y^{-1} = y^{-1}$, a contradiction. Thus $k = 2k$ for some positive integer $k$. We have $y^{2l} = y^l y^l = y^l y^l = y^{-1} y^l = 1$, and so $l = 0$, since $\langle y \rangle$ is infinite. It follows that $G$ has a presentation of the third type. The first statement now follows.

A group of the first type is abelian if and only if $n = 1$, and so $n$ is an invariant of such a group. Such a group is noncyclic and torsion free, a feature which distinguishes it from the other types. A group of the second type has precisely $m$ torsion elements, and so $m$ is an invariant. Suppose that $G$ also has a presentation $\langle x, y \mid y = y^n \rangle$ with $n \in J(m)$. Then there is an automorphism $\alpha$ of $G$ such that $(y \alpha)^{\pi} = (y \alpha)^n$. We must have $y \alpha = y^r$ for some integer $r$ and $x \alpha = x^r y^s$
with \( \varepsilon = \pm 1 \) and \( s \) an integer. Then

\[
y^\varepsilon n = (y^\alpha)^n = (y^\alpha)^{x^s} = y^{\varepsilon x^s}.
\]

Therefore \( y^n = y^{\varepsilon^s} \), showing that \( \bar{n} = n \) or \( n^{-1} \). It follows that \( n \) is an invariant for type (ii) groups. A type (iii) group has infinitely many torsion elements (of the form \( xy^t \) for \( t \in \mathbb{Z} \)), a feature which distinguishes it from type (ii) groups. In type (iii) groups we also have \( k \) as an invariant, since \( |\zeta G| = |x^2| = k \). This proves the second statement. \( \square \)
Bibliography


