Automorphism Groups of Metacyclic p-Groups

Idham Arif Alias

July 2008

A thesis submitted for the degree of Doctor of Philosophy
of the Australian National University

For my mother Fatimah Mohamed and my late father Alias Khalid. Also for Abang Mi, Kak Arni, Abang Pi, Hisyam, Irma and Afzan

Declaration

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

Idham Arif Alias

Acknowledgements

No words can describe how much I want to thank my supervisors Dr Elizabeth Ormerod and Dr John Cossey, for all their valuable guidance, support and kindness throughout my study here. My understanding and appreciation of the subject are entirely due to their influence; I will always remember and value the relationship with them.

I would also like to thank my advisor Dr Bob Bryce for his general advice, and Professor Mike Newman for his general help.

Thanks to all fellow mathematics students for their friendship and tolerance especially Kevin, Liu, Andrew, Bob, Sumaira and Khoo.

My special thanks to everyone in Mathematical Sciences Institute (MSI) for helping me and providing a friendly environment especially Nick, Matthew, Kelly, Michael and Katie. Not to forget Don, thank you for everything. Also Geoff who has been a great help and to everybody in the Australian National University (ANU) who gives me assistance and guidance.

I would like to acknowledge Malaysian Government and Universiti Putra Malaysia for all the financial support, and my referees, Prof Kamel, Dr Habshah and Dr Mat Rofa who supported my application to ANU.

My studies here have been made enjoyable with the company of all my Malaysian and non-Malaysian friends here, especially Normi, Mosfi, Ifah, Kak Ana, Abang Zabri and family, Siti, Khairil, Nadim, Su, Agus and Mona.

To my brothers and sisters, thank you for all the assistance and support. Also many thanks to all my relatives especially Ayah Teh Da, Mak Teh and family.

I like to dedicate this work to my late father Alias who passed away in the midst of my study here. I miss you a lot father and thank you for all your guidance, teaching and love. May you be in peace.

Finally to my mother Fatimah, thank you for your prayer, love and everything you do for me. Without you, I would be lost and you are always my inspiration.

Acknowledgements

No words can describe how much I want to thank my supervisors Dr Elizabeth Ormerod and Dr John Cossey, for all their valuable guidance, support and kindness throughout my study here. My understanding and appreciation of the subject are entirely due to their influence; I will always remember and value the relationship with them.

I would also like to thank my advisor Dr Bob Bryce for his general advice, and Professor Mike Newman for his general help.

Thanks to all fellow mathematics students for their friendship and tolerance especially Kevin, Liu, Andrew, Bob, Sumaira and Kiloo.

My special thanks to everyone in Mathematical Sciences Institute (MSI) for helping me and providing a friendly environment especially Nick, Matthew, Kelly, Michael and Katie. Not to forget Dan, thank you for everything. Also Geoff who has been a great help and to everybody in the Australian National University (ANU) who gives me assistance and guidance.

I would like to acknowledge Malaysian Government and Universiti Putra Malaysia for all the financial support, and my referees, Prof Kamel, Dr Rehshah and Dr Mat Rofa who supported my application to ANU.

My studies here have been made enjoyable with the company of all my Malaysian and non-Malaysian friends here, especially Norma, Mooi, Teh, Kak Ana, Abang Zakri and family, Siti, Khairil, Nadira, Su, Agus and Mona.

To my brothers and sisters, thank you for all the assistance and support. Also many thanks to all my relatives especially Ayah Teh Dr. Mak Teh and family.

I like to dedicate this work to my late father Abas who passed away in the midst of my study here. I miss you a lot father and thanks you for all your guidance, teaching and love. May you be in peace.

Finally to my mother Fatimah, thank you for your prayer, love and everything you do for me. Without you, I would be lost and you are always my inspiration.

Abstract

A metacyclic group G is a group which possess a cyclic normal subgroup N such that G/N is also a cyclic group. In this thesis, the automorphism group $Aut(P)$ of finite nonsplit metacyclic p-groups P where p is an odd prime, is investigated. Menegazzo has shown in this case that $Aut(P)$ is a p-group. The investigation is divided into four cases but only two cases are considered by this thesis.

In these cases it is shown that $Aut(P)$ can be written as a product of subgroups. Elements of $Aut(P)$ can also be written in normal form in terms of generators of $Aut(P)$. In addition, the centre, the upper central series and hence the class of $Aut(P)$ are determined.

Contents

Notation

In the following

- p is a fixed odd prime number;
- P is the finite nonsplit metacylic p-group with the presentation (2.1) (page 8);
- x and y are generators of P (page 8);
- a, b, d and h are generators of the automorphism group of P (page 29)

In the following list of notation, we provide notation specifically used in this thesis with the page they first appear. Other notation is standard and based on the notation in Robinson [18].

Notation

$\phi(G)$	the Frattini subgroup of G (page 1)
$exp(G)$	the exponent of the group G (page 2)
$\zeta(G)$	the centre of G (page 2)
$Aut(P)$	the automorphism group of P (page 3)
α	$1 + p^n$ (page 9)
$\Lambda(u, v)$	$1 + \alpha^u + \alpha^{2u} + \ldots + \alpha^{(v-1)u}$ (page 10)
U	$1 + p^{q-n}$ (page 11)
$p^k \parallel c$	$p^k \mid c$ but $p^{k+1} \nmid c$ (page 12)
$ord(g)$	the order of an element g in G (page 31)
Q	$Aut(P)/\langle h \rangle$ (page 34)

$\bar{g}$	$g\langle h\rangle$ (page 34)
$[x_1, x_2, ..., x_n]$	$[[x_1, x_2, ...x_{n-1}], x_n]$ (page 39)
$[a, ib]$	$[a, \underbrace{b, b, ..., b}_{i\ times}]$ (page 39)
$\zeta_k(G)$	the k^{th} centre of G (page 67)

Chapter 1

Introduction

This thesis will be concerned with the structure of the automorphism group of a finite metacyclic p-group for odd primes p. We begin with some history and introductory notes about metacyclic groups, the automorphism group of a metacyclic group and summary of main results in this thesis. All groups in this thesis are finite.

1.1 Metacyclic groups

A metacyclic group G is a group which has a cyclic normal subgroup N such that G/N is also a cyclic group. Some examples of metacyclic groups are cyclic groups, direct products of two cyclic groups, dihedral groups and all finite groups whose Sylow subgroups are cyclic. Subgroups and quotients of metacyclic groups are also metacyclic.

Huppert [13] in 1953 studied a finite p-group G which is the permutable product of two finite cyclic groups. In the paper he gave some results regarding the structure of G, its Frattini subgroup $\phi(G)$, its centre and the quotient group $G/\phi(G)$.

In 1958 Blackburn [4] proved that if p is a prime, a p-group G is metacyclic if and only if $G/\phi(G')G_3$ is metacyclic, where G_3 is the third term of the lower central series of G. In addition, a p-group G is also metacyclic if it has at most $p+1$ subgroups of index p^2.

If G is a p-group for odd prime p, Blackburn [4] also showed that G is metacyclic if and only if $|G : G^p|$ is less than or equal to p^2. In addition, G is also metacyclic if G can be expressed as a product of two cyclic groups.

It is nice to know when two metacyclic groups are isomorphic. Let G_1 and G_2

be two metacyclic groups with cyclic normal subgroups N_1 and N_2 respectively. If $|N_1| = |N_2|$ and $|G_1/N_1| = |G_2/N_2|$, necessary and sufficient conditions for G_1 and G_2 to be isomorphic, were given by Basmaji [2] in 1969.

To classify metacyclic groups, we need to have presentations of the groups. Presentations of metacyclic p-groups where p is any prime were given by King [14] in 1973. However in the classification of metacyclic 2-groups in [14], Silberberg [20] pointed out an error in the King's result. In 1988, Newman and Xu [16] gave a presentation for describing nonisomorphic metacyclic p-groups, with the aid of an algorithm developed by them.

In later years, more properties of metacyclic p-groups were discovered. Ormerod [17] in 1990 for example, identified the Wielandt subgroup of a metacyclic p-group. In her paper, Ormerod gave a certain form of presentation of a metacyclic p-group for both odd prime p and when p is equal to 2, using mainly the work of Newman and Xu [16]. The relationship between the Wielandt length of the group and its nilpotency class, was then found.

In 1994, Sim [21] gave a presentation of every metacyclic group of odd order. His presentation was formed by choosing convenient generators of some specific cyclic subgroups of the metacyclic group. Hempel [12] took it even further in 2000 when he classified metacyclic groups. Building on the work of Sim [21], his work included the classification of metacyclic 2-groups.

1.2 Automorphisms of metacyclic groups

The automorphism group of a p-group was also a subject of interest, especially regarding its order. If G is a group of order p^m with a Frattini subgroup $\phi(G)$ of index p^r, Hall [11] in 1933 proved that the order of automorphism group of G divides $np^{(m-r)r}$ where n is the order of $GL(r,p)$.

It had been an interesting question whether the order of a p-group divides the order of its automorphism group. For an odd prime p-group G of class two that has no abelian direct factor, Adney and Yen [1] in 1965 gave some conditions for the solution of the question. Let A be the automorphism group of G, A_c its group of central automorphisms, $\zeta(G)$ its centre and G' its commutator subgroup. They proved that $|G|$ divides $|A|$ if one of the following holds: (1) $\zeta(G)$ is cyclic, (2) exp $\zeta(G) =$ exp G', (3) exp $\zeta(G) \geq$ exp G/G', (4) A_c is abelian. Furthermore, Faudree [10] in 1968 showed that the order of a nonabelian nilpotent p-group of class two divides the order of its automorphism group.

One of the earliest works on the automorphism group of a metacyclic p-group was done by Davitt. In his work in 1970, Davitt [9] showed that for a noncyclic metacyclic p-group of order strictly greater than p^2 (where p is an odd prime), the order of its automorphism group is divisible by the order of the group.

It is known that the automorphism group of a p-group is not necessarily a p-group. In 1990, Curran [6] investigated some p-groups whose automorphism group is again a p-group. He showed the existence of some 2-groups of order 2^n, which have the same order as their respective automorphism groups, where $n \geq 3$.

A metacyclic p-group is called split if it has a cyclic normal subgroup with a cyclic complement, and nonsplit otherwise. For examples, dihedral 2-groups are split metacyclic p-groups and the quaternion group is nonsplit. In 1993, Menegazzo [15] established the presentation and the order of automorphisms of p-groups with cyclic commutator subgroup, for odd primes p. In the paper he also included his establishment of the order of the automorphism groups of nonsplit and nonabelian split metacyclic p-groups.

In 2001, Schulte [19] proved that the automorphism of metacyclic p-groups with cyclic maximal subgroups for odd prime p, is a semidirect product of its unique Sylow p-subgroup and a cyclic group of order $p-1$. More recently in 2006, Bidwell and Curran [3] gave some results about the structure of the automorphism group of a split metacyclic p-group for odd prime p, citing some materials from Davitt's work [9] in the process. Curran [8] then extended the study to split metacyclic 2-groups in 2007.

In contrast to the split case, it turns out that in the nonsplit case the automorphism groups are p-groups. This year Curran [7] found generators of the automorphism group of nonsplit metacyclic p-groups where p is an odd prime, and wrote the automorphism group as a product of subgroups.

In this thesis, we study the automorphism group $Aut(P)$ of a finite nonsplit metacyclic p-group P, where p is an odd prime only. Our investigation will be based on a presentation by King [14]. There are a number of presentations available (among them [17] and [21]), but we will use a variation of the presentation given by King [14], as discussed in the first section of the next chapter.

The presentation involves several parameters where naturally we expect the structure of the automorphism group will depend on the relationship between these parameters. We have found it convenient to divide our investigation into four distinct cases, based upon the work of King [14]. However, our study of the automorphism group has been completed for the first two cases only. It turns out that the calculations involved in each case are mostly the same but in some parts of the thesis are different enough to require them to be done separately. We find that the structure of $Aut(P)$ in the first two cases is the same.

For the last two cases we expect the structure of $Aut(P)$ will be more complex. The calculations involved are probably similar, but seem to be substantially more complicated than the first two cases.

In his paper [7], Curran expressed $Aut(P)$ (in our notation) as a product of subgroups. He found generators of $Aut(P)$ and wrote the automorphism group as a product of a 3-generator subgroup and a cyclic subgroup. Although there are some similarities, we used a different approach to obtain our results. Using the algebra program MAGMA [5] to produce some examples so that we could formulate conjectures, we found generators of $Aut(P)$ and wrote $Aut(P)$ as a product of subgroups similar to Curran's. While the generators are similar, the main difference is that one of our generators is a central element of $Aut(P)$.

The calculations in this thesis also give more informations about the structure of $Aut(P)$ than [7]. The fact that one of our generators is a central element of $Aut(P)$ is crucial to our work in this thesis. Much of what we want to do involves calculations in $Aut(P)$ modulo the subgroup generated by our central generator. Another important feature of our result is that each element of $Aut(P)$ can be written in normal form in terms of our generators. With these, we are able to determine the centre, the upper central series and hence, the class of $Aut(P)$. We choose to construct upper central series instead of lower central series, as constructing the lower central series turns out to be much more difficult. We find that the formula for the class depends on parameters in the presentation we use.

To end this section, we note that we have used the algebra program MAGMA [5] extensively in conjunction with our calculations and investigation of the automorphism group and its properties. Besides using MAGMA [5] to find generators for $Aut(P)$, we also looked at examples to conjecture about the normal form of commutators of these generators and the class of the automorphism group.

1.3 Summary of main results

If P is a metacyclic p-group where p is an odd prime number, then P has a presentation of the form

$$P = \langle x, y | x^{p^m} = 1, y^{p^t} = x^{p^q}, yxy^{-1} = x^{1+p^n} \rangle$$

where the parameters m, t, q and n satisfy some conditions. Our results are based only on an odd prime p.

The order of automorphism group $Aut(P)$ of P is p^{2n+q+t}. This was proved by Menegazzo [15] (Theorem 3.0.2 in this thesis), but can also be proved by our method.

The four cases in the case of non-split metacyclic p-groups occur when:

1) $2 \leq n < q < m \leq t$ where $m \leq 2n$,

2) $1 \leq n < q < m \leq t$ where $2n < m \leq q+n$,

3) $3 \leq n < q < t < m \leq 2n$ and

4) $2 \leq n < q < t < m$ where $2n < m \leq q+n$.

However, this thesis concentrates on cases 1 and 2. From now on, all the results mentioned are only for cases 1 and 2.

Let x and y be generators of P satisfying the relation above. From the third relation in the presentation of P we observe that any element of P can be written uniquely in the form $x^u y^v$ where $0 \leq u < p^m$ and $0 \leq v < p^t$. Therefore we represent any automorphism φ of P in the form of a matrix notation, that is $\varphi \sim \begin{bmatrix} i & r \\ j & s \end{bmatrix}$. In Theorem 3.0.5 we find restrictions on i, j, r and s which make φ an automorphism of P.

We define automorphisms a, b, d and h of P as

$$a \sim \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, b \sim \begin{bmatrix} 1+p^{m-q} & 0 \\ 0 & 1 \end{bmatrix}, d \sim \begin{bmatrix} 1 & 0 \\ p^{t-n} & 1+p^{q-n} \end{bmatrix} \text{ and }$$
$$h \sim \begin{bmatrix} 1+p^{m-n} & 0 \\ 0 & 1+p^{m-n} \end{bmatrix}.$$

We show that these automorphisms are generators of $Aut(P)$ where h is central. In fact each element of $Aut(P)$ can be written in normal form in terms of these generators as shown by the following theorem.

Theorem 5.0.2. *If a, b, d and h are the automorphisms of P defined earlier then*

a) any element of $\langle b, a, h\rangle$ can be written in normal form as $b^\beta a^\eta h^\theta$ for $0 \leq \beta < p^q$, $0 \leq \eta < p^q$ and $0 \leq \theta < p^{t+n-q}$ where

i) *$\langle b\rangle \cap \langle a, h\rangle = 1$ and*

ii) *$\langle b, a, h\rangle = \langle b\rangle\langle a\rangle\langle h\rangle$.*

b) any element of $Aut(P)$ can be written in normal form as $d^\gamma b^\beta a^\eta h^\theta$ for $0 \leq \gamma < p^n$, $0 \leq \beta < p^q$, $0 \leq \eta < p^q$ and $0 \leq \theta < p^{t+n-q}$ where

i) $\langle d\rangle \cap \langle b,a,h\rangle = \langle d^{p^n}\rangle$ *and*
ii) $Aut(P) = \langle d\rangle\langle b,a,h\rangle$.

Many of our calculations are made easier by the following theorem.

Theorem 6.0.2 *If h is as defined earlier then $\zeta(Aut(P)) = \langle h\rangle$.*

For example we find the upper central series of $Aut(P)$ by calculating the upper central series of $Aut(P)/\langle h\rangle$ (Lemma 7.0.1). From the upper central series we determine the class. The result depends on the parameters in the presentation of P and is given by the following theorem.

Theorem 7.0.2 *Let $Aut(P)$ be as defined earlier.*

a) *If $m-q \geq q-n$ then the class of $Aut(P)$ is $\lceil \frac{q}{q-n}\rceil + 1$.*
b) *If $m-q < q-n$ then the class of $Aut(P)$ is $\lceil \frac{q}{m-q}\rceil + 1$.*

Chapter 2

Preliminaries

This chapter presents basic definitions and results that will be needed throughout this thesis. We start by discussing presentations of a metacyclic p-group P in section 1. Section 2 provides us with some properties of the powers and product of generators of P. Section 3 presents some other necessary results, especially important are results regarding expansions involving binomial coefficients.

The reader is referred to the list of notation on pages *xiii*$-$*xiv*. Other notation will be defined as it is introduced.

2.1 Presentations of metacyclic p-groups

Let G be a metacyclic group that contains a cyclic normal subgroup N such that G/N is cyclic. Hempel in his paper [12] called N a kernel of G. The following lemma which is part of Lemma 2.1 in [12], gives a presentation of G. It is written as it appeared in [12].

Lemma 2.1.1 *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*

$$\langle x, y | x^k = y^\ell, y^m = 1, y^x = y^n \rangle$$

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

If P is a metacyclic p-group with p an odd prime, the presentation of P can be written as

$$P = \langle x, y | x^{p^m} = 1, y^{p^n} = x^k, yxy^{-1} = x^r \rangle$$

with $m,\ n \geq 0,\ 0 < r,\ k \leq p^m,\ r^{p^n} \equiv 1\ (mod\ p^m)$ and $k(r-1) \equiv 0\ (mod\ p^m)$ [14]. To be more specific, if P is a metacyclic p-group where P is noncyclic and p is an odd prime, then P has a unique presentation of the form

$$P = \langle x, y | x^{p^m} = 1, y^{p^n} = x^{p^{m-s}}, yxy^{-1} = x^{1+p^{m-c}} \rangle$$

where s measures 'how split P can be' while c measures 'how commutative P can be' [14]. Furthermore, the presentation of a metacylic p-group where p is an odd prime is said to be uniquely reduced up to isomorphism if and only if $s = 0$ and $s \leq c < min\{n+1, m\}$ (which is the split case), or $s > 0$ and $max\{1, m-n+1\}$ $\leq s < min\{c, m-c+1\}$ (which is the nonsplit case). Distinct uniquely reduced presentations will give nonisomorphic metacyclic p-groups [14].

To suit our work , the presentation above has been rewritten as

$$P = \langle x, y | x^{p^m} = 1, y^{p^t} = x^{p^q}, yxy^{-1} = x^{1+p^n} \rangle. \tag{2.1}$$

Therefore for the nonsplit case we have

$$max\{1, m-t+1\} \leq m-q < min\{m-n, n+1\}.$$

This can be broken as the following:

(a) $m-t+1 \leq 1 \leq m-q < m-n < n+1$
(b) $m-t+1 \leq 1 \leq m-q < n+1 \leq m-n$
(c) $1 < m-t+1 \leq m-q < m-n < n+1$
(d) $1 < m-t+1 \leq m-q < n+1 \leq m-n.$

We take case (a) for example where the inequality shows that:

i) $m-t+1 \leq 1$ which implies $m \leq t$.
ii) $1 \leq m-q$ which implies $q < m$.
iii) $m-q < m-n$ which implies $n < q$.
iv) $m-n < n+1$ which implies $m \leq 2n$.

We also can see that $m-q < n+1$ which implies $m \leq q+n$, which is true in (b), (c) and (d) as well. Thus (a) can be rewritten as $2 \leq n < q < m \leq t$ where $m \leq 2n$. With a similar method we get the other three cases below.

Therefore we conclude that the four cases in the case of a nonsplit metacyclic p-group for an odd prime p are as follows:

(1) $2 \leq n < q < m \leq t$ where $m \leq 2n$,
(2) $1 \leq n < q < m \leq t$ where $2n < m \leq q+n$,
(3) $3 \leq n < q < t < m \leq 2n$ and

(4) $2 \le n < q < t < m$ where $2n < m \le q + n$.

However in this thesis, we will concentrate on cases 1 and 2 .

From the third relation in the presentation (2.1) we observe that any element of P can be written uniquely in the form $x^u y^v$. In the split case we have $x^{p^m} = 1$ and $y^{p^t} = 1$ so that $0 \le u < p^m$ and $0 \le v < p^t$. In the nonsplit case we also have $x^{p^m} = 1$ but $y^{p^t} = x^{p^q}$ where $q < m$, which implies $y^{p^{t+m-q}} = 1$. Similar to split case however, we assume throughout this thesis that $0 \le u < p^m$ and $0 \le v < p^t$ in the nonsplit case.

Throughout this thesis, p will be a fixed odd prime, P will always denote a finite nonabelian nonsplit metacylic p-group with the presentation (2.1) and x, y will always mean generators of P satisfying the given relations . In addition, n, q, m and t will have the meaning given in the presentation.

2.2 Product of generators in P

The calculations in this thesis involve a lot of multiplications between generators of P. A few results here are similar to those from Schulte [19]. His results only considered metacyclic p-groups with cyclic maximal subgroups and we modify them to suit our more general situations. We begin with the following lemma.

Lemma 2.2.1 *$(g_1g_2)^{p^k} = g_1^{p^k} g_2^{p^k}$ for any $g_1, g_2 \in P$ and $k \ge m - n \ge 1$.*

Proof. With p an odd prime, P is a regular group [13] so that $(g_1g_2)^{p^k} = g_1^{p^k} g_2^{p^k} z^{p^k}$ for any g_1, $g_2 \in P$ and $z \in P'$.

Now, since P' is generated by

$$[x, y^{-1}] = x^{-1}yxy^{-1} = x^{-1}x^{1+p^n} = x^{p^n},$$

we have $z = (x^{p^n})^s$ for some integer $0 \le s < p^{m-n}$. Hence for any integer $k \ge m - n \ge 1$,

$$z^{p^k} = (x^{sp^n})^{p^k} = x^{sp^{n+k}} = 1$$

so that $(g_1g_2)^{p^k} = g_1^{p^k} g_2^{p^k}$. ■

From the third relation in (2.1) we have $yx = x^{1+p^n}y$. We now put $\alpha = 1 + p^n$ so that $yx = x^{\alpha}y$. α will have this meaning throughout this thesis. The next lemma will show a similar relation between powers of x and powers of y.

Lemma 2.2.2 *Let x,y be the generators of P and u, v be integers with $v > 0$. Then $y^v x^u = x^{u\alpha^v} y^v$.*

Proof. Suppose $v > 0$. Then

$$y^v x^u = y^v x^u (y^{-v}) y^v = (y^v x^u y^{-v}) y^v.$$

We will prove by induction that $y^v x^u y^{-v} = x^{u\alpha^v}$ for all integers $v > 0$.

For $v = 1$, $y(x^u)y^{-1} = (x^u)^\alpha$ which is true from the third relation in (2.1).

Now assume $y^v x^u y^{-v} = x^{u\alpha^v}$ for $v > 1$. Thus

$$y^{v+1} x^u y^{-(v+1)} = y(y^v x^u y^{-v})y^{-1} = y(x^{u\alpha^v})y^{-1} = (yxy^{-1})^{u\alpha^v} = (x^\alpha)^{u\alpha^v} = x^{u\alpha^{v+1}}.$$

Hence $y^v x^u y^{-v} = x^{u\alpha^v}$ for any positive integer v. ■

Before we proceed we need the following definition.

Definition 2.2.1 *Let $u > 0$ and $v > 1$. We define $\Lambda(u, v)$ by*

$$\Lambda(u, v) = 1 + \alpha^u + \alpha^{2u} + \ldots + \alpha^{(v-1)u}.$$

The following result regarding $\Lambda(u, v)$ is obvious.

Lemma 2.2.3 *Let $u > 0$ and $v > 1$. Then $\Lambda(u, v)(\alpha^u - 1) = \alpha^{uv} - 1$.*

The next lemma is a further result involving $\Lambda(u, v)$.

Lemma 2.2.4 *Let $u > 0$ and $v > 1$.*

$\Lambda(u, v) \equiv v + 2^{-1}uv(v - 1)p^n$ *(mod p^{2n}).*

Proof.

We observe that $(1 + p^n)^u \equiv 1 + up^n$ *(mod p^{2n})*. Thus **modulo $\mathbf{p^{2n}}$** we have

$$\begin{aligned}\Lambda(u, v) &\equiv 1 + (1 + up^n) + (1 + 2up^n) + \ldots + (1 + (v - 1)up^n)\\ &\equiv (\underbrace{1 + 1 + \ldots + 1}_{v\ times}) + up^n(1 + 2 + \ldots + (v - 1))\\ &\equiv v + 2^{-1}uv(v - 1)p^n. \ ■\end{aligned}$$

We will need to be able to write a power of $(x^u y^v)$ as a product of a power of x and a power of y.

Lemma 2.2.5 *If x and y are the generators of P, u is any integer, $v > 0$ and $w > 1$ then $(x^u y^v)^w = x^{u\Lambda(v,w)} y^{vw}$.*

Proof. For $u > 0$, the proof is as in [19] and is included for completeness.

$$\begin{aligned}
(x^u y^v)^w &= x^u \underbrace{(y^v x^u)(y^v x^u). \; . \; . \; . \; (y^v x^u)}_{w-1 \ times} y^v \\
&= x^u x^{u\alpha^v} y^{2v} x^u . \; . \; . \; x^u y^v \\
&= x^u x^{u\alpha^v} x^{u\alpha^{2v}} y^{3v} x^u . \; . \; . \; x^u y^v \\
&\;\; . \\
&\;\; . \\
&\;\; . \\
&= x^{u(1+\alpha^v+\alpha^{2v}+. \; . \; . \; +\alpha^{(w-1)v})} y^{vw} \\
&= x^{u\Lambda(v,w)} y^{vw}.
\end{aligned}$$

For $u = 0$ the result is clear.

For $u < 0$, the same proof with u replaced by $-f$ for a positive integer f holds. ■

2.3 Miscellaneous results

In this section we present miscellaneous preliminary results which will be needed in the following chapters. We begin with the following lemma which comes from Proposition 4.10(ii) in [14] .

Lemma 2.3.1 *If x and y are generators of P then the centre $\zeta(P)$ of P is $\langle y^{p^{m-n}}, x^{p^{m-n}} \rangle$.*

Throughout this thesis, we will often encounter the term '$1+p^{q-n}$'. We represent it as U and it will always have this meaning. Here is a result regarding U which will be needed many times later.

Lemma 2.3.2 $U^{-1} - 1 \equiv -U^{-1}p^{q-n}$ *(mod p^k) for any positive integer k.*

Proof. Let k be any positive integer. Calculating **modulo $\mathbf{p^k}$**,

$$U^{-1} \equiv 1 - p^{q-n} + p^{2q-2n} - p^{3q-3n} + . \; . \; .$$

It follows that

$$\begin{aligned} U^{-1}-1 &\equiv -p^{q-n}+p^{2q-2n}-p^{3q-3n}+\ldots \\ &\equiv -p^{q-n}(1-p^{q-n}+p^{2q-2n}-p^{3q-3n}+\ldots) \\ &\equiv -U^{-1}p^{q-n}. \blacksquare \end{aligned}$$

In later chapters, our calculations involve a lot of expansion of terms where the expansion involves binomial coefficients. The following lemma and its corollaries are very useful in simplifying these expansions. Before proceeding, we remind the reader that $p^k \parallel c$ means $p^k \mid c$ but $p^{k+1} \nmid c$ for an integer c.

Lemma 2.3.3 *Let $p^\epsilon \parallel w$ where $\epsilon > 0$, and $u \geq 1$.*

If $2 \leq k \leq w$ then the power of p dividing $\binom{w}{k}p^{ku}$ is at least $p^{\epsilon+2u}$.

Proof. We divide our proof into two cases.

Case (i) : $\mathbf{2 \leq k < p^\epsilon}$

Here it is clear that the power of p dividing k is the same as that dividing $w-k$. So the power of p dividing $(k-1)!$ is the same as that dividing $(w-1)(w-2)....(w-k+1)$. Now write $k = \ell p^\nu$ for a positive integer ℓ where $(\ell, p) = 1$. Also since $k < p^\epsilon$, we have $\nu < \epsilon$. Hence the power of p dividing

$$\binom{w}{k}p^{ku} = \frac{w(w-1)(w-2)...(w-k+1)}{k(k-1)!}p^{ku} = \frac{w}{k}\frac{(w-1)(w-2)...(w-k+1)}{(k-1)!}p^{ku}$$

is $p^{\epsilon-\nu+ku}$. Now,

$$\begin{aligned} \epsilon-\nu+ku &= \epsilon-\nu+\ell p^\nu u \\ &= \epsilon+2u+(\ell p^\nu-2)u-\nu. \end{aligned}$$

If $\nu = 0$, then $k = \ell$ where $(\ell, p) = 1$. For any prime $p \geq 3$, $\ell \geq 2$ so that $(\ell p^\nu - 2)u - \nu = (\ell-2)u \geq 0$.
If $\nu > 0$, since $u \geq 1$ and $\ell p^\nu \geq 2+\nu$ where $p \geq 3$, then

$$(\ell p^\nu - 2)u - \nu \geq \ell p^\nu - 2 - \nu \geq 0.$$

Hence $p^{\epsilon+2u}$ divides $\binom{w}{k}p^{ku}$ for $2 \leq k < p^\epsilon$.

Case (ii) : $\mathbf{k \geq p^\epsilon}$

In this case it is enough to see that

$$ku \geq p^{\epsilon}u \geq (\epsilon+2)u \geq \epsilon + 2u$$

where $p^{\epsilon} \geq \epsilon + 2$ for $p \geq 3$. Hence $p^{\epsilon+2u}$ also divides $\binom{w}{k}p^{ku}$ for $k \geq p^{\epsilon}$. ■

Corollary 2.3.4 *If $p^{\epsilon} \parallel w$ for $w \geq 2$, $u \geq 1$ and $(c,p)=1$, then*

$$(1 \pm cp^{u})^{w} = 1 \pm cwp^{u} + kp^{\epsilon+2u}$$

for an integer k.

Proof. We do the proof for $(1+cp^{u})^{w}$ and the proof for $(1-cp^{u})^{w}$ is very similar.

$$(1+cp^{u})^{w} = 1 + cwp^{u} + \binom{w}{2}(c^{2}p^{2u}) + \ldots + (c^{w}p^{wu}).$$

From Lemma 2.3.3, $p^{\epsilon+2u}$ divides $\binom{w}{k}p^{ku}$ for $2 \leq k \leq w$ and thus we obtain the result. ■

We mention the next corollary as a special case of the previous one.

Corollary 2.3.5 $p^{n+k} \parallel (\alpha^{p^{k}} - 1)$ *for all integers $k \geq 0$.*

Corollary 2.3.6 *If $p^{\epsilon} \parallel w$ for $w \geq 2$, $u \geq 1$ and $(c,p)=1$, then*

$$(1 \pm cp^{u})^{-w} \equiv 1 \mp cwp^{u} + k'p^{\epsilon+2u} \ (mod\ p^{\ell})$$

for an integer k' and any positive integer ℓ.

Proof. We do the proof for $(1+cp^{u})^{-w}$ and the proof for $(1-cp^{u})^{-w}$ is very similar.

Let ℓ be any positive integer. We know that $(1+cp^{u})^{-w} = ((1+cp^{u})^{w})^{-1}$ and we will show that there exists an integer k' such that

$$(1+cp^{u})^{-w} \equiv 1 - cwp^{u} + k'p^{\epsilon+2u} \ (mod\ p^{\ell}).$$

By using Corollary 2.3.4 for an integer k we have

$$\begin{aligned}
&(1+cp^{u})^{w}(1-cwp^{u}+k'p^{\epsilon+2u}) \\
&= (1+cwp^{u}+kp^{\epsilon+2u})(1-cwp^{u}+k'p^{\epsilon+2u}) \\
&= 1 - c^{2}w^{2}p^{2u} + k'p^{\epsilon+2u}(1+cwp^{u}) + kp^{\epsilon+2u}(1-cwp^{u}) + kk'p^{2\epsilon+4u} \\
&= 1 - c^{2}w^{2}p^{2u} + kp^{\epsilon+2u}(1-cwp^{u}) + k'(p^{\epsilon+2u}(1+cwp^{u}) + kp^{2\epsilon+4u}).
\end{aligned}$$

Now we show that we can find k' such that

$$1 - c^2w^2p^{2u} + kp^{\epsilon+2u}(1 - cwp^u) + k'(p^{\epsilon+2u}(1 + cwp^u) + kp^{2\epsilon+4u}) \equiv 1 \ (mod\ p^\ell)$$

or equivalently

$$k'(p^{\epsilon+2u}(1 + cwp^u) + kp^{2\epsilon+4u}) \equiv c^2w^2p^{2u} - kp^{\epsilon+2u}(1 - cwp^u) \ (mod\ p^\ell).$$

Put

$$k' \equiv (c^2\frac{w^2}{p^\epsilon} - k(1 - cwp^u))(1 + cwp^u + kp^{\epsilon+2u})^{-1} \ \ (mod\ p^\ell)$$

where $\frac{w^2}{p^\epsilon}$ is clearly an integer, then calculate **modulo $\mathbf{p}^\ell$**,

$$\begin{aligned}
&k'(p^{\epsilon+2u}(1 + cwp^u) + kp^{2\epsilon+4u})\\
&\equiv (c^2\frac{w^2}{p^\epsilon} - k(1 - cwp^u))(1 + cwp^u + kp^{\epsilon+2u})^{-1}(p^{\epsilon+2u}(1 + cwp^u) + kp^{2\epsilon+4u})\\
&\equiv (c^2\frac{w^2}{p^\epsilon} - k(1 - cwp^u))(1 + cwp^u + kp^{\epsilon+2u})^{-1}(p^{\epsilon+2u}(1 + cwp^u + kp^{\epsilon+2u}))\\
&\equiv (c^2\frac{w^2}{p^\epsilon} - k(1 - cwp^u))(1 + cwp^u + kp^{\epsilon+2u})^{-1}(1 + cwp^u + kp^{\epsilon+2u})p^{\epsilon+2u}\\
&\equiv (c^2\frac{w^2}{p^\epsilon} - k(1 - cwp^u))p^{\epsilon+2u}\\
&\equiv (c^2\frac{w^2}{p^\epsilon} - k(1 - cwp^u))p^\epsilon(p^{2u}).
\end{aligned}$$

Now,

$$(c^2\frac{w^2}{p^\epsilon} - k(1 - cwp^u))p^\epsilon \equiv c^2w^2 - kp^\epsilon(1 - cwp^u) \text{ and hence}$$

$$k'(p^{\epsilon+2u}(1 + cwp^u) + kp^{2\epsilon+4u}) \equiv c^2w^2p^{2u} - kp^{\epsilon+2u}(1 - cwp^u). \ \blacksquare$$

The following lemma is particularly useful in Chapter 5.

Lemma 2.3.7 *If χ is a positive integer, $p^\varsigma \parallel \chi$ and $u \geq 1$ then $\Lambda(1, (1 + p^u)^\chi) - 1 = \chi p^u + ep^{\varsigma+\upsilon}$ for an integer e where $\upsilon > u$.*

Proof. Let $V = 1 + p^u$ for $u \geq 1$. From Lemma 2.2.3, $\Lambda(1, V^\chi)(\alpha - 1) = \alpha^{V^\chi} - 1$. Now,

$$\begin{aligned}
\Lambda(1, V^\chi)p^n &= (1 + V^\chi p^n + \binom{V^\chi}{2}p^{2n} + \ \ldots \ + p^{nV^\chi}) - 1\\
&= (V^\chi + \binom{V^\chi}{2}p^n + \ \ldots \ + p^{n(V^\chi-1)})p^n.
\end{aligned}$$

Thus

$$\Lambda(1, V^{\chi}) = V^{\chi} + \binom{V^{\chi}}{2}p^{n} + \binom{V^{\chi}}{3}p^{2n} + \ . \ . \ . \ + p^{n(V^{\chi}-1)}$$

and hence

$$\Lambda(1, V^{\chi}) - 1 = (V^{\chi} - 1) + \binom{V^{\chi}}{2}p^{n} + \binom{V^{\chi}}{3}p^{2n} + \ . \ . \ . \ + p^{n(V^{\chi}-1)}.$$

Using Corollary 2.3.4, $V^{\chi} - 1 = (1 + p^{u})^{\chi} - 1 = \chi p^{u} + cp^{\varsigma+2u}$ for an integer c.

Now we will show that $p^{\varsigma+(u+n)}$ divides $\binom{V^{\chi}}{k}p^{(k-1)n}$ for $2 \leq k \leq V^{\chi}$.

We divide our proof into two cases.

Case (i) : $\mathbf{2 \leq k < p^{\varsigma+u}}$

Here it is clear that the power of p dividing k is the same as that dividing $V^{\chi} - 1 - k$. So the power of p dividing $(k - 2)!$ is the same as that dividing $(V^{\chi} - 2)(V^{\chi} - 3). \ . \ . \ .(V^{\chi} - k + 1)$.

Now at most one of k or $(k - 1)$ is divisible by p. Assume maximum power of p dividing $k(k - 1)$ is p^{w}. So $k = \ell p^{w} + \epsilon$ for $\epsilon = 0$ or $\epsilon = 1$ where ℓ is a positive integer such that $(\ell, p) = 1$.

Hence the power of p dividing $\binom{V^{\chi}}{k}p^{(k-1)n}$ where

$$\begin{aligned}\binom{V^{\chi}}{k}p^{(k-1)n} &= \frac{V^{\chi}(V^{\chi} - 1)(V^{\chi} - 2)...(V^{\chi} - k + 1)}{k(k - 1)(k - 2)!}p^{(k-1)n} \\ &= \frac{V^{\chi}(V^{\chi} - 1)}{k(k - 1)}(\frac{(V^{\chi} - 2)...(V^{\chi} - k + 1)}{(k - 2)!})p^{(k-1)n},\end{aligned}$$

is $p^{\varsigma+u+(k-1)n-w}$. If $w = 0$, there is nothing further to prove.

Suppose $w > 0$.

We will show that $(k - 1)n - w \geq n$.

$$\begin{aligned}(k - 1)n - w &= (\ell p^{w} + \epsilon)n - w \\ &\geq \ell p^{w}n - w \\ &\geq (w + 1)n - w \\ &\geq n + wn - w \\ &\geq n\end{aligned}$$

where for $p \geq 3$, $p^{w} > w + 1$. Hence $p^{\varsigma+u+(k-1)n-w}$ is divisible by $p^{\varsigma+(u+n)}$.

Case (ii) : $\mathbf{p^{\varsigma+u} \leq k \leq V^{\chi}}$

Here it is enough to show that

$$\begin{aligned}(k-1)n &\geq (p^{\varsigma+u}-1)n \\ &\geq np^{\varsigma+u}-n \\ &\geq n(\varsigma+u+2)-n \\ &\geq \varsigma+u+2n-n \\ &\geq \varsigma+(u+n).\end{aligned}$$

Hence $p^{\varsigma+(u+n)}$ divides $\binom{V^{\chi}}{k}p^{(k-1)n}$ for $p^{\varsigma+u} \leq k \leq V^{\chi}$.

Therefore we conclude that for integers c, c' and e,

$$\begin{aligned}\Lambda(1,V^{\chi})-1 &= (V^{\chi}-1)+(\binom{V^{\chi}}{2}p^{n}+\binom{V^{\chi}}{3}p^{2n}+\ \ldots\ +p^{n(V^{\chi}-1)}) \\ &= (\chi p^{u}+cp^{\varsigma+2u})+(c'p^{\varsigma+(u+n)}) \\ &= \chi p^{u}+ep^{\varsigma+v}\end{aligned}$$

where $v > u$. ■

The following lemma will be needed especially in Chapter 5. The proof is straightforward and is omitted.

Lemma 2.3.8 *Let G, K, L be groups.*

If $G = KL$ where $L = \langle \ell \rangle$ and $K \cap L = \langle \ell^{u} \rangle$, then each element of G can be written uniquely in the form $k\ell^{v}$ for $k \in K$, $0 \leq v < u$.

In particular if $K \cap L = 1$ then each element of G can be written uniquely in the form $k\ell$ for $k \in K$ and $\ell \in L$.

Chapter 3

Conditions to be an automorphism

Before proceeding, we remind the reader that we are only considering the structure of the automorphism groups of nonsplit metacyclic p-groups in cases 1 and 2. From the presentation (2.1) of P which is

$$P = \langle x, y | x^{p^m} = 1, y^{p^t} = x^{p^q}, yxy^{-1} = x^{p^n+1} \rangle,$$

we observe that q is always less than m so that y^{p^t} is no longer equal to 1, instead the order of y is p^{t+m-q}. The calculations involved in this chapter will take care of the fact that, if we have two single prime powers of y on both sides of an equivalence relation modulo some normal subgroup for example, these two powers in general are not necessarily congruent modulo p^t, unlike in the split case.

In this chapter we look at restrictions on i, j, r and s which give conditions for a matrix $\begin{bmatrix} i & r \\ j & s \end{bmatrix}$ to represent an automorphism of P. We begin with the following lemma.

Lemma 3.0.1 *Let φ be an automorphism of P where $\varphi \sim \begin{bmatrix} i & r \\ j & s \end{bmatrix}$. If x, y are generators of P and m, n are parameters as in the presentation (2.1) of P then*

$$x^{r+i\alpha^s - r\alpha^j} y^j = x^{i(\Lambda(j,p^n)+\alpha^{jp^n})} y^{j\alpha}.$$

In particular, if $m \leq 2n$ then

$$x^{r+i\alpha^s-r\alpha^j}y^j = x^{i(p^n+\alpha^{jp^n})}y^{j\alpha}.$$

Proof.

We apply φ to both sides of the third relation in presentation (2.1) which is $yxy^{-1} = x^{p^n+1}$.

$$\begin{aligned}
\varphi(yxy^{-1}) &= \varphi(y)\varphi(x)\varphi(y^{-1}) \\
&= (x^r y^s)(x^i y^j)(x^r y^s)^{-1} \\
&= x^r y^s x^i y^j y^{-s} x^{-r} \\
&= x^r (y^s x^i)(y^{j-s} x^{-r}) \\
&= x^r (x^{i\alpha^s} y^s)(x^{-r\alpha^{j-s}} y^{j-s}) \text{ (by Lemma 2.2.2)} \\
&= x^r x^{i\alpha^s} (y^s x^{-r\alpha^{j-s}}) y^{j-s} \\
&= x^r x^{i\alpha^s} (x^{-r\alpha^{j-s}\alpha^s} y^s) y^{j-s} \text{ (by Lemma 2.2.2)} \\
&= x^{r+i\alpha^s-r\alpha^j} y^j
\end{aligned}$$

whereas

$$\begin{aligned}
\varphi(x^{p^n+1}) &= (x^i y^j)^{p^n} (x^i y^j) \\
&= x^{i\Lambda(j,p^n)} y^{jp^n} x^i y^j \text{ (by Lemma 2.2.5)} \\
&= x^{i\Lambda(j,p^n)} (y^{jp^n} x^i) y^j \\
&= x^{i\Lambda(j,p^n)} x^{i\alpha^{jp^n}} y^{jp^n} y^j \text{ (by Lemma 2.2.2)} \\
&= x^{i(\Lambda(j,p^n)+\alpha^{jp^n})} y^{j(p^n+1)} \\
&= x^{i(\Lambda(j,p^n)+\alpha^{jp^n})} y^{j\alpha}.
\end{aligned}$$

In particular if $m \leq 2n$ so that $m - n \leq n$,

$$\begin{aligned}
\varphi(x^{p^n+1}) &= (x^i y^j)^{p^n} (x^i y^j) \\
&= x^{ip^n} y^{jp^n} x^i y^j \text{ (by Lemma 2.2.1)} \\
&= x^{ip^n} (y^{jp^n} x^i) y^j \\
&= x^{ip^n} x^{i\alpha^{jp^n}} y^{jp^n} y^j \text{ (by Lemma 2.2.2)} \\
&= x^{i(p^n+\alpha^{jp^n})} y^{j(p^n+1)} \\
&= x^{i(p^n+\alpha^{jp^n})} y^{j\alpha}.
\end{aligned}$$

Hence the lemma is obtained since $\varphi(yxy^{-1}) = \varphi(x^{p^n+1})$. ■

The order of the automorphism group of nonsplit metacyclic p-groups for odd primes p, is p^{2n+q+t} (in our notation) as proved by Menegazzo in his result (A.2) [15]. We write his result as a theorem, exactly as it appeared in [15] where G is a nonsplit metacyclic p-group where p is an odd prime.

Theorem 3.0.2

$$G = \langle a, b | b^{p^m} = 1, b^a = b^{1+p^s}, a^{p^\ell} = b^{p^h} \rangle$$

where $1 \leq s < h < m$ *and* $m - s \leq h < \ell$.

$|Aut(G)| = p^{\ell+h+2s}$.

We will show that in both cases 1 and 2, φ is an automorphism of P if and only if i, j, r and s satisfy certain restrictions where $\varphi \sim \begin{bmatrix} i & r \\ j & s \end{bmatrix}$. With these restrictions, the number of distinct automorphisms φ is equal to p^{2n+q+t}, that is the order of $Aut(P)$.

Before proceeding to the next proposition, we need the following two lemmas.

Lemma 3.0.3 *If* $\varphi \in Aut(P)$ *where* $\varphi \sim \begin{bmatrix} i & r \\ j & s \end{bmatrix}$, *then is* $- rj \not\equiv 0$ *(mod p).*

Proof.

Since P is a 2-generator group, $P/\phi(P) \cong Z_p \times Z_p$ and φ defines an automorphism on $P/\phi(P)$ with matrix $\begin{bmatrix} i & r \\ j & s \end{bmatrix}$, where i, j, r and s are taken modulo p. This matrix is thus in $GL(2, p)$ and so, $is - rj$ is not congruent to zero modulo p. ■

Lemma 3.0.4 *Recall* $\alpha = 1 + p^n$ *and let* $s > 1$ *be an integer.*

Then $\alpha^s - \alpha \equiv (s-1)p^n + 2^{-1}s(s-1)p^{2n}$ *(mod* p^{3n}*).*

Proof.

From Lemma 2.2.3, $\alpha^s - 1 = \Lambda(1, s)(\alpha - 1)$. From Lemma 2.2.4,

$$\Lambda(1, s) \equiv s + 2^{-1}s(s-1)p^n \ (mod\ p^{2n}).$$

Thus

$$\alpha^s - 1 \equiv sp^n + 2^{-1}s(s-1)p^{2n} \ (mod\ p^{3n}).$$

Hence

$$\alpha^s - \alpha \equiv (s-1)p^n + 2^{-1}s(s-1)p^{2n} \ (mod\ p^{3n}). \ \blacksquare$$

We now come to the main result in this chapter.

Theorem 3.0.5 *Let* $\varphi \sim \begin{bmatrix} i & r \\ j & s \end{bmatrix}$. *Then* $\varphi \in Aut(P)$ *if and only if*

i) $i \equiv 1 \ (mod\ p^{m-q})$,

ii) $r \in \mathbb{Z}_{p^m}$,

iii) $j \equiv 0 \ (mod\ p^{t-n})$,

iv) $s \equiv 1 + cp^{q-n} \ (mod\ p^{m-n})$ *where* $j = cp^{t-n}$ *for* $0 \le c < p^n$.

Proof. We will do the proof by each case and show that these restrictions are the same for both cases 1 and 2. As before, we write $\varphi(\mathrm{x}) = x^i y^j$ and $\varphi(\mathrm{y}) = x^r y^s$ where i, r are taken modulo p^m and j, s are taken modulo p^t. In the proof we note that when necessary, we will write α as $1 + p^n$. Otherwise we will leave it as α.

Let $\varphi \in Aut(P)$.

Case 1 :

The first case has the inequalities of the parameters as $2 \le n < q < m \le t$ where $m \le 2n$.

By Lemma 3.0.1 since $m \le 2n$,

$$x^{r+i\alpha^s - r\alpha^j} y^j = x^{i(p^n + \alpha^{jp^n})} y^{j(1+p^n)}.$$

Hence

$$x^{r+i\alpha^s - r\alpha^j} = x^{i(p^n + \alpha^{jp^n})} y^{jp^n}$$

which implies $jp^n \equiv 0 \ (mod\ p^t)$, so that $j \equiv 0 \ (mod\ p^{t-n})$. It follows that $i \not\equiv 0$ $(mod\ p)$ and $s \not\equiv 0 \ (mod\ p)$ since from Lemma 3.0.3, $is - rj \not\equiv 0 \ (mod\ p)$.

Now from Corollary 2.3.5,

$$\alpha^{p^n} \equiv 1 \ (mod\ p^{2n}) \equiv 1 \ (mod\ p^m)$$

and also since

$$\alpha^{p^{t-n}} \equiv 1 \ (mod\ p^t) \equiv 1 \ (mod\ p^m),$$

we have

$$x^{r+i\alpha^s - r} = x^{i\alpha} y^{jp^n}$$

or

$$x^{i\alpha^s} = x^{i\alpha}y^{jp^n}.$$

Now since $j \equiv 0 \ (mod \ p^{t-n})$, we write $j = cp^{t-n}$ for an integer c where $0 \leq c < p^n$. Thus $x^{i\alpha^s} = x^{i\alpha}y^{cp^t}$. It follows that $x^{i\alpha^s} = x^{i\alpha}x^{cp^q}$. This implies

$$i(\alpha^s - \alpha) \equiv cp^q \ (mod \ p^m).$$

By referring to Lemma 3.0.4, $\alpha^s - \alpha \equiv (s-1)p^n \ (mod \ p^m)$ since in case 1 $m \leq 2n$ and hence, $i(s-1)p^n \equiv cp^q \ (mod \ p^m)$ so that,

$$s \equiv 1 + i^{-1}cp^{q-n} \ (mod \ p^{m-n}). \tag{3.1}$$

Now, using the second relation in (2.1) we have $\varphi(y^{p^t}) = \varphi(x^{p^q})$. Thus $(x^r y^s)^{p^t} = (x^i y^j)^{p^q}$. Since $t \geq m-n$ and $q \geq m-n$, by using Lemma 2.2.1 we have

$$(x^r)^{p^t}(y^s)^{p^t} = (x^i)^{p^q}(y^j)^{p^q}.$$

It follows that since $t \geq m$, $(x^r)^{p^t} = 1$ and thus

$$\begin{aligned}(y^s)^{p^t} &= (x^i)^{p^q}(y^j)^{p^q} \\ &= (x^i)^{p^q}y^{cp^{t-n+q}} \\ &= (x^i)^{p^q}\left(y^{p^t}\right)^{cp^{q-n}} \\ &= (x^i)^{p^q}\left(x^{p^q}\right)^{cp^{q-n}}.\end{aligned}$$

But $(y^s)^{p^t} = (x^s)^{p^q}$ and hence $sp^q \equiv ip^q + cp^{2q-n} \ (mod \ p^m)$. Therefore

$$i \equiv s - cp^{q-n} \ (mod \ p^{m-q}). \tag{3.2}$$

We now calculate i **modulo $\mathbf{p^{m-q}}$**. Putting s from (3.1) into (3.2) we have **modulo $\mathbf{p^{m-q}}$**

$$\begin{aligned}i &\equiv 1 + i^{-1}cp^{q-n} + zp^{m-n} - cp^{q-n} \text{ (for an integer } z\text{)} \\ &\equiv 1 + i^{-1}cp^{q-n} - cp^{q-n} \\ &\equiv W - (W-1)i \\ &\equiv W - Wi + i\end{aligned}$$

where $W = 1 + i^{-1}cp^{q-n}$. Thus

$$Wi \equiv W \ (mod\ p^{m-q})$$

or

$$W(i-1) \equiv 0 \ (mod\ p^{m-q})$$

which implies $i \equiv 1 \ (mod\ p^{m-q})$ since $W \equiv 1 \ (mod\ p)$ and so W is invertible **modulo** $\mathbf{p^{m-q}}$.

We now calculate s **modulo** $\mathbf{p^{m-n}}$. Since $i \equiv 1 \ (mod\ p^{m-q})$, we have $i^{-1} \equiv 1 \ (mod\ p^{m-q})$. Replacing this into (3.1) and calculating **modulo** $\mathbf{p^{m-n}}$,

$$\begin{aligned} s &\equiv 1 + (1 + z'p^{m-q})cp^{q-n} \text{ (for an integer } z') \\ &\equiv 1 + cp^{q-n} + cz'p^{m-n} \\ &\equiv 1 + cp^{q-n}. \end{aligned}$$

In addition, we have no further restriction about r and so r can be any element in $\mathbf{Z_{p^m}}$.

Case 2 :

The second case has the inequalities of the parameters as $1 \le n < q < m \le t$ where $2n < m \le q + n$.

By Lemma 3.0.1 where $m > 2n$ in this case, we have

$$x^{r+i\alpha^s - r\alpha^j}y^j = x^{i(\Lambda(j,p^n)+\alpha^{jp^n})}y^{j(1+p^n)}.$$

Hence

$$x^{r+i\alpha^s - r\alpha^j} = x^{i(\Lambda(j,p^n)+\alpha^{jp^n})}y^{jp^n}$$

which implies $jp^n \equiv 0 \ (mod\ p^t)$, so that $j \equiv 0 \ (mod\ p^{t-n})$. As in case 1, $i \not\equiv 0 \ (mod\ p)$ and $s \not\equiv 0 \ (mod\ p)$ since from Lemma 3.0.3, $is - rj \not\equiv 0 \ (mod\ p)$.

Now let $j = cp^{t-n}$ for any integer c where $0 \le c < p^n$. Hence by Corollary 2.3.5

$$\alpha^j \equiv 1 \ (mod\ p^t) \equiv 1 \ (mod\ p^m),$$

which also implies $\alpha^{jp^n} \equiv 1 \ (mod\ p^m)$ and $\Lambda(j, p^n) \equiv p^n \ (mod\ p^m)$. Thus we have $x^{i\alpha^s} = x^{i\alpha}y^{jp^n}$ and obtain as in case 1,

$$i(\alpha^s - \alpha) \equiv cp^q \ (mod\ p^m). \tag{3.3}$$

Now using Lemma 3.0.4, we can rewrite $\alpha^s - \alpha$ as

$$\alpha^s - \alpha = (s-1)p^n + kp^{2n}$$

for an integer k, and putting this into (3.3) we have

$$i((s-1)p^n + kp^{2n}) \equiv cp^q \ (mod\ p^m).$$

Hence

$$i(s-1+kp^n) \equiv cp^{q-n} \ (mod\ p^{m-n})$$

so that

$$s \equiv 1 + i^{-1}cp^{q-n} - kp^n \ (mod\ p^{m-n}). \tag{3.4}$$

Now by using the second relation in (2.1), we repeat the same steps as in case 1 to also have

$$i \equiv s - cp^{q-n} \ (mod\ p^{m-q}). \tag{3.5}$$

We now calculate i **modulo $\mathbf{p^{m-q}}$**. Putting s from (3.4) into (3.5), for an integer ℓ we have **modulo $\mathbf{p^{m-q}}$**,

$$\begin{aligned} i &\equiv 1 + i^{-1}cp^{q-n} - kp^n + \ell p^{m-n} - cp^{q-n} \\ &\equiv 1 + i^{-1}cp^{q-n} - cp^{q-n} \ (\text{since } m \leq q+n \text{ and } m-n > m-q) \\ &\equiv W - (W-1)i \\ &\equiv W - Wi + i \end{aligned}$$

where $W = 1 + i^{-1}cp^{q-n}$. Thus as in case 1, $i \equiv 1 \ (mod\ p^{m-q})$.

We now calculate s **modulo $\mathbf{p^{m-n}}$**. In case 2 due to $m > 2n$, the proof for this part is more complicated and for that, we divide the proof into two subcases.

a) $\mathbf{q - n \leq n}$

Here, $q \leq 2n$ and so $m \leq q + n \leq 3n$. Hence from Lemma 3.0.4,

$$\alpha^s - \alpha \equiv (s-1)p^n + 2^{-1}s(s-1)p^{2n} \ (mod\ p^m).$$

But from (3.4), $s - 1 \equiv 0 \ (mod\ p^{q-n})$ since $n \geq q - n$ and so $(s-1)p^{2n}$ is divisible by $p^{q-n}p^{2n} = p^{q+n} \equiv 0\ (mod\ p^m)$. Thus $\alpha^s - \alpha \equiv (s-1)p^n\ (mod\ p^m)$. Using this in (3.3),

$$i((s-1)p^n) \equiv cp^q\ (mod\ p^m)$$

so that

$$i(s-1) \equiv cp^{q-n}\ (mod\ p^{m-n})$$

which implies

$$s \equiv 1 + i^{-1}cp^{q-n}\ (mod\ p^{m-n}).$$

Write $i^{-1} = 1 + ep^{m-q}$ for an integer e, we have **modulo $\mathbf{p^{m-n}}$**

$$\begin{aligned} s &\equiv 1 + (1 + ep^{m-q})(cp^{q-n}) \\ &\equiv 1 + cp^{q-n}. \end{aligned}$$

b) $\mathbf{q - n > n}$

From (3.4), $s = 1 + fp^\nu$ where f is prime to p and $\nu \geq n$. Now we calculate $\alpha^s - \alpha$ **modulo $\mathbf{p^q}$**. Since $i \equiv 1\ (mod\ p^{m-q})$ we have $i \equiv 1\ (mod\ p)$ and since $\alpha = 1 + p^n$ we have $\alpha \equiv 1\ (mod\ p)$. Therefore i and α are invertible modulo p^q. Hence by (3.3),

$$\begin{aligned} 0 &\equiv (\alpha^s - \alpha) \\ &\equiv (\alpha^{s-1} - 1) \\ &\equiv (\alpha^{fp^\nu} - 1) \\ &\equiv (1 + \alpha^{p^\nu} + \alpha^{2p^\nu} + \ldots + \alpha^{(f-1)p^\nu})(\alpha^{p^\nu} - 1) \text{ (by lemma 2.2.3).} \end{aligned}$$

But

$$(1 + \alpha^{p^\nu} + \alpha^{2p^\nu} + \ldots + \alpha^{(f-1)p^\nu}) \equiv f\ (mod\ p)$$

and thus

$$(1 + \alpha^{p^\nu} + \alpha^{2p^\nu} + \ldots + \alpha^{(f-1)p^\nu}) \not\equiv 0\ (mod\ p).$$

Hence $\alpha^{p^\nu} - 1 \equiv 0\ (mod\ p^q)$. Since by Corollary 2.3.5 the highest power of p dividing $\alpha^{p^\nu} - 1$ is $p^{n+\nu}$, we must have $p^{n+\nu}$ is divisible by p^q so that p^ν is divisible by p^{q-n}. Thus

$$\begin{aligned} s - 1 &= fp^\nu \\ &\equiv 0\ (mod\ p^{q-n}). \end{aligned}$$

Now we calculate $\alpha^s - \alpha$ **modulo** $\mathbf{p^m}$. Here we first have to write

$$\begin{aligned}\alpha^s - \alpha &= (1+p^n)^s - (1+p^n)\\ &= (s-1)p^n + \binom{s}{2}p^{2n} + \binom{s}{3}p^{3n} + \ . \ . \ . \ + p^{sn}.\end{aligned}$$

We show that $\binom{s}{u}p^{un} \equiv 0 \ (mod \ p^m)$ for $2 \leq u \leq s$. We note that we cannot use Lemma 2.3.3 here because $s \not\equiv 0 \ (mod \ p)$, although the method used has some similarities.

We divide the problem into two cases:

Case (i) : $\mathbf{2 \leq u < p^{q-n}}$

Let $u = cp^\kappa$ for $\kappa < q-n$ and $(c,p) = 1$. It is clear that the power of p dividing $s-1-u$ is exactly the same as the power of p dividing u. Thus if p^v is the power of p dividing $(u-2)!$, then $s(s-1)(s-2). \ . \ .(s-u+1)$ is divisible by p^{q-n+v} where from before we have $s-1 \equiv 0 \ (mod \ p^{q-n})$. Then $s(s-1)(s-2). \ . \ .(s-u+1)p^{un}$ is divisible by $p^{q-n+v+un}$.

Now, at most u or $u-1$ is not divisible by p. Suppose the highest power of p dividing either of them is p^w. Since $u! = u(u-1)(u-2)!$, the highest power of p dividing $u!$ is p^{v+w}. Thus

$$\binom{s}{u}p^{un} = \frac{s(s-1)(s-2). \ . \ .(s-u+1)}{u!}p^{un}$$

is divisible by $p^{q-n+v+un-v-w} = p^{q-n+un-w}$. If $w = 0$ then $\binom{s}{u}p^{un}$ is divisible by p^{q-n+un} which is divisible by p^m, since $q-n+un \geq q+n(u-1) \geq q+n \geq m$ so that $\binom{s}{u}p^{un} \equiv 0 \ (mod \ p^m)$.

Now suppose $w > 0$.

Let $u = k'p^w + \epsilon$ for a positive integer k' where $(k',p) = 1$ and $\epsilon = 0$ or 1, depending on which of u and $u-1$ coprime to p. We will show that $un - w \geq 2n$.

To see this, we observe that $un - w \geq n(u-w)$ and so it will be enough to show that

$$u - w = k'p^w - w + \epsilon \geq 2.$$

For $w = 1$, we have

$$\begin{aligned} u - 1 &= k'p - 1 + \epsilon \\ &= k'p + (\epsilon - 1) \\ &\geq p - 1 \\ &\geq 2. \end{aligned}$$

For $w > 1$, we observe that $k'p^w - w + \epsilon$ is a monotone increasing function of w and thus the result follows.

So since we now have $un - w \geq 2n$,

$$\begin{aligned} q - n + un - w &\geq q - n + 2n \\ &\geq q + n \\ &\geq m \end{aligned}$$

so that, $\binom{s}{u}p^{un} \equiv 0 \ (mod \ p^m)$ in this case.

Case (ii) : $\mathbf{p^{q-n} \leq u \leq s}$

In this case, the term $\binom{s}{u}p^{un} \equiv 0 \ (mod \ p^m)$ since $p^{un} \geq p^{np^{q-n}} > p^m$ as the following shows.

For $p \geq 3$:

$$\begin{aligned} np^{q-n} &> n(q - n + 2) \\ &\geq n(q - n) + 2n \\ &\geq q - n + 2n \\ &\geq q + n \\ &\geq m. \end{aligned}$$

Hence we conclude, $\binom{s}{u}p^{un} \equiv 0 \ (mod \ p^m)$ for $2 \leq u \leq s$. Therefore

$$\alpha^s - \alpha \equiv (s - 1)p^n \ (mod \ p^m)$$

and the rest of the proof is similar to case (a) above to obtain

$$s \equiv 1 + cp^{q-n} \ (mod \ p^{m-n})$$

also.

In addition, we have no further restriction about r and so r can be any element in $\mathbf{Z}_{\mathbf{p^m}}$.

Therefore $\varphi \in A$ where A is the set of mappings of P that satisfy these restrictions, and so $Aut(P) \subseteq A$.

Now it is clear that the number of choices for i is p^q, the number of choices for j is p^n and the number of choices for r is p^m since $r \in \mathbb{Z}_{p^m}$.

In addition for each $j = cp^{t-n}$ where $0 \leq c < p^n$, the number of choices for s is $p^{t-(m-n)} = p^{t-m+n}$. From this, we see that the number of choices for the pair (s,j) is $(p^{t-m+n})(p^n) = p^{t-m+2n}$.

Therefore the number of distinct mappings in A or the order of A is

$$(p^q)(p^{t-m+2n})(p^m) = p^{2n+q+t}$$

which is also the order of $Aut(P)$ by Theorem 3.0.2. Hence we get the result. ■

Chapter 4

The commutators

In this chapter we introduce particular automorphisms of P that we will show in the next chapter to be generators of $Aut(P)$ in cases 1 and 2. Our results on the structure of $Aut(P)$ in later chapters depend heavily on calculations involving these generators and it is convenient to collect calculations of their powers, inverses and commutators between them together in this chapter.

4.1 Particular automorphisms

We now introduce the automorphisms a, b, d and h of P where they have the following meaning:

$$a \sim \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, b \sim \begin{bmatrix} 1+p^{m-q} & 0 \\ 0 & 1 \end{bmatrix}, d \sim \begin{bmatrix} 1 & 0 \\ p^{t-n} & U \end{bmatrix} \text{ and } h \sim \begin{bmatrix} 1+p^{m-n} & 0 \\ 0 & 1+p^{m-n} \end{bmatrix}$$

where $U = 1 + p^{q-n}$.

Furthermore we calculate the powers we need of these automorphisms in the following lemma.

Lemma 4.1.1 *Let a, b, d and h be the automorphisms of P defined earlier. Then for any integers η, β, γ and θ,*

$$a^\eta \sim \begin{bmatrix} 1 & \eta \\ 0 & 1 \end{bmatrix}, b^\beta \sim \begin{bmatrix} (1+p^{m-q})^\beta & 0 \\ 0 & 1 \end{bmatrix}, d^\gamma \sim \begin{bmatrix} 1 & 0 \\ p^{t-q}(U^\gamma - 1) & U^\gamma \end{bmatrix} \text{ and}$$

$$h^\theta \sim \begin{bmatrix} (1+p^{m-n})^\theta & 0 \\ 0 & (1+p^{m-n})^\theta \end{bmatrix}.$$

In particular, $d^{-1} \sim \begin{bmatrix} 1 & 0 \\ -U^{-1}p^{t-n} & U^{-1} \end{bmatrix}$ *since* $U^{-1} - 1 \equiv -U^{-1}p^{q-n}$ *(mod* p^k*)* *for any positive integer* k.

Proof. The calculations for a^η, b^β and h^θ are straightforward and are omitted.

Now, $d(x) = xy^{p^{t-n}}$ and $d(y) = y^U$. We prove the result for d^γ for any positive integer $\gamma \geq 1$ by induction.

For $\gamma = 1$, the result follows from the definition of d.

Now suppose $d^\gamma(x) = xy^{p^{t-q}(U^\gamma - 1)}$ for any positive integer $\gamma > 1$. Then

$$\begin{aligned} d^{\gamma+1}(x) &= d(d^\gamma(x)) \\ &= d(xy^{p^{t-q}(U^\gamma-1)}) \\ &= xy^{p^{t-n}}(y^U)^{p^{t-q}(U^\gamma-1)} \\ &= xy^{p^{t-n}}y^{p^{t-q}(U^{\gamma+1})-Up^{t-q}} \\ &= xy^{p^{t-q}(p^{q-n}+U^{\gamma+1}-U)} \\ &= xy^{p^{t-q}(p^{q-n}-(1+p^{q-n})+U^{\gamma+1})} \\ &= xy^{p^{t-q}(U^{\gamma+1}-1)}. \end{aligned}$$

Now suppose $d^\gamma(y) = y^{U^\gamma}$ for any positive integer $\gamma > 1$. Thus

$$d^{\gamma+1}(y) = d(d^\gamma(y)) = d(y^{U^\gamma}) = (y^U)^{U^\gamma} = y^{U^{\gamma+1}}$$

and hence the result is proved inductively.

Now let

$$d^\gamma \sim \begin{bmatrix} 1 & 0 \\ p^{t-q}(U^\gamma - 1) & U^\gamma \end{bmatrix}$$

and

$$d^* \sim \begin{bmatrix} 1 & 0 \\ p^{t-q}(U^{-\gamma} - 1) & U^{-\gamma} \end{bmatrix}.$$

We show that $d^\gamma d^* \sim \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ and hence $d^* = d^{-\gamma}$.

$$\begin{aligned} d^\gamma d^*(x) &= d^\gamma(xy^{p^{t-q}(U^{-\gamma}-1)}) \\ &= (xy^{p^{t-q}(U^\gamma-1)})(y^{U^\gamma})^{p^{t-q}(U^{-\gamma}-1)} \\ &= xy^{p^{t-q}(U^\gamma-1)+p^{t-q}(1-U^\gamma)} \\ &= x. \end{aligned}$$

On the other hand, $d^{\gamma}d^{*}(y) = d^{\gamma}(y^{U^{-\gamma}}) = (y^{U^{\gamma}})^{U^{-\gamma}} = y$. Therefore $d^{*} = d^{-\gamma}$. ■

We now find the order of each automorphism.

Lemma 4.1.2 *Let a, b, d and h be the automorphisms of P defined earlier. Then $ord(a) = p^{m}$, $ord(b) = p^{q}$, $ord(d) = p^{t+m+n-2q}$ and $ord(h) = p^{t+n-q}$.*

Proof. First we remind the reader that $x^{p^{m}} = 1$ and $y^{p^{t}} = x^{p^{q}}$.

Clearly $ord(a) = p^{m}$ and $ord(b) = p^{q}$.

Now we find $ord(d)$. By using Corollary 2.3.4 where ℓ and ℓ' are integers,

$$U^{p^{t+m+n-2q}} = (1+p^{q-n})^{p^{t+m+n-2q}} = 1 + p^{t+m-q} + \ell p^{t+m-n}$$

and

$$U^{p^{t+m+n-2q-1}} = (1+p^{q-n})^{p^{t+m+n-2q-1}} = 1 + p^{t+m-q-1} + \ell' p^{t+m-n-1}.$$

Hence from Lemma 4.1.1,

$$\begin{aligned} d^{p^{t+m+n-2q}} &\sim \begin{bmatrix} 1 & 0 \\ p^{t-q}(U^{p^{t+m+n-2q}} - 1) & U^{p^{t+m+n-2q}} \end{bmatrix} \\ &\sim \begin{bmatrix} 1 & 0 \\ p^{t-q}(p^{t+m-q} + \ell p^{t+m-n}) & 1 + p^{t+m-q} + \ell p^{t+m-n} \end{bmatrix} \\ &\sim \begin{bmatrix} 1 + p^{m+t-q} + \ell p^{m+t-n} & 0 + p^{m} + \ell p^{m+q-n} \\ 0 & 1 \end{bmatrix} \\ &\sim \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \text{ and} \end{aligned}$$

$$\begin{aligned} d^{p^{t+m+n-2q-1}} &\sim \begin{bmatrix} 1 & 0 \\ p^{t-q}(U^{p^{t+m+n-2q-1}} - 1) & U^{p^{t+m+n-2q-1}} \end{bmatrix} \\ &\sim \begin{bmatrix} 1 & 0 \\ p^{t-q}(p^{t+m-q-1} + \ell' p^{t+m-n-1}) & 1 + p^{t+m-q-1} + \ell' p^{t+m-n-1} \end{bmatrix} \\ &\sim \begin{bmatrix} 1 + p^{m+t-q-1} + \ell' p^{m+t-n-1} & 0 + p^{m-1} + \ell' p^{m+q-n-1} \\ 0 & 1 \end{bmatrix} \\ &\sim \begin{bmatrix} 1 & p^{m-1} \\ 0 & 1 \end{bmatrix} \\ &\neq \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \end{aligned}$$

and thus $ord(d) = p^{t+m+n-2q}$.

Now we find $ord(h)$. From Lemma 4.1.1,

$$\begin{aligned} h^{p^{t+n-q}} &\sim \begin{bmatrix} (1+p^{m-n})^{p^{t+n-q}} & 0 \\ 0 & (1+p^{m-n})^{p^{t+n-q}} \end{bmatrix} \\ &\sim \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \end{aligned}$$

since from Corollary 2.3.4 for an integer k,

$$\begin{aligned} (1+p^{m-n})^{p^{t+n-q}} &= 1 + p^{t+m-q} + kp^{t+2m-q-n} \\ &\equiv 1 \ (mod\ p^{t+m-q}). \end{aligned}$$

On the other hand from Lemma 4.1.1,

$$\begin{aligned} h^{p^{t+n-q-1}} &\sim \begin{bmatrix} (1+p^{m-n})^{p^{t+n-q-1}} & 0 \\ 0 & (1+p^{m-n})^{p^{t+n-q-1}} \end{bmatrix} \\ &\sim \begin{bmatrix} 1+p^{t+m-q-1} & 0 \\ 0 & 1+p^{t+m-q-1} \end{bmatrix} \\ &\sim \begin{bmatrix} 1 & p^{m-1} \\ 0 & 1 \end{bmatrix} \\ &\neq \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \end{aligned}$$

since from Corollary 2.3.4 for an integer k',

$$\begin{aligned} (1+p^{m-n})^{p^{t+n-q-1}} &= 1 + p^{t+m-q-1} + k'p^{t+2m-q-n-1} \\ &\equiv 1 + p^{t+m-q-1} \ (mod\ p^{t+m-q}). \end{aligned}$$

Thus $ord(h) = p^{t+n-q}$. ■.

We now show that h commutes with the other three automorphisms and so $\langle h \rangle$ is a normal subgroup of $Aut(P)$.

Lemma 4.1.3 *If a, b, d and h are the automorphisms of P defined earlier then h commutes with a, b and d.*

Proof. In the following proof we note that from Lemma 2.3.1, $x^{p^{m-n}}$ and $y^{p^{m-n}}$

and thus $y^{p^{t-n}}$, are central elements of P where in cases 1 and 2, $t \geq m$. Now,

$$ha(x) = h(x) = x^{1+p^{m-n}}$$

and

$$ah(x) = a(x^{1+p^{m-n}}) = x^{1+p^{m-n}}.$$

On the other hand,

$$ha(y) = h(xy) = x^{1+p^{m-n}}y^{1+p^{m-n}}$$

and

$$\begin{aligned} ah(y) &= a(y^{1+p^{m-n}}) \\ &= (xy)^{1+p^{m-n}} \\ &= (xy)(xy)^{p^{m-n}} \\ &= (xy)(x^{p^{m-n}}y^{p^{m-n}}) \text{ (by Lemma 2.2.1)} \\ &= xx^{p^{m-n}}yy^{p^{m-n}} \\ &= x^{1+p^{m-n}}y^{1+p^{m-n}}. \end{aligned}$$

From that we conclude that $[a, h] = 1$. Now,

$$hb(x) = h(x^{1+p^{m-q}}) = (x^{1+p^{m-n}})^{(1+p^{m-q})} = x^{(1+p^{m-n})(1+p^{m-q})}$$

and

$$bh(x) = b(x^{1+p^{m-n}}) = (x^{1+p^{m-q}})^{(1+p^{m-n})} = x^{(1+p^{m-n})(1+p^{m-q})}.$$

On the other hand,

$$hb(y) = h(y) = y^{1+p^{m-n}}$$

and

$$bh(y) = b(y^{1+p^{m-n}}) = y^{1+p^{m-n}}.$$

Thus $[b, h] = 1$. Now,

$$hd(x) = h(xy^{p^{t-n}}) = x^{1+p^{m-n}}(y^{1+p^{m-n}})^{p^{t-n}} = x^{1+p^{m-n}}y^{p^{t-n}+p^{t+m-2n}}$$

and

$$dh(x) = d(x^{1+p^{m-n}}) = (xy^{p^{t-n}})^{1+p^{m-n}} = x^{1+p^{m-n}}y^{p^{t-n}+p^{t+m-2n}}.$$

On the other hand,

$$hd(y) = h(y^U) = (y^{1+p^{m-n}})^U = y^{U(1+p^{m-n})}$$

and

$$dh(y) = d(y^{1+p^{m-n}}) = (y^U)^{1+p^{m-n}} = y^{U(1+p^{m-n})}.$$

Hence $[d,h] = 1$. ■

Lemma 4.1.2 gives the order of each automorphism. However much of what we want to do involves calculations in $\mathbf{Aut(P)}/\langle\mathbf{h}\rangle = \mathbf{Q}$, which is generated by $\mathbf{a}\langle\mathbf{h}\rangle = \bar{\mathbf{a}}$, $\mathbf{b}\langle\mathbf{h}\rangle = \bar{\mathbf{b}}$ and $\mathbf{d}\langle\mathbf{h}\rangle = \bar{\mathbf{d}}$. We now find the order of each $\bar{a}, \bar{b}$ and $\bar{d}$.

Lemma 4.1.4 *Let $\bar{a}, \bar{b}$ and $\bar{d}$ be as defined above. Then $ord(\bar{a}) = p^q$, $ord(\bar{b}) = p^q$ and $ord(\bar{d}) = p^n$.*

Proof. Before we proceed, we remind the reader that $x^{p^m} = 1$ and $y^{p^t} = x^{p^q}$. First we have

$$a^{p^q} \sim \begin{bmatrix} 1 & p^q \\ 0 & 1 \end{bmatrix}$$

and

$$h^{p^{t-m+n}} \sim \begin{bmatrix} (1+p^{m-n})^{p^{t-m+n}} & 0 \\ 0 & (1+p^{m-n})^{p^{t-m+n}} \end{bmatrix}.$$

Now by using Corollary 2.3.4 for an integer k,

$$\begin{aligned} (1+p^{m-n})^{p^{t-m+n}} &= 1 + p^t + kp^{t+m-n} \\ &\equiv 1 + p^t \ (mod\ p^{t+m-q}) \end{aligned}$$

since $t+m-n > t+m-q > m$. Thus

$$h^{p^{t-m+n}}(x) = x^{1+p^t} = x$$

and

$$h^{p^{t-m+n}}(y) = y^{1+p^t} = x^{p^q}y.$$

On the other hand, $a^{p^q}(x) = x$ and $a^{p^q}(y) = x^{p^q}y$. Thus $a^{p^q} = h^{p^{t-m+n}} \in \langle h \rangle$.

We now show that $a^{p^{q-1}} \notin \langle h \rangle$. We have

$$a^{p^{q-1}}(y) = x^{p^{q-1}}y \notin \langle y \rangle.$$

On the other hand for an integer k',

$$h^{k'}(y) = y^{(1+p^{m-n})^{k'}} \in \langle y \rangle.$$

Hence $a^{p^{q-1}} \notin \langle h \rangle$ and thus we conclude that $ord(\bar{a}) = p^q$.

It is clear that $ord(\bar{b}) = p^q$.

Now we find $ord(\bar{d})$ and before we proceed we remind the reader that $U = 1 + p^{q-n}$. From Lemma 4.1.1,

$$d^{p^n} \sim \begin{bmatrix} 1 & 0 \\ p^{t-q}(U^{p^n} - 1) & U^{p^n} \end{bmatrix}.$$

From Corollary 2.3.4 for an integer ℓ,

$$U^{p^n} = (1 + p^{q-n})^{p^n} = 1 + p^q + \ell p^{n+2(q-n)} = 1 + p^q + \ell p^{2q-n}.$$

Thus

$$\begin{aligned} d^{p^n}(x) &= xy^{p^{t-q}(U^{p^n}-1)} \\ &= xy^{p^{t-q}(p^q+\ell p^{2q-n})} \\ &= xy^{p^t+\ell p^{t+q-n}} \\ &= x^{1+p^q+\ell p^{2q-n}} \\ &\in \langle x \rangle \end{aligned}$$

and

$$\begin{aligned} d^{p^n}(y) &= y^{U^{p^n}} \\ &= y^{1+p^q+\ell p^{2q-n}} \\ &\in \langle y \rangle \end{aligned}$$

which shows $d^{p^n} \in \langle h \rangle$. Now,

$$d^{p^{n-1}} \sim \begin{bmatrix} 1 & 0 \\ p^{t-q}(U^{p^{n-1}} - 1) & U^{p^{n-1}} \end{bmatrix}.$$

Also from Corollary 2.3.4 for an integer ℓ',

$$U^{p^{n-1}} = (1 + p^{q-n})^{p^{n-1}} = 1 + p^{q-1} + \ell' p^{n-1+2(q-n)} = 1 + p^{q-1} + \ell' p^{2q-n-1}.$$

Thus $d^{p^{n-1}} \notin \langle h \rangle$ as the following shows:

$$\begin{aligned} d^{p^{n-1}}(x) &= xy^{p^{t-q}(U^{p^{n-1}}-1)} \\ &= xy^{p^{t-q}(p^{q-1}+\ell' p^{2q-n-1})} \\ &= xy^{p^{t-1}+\ell' p^{t+q-n-1}} \\ &\notin \langle x \rangle. \ \blacksquare \end{aligned}$$

A number of examples obtained by doing calculation using the algebra program MAGMA [5], enable us to conjecture that all commutators involving these automorphisms, can be written as the product $d^\gamma\ b^\beta\ a^\eta\ h^\theta$ for $0 \leq \gamma < p^n$, $0 \leq \beta < p^q$, $0 \leq \eta < p^q$ and $0 \leq \theta < p^{t+n-q}$. We will show that this is the case and that in fact gives us a normal form for the elements of $Aut(P)$. Thus we find the matrix associated with this product, which is shown in the following lemma.

Lemma 4.1.5 *Let a, b, d and h be the automorphisms of P defined earlier. Then $d^\gamma\ b^\beta\ a^\eta\ h^\theta$ for $0 \leq \gamma < p^n$, $0 \leq \beta < p^q$, $0 \leq \eta < p^q$ and $0 \leq \theta < p^{t+n-q}$ can be represented as*

$$\begin{bmatrix} (1+p^{m-q})^\beta(1+p^{m-n})^\theta & \eta(1+p^{m-q})^\beta(1+p^{m-n})^\theta \\ p^{t-q}(U^\gamma-1)(1+p^{m-q})^\beta(1+p^{m-n})^\theta & H \end{bmatrix} \textit{ where}$$

$$H = (1+p^{m-n})^\theta(\eta(1+p^{m-q})^\beta p^{t-q}(U^\gamma-1)+U^\gamma).$$

Proof. We refer to Lemma 4.1.1 for the representations of a^η, b^β, d^γ and h^θ as matrices. We find it easier to calculate $h^\theta\ d^\gamma\ b^\beta\ a^\eta$ and since h is a central element of $Aut(P)$ from Lemma 4.1.3, $d^\gamma\ b^\beta\ a^\eta\ h^\theta = h^\theta\ d^\gamma\ b^\beta\ a^\eta$. Also from lemma 4.1.4, we have shown that $d^{p^n} \in \langle h \rangle$ and $a^{p^q} \in \langle h \rangle$.

In the following proof we note that $y^{p^{t-n}}$ is a central element of P from Lemma 2.3.1 as $t \geq m$. Also $p^{t-q}(U^\gamma - 1)$ is clearly a multiple of p^{t-n}. Now,

$$b^\beta a^\eta(x) = b^\beta(x) = x^{(1+p^{m-q})^\beta}.$$

Thus

$$\begin{aligned} d^\gamma b^\beta a^\eta(x) &= d^\gamma(x^{(1+p^{m-q})^\beta}) \\ &= (xy^{p^{t-q}(U^\gamma-1)})^{(1+p^{m-q})^\beta} \\ &= x^{(1+p^{m-q})^\beta} y^{p^{t-q}(U^\gamma-1)(1+p^{m-q})^\beta}. \end{aligned}$$

Hence

$$\begin{aligned}h^\theta d^\gamma b^\beta a^\eta(x) &= h^\theta(x^{(1+p^{m-q})^\beta} y^{p^{t-q}(U^\gamma-1)(1+p^{m-q})^\beta})\\ &= (x^{(1+p^{m-n})^\theta})^{(1+p^{m-q})^\beta} (y^{(1+p^{m-n})^\theta})^{p^{t-q}(U^\gamma-1)(1+p^{m-q})^\beta}\\ &= x^{(1+p^{m-q})^\beta(1+p^{m-n})^\theta} y^{(1+p^{m-q})^\beta(1+p^{m-n})^\theta p^{t-q}(U^\gamma-1)}.\end{aligned}$$

In addition,

$$\begin{aligned}b^\beta a^\eta(y) &= b^\beta(x^\eta y)\\ &= (x^{(1+p^{m-q})^\beta})^\eta y\\ &= x^{\eta(1+p^{m-q})^\beta} y.\end{aligned}$$

Thus

$$\begin{aligned}d^\gamma b^\beta a^\eta(y) &= d^\gamma(x^{\eta(1+p^{m-q})^\beta} y)\\ &= (xy^{p^{t-q}(U^\gamma-1)})^{\eta(1+p^{m-q})^\beta} (y^{U^\gamma})\\ &= x^{\eta(1+p^{m-q})^\beta} y^{p^{t-q}(U^\gamma-1)\eta(1+p^{m-q})^\beta+U^\gamma}\\ &= x^{\eta(1+p^{m-q})^\beta} y^{\eta(1+p^{m-q})^\beta p^{t-q}(U^\gamma-1)+U^\gamma}.\end{aligned}$$

Hence

$$\begin{aligned}h^\theta d^\gamma b^\beta a^\eta(y) &= h^\theta(x^{\eta(1+p^{m-q})^\beta} y^{\eta(1+p^{m-q})^\beta p^{t-q}(U^\gamma-1)+U^\gamma})\\ &= (x^{(1+p^{m-n})^\theta})^{\eta(1+p^{m-q})^\beta} (y^{(1+p^{m-n})^\theta})^{\eta(1+p^{m-q})^\beta p^{t-q}(U^\gamma-1)+U^\gamma}\\ &= x^{\eta(1+p^{m-q})^\beta(1+p^{m-n})^\theta} y^{(1+p^{m-n})^\theta(\eta(1+p^{m-q})^\beta p^{t-q}(U^\gamma-1)+U^\gamma)}. \blacksquare\end{aligned}$$

4.2 The necessary commutators

In our effort to find the centre $\zeta(Aut(P))$ of $Aut(P)$ later in Chapter 6, we need to use information regarding commutators between automorphisms a, b, d and h of P defined earlier. In this section we show that those commutators can be written as the product $d^\gamma\ b^\beta\ a^\eta\ h^\theta$ for $0 \le \gamma < p^n$, $0 \le \beta < p^q$, $0 \le \eta < p^q$ and $0 \le \theta < p^{t+n-q}$.

We first calculate commutators between a and b but before that we need the following lemma.

Lemma 4.2.1 *Let a and b be the elements of $Aut(P)$ defined earlier. Then $[b, a] = a^{cp^{m-q}}$ for $c \equiv (1 + p^{m-q})^{-1}$ (mod p^m) and hence $\langle a, b\rangle$ is metabelian.*

Proof. As defined earlier,

$$a \sim \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \text{ and } b \sim \begin{bmatrix} 1+p^{m-q} & 0 \\ 0 & 1 \end{bmatrix}.$$

We have

$$ba(x) = b(x) = x^{1+p^{m-q}}.$$

Thus

$$a^{-1}ba(x) = a^{-1}(x^{1+p^{m-q}}) = x^{1+p^{m-q}}.$$

It follows that

$$b^{-1}a^{-1}ba(x) = b^{-1}(x^{1+p^{m-q}}) = \left(x^{(1+p^{m-q})^{-1}}\right)^{1+p^{m-q}} = x.$$

In addition,

$$ba(y) = b(xy) = x^{1+p^{m-q}}y.$$

Thus

$$a^{-1}ba(y) = a^{-1}(x^{1+p^{m-q}}y) = x^{1+p^{m-q}}x^{-1}y = x^{p^{m-q}}y.$$

It follows that

$$b^{-1}a^{-1}ba(y) = b^{-1}(x^{p^{m-q}}y) = \left(x^{(1+p^{m-q})^{-1}}\right)^{p^{m-q}} y.$$

Hence

$$[b,a] \sim \begin{bmatrix} 1 & (1+p^{m-q})^{-1}(p^{m-q}) \\ 0 & 1 \end{bmatrix}$$

so that

$$[b,a] = a^{(1+p^{m-q})^{-1}(p^{m-q})} = a^{cp^{m-q}}$$

for $c \equiv (1+p^{m-q})^{-1}$ $(mod\ p^m)$ and thus $\langle a, b\rangle$ is metabelian. ■

We remind the reader that the following identity holds in any metabelian group G. For any positive integer k and $v, w \in G$,

$$[v, w^k] = \prod_{1 \le i \le k} [v, iw]^{\binom{k}{i}}.$$

Lemma 4.2.2 *Let a and b be the elements of $Aut(P)$ defined earlier. Then for $c \equiv (1+p^{m-q})^{-1}$ $(mod\ p^m)$ and v an integer such that $0 < v < p^q$,*

i) $[a^v, b] = a^{-vcp^{m-q}}$,
ii) $[a, b^v] = a^{(1-cp^{m-q})^v-1}$.

Proof. Before proceeding we remind the reader that $[b, ia]$ means $[b, \underbrace{a, a, ..., a}_{i\ times}]$.

i) $[a^v, b] = [b, a^v]^{-1}$. Now,

$$\begin{aligned} [b, a^v] &= \prod_{1 \le i \le v} [b, ia]^{\binom{v}{i}} \\ &= [b, a]^{\binom{v}{1}} [b, 2a]^{\binom{v}{2}} ... [b, va]^{\binom{v}{v}} \\ &= [b, a]^v \\ &= a^{vcp^{m-q}} \end{aligned}$$

for $c \equiv (1 + p^{m-q})^{-1}$ $(mod\ p^m)$ and therefore

$$[a^v, b] = a^{-vcp^{m-q}}. \tag{4.1}$$

ii) We first show by induction that $[a, \ell b] = a^{(-1)^\ell (cp^{m-q})^\ell}$ for any positive integer $\ell \geq 1$. For $\ell = 1$,

$$[a, b] = [b, a]^{-1} = \left(a^{cp^{m-q}}\right)^{-1} = a^{-cp^{m-q}}.$$

Now assume $[a, \ell b] = a^{(-1)^\ell (cp^{m-q})^\ell}$ for any positive integer $\ell > 1$. Thus

$$\begin{aligned} [a, (\ell + 1)b] &= [a, \ell b, b] \\ &= [a^{(-1)^\ell (cp^{m-q})^\ell}, b] \\ &= a^{(-1)(-1)^\ell (cp^{m-q})^\ell (cp^{m-q})} \text{ (by (4.1))} \\ &= a^{(-1)^{\ell+1} (cp^{m-q})^{\ell+1}} \end{aligned}$$

and hence the result is proved inductively. Now,

$$\begin{aligned} [a, b^v] &= \prod_{1 \le i \le v} [a, ib]^{\binom{v}{i}} \\ &= [a, b]^{\binom{v}{1}} [a, 2b]^{\binom{v}{2}} [a, 3b]^{\binom{v}{3}} \ . \ . \ . \ [a, vb]^{\binom{v}{v}} \\ &= a^{-vcp^{m-q}} \left(a^{(cp^{m-q})^2}\right)^{\binom{v}{2}} \left(a^{-(cp^{m-q})^3}\right)^{\binom{v}{3}} . \ . \ . \ a^{(-1)^v (cp^{m-q})^v} \\ &= a^{(1-cp^{m-q})^v-1}. \ \blacksquare \end{aligned}$$

We now calculate commutators between b and d which are more complicated.

Lemma 4.2.3 *Let b and d be the elements of $Aut(P)$ defined earlier. Then*

$$[b^\mu, d^\chi] \sim \begin{bmatrix} 1 & 0 \\ p^{t-q}(U^{-\chi}-1)((1+p^{m-q})^\mu - 1) & 1 \end{bmatrix}$$

for $0 < \mu < p^q$ and $0 < \chi < p^n$.

Proof. From Lemma 4.1.1,

$$b^\mu \sim \begin{bmatrix} (1+p^{m-q})^\mu & 0 \\ 0 & 1 \end{bmatrix} \text{ and } (b^\mu)^{-1} \sim \begin{bmatrix} (1+p^{m-q})^{-\mu} & 0 \\ 0 & 1 \end{bmatrix}.$$

Also,

$$d^\chi \sim \begin{bmatrix} 1 & 0 \\ p^{t-q}(U^\chi - 1) & U^\chi \end{bmatrix} \text{ and } (d^\chi)^{-1} \sim \begin{bmatrix} 1 & 0 \\ p^{t-q}(U^{-\chi} - 1) & U^{-\chi} \end{bmatrix}.$$

In the following proof we note that $y^{p^{t-n}}$ is a central element of P from Lemma 2.3.1 as $t \geq m$. Note also that $y^{p^{t-q}(U^{-\chi}-1)}$ is a central element of P since p^{t-n} divides $p^{t-q}(U^{-\chi}-1)$. Now,

$$b^\mu d^\chi(x) = b^\mu(xy^{p^{t-q}(U^\chi-1)}) = x^{(1+p^{m-q})^\mu} y^{p^{t-q}(U^\chi-1)}$$

and thus

$$\begin{aligned}
&(d^\chi)^{-1} b^\mu d^\chi(x) \\
&= (d^\chi)^{-1}(x^{(1+p^{m-q})^\mu} y^{p^{t-q}(U^\chi-1)}) \\
&= (xy^{p^{t-q}(U^{-\chi}-1)})^{(1+p^{m-q})^\mu} (y^{U^{-\chi}})^{p^{t-q}(U^\chi-1)} \\
&= x^{(1+p^{m-q})^\mu} y^{p^{t-q}(U^{-\chi}-1)(1+p^{m-q})^\mu + p^{t-q}(1-U^{-\chi})} \\
&= x^{(1+p^{m-q})^\mu} y^{p^{t-q}(U^{-\chi}-1)((1+p^{m-q})^\mu - 1)}.
\end{aligned}$$

It follows that

$$\begin{aligned}
&(b^\mu)^{-1}(d^\chi)^{-1} b^\mu d^\chi(x) \\
&= (b^\mu)^{-1}(x^{(1+p^{m-q})^\mu} y^{p^{t-q}(U^{-\chi}-1)((1+p^{m-q})^\mu-1)}) \\
&= (x^{(1+p^{m-q})^{-\mu}})^{(1+p^{m-q})^\mu} y^{p^{t-q}(U^{-\chi}-1)((1+p^{m-q})^\mu-1)} \\
&= xy^{p^{t-q}(U^{-\chi}-1)((1+p^{m-q})^\mu-1)}.
\end{aligned}$$

Now,

$$b^{\mu}d^{\chi}(y) = b^{\mu}(y^{U^{\chi}}) = y^{U^{\chi}}.$$

Thus

$$(d^{\chi})^{-1}b^{\mu}d^{\chi}(y) = (d^{\chi})^{-1}(y^{U^{\chi}}) = \left(y^{U^{-\chi}}\right)^{U^{\chi}} = y.$$

It follows that

$$(b^{\mu})^{-1}(d^{\chi})^{-1}b^{\mu}d^{\chi}(y) = (b^{\mu})^{-1}(y) = y. \blacksquare$$

The following theorem shows that $[b^{\mu}, d^{\chi}]$ can be written as the product $d^{\gamma}b^{\beta}h^{\theta}$.

Theorem 4.2.4 *Let b, d and h be the elements of $Aut(P)$ defined earlier and $U = 1 + p^{q-n}$. Then*

$$[b^{\mu}, d^{\chi}] = d^{\gamma}b^{\beta}h^{\theta}$$

for $0 \leq \gamma < p^n$, $0 \leq \beta < p^q$, $0 \leq \theta < p^{t+n-q}$, $0 < \mu < p^q$ and $0 < \chi < p^n$ where

i) γ is the solution modulo p^m to the congruence

$$U^{\gamma} - 1 \equiv (U^{-\chi} - 1)((1 + p^{m-q})^{\mu} - 1),$$

ii) θ is the solution modulo p^{t+m-q} to the congruence

$$U^{\gamma}(1 + p^{m-n})^{\theta} \equiv 1 \text{ and}$$

iii) β is the solution modulo p^m to the congruence

$$(1 + p^{m-q})^{\beta}(1 + p^{m-n})^{\theta} \equiv 1.$$

Proof. As a special case of Lemma 4.1.5,

$$d^{\gamma}b^{\beta}h^{\theta} \sim \begin{bmatrix} (1 + p^{m-q})^{\beta}(1 + p^{m-n})^{\theta} & 0 \\ p^{t-q}(U^{\gamma} - 1)(1 + p^{m-q})^{\beta}(1 + p^{m-n})^{\theta} & U^{\gamma}(1 + p^{m-n})^{\theta} \end{bmatrix}.$$

Let γ, θ and β be the solutions to the respective congruences as in the hypothesis. From Lemma 4.2.3,

$$[b^{\mu}, d^{\chi}] \sim \begin{bmatrix} 1 & 0 \\ p^{t-q}(U^{-\chi} - 1)((1 + p^{m-q})^{\mu} - 1) & 1 \end{bmatrix}.$$

From our hypothesis (iii),

$$(1+p^{m-q})^{\beta}(1+p^{m-n})^{\theta} \equiv 1 \ (mod \ p^m)$$

so that the entries of the top left corner of both our matrix notations above are equal. Now from (i),

$$U^{\gamma} - 1 \equiv (U^{-\chi} - 1)((1+p^{m-q})^{\mu} - 1) \ (mod \ p^m).$$

Hence **modulo $\mathbf{p^{t+m-q}}$**

$$\begin{aligned}(p^{t-q})(U^{-\chi} - 1)((1+p^{m-q})^{\mu} - 1) &\equiv (p^{t-q})(U^{\gamma} - 1)\\ &\equiv (p^{t-q})(U^{\gamma} - 1)(1+p^{m-q})^{\beta}(1+p^{m-n})^{\theta}\end{aligned}$$

by using (iii). Thus the entries of the bottom left corner of both our matrix notations above are equal. Now from (ii),

$$U^{\gamma}(1+p^{m-n})^{\theta} \equiv 1 \ (mod \ p^{t+m-q}).$$

Thus the entries of the bottom right corner of both our matrix notations above are equal. ■

Calculating commutators between a and d are the most complicated. We repeat the same process as before.

Lemma 4.2.5 *Let a and d be the elements of $Aut(P)$ defined earlier. Then $[a^{\mu}, d^{\chi}]$ can be represented as*

$$\begin{bmatrix} 1+\mu p^{t-q}(U^{\chi}-1)(1-\mu p^{t-q}(U^{-\chi}-1)) & T \\ \mu p^{2t-2q}(U^{\chi}-1)(U^{-\chi}-1) & 1+\mu p^{t-q}(U^{-\chi}-1)\Lambda(1,U^{\chi}) \end{bmatrix}$$

for $0 < \mu < p^q$ and $0 < \chi < p^n$, where

$$T = \mu(\Lambda(1,U^{\chi}) - 1) - \mu^2 p^{t-q}(U^{-\chi}-1)\Lambda(1,U^{\chi}).$$

Proof. From Lemma 4.1.1,

$$d^{\chi} \sim \begin{bmatrix} 1 & 0 \\ p^{t-q}(U^{\chi}-1) & U^{\chi} \end{bmatrix} \text{ and } (d^{\chi})^{-1} \sim \begin{bmatrix} 1 & 0 \\ p^{t-q}(U^{-\chi}-1) & U^{-\chi} \end{bmatrix}.$$

Also,

$$a^\mu \sim \begin{bmatrix} 1 & \mu \\ 0 & 1 \end{bmatrix} \text{ and } (a^\mu)^{-1} \sim \begin{bmatrix} 1 & -\mu \\ 0 & 1 \end{bmatrix}.$$

In the following calculations we use extensively the fact that $x^{p^{m-n}}$ and $y^{p^{m-n}}$ are central elements of P, which is from Lemma 2.3.1. Since $t \geq m$ in cases 1 and 2, $x^{p^{t-n}}$ and $y^{p^{t-n}}$ are central elements of P. Note also that $x^{p^{t-q}(U^\chi-1)}$ and $y^{p^{t-q}(U^\chi-1)}$ are central elements of P since p^{t-n} divides $p^{t-q}(U^\chi - 1)$. Hence,

$$\begin{aligned} a^\mu d^\chi(x) &= a^\mu(xy^{p^{t-q}(U^\chi-1)}) \\ &= x(x^\mu y)^{p^{t-q}(U^\chi-1)} \\ &= xx^{\mu p^{t-q}(U^\chi-1)}y^{p^{t-q}(U^\chi-1)} \text{ (by Lemma 2.2.1)} \\ &= x^{1+\mu p^{t-q}(U^\chi-1)}y^{p^{t-q}(U^\chi-1)} \end{aligned}$$

and thus

$$\begin{aligned} &(d^\chi)^{-1}a^\mu d^\chi(x) \\ &= (d^\chi)^{-1}(x^{1+\mu p^{t-q}(U^\chi-1)}y^{p^{t-q}(U^\chi-1)}) \\ &= (xy^{p^{t-q}(U^{-\chi}-1)})^{(1+\mu p^{t-q}(U^\chi-1))}(y^{U^{-\chi}})^{p^{t-q}(U^\chi-1)} \\ &= x^{1+\mu p^{t-q}(U^\chi-1)}y^{p^{t-q}(U^{-\chi}-1)(1+\mu p^{t-q}(U^\chi-1))+p^{t-q}(1-U^{-\chi})} \\ &= x^{1+\mu p^{t-q}(U^\chi-1)}y^{p^{t-q}(U^{-\chi}-1)(1+\mu p^{t-q}(U^\chi-1)-1)} \\ &= x^{1+\mu p^{t-q}(U^\chi-1)}y^{p^{t-q}(U^{-\chi}-1)(\mu p^{t-q}(U^\chi-1))} \\ &= x^{1+\mu p^{t-q}(U^\chi-1)}y^{\mu p^{2t-2q}(U^{-\chi}-1)(U^\chi-1)}. \end{aligned}$$

It follows that

$$\begin{aligned} &(a^\mu)^{-1}(d^\chi)^{-1}a^\mu d^\chi(x) \\ &= (a^\mu)^{-1}(x^{1+\mu p^{t-q}(U^\chi-1)}y^{\mu p^{2t-2q}(U^{-\chi}-1)(U^\chi-1)}) \\ &= x^{1+\mu p^{t-q}(U^\chi-1)}(x^{-\mu}y)^{\mu p^{2t-2q}(U^{-\chi}-1)(U^\chi-1)} \\ &= x^{1+\mu p^{t-q}(U^\chi-1)-\mu^2p^{2(t-q)}(U^{-\chi}-1)(U^\chi-1)}y^{\mu p^{2t-2q}(U^\chi-1)(U^{-\chi}-1)} \text{ (by using Lemma 2.2.1)} \\ &= x^{1+\mu p^{t-q}(U^\chi-1)(1-\mu p^{t-q}(U^{-\chi}-1))}y^{\mu p^{2t-2q}(U^\chi-1)(U^{-\chi}-1)}. \end{aligned}$$

Now,

$$a^\mu d^\chi(y) = a^\mu(y^{U^\chi}) = (x^\mu y)^{U^\chi} = x^{\mu\Lambda(1,U^\chi)}y^{U^\chi}$$

by using Lemma 2.2.5. Thus

$$\begin{aligned}
&(d^{\chi})^{-1}a^{\mu}d^{\chi}(y)\\
&= (d^{\chi})^{-1}(x^{\mu\Lambda(1,U^{\chi})}y^{U^{\chi}})\\
&= (xy^{p^{t-q}(U^{-\chi}-1)})^{\mu\Lambda(1,U^{\chi})}(y^{U^{-\chi}})^{U^{\chi}}\\
&= x^{\mu\Lambda(1,U^{\chi})}y^{1+\mu p^{t-q}(U^{-\chi}-1)\Lambda(1,U^{\chi})}.
\end{aligned}$$

It follows that

$$\begin{aligned}
&(a^{\mu})^{-1}(d^{\chi})^{-1}a^{\mu}d^{\chi}(y)\\
&= (a^{\mu})^{-1}(x^{\mu\Lambda(1,U^{\chi})}y^{1+\mu p^{t-q}(U^{-\chi}-1)\Lambda(1,U^{\chi})})\\
&= x^{\mu\Lambda(1,U^{\chi})}(x^{-\mu}y)^{1+\mu p^{t-q}(U^{-\chi}-1)\Lambda(1,U^{\chi})}\\
&= x^{\mu\Lambda(1,U^{\chi})}(x^{-\mu}y)(x^{-\mu}y)^{\mu p^{t-q}(U^{-\chi}-1)\Lambda(1,U^{\chi})}\\
&= x^{\mu\Lambda(1,U^{\chi})-\mu}yx^{-\mu^2p^{t-q}(U^{-\chi}-1)\Lambda(1,U^{\chi})}y^{\mu p^{t-q}(U^{-\chi}-1)\Lambda(1,U^{\chi})} \text{ (by using Lemma 2.2.1)}\\
&= x^{\mu(\Lambda(1,U^{\chi})-1)}x^{-\mu^2p^{t-q}(U^{-\chi}-1)\Lambda(1,U^{\chi})}y^{1+\mu p^{t-q}(U^{-\chi}-1)\Lambda(1,U^{\chi})}\\
&= x^{\mu(\Lambda(1,U^{\chi})-1)-\mu^2p^{t-q}(U^{-\chi}-1)\Lambda(1,U^{\chi})}y^{1+\mu p^{t-q}(U^{-\chi}-1)\Lambda(1,U^{\chi})}. \blacksquare
\end{aligned}$$

The steps in the following theorem are similar to the previous one.

Theorem 4.2.6 *Let a, b, d and h be the elements of $Aut(P)$ defined earlier and $U = 1 + p^{q-n}$. Then*

$$[a^{\mu}, d^{\chi}] = d^{\gamma}b^{\beta}a^{\eta}h^{\theta}$$

for $0 \le \gamma < p^n$, $0 \le \beta < p^q$, $0 \le \eta < p^q$, $0 \le \theta < p^{t+n-q}$, $0 < \mu < p^q$ and $0 < \chi < p^n$ where

i) γ is the solution modulo p^m to the congruence

$$(U^{\gamma} - 1)(1 + \mu p^{t-q}(U^{\chi} - 1)(1 - \mu p^{t-q}(U^{-\chi} - 1))) \equiv \mu p^{t-q}(U^{\chi} - 1)(U^{-\chi} - 1),$$

ii) θ is the solution modulo p^{t+m-q} to the congruence

$$U^{\gamma}((1 + p^{m-n})^{\theta} + Tp^{t-q}) \equiv 1 + p^{t-q}(T + \mu(U^{-\chi} - 1)\Lambda(1, U^{\chi}))$$

where

$$T = \mu(\Lambda(1, U^{\chi}) - 1) - \mu^2p^{t-q}(U^{-\chi} - 1)\Lambda(1, U^{\chi}),$$

iii) β is the solution modulo p^m to the congruence

$$(1+p^{m-q})^{\beta}(1+p^{m-n})^{\theta} \equiv 1+\mu p^{t-q}(U^{\chi}-1)(1-\mu p^{t-q}(U^{-\chi}-1)) \text{ and}$$

iv) η is the solution modulo p^m to the congruence

$$\eta(1+\mu p^{t-q}(U^{\chi}-1)(1-\mu p^{t-q}(U^{-\chi}-1))) \equiv T.$$

Proof. From Lemma 4.1.5, $d^{\gamma}\, b^{\beta}\, a^{\eta}\, h^{\theta}$ can be represented as

$$\begin{bmatrix} (1+p^{m-q})^{\beta}(1+p^{m-n})^{\theta} & \eta(1+p^{m-q})^{\beta}(1+p^{m-n})^{\theta} \\ p^{t-q}(U^{\gamma}-1)(1+p^{m-q})^{\beta}(1+p^{m-n})^{\theta} & H \end{bmatrix}.$$

where

$$H = (1+p^{m-n})^{\theta}(\eta(1+p^{m-q})^{\beta}p^{t-q}(U^{\gamma}-1)+U^{\gamma}).$$

Let γ, θ, β and η be the solutions to the respective congruences as in the hypothesis.

From Lemma 4.2.5, $[a^{\mu}, d^{\chi}]$ can be represented as

$$\begin{bmatrix} 1+\mu p^{t-q}(U^{\chi}-1)(1-\mu p^{t-q}(U^{-\chi}-1)) & T \\ \mu p^{2t-2q}(U^{\chi}-1)(U^{-\chi}-1) & 1+\mu p^{t-q}(U^{-\chi}-1)\Lambda(1,U^{\chi}) \end{bmatrix}$$

where

$$T = \mu(\Lambda(1,U^{\chi})-1) - \mu^2 p^{t-q}(U^{-\chi}-1)\Lambda(1,U^{\chi}).$$

From our hypothesis (iii),

$$(1+p^{m-q})^{\beta}(1+p^{m-n})^{\theta} \equiv 1+\mu p^{t-q}(U^{\chi}-1)(1-\mu p^{t-q}(U^{-\chi}-1)) \ (mod\ p^m)$$

so that the entries of the top left corner of both our matrix notations above are equal.

Now as in (i), let γ be the solution **modulo $\mathbf{p^m}$** to the congruence

$$(U^{\gamma}-1)(1+\mu p^{t-q}(U^{\chi}-1)(1-\mu p^{t-q}(U^{-\chi}-1))) \equiv \mu p^{t-q}(U^{\chi}-1)(U^{-\chi}-1).$$

Thus **modulo $\mathbf{p^{t+m-q}}$**,

$$\begin{aligned} & p^{t-q}(U^{\gamma}-1)(1+\mu p^{t-q}(U^{\chi}-1)(1-\mu p^{t-q}(U^{-\chi}-1))) \\ & \equiv p^{t-q}\mu p^{t-q}(U^{\chi}-1)(U^{-\chi}-1). \end{aligned}$$

Hence

$$\begin{aligned}&\mu p^{2t-2q}(U^{\chi}-1)(U^{-\chi}-1)\\ &\equiv p^{t-q}(U^{\gamma}-1)(1+\mu p^{t-q}(U^{\chi}-1)(1-\mu p^{t-q}(U^{-\chi}-1)))\\ &\equiv p^{t-q}(U^{\gamma}-1)(1+p^{m-q})^{\beta}(1+p^{m-n})^{\theta} \text{ (by using (iii))}\end{aligned}$$

so that the entries of the bottom left corner of both our matrix notations above are equal.

Now as in (iv), let η be the solution **modulo $\mathbf{p^m}$** to the congruence

$$\eta(1+\mu p^{t-q}(U^{\chi}-1)(1-\mu p^{t-q}(U^{-\chi}-1)))\equiv T.$$

Thus by using (iii) and calculating **modulo $\mathbf{p^m}$**,

$$\eta(1+p^{m-q})^{\beta}(1+p^{m-n})^{\theta}\equiv T$$

so that the entries of the top right corner of both our matrix notations above are equal.

Now as in (ii), let θ be the solution **modulo $\mathbf{p^{t+m-q}}$** to the congruence

$$U^{\gamma}((1+p^{m-n})^{\theta}+Tp^{t-q})\equiv 1+p^{t-q}(T+\mu(U^{-\chi}-1)\Lambda(1,U^{\chi})).$$

Thus

$$U^{\gamma}(1+p^{m-n})^{\theta}+U^{\gamma}Tp^{t-q}-Tp^{t-q}\equiv 1+\mu p^{t-q}(U^{-\chi}-1)\Lambda(1,U^{\chi}).$$

Hence calculating **modulo $\mathbf{p^{t+m-q}}$** we have

$$Tp^{t-q}(U^{\gamma}-1)+U^{\gamma}(1+p^{m-n})^{\theta}\equiv 1+\mu p^{t-q}(U^{-\chi}-1)\Lambda(1,U^{\chi}).$$

But from above,

$$T\equiv\eta(1+p^{m-q})^{\beta}(1+p^{m-n})^{\theta}\ (mod\ p^{m}).$$

It follows that

$$\begin{aligned}&\eta(1+p^{m-q})^{\beta}(1+p^{m-n})^{\theta}p^{t-q}(U^{\gamma}-1)+U^{\gamma}(1+p^{m-n})^{\theta}\\ &\equiv 1+\mu p^{t-q}(U^{-\chi}-1)\Lambda(1,U^{\chi})\end{aligned}$$

and thus the entries of the bottom right corner of both our matrix notations above are equal. ■

Chapter 5

Product of subgroups

Curran [7] wrote $Aut(P)$ as a product of subgroups where he used similar generators of $Aut(P)$ as ours. However in this thesis, we have a central element $h \sim \begin{bmatrix} 1+p^{m-n} & 0 \\ 0 & 1+p^{m-n} \end{bmatrix}$ of $Aut(P)$ which we can choose as one of the generators of $Aut(P)$.

This choice of generator has simplified our study of the structure of $Aut(P)$ and allows us to write $Aut(P)$ as an ascending sequence of subgroups, each a product of a cyclic group with the previous. It follows that we are able to write each element of $Aut(P)$ in normal form, as we will show in this chapter. From that, we find the upper central series and hence the class of $Aut(P)$, as shown in Chapter 7.

Before we proceed we remind the reader that these automorphisms have the following meaning.

$$a \sim \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, b \sim \begin{bmatrix} 1+p^{m-q} & 0 \\ 0 & 1 \end{bmatrix}, d \sim \begin{bmatrix} 1 & 0 \\ p^{t-n} & U \end{bmatrix} \text{ and } h \sim \begin{bmatrix} 1+p^{m-n} & 0 \\ 0 & 1+p^{m-n} \end{bmatrix}.$$

We start by first studying the subgroup $\langle a, h \rangle$.

Lemma 5.0.1 *If a and h are the automorphisms of P defined earlier then $\langle a, h \rangle = \langle a \rangle \langle h \rangle$, and each element of $\langle a, h \rangle$ can be written in normal form as $a^{\eta} h^{\theta}$ for $0 \le \eta < p^q$ and $0 \le \theta < p^{t+n-q}$.*

Proof.

Since $\langle a, h \rangle$ is abelian where $[h, a] = 1$ by Lemma 4.1.3, $\langle a, h \rangle = \langle a \rangle \langle h \rangle$. From Lemma 4.1.4,

$$\langle a \rangle \cap \langle h \rangle = \langle a^{p^q} \rangle = \langle h^{p^{t-m+n}} \rangle,$$

and the result follows from Lemma 2.3.8. ■

We now prove one of our major results in this thesis. We show that $Aut(P)$ can be written as the product $\langle d\rangle\langle b,a,h\rangle$. This also implies that a, b, d and h are generators of $Aut(P)$. Furthermore, we also show that each element of $Aut(P)$ can be written in normal form in terms of these generators.

Theorem 5.0.2 *If a, b, d and h are the automorphisms of P defined earlier then*

a) any element of $\langle b,a,h\rangle$ can be written in normal form as $b^{\beta}a^{\eta}h^{\theta}$ for $0 \leq \beta < p^q$, $0 \leq \eta < p^q$ and $0 \leq \theta < p^{t+n-q}$ where

i) $\langle b\rangle \cap \langle a,h\rangle = 1$ and

ii) $\langle b,a,h\rangle = \langle b\rangle\langle a\rangle\langle h\rangle$.

b) any element of $Aut(P)$ can be written in normal form as $d^{\gamma}\ b^{\beta}\ a^{\eta}\ h^{\theta}$ for $0 \leq \gamma < p^n$, $0 \leq \beta < p^q$, $0 \leq \eta < p^q$ and $0 \leq \theta < p^{t+n-q}$ where

i) $\langle d\rangle \cap \langle b,a,h\rangle = \langle d^{p^n}\rangle$ and

ii) $Aut(P) = \langle d\rangle\langle b,a,h\rangle$.

Proof. We remind the reader that $x^{p^m} = 1$ and $y^{p^t} = x^{p^q}$.

a)

i) First we find the intersection $\langle b\rangle \cap \langle a,h\rangle$. From Lemma 4.1.1 for $0 \leq \beta < p^q$,

$$b^{\beta} \sim \begin{bmatrix} (1+p^{m-q})^{\beta} & 0 \\ 0 & 1 \end{bmatrix}$$

and for $0 \leq \eta < p^q$ and $0 \leq \theta < p^{t+n-q}$, a straight forward calculation shows

$$a^{\eta}h^{\theta} \sim \begin{bmatrix} (1+p^{m-n})^{\theta} & \eta(1+p^{m-n})^{\theta} \\ 0 & (1+p^{m-n})^{\theta} \end{bmatrix}.$$

But

$$\eta(1+p^{m-n})^{\theta} \not\equiv 0\ (mod\ p^q)$$

since $0 \leq \eta < p^q$. Hence if $a^{\eta}h^{\theta} \neq 1$ then

$$\begin{aligned} a^{\eta}h^{\theta}(y) &= x^{\eta(1+p^{m-n})^{\theta}}y^{(1+p^{m-n})^{\theta}} \\ &\notin \langle y\rangle. \end{aligned}$$

On the other hand,

$$b^{\beta}(y) = y \in \langle y\rangle.$$

It follows that $b^{\beta}(y) \neq a^{\eta}h^{\theta}(y)$ and thus $b^{\beta} \neq a^{\eta}h^{\theta}$. Therefore $\langle b\rangle \cap \langle a,h\rangle = 1$.

ii) Since a is normalised by b from Lemma 4.2.1 and h is central from Lemma 4.1.3 we have,

$$\langle b, a, h\rangle = \langle b\rangle\langle a, h\rangle = \langle b\rangle\langle a\rangle\langle h\rangle$$

as $\langle a, h\rangle = \langle a\rangle\langle h\rangle$ by Lemma 5.0.1. Therefore by Lemma 2.3.8 we can write any element of $\langle b, a, h\rangle$ uniquely as a product of an element of $\langle b\rangle$ and an element of $\langle a, h\rangle$ as described.

b)

i) By Lemma 4.1.4, $d^{p^n} \in \langle h\rangle$ which means $d^{p^n} \in \langle b, a, h\rangle$. Now we show that $d^{p^{n-1}} \notin \langle b, a, h\rangle$. As a special case of Lemma 4.1.5 we have

$$b^\beta a^\eta h^\theta \sim \begin{bmatrix} (1+p^{m-q})^\beta(1+p^{m-n})^\theta & \eta(1+p^{m-q})^\beta(1+p^{m-n})^\theta \\ 0 & (1+p^{m-n})^\theta \end{bmatrix}$$

and from Lemma 4.1.1,

$$d^{p^{n-1}} \sim \begin{bmatrix} 1 & 0 \\ p^{t-q}(U^{p^{n-1}}-1) & U^{p^{n-1}} \end{bmatrix}.$$

Also from Corollary 2.3.4 for an integer k,

$$U^{p^{n-1}} = (1+p^{q-n})^{p^{n-1}} = 1 + p^{q-1} + kp^{n-1+2(q-n)} = 1 + p^{q-1} + kp^{2q-n-1}.$$

Thus

$$\begin{aligned} d^{p^{n-1}}(x) &= xy^{p^{t-q}(U^{p^{n-1}}-1)} \\ &= xy^{p^{t-q}(p^{q-1}+kp^{2q-n-1})} \\ &= xy^{p^{t-1}+kp^{t+q-n-1}} \\ &\notin \langle x\rangle. \end{aligned}$$

which shows $d^{p^{n-1}} \notin \langle b, a, h\rangle$, since $b^\beta a^\eta h^\theta(x) \in \langle x\rangle$. Therefore $\langle d\rangle \cap \langle b, a, h\rangle = \langle d^{p^n}\rangle$.

ii)

$$\begin{aligned} \mid \langle d\rangle\langle b, a, h\rangle \mid &= \frac{\mid \langle d\rangle \mid\mid \langle b, a, h\rangle \mid}{\mid \langle d\rangle \cap \langle b, a, h\rangle \mid} \\ &= p^{t+2n+q} \\ &= \mid Aut(P) \mid. \end{aligned}$$

That is $\langle d\rangle\langle b,a,h\rangle$ is a subset of $Aut(P)$ with the same order of $Aut(P)$, which implies $\langle d\rangle\langle b,a,h\rangle = Aut(P)$.
By Lemma 2.3.8 we can write any element of $Aut(P)$ as described. ■

It would be nice to be able to give the normal form for a product in terms of the powers involved in the normal form of each element. This turns out to be very complicated, as the powers in the product are difficult to determine. However as mentioned before, much of what we want to do involves calculations in $Aut(P)/\langle h\rangle = Q$, which is generated by $\bar{a}$, $\bar{b}$ and $\bar{d}$. Here we need the normal form of commutators of these generators and we now calculate these forms.

Before we proceed, we need the following lemma. We remind the reader that $U = 1 + p^{q-n}$.

Lemma 5.0.3 *Let μ and χ be positive integers. If $p^\nu \parallel \mu$ and $p^\varsigma \parallel \chi$ then*

$$(U^{-\chi}-1)((1+p^{m-q})^\mu - 1) \equiv -\chi\mu p^{m-n} + \ell p^\omega \ (mod\ p^m)$$

for an integer ℓ where ω is strictly greater than the power of p dividing $-\chi\mu p^{m-n}$.

Proof. Using Corollaries 2.3.4 and 2.3.6 for integers k and k', and calculating **modulo $\mathbf{p^m}$**,

$$\begin{aligned}
&(U^{-\chi}-1)((1+p^{m-q})^\mu - 1)\\
&\equiv (-\chi p^{q-n} + kp^{\varsigma+2(q-n)})(\mu p^{m-q} + k'p^{\nu+2(m-q)})\\
&\equiv -\chi\mu p^{m-n} - \chi k' p^{\nu+2m-q-n} + \mu k p^{\varsigma+m+q-2n} + kk'p^{\varsigma+\nu+2(m-n)}\\
&\equiv -\chi\mu p^{m-n} + \ell p^\omega
\end{aligned}$$

for an integer ℓ where ω is strictly greater than the power of p dividing $-\chi\mu p^{m-n}$.
■

We now calculate γ and β.

Lemma 5.0.4 *Let a, b, d and h be the generators of $Aut(P)$ and $\bar{a}$, $\bar{b}$ and $\bar{d}$ be the generators of Q defined earlier. If as in Theorem 4.2.4 $[b^\mu, d^\chi] = d^\gamma\ b^\beta\ h^\theta$ for $0 \leq \gamma < p^n$, $0 \leq \beta < p^q$, $0 \leq \theta < p^{t+n-q}$, $0 < \mu < p^q$ and $0 < \chi < p^n$, where $p^\nu \parallel \mu$ and $p^\varsigma \parallel \chi$, then*

$$\gamma = k_1 p^{m-q+\nu+\varsigma} \text{ and } \beta = k_2 p^{q-n+\nu+\varsigma},$$

that is

$$[\bar{b}^\mu, \bar{d}^\chi] = \bar{d}^{k_1 p^{m-q+\nu+\varsigma}} \bar{b}^{k_2 p^{q-n+\nu+\varsigma}}$$

for k_1 and $k_2 \in \mathbb{Z}$, where $(k_1 k_2, p) = 1$. Similarly

$$[\bar{d}^{\chi}, \bar{b}^{\mu}] = \bar{d}^{k_1' p^{m-q+\nu+\varsigma}} \bar{b}^{k_2' p^{q-n+\nu+\varsigma}}$$

for k_1' and $k_2' \in \mathbb{Z}$, where $(k_1' k_2', p) = 1$.

Proof. Let $[b^{\mu}, d^{\chi}] = d^{\gamma}\ b^{\beta}\ h^{\theta}$ as in Theorem 4.2.4.

Assume γ and β are all nonzero and suppose $p^{\epsilon_1} \parallel \gamma$ and $p^{\epsilon_2} \parallel \beta$.

By Theorem 4.2.4(i),

$$U^{\gamma} - 1 \equiv (U^{-\chi} - 1)((1 + p^{m-q})^{\mu} - 1)\ (mod\ p^m).$$

Now on the LHS for an integer w, using Corollary 2.3.4 and calculating **modulo $\mathbf{p^m}$**,

$$\begin{aligned} U^{\gamma} - 1 &\equiv (1 + p^{q-n})^{\gamma} - 1 \\ &\equiv \gamma p^{q-n} + w p^{\epsilon_1 + 2(q-n)}. \end{aligned}$$

On the RHS by Lemma 5.0.3,

$$(U^{-\chi} - 1)((1 + p^{m-q})^{\mu} - 1) \equiv -\chi \mu p^{m-n} + \ell p^{\omega}\ (mod\ p^m)$$

for an integer ℓ where ω is strictly greater than the power of p dividing $-\chi\mu p^{m-n}$. Thus comparing the term that has the lowest nonzero exponent of p on the LHS and RHS we have

$$q - n + \epsilon_1 \equiv m - n + \nu + \varsigma\ (mod\ m) \text{ or}$$

$$\epsilon_1 \equiv m - q + \nu + \varsigma\ (mod\ m). \qquad (5.1)$$

Now by Theorem 4.2.4(iii),

$$(1 + p^{m-q})^{\beta} (1 + p^{m-n})^{\theta} \equiv 1\ (mod\ p^m).$$

But by Theorem 4.2.4(ii) we also have

$$U^{\gamma} (1 + p^{m-n})^{\theta} \equiv 1\ (mod\ p^{t+m-q}) \equiv 1\ (mod\ p^m).$$

Thus calculating **modulo $\mathbf{p^m}$** we have

$$(1 + p^{m-q})^{\beta} \equiv U^{\gamma}.$$

This implies by using Corollary 2.3.4,

$$1 + \beta p^{m-q} + z p^{\epsilon_2 + 2(m-q)} \equiv 1 + \gamma p^{q-n} + w' p^{\epsilon_1 + 2(q-n)}$$

for integers z and w'. Thus comparing the term that has the lowest nonzero exponent of p on the LHS and RHS we have **modulo m**,

$$\begin{aligned} \epsilon_2 + m - q &\equiv \epsilon_1 + q - n \\ &\equiv (m - q + \nu + \varsigma) + q - n \text{ (from (5.1))} \\ &\equiv m - n + \nu + \varsigma \end{aligned}$$

and so

$$\epsilon_2 \equiv q - n + \nu + \varsigma \ (mod\ m).$$

With similar calculations,

$$[\bar{d}^{\chi}, \bar{b}^{\mu}] = \bar{d}^{k_1' p^{m-q+\nu+\varsigma}} \bar{b}^{k_2' p^{q-n+\nu+\varsigma}}$$

for k_1' and $k_2' \in \mathbb{Z}$, where $(k_1' k_2', p) = 1$. Finally we note that if any of γ or β is zero, the proof will be similar but easier. ■

We now calculate commutators involving a and d. Before that we need the following three lemmas.

Lemma 5.0.5 *If χ is a positive integer and $p^{\varsigma} \parallel \chi$ then*

$$(U^{\chi} - 1)(U^{-\chi} - 1) \equiv -\chi^2 p^{2q-2n} + \ell p^{\omega} \ (mod\ p^m)$$

for an integer ℓ where ω is strictly greater than the power of p dividing $-\chi^2 p^{2q-2n}$.

Proof. For integers k and k' and calculating **modulo p^m**, by using Corollaries 2.3.4 and 2.3.6,

$$\begin{aligned} &(U^{\chi} - 1)(U^{-\chi} - 1) \\ &\equiv (\chi p^{q-n} + k p^{\varsigma + 2(q-n)})(-\chi p^{q-n} + k' p^{\varsigma + 2(q-n)}) \\ &\equiv -\chi^2 p^{2q-2n} + k' \chi p^{\varsigma + 3(q-n)} - k \chi p^{\varsigma + 3(q-n)} + k k' p^{2\varsigma + 4(q-n)} \\ &\equiv -\chi^2 p^{2q-2n} + \ell p^{\omega} \end{aligned}$$

for an integer ℓ where ω is strictly greater than the power of p dividing $-\chi^2 p^{2q-2n}$.
■

Lemma 5.0.6 *If χ is a positive integer and $p^{\varsigma} \parallel \chi$ then*

$$1 + \mu p^{t-q}(U^{\chi} - 1)(1 - \mu p^{t-q}(U^{-\chi} - 1)) \equiv 1 + \mu\chi p^{t-n} + \ell p^{\omega} \ (mod\ p^m)$$

for an integer ℓ where ω is strictly greater than the power of p dividing $\mu\chi p^{t-n}$.

Proof. For integers k and k' and calculating **modulo $\mathbf{p^m}$**, by using Corollaries 2.3.4 and 2.3.6,

$$\begin{aligned}
&1 + \mu p^{t-q}(U^{\chi} - 1)(1 - \mu p^{t-q}(U^{-\chi} - 1)) \\
&\equiv 1 + \mu p^{t-q}(\chi p^{q-n} + k p^{\varsigma+2(q-n)})(1 - \mu p^{t-q}(-\chi p^{q-n} + k' p^{\varsigma+2(q-n)})) \\
&\equiv 1 + (\mu\chi p^{t-n} + \mu k p^{\varsigma+t+q-2n})(1 - \mu p^{t-q}(-\chi p^{q-n} + k' p^{\varsigma+2(q-n)})) \\
&\equiv 1 + \mu\chi p^{t-n} + \ell p^{\omega}
\end{aligned}$$

for an integer ℓ where ω is strictly greater than the power of p dividing $\mu\chi p^{t-n}$. ■

Lemma 5.0.7 *If χ is a positive integer and $p^{\varsigma} \parallel \chi$ then*

$$\mu(\Lambda(1, U^{\chi}) - 1) - \mu^2 p^{t-q}(U^{-\chi} - 1)\Lambda(1, U^{\chi}) \equiv \mu\chi p^{q-n} + \ell p^{\omega} \ (mod\ p^m)$$

for an integer ℓ where ω is strictly greater than the power of p dividing $\mu\chi p^{q-n}$.

Proof. For integers e and k and calculating **modulo $\mathbf{p^m}$**, by using Corollary 2.3.6 and Lemma 2.3.7 with $\upsilon > q - n$,

$$\begin{aligned}
&\mu(\Lambda(1, U^{\chi}) - 1) - \mu^2 p^{t-q}(U^{-\chi} - 1)\Lambda(1, U^{\chi}) \\
&\equiv \mu(\chi p^{q-n} + e p^{\varsigma+\upsilon}) - \mu^2 p^{t-q}(-\chi p^{q-n} + k p^{\varsigma+2(q-n)})(1 + \chi p^{q-n} + e p^{\varsigma+\upsilon}) \\
&\equiv \mu\chi p^{q-n} + \mu e p^{\varsigma+\upsilon} + (\mu^2\chi p^{t-n} - k\mu^2 p^{\varsigma+t+q-2n})(1 + \chi p^{q-n} + e p^{\varsigma+\upsilon}) \\
&\equiv \mu\chi p^{q-n} + \ell p^{\omega}
\end{aligned}$$

for an integer ℓ where ω is strictly greater than the power of p dividing $\mu\chi p^{q-n}$. ■

We now find γ, β and η.

Lemma 5.0.8 *Let a, b, d and h be the generators of $Aut(P)$ and $\bar{a}$, $\bar{b}$, $\bar{d}$ be the generators of Q defined earlier. If as in Theorem 4.2.6 $[a^{\mu}, d^{\chi}] = d^{\gamma}\ b^{\beta}\ a^{\eta}\ h^{\theta}$ for $0 \leq \gamma < p^n$, $0 \leq \beta < p^q$, $0 \leq \eta < p^q$, $0 \leq \theta < p^{t+n-q}$, $0 < \mu < p^q$ and $0 < \chi < p^n$, where $p^{\nu} \parallel \mu$ and $p^{\varsigma} \parallel \chi$ then*

$$\gamma = k_1 p^{t-n+\nu+2\varsigma}, \beta = k_2 p^{t-m+q-n+\nu+\varsigma} \text{ and } \eta = k_3 p^{q-n+\nu+\varsigma},$$

that is

$$[\bar{a}^{\mu}, \bar{d}^{\chi}] = \bar{d}^{k_1 p^{t-n+\nu+2\varsigma}} \bar{b}^{k_2 p^{t-m+q-n+\nu+\varsigma}} \bar{a}^{k_3 p^{q-n+\nu+\varsigma}}$$

for k_1, k_2 and $k_3 \in \mathbb{Z}$ where $(k_1 k_2 k_3, p) = 1$. Similarly

$$[\bar{d}^{\chi}, \bar{a}^{\mu}] = \bar{d}^{k'_1 p^{t-n+\nu+2\varsigma}} \bar{b}^{k'_2 p^{t-m+q-n+\nu+\varsigma}} \bar{a}^{k'_3 p^{q-n+\nu+\varsigma}}$$

for k'_1, k'_2, $k'_3 \in \mathbb{Z}$ where $(k'_1 k'_2 k'_3, p) = 1$.

Proof. Let $[a^{\mu}, d^{\chi}] = d^{\gamma}\ b^{\beta}\ a^{\eta}\ h^{\theta}$ as in Theorem 4.2.6.

Assume γ, β and η are all nonzero and suppose $p^{\epsilon_1} \parallel \gamma$, $p^{\epsilon_2} \parallel \beta$ and $p^{\epsilon_3} \parallel \eta$. By Theorem 4.2.6(i),

$$(U^{\gamma}-1)(1+\mu p^{t-q}(U^{\chi}-1)(1-\mu p^{t-q}(U^{-\chi}-1))) \equiv \mu p^{t-q}(U^{\chi}-1)(U^{-\chi}-1)\ (mod\ p^m)$$

where $U = 1 + p^{q-n}$. Now, looking at the LHS and calculating **modulo $\mathbf{p^m}$**, by using Corollary 2.3.4 and Lemma 5.0.6 for integers e and ℓ, where ω is strictly greater than the power of p dividing $\mu\chi p^{t-n}$,

$$\begin{aligned}
&(U^{\gamma} - 1)(1 + \mu p^{t-q}(U^{\chi} - 1)(1 - \mu p^{t-q}(U^{-\chi} - 1))) \\
&\equiv (\gamma p^{q-n} + e p^{\epsilon_1 + 2(q-n)})(1 + \mu\chi p^{t-n} + \ell p^{\omega}) \\
&\equiv \gamma p^{q-n} + e p^{\epsilon_1 + 2(q-n)} + \ell' p^{\omega'}
\end{aligned}$$

for an integer ℓ' where ω' is strictly greater than the power of p dividing $e p^{\epsilon_1 + 2(q-n)}$.

On the other hand on the RHS and calculating **modulo $\mathbf{p^m}$**, by using Lemma 5.0.5 and for an integer ℓ'' where ω'' is strictly greater than the power of p dividing $-\chi^2 p^{2q-2n}$,

$$\begin{aligned}
\mu p^{t-q}(U^{\chi} - 1)(U^{-\chi} - 1) &\equiv \mu p^{t-q}(-\chi^2 p^{2q-2n} + \ell'' p^{\omega''}) \\
&\equiv -\mu\chi^2 p^{t+q-2n} + \ell''' p^{\omega'''}
\end{aligned}$$

for an integer ℓ''' where ω''' is strictly greater than the power of p dividing $-\mu\chi^2 p^{t+q-2n}$. So we have **modulo $\mathbf{p^m}$**,

$$\gamma p^{q-n} + e p^{\epsilon_1 + 2(q-n)} + \ell' p^{\omega'} \equiv -\mu\chi^2 p^{t+q-2n} + \ell''' p^{\omega'''}. \tag{5.2}$$

Thus comparing the term that has the lowest nonzero exponent of p on the LHS and RHS of (5.2) we have

$$q - n + \epsilon_1 \equiv t + q - 2n + \nu + 2\varsigma\ (mod\ m) \text{ or}$$

$$\epsilon_1 \equiv t - n + \nu + 2\varsigma \ (mod\ m). \tag{5.3}$$

Now by Theorem 4.2.6(ii) **modulo $\mathbf{p^{t+m-q}}$**,

$$U^{\gamma}((1+p^{m-n})^{\theta} + Tp^{t-q}) \equiv 1 + p^{t-q}(T + \mu(U^{-\chi} - 1)\Lambda(1, U^{\chi}))$$

where

$$T = \mu(\Lambda(1, U^{\chi}) - 1) - \mu^2 p^{t-q}(U^{-\chi} - 1)\Lambda(1, U^{\chi}).$$

This is equivalent to

$$(1+p^{m-n})^{\theta} + Tp^{t-q} \equiv U^{-\gamma}(1 + p^{t-q}(T + \mu(U^{-\chi} - 1)\Lambda(1, U^{\chi}))) \text{ or}$$

$$(1+p^{m-n})^{\theta} \equiv U^{-\gamma}(1 + p^{t-q}(T + \mu(U^{-\chi} - 1)\Lambda(1, U^{\chi}))) - Tp^{t-q}. \tag{5.4}$$

By Corollary 2.3.4, the LHS of (5.4) can be written as

$$1 + \theta p^{m-n} + zp^{\psi}$$

for an integer z where ψ is strictly greater than the power of p dividing θp^{m-n}. We are now focusing on the RHS of (5.4). Before we proceed, from lemma 5.0.7 we have

$$T \equiv \mu\chi p^{q-n} + kp^{\psi'} \ (mod\ p^{m})$$

for an integer k where ψ' is strictly greater than the power of p dividing $\mu\chi p^{q-n}$. Also we calculate the following by using Corollary 2.3.6 and Lemma 2.3.7 where c and c' are integers and $\upsilon > q - n$.

$$\begin{aligned} \mu p^{t-q}(U^{-\chi} - 1)\Lambda(1, U^{\chi}) &= \mu p^{t-q}(-\chi p^{q-n} + cp^{\varsigma+2(q-n)})(1 + \chi p^{q-n} + c'p^{\varsigma+\upsilon}) \\ &= (-\mu\chi p^{t-n} + c\mu p^{\varsigma+t+q-2n})(1 + \chi p^{q-n} + c'p^{\varsigma+\upsilon}) \\ &= -\mu\chi p^{t-n} + z'p^{\kappa} \end{aligned} \tag{5.5}$$

for an integer z' where κ is strictly greater than the power of p dividing $-\mu\chi p^{t-n}$. Now we observe that by using (5.3) **modulo m**,

$$\begin{aligned} \epsilon_1 + 2(q-n) &\equiv t - n + \nu + 2\varsigma + 2(q-n) \\ &\equiv t + 2q - 3n + \nu + 2\varsigma. \end{aligned} \tag{5.6}$$

Replacing this into (5.2) we have **modulo $\mathbf{p^m}$**,

$$\begin{aligned}\gamma p^{q-n} &\equiv -\mu\chi^2 p^{t+q-2n} + \ell''' p^{\omega'''} - e p^{\epsilon_1+2(q-n)} - \ell' p^{\omega'} \\ &\equiv -\mu\chi^2 p^{t+q-2n} + \ell''' p^{\omega'''} - e p^{t+2q-3n+\nu+2\varsigma} - \ell' p^{\omega'} \\ &\equiv -\mu\chi^2 p^{t+q-2n} + f p^{\xi}\end{aligned} \tag{5.7}$$

for an integer f where ξ is strictly greater than the power of p dividing $-\mu\chi^2 p^{t+q-2n}$ where ω' is strictly greater than the power of p dividing $ep^{t+2q-3n+\nu+2\varsigma}$. Now by using Corollary 2.3.6 for an integer k' and using (5.6) and (5.7), we have **modulo $\mathbf{p^m}$**,

$$\begin{aligned}U^{-\gamma} &\equiv 1 - \gamma p^{q-n} + k' p^{\epsilon_1+2(q-n)} \\ &\equiv 1 + \mu\chi^2 p^{t+q-2n} - f p^{\xi} + k' p^{\epsilon_1+2(q-n)} \\ &\equiv 1 + \mu\chi^2 p^{t+q-2n} - f p^{\xi} + k' p^{t+2q-3n+\nu+2\varsigma} \\ &\equiv 1 + \mu\chi^2 p^{t+q-2n} - f' p^{\xi'}\end{aligned} \tag{5.8}$$

for an integer f' where ξ' is strictly greater than the power of p dividing $\mu\chi^2 p^{t+q-2n}$. Therefore using (5.5) and (5.8) and for an integer e', the RHS of (5.4) can be written in **modulo $\mathbf{p^{t+m-q}}$** as

$$\begin{aligned}&(1 + \mu\chi^2 p^{t+q-2n} - f' p^{\xi'} + e' p^m)(1 + T p^{t-q} + \mu p^{t-q}(U^{-\chi} - 1)\Lambda(1, U^{\chi})) - T p^{t-q} \\ &\equiv (1 + \mu\chi^2 p^{t+q-2n} - f' p^{\xi'})(1 + T p^{t-q} + \mu p^{t-q}(U^{-\chi} - 1)\Lambda(1, U^{\chi})) - T p^{t-q} + e' p^m \\ &\equiv (1 + \mu\chi^2 p^{t+q-2n} - f' p^{\xi'})(1 + T p^{t-q} - \mu\chi p^{t-n} + z' p^{\kappa}) - T p^{t-q} + e' p^m \\ &\equiv (1 + T p^{t-q} - \mu\chi p^{t-n} + z' p^{\kappa}) + (\mu\chi^2 p^{t+q-2n} + f'' p^{\xi''}) + (-f' p^{\xi'} + f''' p^{\xi'''}) \\ &\qquad - T p^{t-q} + e' p^m \\ &\equiv 1 - \mu\chi p^{t-n} + z'' p^{\kappa'} + e' p^m\end{aligned}$$

for an integer f'' where ξ'' is strictly greater than the power of p dividing $\mu\chi^2 p^{t+q-2n}$, for an integer f''' where ξ''' is strictly greater than the power of p dividing $-f' p^{\xi'}$ and for an integer z'' where κ' is strictly greater than the power of p dividing $-\mu\chi p^{t-n}$. Thus comparing the terms on the LHS and RHS of (5.4) we have

$$\theta p^{m-n} + z p^{\psi} \equiv -\mu\chi p^{t-n} + z'' p^{\kappa'} + e' p^m \ (mod\ p^{t+m-q}). \tag{5.9}$$

Now by Theorem 4.2.6(iii),

$$(1 + p^{m-q})^{\beta}(1 + p^{m-n})^{\theta} \equiv 1 + \mu p^{t-q}(U^{\chi} - 1)(1 - \mu p^{t-q}(U^{-\chi} - 1)) \ (mod\ p^m).$$

Looking at the LHS, calculating **modulo $\mathbf{p^m}$** and using Corollary 2.3.4 for an integer e'' as well as using (5.9), we have

$$\begin{aligned}
&(1+p^{m-q})^{\beta}(1+p^{m-n})^{\theta}\\
&\equiv (1+\beta p^{m-q}+e''p^{\epsilon_2+2m-2q})(1+\theta p^{m-n}+zp^{\psi})\\
&\equiv (1+\beta p^{m-q}+e''p^{\epsilon_2+2m-2q})(1-\mu\chi p^{t-n}+z''p^{\kappa'}+e'p^{m})\\
&\equiv (1+\beta p^{m-q}+e''p^{\epsilon_2+2m-2q})(1-\mu\chi p^{t-n}+z''p^{\kappa'})\\
&\equiv 1+\beta p^{m-q}+e''p^{\epsilon_2+2m-2q}-\mu\chi p^{t-n}+wp^{\tau'}
\end{aligned}$$

for an integer w where τ' is strictly greater than the power of p dividing $-\mu\chi p^{t-n}$. On the other hand on the RHS, calculating **modulo $\mathbf{p^m}$** and by Lemma 5.0.6

$$\begin{aligned}
&1+\mu p^{t-q}(U^{\chi}-1)(1-\mu p^{t-q}(U^{-\chi}-1))\\
&\equiv 1+\mu\chi p^{t-n}+w'p^{\sigma}
\end{aligned}$$

for an integer w' where σ is strictly greater than power of p dividing $\mu\chi p^{t-n}$. Thus comparing the terms on the LHS and RHS we have

$$\beta p^{m-q}+e''p^{\epsilon_2+2m-2q}-\mu\chi p^{t-n}+wp^{\tau'}\equiv \mu\chi p^{t-n}+w'p^{\sigma}\ (mod\ p^{m}).$$

Calculating **modulo $\mathbf{p^m}$**, this is equivalent to

$$\beta p^{m-q}+e''p^{\epsilon_2+2m-2q}\equiv 2\mu\chi p^{t-n}+w''p^{\sigma'}$$

for an integer w'' where σ' is strictly greater than the power of p dividing $\mu\chi p^{t-n}$. It follows that by comparing the term that has the lowest nonzero exponent of p on the LHS and RHS we have

$$m-q+\epsilon_2\equiv t-n+\nu+\varsigma\ (mod\ m)$$

or

$$\epsilon_2\equiv t-m+q-n+\nu+\varsigma\ (mod\ m).$$

Now by Theorem 4.2.6(iv) **modulo $\mathbf{p^m}$**,

$$\eta(1+\mu p^{t-q}(U^{\chi}-1)(1-\mu p^{t-q}(U^{-\chi}-1)))\equiv T.$$

Now looking at the RHS and calculating **modulo $\mathbf{p^m}$**, by Lemma 5.0.7 as seen earlier,

$$T \equiv \mu\chi p^{q-n} + kp^{\psi'} \ (mod\ p^m)$$

for an integer k where ψ' is strictly greater than the power of p dividing $\mu\chi p^{q-n}$. Thus comparing the term that has the lowest nonzero exponent of p on the LHS and RHS we have

$$\epsilon_3 \equiv q - n + \nu + \varsigma \ (mod\ m).$$

With similar calculations,

$$[\bar{d}^{\chi}, \bar{a}^{\mu}] = \bar{d}^{k_1' p^{t-n+\nu+2\varsigma}} \bar{b}^{k_2' p^{t-m+q-n+\nu+\varsigma}} \bar{a}^{k_3' p^{q-n+\nu+\varsigma}}$$

for k_1', k_2', $k_3' \in \mathbb{Z}$ where $(k_1' k_2' k_3', p) = 1$.

Finally we note that if any of γ, β or η is zero, the proof will be similar but easier. ■

Chapter 6

The centre

In this chapter we will show that the centre $\zeta(Aut(P))$ of $Aut(P)$ is cyclic and generated by h. We have seen that h is a central element of $Aut(P)$ and so $\zeta(Aut(P))/\langle h\rangle \leq \zeta(Q)$ where $Q = Aut(P)/\langle h\rangle$. In the next chapter we will calculate the upper central series of $Aut(P)$ and so we need to find $\zeta(Q)$. It turns out to be more efficient to calculate $\zeta(Q)$ first and then use this to show that $\zeta(Aut(P)) = \langle h\rangle$. As one might expect, $\zeta(Q)$ will depend on the relation between the invariants defining P.

In the following lemma we show that in cases 1 and 2, $\zeta(Q)$ depends on whether $m - q \geq q - n$ or otherwise.

Lemma 6.0.1 *Let $\bar{a}$, $\bar{b}$ and $\bar{d}$ be as defined earlier. If $Q = \langle \bar{a}, \bar{b}, \bar{d}\rangle$ then the centre $\zeta(Q)$ of Q is $\langle \bar{a}^{p^{\ell}}, \bar{b}^{p^{\ell}}\rangle$ for $\ell =$ max$\{2q - m, n\}$.*

Proof.

First we remind the reader that from Lemma 4.1.4, the order of $\bar{a}$ is p^q, the order of $\bar{b}$ is p^q and the order of $\bar{d}$ is p^n.

Now let $\bar{x}$ be any element of Q so that $\bar{x} = \bar{d}^{\gamma}\bar{b}^{\beta}\bar{a}^{\eta}$ for $0 \leq \gamma < p^n$, $0 \leq \beta < p^q$ and $0 \leq \eta < p^q$.

Assume γ, β and η are all nonzero and suppose $p^{\epsilon_1} \parallel \gamma$, $p^{\epsilon_2} \parallel \beta$ and $p^{\epsilon_3} \parallel \eta$.

Now, $\bar{x}$ is an element of $\zeta(Q)$ if and only if $[\bar{x}, \bar{a}] = [\bar{x}, \bar{b}] = [\bar{x}, \bar{d}] = 1$.

Let $\bar{x} \in \zeta(Q)$. We will look at each commutator, and first we calculate $[\bar{x}, \bar{b}]$:

$$\begin{aligned}[\bar{x}, \bar{b}] &= [\bar{d}^{\gamma}\bar{b}^{\beta}\bar{a}^{\eta}, \bar{b}] \\ &= [\bar{d}^{\gamma}\bar{b}^{\beta}, \bar{b}]^{\bar{a}^{\eta}}[\bar{a}^{\eta}, \bar{b}].\end{aligned}$$

Since $[\bar{x}, \bar{b}] = 1$ (and $[\bar{a}^{\eta}, \bar{b}]$ is a power of $\bar{a}$ from Lemma 4.2.2), by conjugating with $\bar{a}^{-\eta}$ we have

$$\begin{aligned}1 &= [\bar{x}, \bar{b}]^{\bar{a}^{-\eta}} \\ &= [\bar{d}^{\gamma}\bar{b}^{\beta}, \bar{b}][\bar{a}^{\eta}, \bar{b}] \\ &= [\bar{d}^{\gamma}, \bar{b}]^{\bar{b}^{\beta}}[\bar{a}^{\eta}, \bar{b}].\end{aligned}$$

Then conjugating by $\bar{b}^{-\beta}$ we get

$$1 = [\bar{d}^{\gamma}, \bar{b}][\bar{a}^{\eta}, \bar{b}]^{\bar{b}^{-\beta}}.$$

Now, $[\bar{a}^{\eta}, \bar{b}]^{\bar{b}^{-\beta}}$ is just a power of $\bar{a}$ from Lemma 4.2.2, while from Lemma 5.0.4 where $p^{\epsilon_1} \parallel \gamma$,

$$[\bar{d}^{\gamma}, \bar{b}] = \bar{d}^{f_1 p^{m-q+\epsilon_1}} \bar{b}^{f_2 p^{q-n+\epsilon_1}}$$

for integers f_1 and f_2 such that $(f_1 f_2, p) = 1$. Since the product

$$1 = [\bar{d}^{\gamma}, \bar{b}][\bar{a}^{\eta}, \bar{b}]^{\bar{b}^{-\beta}}$$

is in normal form, it follows that the power p for $\bar{b}$ must satisfy $q - n + \epsilon_1 \geq q$ or $\epsilon_1 \geq n$. This tells us that $\bar{d}^{\gamma} = 1$ and so $\bar{x} = \bar{b}^{\beta}\bar{a}^{\eta}$. Now recalculate the commutators:

$$\begin{aligned}[\bar{x}, \bar{b}] &= [\bar{b}^{\beta}\bar{a}^{\eta}, \bar{b}] \\ &= [\bar{b}^{\beta}, \bar{b}]^{\bar{a}^{\eta}}[\bar{a}^{\eta}, \bar{b}] \\ &= [\bar{a}^{\eta}, \bar{b}].\end{aligned}$$

Thus using Lemma 4.2.2,

$$1 = [\bar{a}^{\eta}, \bar{b}] = \bar{a}^{-\eta c p^{m-q}}$$

where $c \equiv (1 + p^{m-q})^{-1}$ $(mod\ p^{m})$. Therefore since $p^{\epsilon_3} \parallel \eta$, $\epsilon_3 + m - q \geq q$ so that $\epsilon_3 \geq 2q - m$. Now,

$$\begin{aligned}[\bar{x}, \bar{a}] &= [\bar{b}^{\beta}\bar{a}^{\eta}, \bar{a}] \\ &= [\bar{b}^{\beta}, \bar{a}]^{\bar{a}^{\eta}}[\bar{a}^{\eta}, \bar{a}] \\ &= [\bar{b}^{\beta}, \bar{a}].\end{aligned}$$

Hence using Lemma 4.2.2,

$$1 = [\bar{b}^{\beta}, \bar{a}] = \bar{a}^{1-(1-cp^{m-q})^{\beta}}$$

where $c \equiv (1+p^{m-q})^{-1}$ $(mod\ p^m)$. Now from Corollary 2.3.4 for an integer k,

$$(1-cp^{m-q})^{\beta} = 1 - c\beta p^{m-q} + kp^{\epsilon_2+2(m-q)}.$$

It follows that

$$1 - ((1-cp^{m-q})^{\beta}) = c\beta p^{m-q} - kp^{\epsilon_2+2(m-q)}$$

is divisible by p^q. Since $p^{\epsilon_2} \parallel \beta$, we have $\epsilon_2 + m - q \geq q$ so that $\epsilon_2 \geq 2q - m$. Now,

$$\begin{aligned}
[\bar{x}, \bar{d}] &= [\bar{b}^{\beta}\bar{a}^{\eta}, \bar{d}] \\
&= [\bar{b}^{\beta}, \bar{d}]^{\bar{a}^{\eta}} [\bar{a}^{\eta}, \bar{d}] \\
&= (\bar{d}^{v_1 p^{m-q+\epsilon_2}} \bar{b}^{v_2 p^{q-n+\epsilon_2}})^{\bar{a}^{\eta}} (\bar{d}^{e_1 p^{t-n+\epsilon_3}} \bar{b}^{e_2 p^{t-m+q-n+\epsilon_3}} \bar{a}^{e_3 p^{q-n+\epsilon_3}}).
\end{aligned}$$

by using Lemmas 5.0.4 and 5.0.8 where v_1, v_2, e_1, e_2 and e_3 are integers such that $(v_1 v_2 e_1 e_2 e_3, p) = 1$. We now look at the power p for $\bar{d}$ in this product:

Since ϵ_2 and ϵ_3 are both at least $2q - m$, we have

$$m - q + \epsilon_2 \geq m - q + 2q - m = q > n$$

and

$$t - n + \epsilon_3 \geq t - n + 2q - m \geq q > n.$$

Thus the powers on $\bar{d}$ disappear. Hence

$$1 = [\bar{x}, \bar{d}] = (\bar{b}^{v_2 p^{q-n+\epsilon_2}})^{\bar{a}^{\eta}} (\bar{b}^{e_2 p^{t-m+q-n+\epsilon_3}} \bar{a}^{e_3 p^{q-n+\epsilon_3}}).$$

Now, conjugating by $\bar{a}^{-\eta}$ we get

$$1 = (\bar{b}^{v_2 p^{q-n+\epsilon_2}})(\bar{b}^{e_2 p^{t-m+q-n+\epsilon_3}})^{\bar{a}^{-\eta}} (\bar{a}^{e_3 p^{q-n+\epsilon_3}}).$$

Now using Lemma 4.2.2 for $c \equiv (1+p^{m-q})^{-1}$ $(mod\ p^m)$,

$$\begin{aligned}
(\bar{b}^{e_2 p^{t-m+q-n+\epsilon_3}})^{\bar{a}^{-\eta}} &= \bar{b}^{e_2 p^{t-m+q-n+\epsilon_3}} [\bar{b}^{e_2 p^{t-m+q-n+\epsilon_3}}, \bar{a}^{-\eta}] \\
&= \bar{b}^{e_2 p^{t-m+q-n+\epsilon_3}} \bar{a}^{e p^{v}}
\end{aligned}$$

for an integer e where υ is strictly greater than the power of p dividing

$$ce_2p^{t-m+q-n+\epsilon_3}p^{m-q} = ce_2p^{t-n+\epsilon_3}.$$

Thus

$$\begin{aligned}1 &= (\bar{b}^{\upsilon_2p^{q-n+\epsilon_2}})(\bar{b}^{e_2p^{t-m+q-n+\epsilon_3}})^{\bar{a}^{-\eta}}(\bar{a}^{e_3p^{q-n+\epsilon_3}})\\ &= (\bar{b}^{\upsilon_2p^{q-n+\epsilon_2}})(\bar{b}^{e_2p^{t-m+q-n+\epsilon_3}}\bar{a}^{ep^{\upsilon}})(\bar{a}^{e_3p^{q-n+\epsilon_3}})\end{aligned}$$

which is in normal form. It follows that the power p for $\bar{a}$ must satisfy $q-n+\epsilon_3 \geq q$ or $\epsilon_3 \geq n$. Therefore

$$t-m+q-n+\epsilon_3 \geq t-m+q-n+n = t-m+q \geq q$$

so that

$$\bar{b}^{e_2p^{t-m+q-n+\epsilon_3}} = 1.$$

Hence

$$(\bar{b}^{\upsilon_2p^{q-n+\epsilon_2}})(\bar{a}^{ep^{\upsilon}}\bar{a}^{e_3p^{q-n+\epsilon_3}}) = 1$$

so that the power p for $\bar{b}$ must satisfy $q-n+\epsilon_2 \geq q$ or $\epsilon_2 \geq n$.

Therefore we conclude that for $\bar{x}$ to be in $\zeta(Q)$, we have ϵ_3 and ϵ_2 are at least ℓ for $\ell = \max\{2q-m, n\}$.

Hence the centre $\zeta(Q)$ of Q is $\langle \bar{a}^{p^{\ell}}, \bar{b}^{p^{\ell}} \rangle$ for $\ell = \max\{2q-m, n\}$.

Finally we note that if either γ, β or η is zero, the proof will be similar but easier. ■

We now look at the main result of this chapter.

Theorem 6.0.2 *If h is as defined earlier then $\zeta(Aut(P)) = \langle h \rangle$.*

Proof. Since a, b, d and h are generators of $Aut(P)$ by Theorem 5.0.2, and h commutes with a, b and d by Lemma 4.1.3, we have $\langle h \rangle \subseteq \zeta(Aut(P))$.
On the other hand, let $x' \in \zeta(Aut(P))$. Write x' in normal form as

$$x' = d^{\gamma}b^{\beta}a^{\eta}h^{\theta}$$

for $0 \leq \gamma < p^n$, $0 \leq \beta < p^q$, $0 \leq \eta < p^q$ and $0 \leq \theta < p^{t+n-q}$. We then have

$$x = x'h^{-\theta} = d^{\gamma}b^{\beta}a^{\eta} \in \zeta(Aut(P))$$

and we will show that $x \in \langle h \rangle$.

Assume β and η are nonzero and suppose $p^{\epsilon_2} \parallel \beta$ and $p^{\epsilon_3} \parallel \eta$.

Now we consider x modulo $\langle h \rangle = \bar{x}$ so that

$$\bar{x} = \bar{d}^{\gamma}\bar{b}^{\beta}\bar{a}^{\eta}.$$

From Lemma 6.0.1 we have

$$\zeta(Q) = \langle \bar{a}^{p^{\ell}}, \bar{b}^{p^{\ell}} \rangle$$

for $\ell = \max\{2q - m, n\}$, so that if $\bar{x} \in \zeta(Q)$ then $\bar{d}^{\gamma} = 1$, that is γ is divisible by p^n.

But $x \in \zeta(Aut(P))$ implies $\bar{x} \in \zeta(Q)$ and so, $d^{\gamma} \in \langle h \rangle$.

Now since $x \in \zeta(Aut(P))$, we have $[x, a] = [x, b] = [x, d] = 1$. We now look at the commutators.

$$\begin{aligned}
[x, a] &= [d^{\gamma}b^{\beta}a^{\eta}, a] \\
&= [d^{\gamma}, a]^{b^{\beta}a^{\eta}}[b^{\beta}a^{\eta}, a] \\
&= [b^{\beta}a^{\eta}, a] \\
&= [b^{\beta}, a] \\
&= 1.
\end{aligned}$$

Using Lemma 4.2.2 where $c \not\equiv 0 \ (mod\ p)$, and Corollary 2.3.4 for an integer k,

$$\begin{aligned}
[b^{\beta}, a] &= a^{1-(1-cp^{m-q})^{\beta}} \\
&= a^{c\beta p^{m-q} + kp^{\epsilon_2 + 2(m-q)}}.
\end{aligned}$$

Since the order of a is p^m by Lemma 4.1.2, $\epsilon_2 + m - q \geq m$ which implies $\epsilon_2 \geq q$ and thus $b^{\beta} \in \langle h \rangle$. Now,

$$\begin{aligned}
[x, b] &= [d^{\gamma}b^{\beta}a^{\eta}, b] \\
&= [d^{\gamma}, b]^{b^{\beta}a^{\eta}}[b^{\beta}a^{\eta}, b] \\
&= [b^{\beta}a^{\eta}, b] \\
&= [a^{\eta}, b] \\
&= 1.
\end{aligned}$$

But from Lemma 4.2.2 where $c \not\equiv 0 \ (mod\ p)$,

$$\begin{aligned}
[a^{\eta}, b] &= a^{-\eta c p^{m-q}} \\
&= a^{c' p^{\epsilon_3 + m - q}}
\end{aligned}$$

for an integer c' such that $(c', p) = 1$, so that $\epsilon_3 + m - q \geq m$ and thus $\epsilon_3 \geq q$. Hence $a^\eta \in \langle h \rangle$ since $a^{p^q} \in \langle h \rangle$.

Therefore

$$x = d^\gamma b^\beta a^\eta h^\theta \in \langle h \rangle.$$

Finally we note that if either β or η is zero, the proof will be similar but easier.
■

Chapter 7

The class

The class of $Aut(P)$ is found by constructing its upper central series. We find that this is much easier than constructing its lower central series because in this problem, it is easier to calculate higher centres than to calculate higher commutators.

Since we have shown that $\zeta(Aut(P)) = \langle h \rangle$, to construct the upper central series of $Aut(P)$ it will be enough to construct the upper central series of $Q = Aut(P)/\langle h \rangle$. Lemma 6.0.1 gives the centre $\zeta(Q)$ of Q which depends on whether $m - q \geq q - n$ or otherwise, and the remaining terms of the upper central series also depend on this dichotomy.

Lemma 7.0.1 gives the upper central series of Q and then Theorem 7.0.2 gives the class of $Aut(P)$.

Lemma 7.0.1 *Let $\bar{a}$, $\bar{b}$ and $\bar{d}$ be as defined earlier and k be a positive integer.*
a) If $m - q \geq q - n$ then
i) for $kn - (k-1)q > 0$, $\zeta_k(Q) = \langle \bar{a}^{p^{kn-(k-1)q}}, \bar{b}^{p^{kn-(k-1)q}}, \bar{d}^{p^{kn-(k-1)q}} \rangle$
and
ii) for $kn - (k-1)q \leq 0$, $\zeta_k(Q) = \langle \bar{a}, \bar{b}, \bar{d} \rangle$.

b) If $m - q < q - n$ then
i) for $(k-1)q-(k-1)m+n > 0$, $\zeta_k(Q) = \langle \bar{a}^{p^{(k+1)q-km}}, \bar{b}^{p^{(k+1)q-km}}, \bar{d}^{p^{(k-1)q-(k-1)m+n}} \rangle$
and
ii) for $(k-1)q-(k-1)m+n \leq 0 < (k+1)q-km$, $\zeta_k(Q) = \langle \bar{a}^{p^{(k+1)q-km}}, \bar{b}^{p^{(k+1)q-km}}, \bar{d} \rangle$
and
iii) for $(k+1)q - km \leq 0$, $\zeta_k(Q) = \langle \bar{a}, \bar{b}, \bar{d} \rangle$.

Proof.

Let $\bar{x}$ be any nontrivial element of Q so that $\bar{x} = \bar{d}^{\gamma}\bar{b}^{\beta}\bar{a}^{\eta}$ for $0 \leq \gamma < p^n$, $0 \leq \beta < p^q$ and $0 \leq \eta < p^q$.

Assume γ, β and η are all nonzero and suppose $p^{\epsilon_1} \parallel \gamma$, $p^{\epsilon_2} \parallel \beta$ and $p^{\epsilon_3} \parallel \eta$.

We will prove the result by induction. To begin, we know that

$$\bar{x} \in \zeta_{k+1}(Q) \text{ if and only if } [\bar{x}, \bar{a}] \equiv [\bar{x}, \bar{b}] \equiv [\bar{x}, \bar{d}] \equiv 1 \ (mod\ \zeta_k(Q)).$$

We will calculate **modulo $\zeta_{\mathbf{k}}(\mathbf{Q})$** throughout the proof.

Case (a) : $\mathbf{m - q \geq q - n}$

By Lemma 6.0.1, the result is true for $k = 1$.

i) Now suppose for $k > 1$ and $kn - (k-1)q > 0$,

$$\zeta_k(Q) = \langle \bar{a}^{p^{kn-(k-1)q}}, \bar{b}^{p^{kn-(k-1)q}}, \bar{d}^{p^{kn-(k-1)q}} \rangle.$$

Let $\bar{x} \in \zeta_{k+1}(Q)$. We will calculate each commutator. We have

$$\begin{aligned} [\bar{x}, \bar{b}] &\equiv [\bar{d}^{\gamma}\bar{b}^{\beta}\bar{a}^{\eta}, \bar{b}] \\ &\equiv [\bar{d}^{\gamma}\bar{b}^{\beta}, \bar{b}]^{\bar{a}^{\eta}} [\bar{a}^{\eta}, \bar{b}] \end{aligned}$$

and then since $[\bar{x}, \bar{b}] \equiv 1$ (and $[\bar{a}^{\eta}, \bar{b}]$ is a power of $\bar{a}$ from Lemma 4.2.2) we also have

$$1 \equiv [\bar{x}, \bar{b}]^{\bar{a}^{-\eta}} \equiv [\bar{d}^{\gamma}\bar{b}^{\beta}, \bar{b}][\bar{a}^{\eta}, \bar{b}] \equiv [\bar{d}^{\gamma}, \bar{b}]^{\bar{b}^{\beta}} [\bar{a}^{\eta}, \bar{b}]. \tag{7.1}$$

Conjugating by $\bar{b}^{-\beta}$ we get

$$1 \equiv [\bar{d}^{\gamma}, \bar{b}][\bar{a}^{\eta}, \bar{b}]^{\bar{b}^{-\beta}}. \tag{7.2}$$

Now from Lemma 5.0.4 where $p^{\epsilon_1} \parallel \gamma$,

$$[\bar{d}^{\gamma}, \bar{b}] = \bar{d}^{f_1 p^{m-q+\epsilon_1}} \bar{b}^{f_2 p^{q-n+\epsilon_1}}$$

for integers f_1 and f_2 such that $(f_1 f_2, p) = 1$. Also from Lemma 4.2.2 for $c \equiv$

$(1+p^{m-q})^{-1}$ $(mod\ p^m)$,

$$\begin{aligned}[\bar{a}^{\eta}, \bar{b}]^{\bar{b}^{-\beta}} &= (\bar{a}^{-\eta c p^{m-q}})^{\bar{b}^{-\beta}} \\ &= \bar{a}^{-\eta c p^{m-q}}[\bar{a}^{-\eta c p^{m-q}}, \bar{b}^{-\beta}] \\ &= \bar{a}^{-\eta c p^{m-q}} \bar{a}^{\ell p^{\omega}}\end{aligned}$$

for an integer ℓ where ω is strictly greater than the power of p dividing $-\eta c p^{m-q}$. Since the product

$$1 \equiv [\bar{d}^{\gamma}, \bar{b}][\bar{a}^{\eta}, \bar{b}]^{\bar{b}^{-\beta}}$$

is in normal form, it now follows that the power p for $\bar{b}$ must satisfy

$$q - n + \epsilon_1 \geq kn - (k-1)q$$

or

$$\epsilon_1 \geq (k+1)n - kq.$$

We observe that this implies

$$\begin{aligned}m - q + \epsilon_1 &\geq m - q + (k+1)n - kq = kn - kq + (m+n-q) \\ &\geq kn - (k-1)q\end{aligned}$$

since $m + n \geq 2q$. Thus $\bar{d}^{f_1 p^{m-q+\epsilon_1}} \equiv 1$. Also by looking at the power p for $\bar{a}$,

$$\epsilon_3 + m - q \geq kn - (k-1)q$$

and therefore

$$\epsilon_3 \geq kn - kq + (2q - m).$$

Now,

$$1 \equiv [\bar{x}, \bar{a}] \equiv [\bar{d}^{\gamma}\bar{b}^{\beta}\bar{a}^{\eta}, \bar{a}] \equiv [\bar{d}^{\gamma}\bar{b}^{\beta}, \bar{a}]^{\bar{a}^{\eta}} \equiv \left([\bar{d}^{\gamma}, \bar{a}]^{\bar{b}^{\beta}}[\bar{b}^{\beta}, \bar{a}]\right)^{\bar{a}^{\eta}}. \tag{7.3}$$

However $[\bar{d}^{\gamma}, \bar{a}] \equiv 1$ as the following shows: From Lemma 5.0.8 where $p^{\epsilon_1} \parallel \gamma$,

$$[\bar{d}^{\gamma}, \bar{a}] = \bar{d}^{e_1 p^{t-n+2\epsilon_1}} \bar{b}^{e_2 p^{t-m+q-n+\epsilon_1}} \bar{a}^{e_3 p^{q-n+\epsilon_1}}$$

for integers e_1, e_2 and e_3 such that $(e_1 e_2 e_3, p) = 1$. Since $\epsilon_1 \geq (k+1)n - kq$, each of $t-n+2\epsilon_1$, $t-m+q-n+\epsilon_1$ and $q-n+\epsilon_1$ is at least $kn-(k-1)q$. Hence

$$[\bar{x},\bar{a}] \equiv ([\bar{b}^{\beta},\bar{a}])^{\bar{a}^{\eta}} \equiv [\bar{b}^{\beta},\bar{a}]$$

since $[\bar{b}^{\beta},\bar{a}]$ is a power of $\bar{a}$ from Lemma 4.2.2. By using Lemma 4.2.2 again,

$$1 \equiv [\bar{b}^{\beta},\bar{a}] \equiv \bar{a}^{1-(1-cp^{m-q})^{\beta}}$$

where $c \equiv (1+p^{m-q})^{-1}$ $(mod\ p^m)$. Now by using Corollary 2.3.4, for an integer k' and where $p^{\epsilon_2} \parallel \beta$,

$$1-(1-cp^{m-q})^{\beta} = c\beta p^{m-q} - k'p^{\epsilon_2+2(m-q)}.$$

It follows that

$$\epsilon_2 + m - q \geq kn-(k-1)q$$

and hence

$$\epsilon_2 \geq kn - kq + (2q-m).$$

Now,

$$1 \equiv [\bar{x},\bar{d}] \equiv [\bar{d}^{\gamma}\bar{b}^{\beta}\bar{a}^{\eta},\bar{d}] \equiv [\bar{d}^{\gamma}\bar{b}^{\beta},\bar{d}]^{\bar{a}^{\eta}}[\bar{a}^{\eta},\bar{d}] \equiv [\bar{b}^{\beta},\bar{d}]^{\bar{a}^{\eta}}[\bar{a}^{\eta},\bar{d}]. \tag{7.4}$$

Using Lemma 5.0.4 where $p^{\epsilon_2} \parallel \beta$ and for integers f_1' and f_2' such that $(f_1'f_2',p)=1$,

$$\begin{aligned}[\bar{b}^{\beta},\bar{d}] &= \bar{d}^{f_1'p^{m-q+\epsilon_2}}\bar{b}^{f_2'p^{q-n+\epsilon_2}}\\ &\equiv \bar{b}^{f_2'p^{q-n+\epsilon_2}}\end{aligned}$$

since

$$m-q+\epsilon_2 \geq m-q+kn-kq+(2q-m) = kn-(k-1)q$$

so that $\bar{d}^{f_1'p^{m-q+\epsilon_2}} \equiv 1$. Thus

$$1 \equiv [\bar{x},\bar{d}] \equiv [\bar{b}^{\beta},\bar{d}]^{\bar{a}^{\eta}}[\bar{a}^{\eta},\bar{d}] \equiv (\bar{b}^{f_2'p^{q-n+\epsilon_2}})^{\bar{a}^{\eta}}[\bar{a}^{\eta},\bar{d}].$$

Now using Lemma 4.2.2,

$$\begin{aligned}(\bar{b}^{f_2'p^{q-n+\epsilon_2}})^{\bar{a}^{\eta}} &= \bar{b}^{f_2'p^{q-n+\epsilon_2}}[\bar{b}^{f_2'p^{q-n+\epsilon_2}},\bar{a}^{\eta}]\\ &= \bar{b}^{f_2'p^{q-n+\epsilon_2}}\bar{a}^{ep^{v}}\end{aligned}$$

for an integer e where v is greater than or equal to the power of p dividing

$$cf_2'p^{q-n+\epsilon_2}p^{m-q} = cf_2'p^{m-n+\epsilon_2}$$

where $c \equiv (1+p^{m-q})^{-1}$ $(mod\ p^m)$. But

$$\begin{aligned} m-n+\epsilon_2 &\geq m-n+kn-kq+(2q-m) = kn-(k-1)q+(q-n) \\ &\geq kn-(k-1)q \end{aligned}$$

so that $\bar{a}^{ep^v} \equiv 1$. Hence

$$1 \equiv [\bar{x}, \bar{d}] \equiv \bar{b}^{f_2'p^{q-n+\epsilon_2}}[\bar{a}^\eta, \bar{d}].$$

Now from Lemma 5.0.8 where $p^{\epsilon_3} \parallel \eta$,

$$[\bar{a}^\eta, \bar{d}] = \bar{d}^{v_1p^{t-n+\epsilon_3}}\bar{b}^{v_2p^{t-m+q-n+\epsilon_3}}\bar{a}^{v_3p^{q-n+\epsilon_3}}$$

for integers v_1, v_2 and v_3 such that $(v_1v_2v_3, p) = 1$. Since $\epsilon_3 \geq kn-kq+(2q-m)$, by looking at the power p for $\bar{d}$ we have

$$\begin{aligned} t-n+\epsilon_3 &\geq t-n+kn-kq+(2q-m) = kn-(k-1)q+(t-m+q-n) \\ &\geq kn-(k-1)q. \end{aligned}$$

Thus $\bar{d}^{v_1p^{t-n+\epsilon_3}} \equiv 1$. It follows that

$$1 \equiv [\bar{x}, \bar{d}] \equiv \bar{b}^{f_2'p^{q-n+\epsilon_2}}\bar{b}^{v_2p^{t-m+q-n+\epsilon_3}}\bar{a}^{v_3p^{q-n+\epsilon_3}}$$

which is in normal form. Hence by looking at the power p for $\bar{a}$ we have

$$q-n+\epsilon_3 \geq kn-(k-1)q$$

or

$$\epsilon_3 \geq (k+1)n-kq$$

which also implies that $\bar{b}^{v_2p^{t-m+q-n+\epsilon_3}} \equiv 1$. So we have

$$1 \equiv [\bar{x}, \bar{d}] \equiv \bar{b}^{f_2'p^{q-n+\epsilon_2}}\bar{a}^{v_3p^{q-n+\epsilon_3}}$$

and so by looking at the power p for $\bar{b}$,

$$q - n + \epsilon_2 \geq kn - (k-1)q$$

or

$$\epsilon_2 \geq (k+1)n - kq.$$

Therefore

$$\zeta_{k+1}(Q) = \langle \bar{a}^{p^{(k+1)n-kq}}, \bar{b}^{p^{(k+1)n-kq}}, \bar{d}^{p^{(k+1)n-kq}} \rangle \neq Q$$

for $(k+1)n - kq > 0$.

Now if $k > 1$ and $(k+1)n - kq \leq 0$ then it is clear that

$$\zeta_{k+1}(Q) = \langle \bar{a}, \bar{b}, \bar{d} \rangle = Q.$$

ii) Suppose for $k > 1$ and for $kn - (k-1)q \leq 0$, $\zeta_k(Q) = \langle \bar{a}, \bar{b}, \bar{d} \rangle$. It is then clear that

$$\zeta_{k+1}(Q) = \langle \bar{a}, \bar{b}, \bar{d} \rangle = Q.$$

Case (b) : $\mathbf{m - q < q - n}$.

By Lemma 6.0.1, it is true for $k = 1$. In this subcase we note that the power p for $\bar{d}$ become zero and negative before the power p for $\bar{a}$ and $\bar{b}$.

i) Suppose for $k > 1$ and $(k-1)q - (k-1)m + n > 0$,

$$\zeta_k(Q) = \langle \bar{a}^{p^{(k+1)q-km}}, \bar{b}^{p^{(k+1)q-km}}, \bar{d}^{p^{(k-1)q-(k-1)m+n}} \rangle.$$

Let $\bar{x} \in \zeta_{k+1}(Q)$. Now by calculating $[\bar{x}, \bar{b}]$ with steps similar as in (a) we have (7.2) which is,

$$1 \equiv [\bar{d}^{\gamma}, \bar{b}][\bar{a}^{\eta}, \bar{b}]^{\bar{b}^{-\beta}}$$

where

$$[\bar{d}^{\gamma}, \bar{b}] = \bar{d}^{f_1 p^{m-q+\epsilon_1}} \bar{b}^{f_2 p^{q-n+\epsilon_1}}$$

for integers f_1 and f_2 such that $(f_1 f_2, p) = 1$ and

$$[\bar{a}^{\eta}, \bar{b}]^{\bar{b}^{-\beta}} = \bar{a}^{-\eta c p^{m-q}} \bar{a}^{\ell p^{\omega}}$$

for an integer ℓ where ω is strictly greater than the power of p dividing $-\eta c p^{m-q}$, where $c \equiv (1 + p^{m-q})^{-1}$ $(mod\ p^m)$. Therefore

$$1 \equiv [\bar{d}^\gamma, \bar{b}][\bar{a}^\eta, \bar{b}]^{\bar{b}^{-\beta}} \equiv \bar{d}^{f_1 p^{m-q+\epsilon_1}} \bar{b}^{f_2 p^{q-n+\epsilon_1}} \bar{a}^{-\eta c p^{m-q}} \bar{a}^{\ell p^\omega}$$

is in normal form and so we have the power of p for $\bar{d}$ must satisfy

$$m - q + \epsilon_1 \geq (k-1)q - (k-1)m + n$$

or

$$\epsilon_1 \geq kq - km + n.$$

We observe that by looking at the power p for $\bar{b}$ we have

$$q - n + \epsilon_1 \geq q - n + kq - km + n = (k+1)q - km$$

so that $\bar{b}^{f_2 p^{q-n+\epsilon_1}} \equiv 1$. Also by looking at the power p for $\bar{a}$ we have,

$$\epsilon_3 + m - q \geq (k+1)q - km$$

and therefore

$$\epsilon_3 \geq (k+2)q - (k+1)m.$$

Now by calculating $[\bar{x}, \bar{a}]$ with steps similar as in (a), we have (7.3) which is

$$1 \equiv [\bar{x}, \bar{a}] \equiv \left([\bar{d}^\gamma, \bar{a}]^{\bar{b}^\beta} [\bar{b}^\beta, \bar{a}]\right)^{\bar{a}^\eta}.$$

However $[\bar{d}^\gamma, \bar{a}] \equiv 1$ as the following shows: From Lemma 5.0.8 where $p^{\epsilon_1} \parallel \gamma$,

$$[\bar{d}^\gamma, \bar{a}] = \bar{d}^{e_1 p^{t-n+2\epsilon_1}} \bar{b}^{e_2 p^{t-m+q-n+\epsilon_1}} \bar{a}^{e_3 p^{q-n+\epsilon_1}}$$

for integers e_1, e_2 and e_3 such that $(e_1 e_2 e_3, p) = 1$. Since $\epsilon_1 \geq kq - km + n$, by looking at the power p for $\bar{d}$ we have

$$\begin{aligned} t - n + 2\epsilon_1 &\geq t - n + \epsilon_1 \\ &\geq t - n + kq - km + n = kq - km + t \\ &> kq - km + (m + n - q) = (k-1)q - (k-1)m + n. \end{aligned}$$

Also by looking at the power p for $\bar{a}$ we have,

$$q - n + \epsilon_1 \geq q - n + kq - km + n = (k+1)q - km$$

and clearly by looking at the power p for $\bar{b}$ we have

$$t - m + q - n + \epsilon_1 \geq (k+1)q - km.$$

It follows that

$$1 \equiv [\bar{x}, \bar{a}] \equiv ([\bar{b}^\beta, \bar{a}])^{\bar{a}^\eta} \equiv [\bar{b}^\beta, \bar{a}]$$

since $[\bar{b}^\beta, \bar{a}]$ is a power of $\bar{a}$ from Lemma 4.2.2. By using Lemma 4.2.2 again,

$$1 \equiv [\bar{b}^\beta, \bar{a}] \equiv \bar{a}^{1-(1-cp^{m-q})^\beta}$$

where $c \equiv (1+p^{m-q})^{-1}$ $(mod\ p^m)$. Now by using Corollary 2.3.4 for an integer k' and where $p^{\epsilon_2} \parallel \beta$,

$$1 - (1 - cp^{m-q})^\beta = c\beta p^{m-q} - k' p^{\epsilon_2 + 2(m-q)}.$$

It follows that

$$\epsilon_2 + m - q \geq (k+1)q - km$$

and hence

$$\epsilon_2 \geq (k+2)q - (k+1)m.$$

Now we show that commutativity with $\bar{d}$ imposes no further restrictions. By calculating $[\bar{x}, \bar{d}]$ with steps similar as in (a) we have (7.4) which is,

$$1 \equiv [\bar{x}, \bar{d}] \equiv [\bar{b}^\beta, \bar{d}]^{\bar{a}^\eta} [\bar{a}^\eta, \bar{d}].$$

However $[\bar{b}^\beta, \bar{d}] \equiv 1$ as the following shows: From Lemma 5.0.4 where $p^{\epsilon_2} \parallel \beta$,

$$[\bar{b}^\beta, \bar{d}] = \bar{d}^{f_1 p^{m-q+\epsilon_2}} \bar{b}^{f_2 p^{q-n+\epsilon_2}}$$

for integers f_1 and f_2 such that $(f_1 f_2, p) = 1$. Since $\epsilon_2 \geq (k+2)q - (k+1)m$, by looking at the power p for $\bar{d}$ we have

$$\begin{aligned} m - q + \epsilon_2 &\geq m - q + (k+2)q - (k+1)m = kq - km + q \\ &> kq - km + (m + n - q) = (k-1)q - (k-1)m + n \end{aligned}$$

since $2q - m > n$. Also by looking at the power p for $\bar{b}$,

$$\begin{aligned} q - n + \epsilon_2 &\geq q - n + (k+2)q - (k+1)m = kq - km + q + (2q - m - n) \\ &> kq - km + q = (k+1)q - km. \end{aligned}$$

Hence

$$1 \equiv [\bar{x}, \bar{d}] \equiv [\bar{a}^\eta, \bar{d}].$$

From Lemma 5.0.8 where $p^{\epsilon_3} \parallel \eta$,

$$[\bar{a}^\eta, \bar{d}] = \bar{d}^{v_1 p^{t-n+\epsilon_3}} \bar{b}^{v_2 p^{t-m+q-n+\epsilon_3}} \bar{a}^{v_3 p^{q-n+\epsilon_3}}$$

for integers v_1, v_2 and v_3 such that $(v_1 v_2 v_3, p) = 1$. Since $\epsilon_3 \geq (k+2)q - (k+1)m$, by looking at the power p for $\bar{a}$ we have

$$\begin{aligned} q - n + \epsilon_3 &\geq q - n + (k+2)q - (k+1)m = (k+1)q - km + (2q - m - n) \\ &> (k+1)q - km \end{aligned}$$

since $2q - m - n > 0$. Similarly by looking at the power p for $\bar{b}$ we have,

$$t - m + q - n + \epsilon_3 > (k+1)q - km.$$

Now by looking at the power p for $\bar{d}$,

$$\begin{aligned} t - n + \epsilon_3 &\geq t - n + (k+2)q - (k+1)m = kq - km + (t - n + 2q - m) \\ &> kq - km + (t - n + n) = kq - km + t \\ &> kq - km + (m + n - q) = (k-1)q - (k-1)m + n. \end{aligned}$$

Therefore we have

$$\bar{d}^{v_1 p^{t-n+\epsilon_3}} \equiv \bar{b}^{v_2 p^{t-m+q-n+\epsilon_3}} \equiv \bar{a}^{v_3 p^{q-n+\epsilon_3}} \equiv 1$$

as required. We conclude that

$$\zeta_{k+1}(Q) = \langle \bar{a}^{p^{(k+2)q-(k+1)m}}, \bar{b}^{p^{(k+2)q-(k+1)m}}, \bar{d}^{p^{kq-km+n}} \rangle \neq Q$$

and the result is proved inductively.

Now if $k > 1$ and $kq - km + n \leq 0 < (k+2)q - (k+1)m$ then it is clear that

$$\zeta_{k+1}(Q) = \langle \bar{a}^{p^{(k+2)q-(k+1)m}}, \bar{b}^{p^{(k+2)q-(k+1)m}}, \bar{d} \rangle \neq Q.$$

Now if $k > 1$ and $(k+2)q - (k+1)m \leq 0$ then it is clear that

$$\zeta_{k+1}(Q) = \langle \bar{a}, \bar{b}, \bar{d} \rangle = Q.$$

ii) Suppose for $k > 1$ and for $(k-1)q - (k-1)m + n \leq 0 < (k+1)q - km$,

$$\zeta_k(Q) = \langle \bar{a}^{p^{(k+1)q-km}}, \bar{b}^{p^{(k+1)q-km}}, \bar{d} \rangle.$$

We again do our calculation **modulo $\zeta_{\mathbf{k}}(\mathbf{Q})$**. Now by calculating $[\bar{x}, \bar{b}]$, with steps similar as in (a), we have (7.1) which is

$$1 \equiv [\bar{d}^{\gamma}, \bar{b}]^{\bar{b}^{\beta}} [\bar{a}^{\eta}, \bar{b}].$$

But $\bar{d} \equiv 1$ so that

$$1 \equiv [\bar{a}^{\eta}, \bar{b}].$$

Using Lemma 4.2.2 where $c \equiv (1 + p^{m-q})^{-1}$ $(mod\ p^m)$, we have

$$1 \equiv \bar{a}^{-\eta c p^{m-q}}$$

so that

$$m - q + \epsilon_3 \geq (k+1)q - km$$

and hence

$$\epsilon_3 \geq (k+2)q - (k+1)m.$$

Now, calculating $[\bar{x}, \bar{a}]$, with steps similar as in (a), we have (7.3) which is

$$1 \equiv \left([\bar{d}^{\gamma}, \bar{a}]^{\bar{b}^{\beta}} [\bar{b}^{\beta}, \bar{a}]\right)^{\bar{a}^{\eta}}.$$

But $\bar{d} \equiv 1$ so that

$$\begin{aligned} 1 &\equiv [\bar{b}^{\beta}, \bar{a}])^{\bar{a}^{\eta}} \\ &\equiv [\bar{b}^{\beta}, \bar{a}] \\ &\equiv \bar{a}^{1-(1-cp^{m-q})^{\beta}} \\ &\equiv \bar{a}^{c\beta p^{m-q} - k' p^{\epsilon_2 + 2(m-q)}} \end{aligned}$$

by using Lemma 4.2.2 and Corollary 2.3.4 where $c \equiv (1 + p^{m-q})^{-1}$ $(mod\ p^m)$, k'

an integer and $p^{\epsilon_2} \parallel \beta$. Thus

$$\epsilon_2 + m - q \geq (k+1)q - km$$

and hence

$$\epsilon_2 \geq (k+2)q - (k+1)m.$$

We conclude that

$$\zeta_{k+1}(Q) = \langle \bar{a}^{p^{(k+2)q-(k+1)m}}, \bar{b}^{p^{(k+2)q-(k+1)m}}, \bar{d} \rangle \neq Q.$$

Now if $k > 1$ and $(k+2)q - (k+1)m < 0$ then it is clear that

$$\zeta_{k+1}(Q) = \langle \bar{a}, \bar{b}, \bar{d} \rangle = Q.$$

iii) Suppose for $k > 1$ and for $(k+1)q - km \leq 0$, $\zeta_k(Q) = \langle \bar{a}, \bar{b}, \bar{d} \rangle$. It is clear that

$$\zeta_{k+1}(Q) = \langle \bar{a}, \bar{b}, \bar{d} \rangle = Q.$$

Finally we note that if any of γ, β or η is zero, the proof will be similar but easier. ■

We now are able to calculate the class of $Aut(P)$.

Theorem 7.0.2 *Let $Aut(P)$ be as defined earlier.*

a) If $m - q \geq q - n$ then the class of $Aut(P)$ is $\lceil \frac{q}{q-n} \rceil + 1$.
b) If $m - q < q - n$ then the class of $Aut(P)$ is $\lceil \frac{q}{m-q} \rceil + 1$.

Proof.

Since $\zeta(Aut(P)) = \langle h \rangle$, the class of $Aut(P)$ is one more than the class of Q and hence it is enough to calculate the class of Q where $Q = \langle \bar{a}, \bar{b}, \bar{d} \rangle$ such that $\bar{a}^{p^q} = \bar{b}^{p^q} = \bar{d}^{p^n} = 1$. Let k be a positive integer.

Case (a) : $\mathbf{m - q \geq q - n}$

Since $kn - (k-1)q$ is a monotone decreasing function of k, it follows from Lemma 7.0.1 that $\zeta_k(Q) = Q$ for the smallest k such that

$$kn - (k-1)q \leq 0 < (k-1)n - (k-2)q.$$

So we have

$$\frac{q}{q-n} \leq k < \frac{q}{q-n} + 1$$

or $k = \lceil \frac{q}{q-n} \rceil$ which is the class of Q. Therefore the class of $Aut(P)$ is $\lceil \frac{q}{q-n} \rceil + 1$.

Case (b) : $\mathbf{m - q < q - n}$.

Since $(k-1)q - (k-1)m + n < (k+1)q - km$, we have $\zeta_k(Q) \neq Q$ for $(k+1)q - km > 0$ by Lemma 7.0.1(i) and (ii), and $\zeta_k(Q) = Q$ when $(k+1)q - km \leq 0$ by Lemma 7.0.1(iii).

Since $(k+1)q - km$ is a monotone decreasing function of k, it follows that $\zeta_k(Q) = Q$ for the smallest k such that

$$(k+1)q - km \leq 0 < kq - (k-1)m.$$

So we have

$$\frac{q}{m-q} \leq k < \frac{q}{m-q} + 1$$

or $k = \lceil \frac{q}{m-q} \rceil$ which is the class of Q. Therefore the class of $Aut(P)$ is $\lceil \frac{q}{m-q} \rceil + 1$.
■

Chapter 8

Further research

We remind the reader that the four cases in the case of finite nonsplit metacyclic p-groups where p is an odd prime occur when:

1) $2 \leq n < q < m \leq t$ where $m \leq 2n$,

2) $1 \leq n < q < m \leq t$ where $2n < m \leq q + n$,

3) $3 \leq n < q < t < m \leq 2n$ and

4) $2 \leq n < q < t < m$ where $2n < m \leq q + n$.

In this thesis, we find results for only cases 1 and 2. The extension of the method to cases 3 and 4 is found to be more complicated. One of the complications is that $x^{p^{t-n}}$ and $y^{p^{t-n}}$ are no longer central elements of P because $t < m$ in cases 3 and 4. The calculations become even more complicated in case 4 especially, since $m > 2n$.

In checking the requirements for a matrix $\begin{bmatrix} i & r \\ j & s \end{bmatrix}$ to represent an automorphism of P we conjecture that in cases 3 and 4,

Conjecture 8.0.1 *Let* $\varphi \sim \begin{bmatrix} i & r \\ j & s \end{bmatrix}$. *Then* $\varphi \in Aut(P)$ *if and only if*

i) $r \in \mathbb{Z}_{p^m}$,

ii) $i \equiv 1 + rp^{t-q}$ *(mod* p^{m-q}*)*,

iii) $j \equiv 0$ *(mod* p^{t-n}*)*,

iv) $s \equiv 1 + cp^{q-n}$ *(mod* p^{m-n}*) where* $j = cp^{t-n}$ *for* $0 \leq c < p^n$.

Furthermore, the set of generators of $Aut(P)$ that we have for cases 1 and 2 are no longer the same for cases 3 and 4. In particular the mapping a represented by the matrix $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ is no longer an automorphism of P in cases 3 and 4.

Finding a new set of generators has proved difficult, but we conjecture that the following automorphisms of P which can be represented by the following matrices form a set of generators in these cases:

$$\begin{bmatrix} 1 & p^{m-t} \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1+p^{t-q} & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1+p^{m-n} & 0 \\ 0 & 1+p^{m-n} \end{bmatrix} \text{ and } \begin{bmatrix} 1 & 0 \\ p^{t-n} & 1+p^{q-n} \end{bmatrix}.$$

These generators are closely related to Curran's generators when $t < m$ (in our notation). If they are correct, we expect to be able to find the centre, the upper central series and the class of $Aut(P)$ by similar methods to those used in this thesis.

Once these are done, there are still many questions remaining for the nonsplit case. Perhaps, the most important are to find a presentation of $Aut(P)$ and to find its derived length. We expect the method and results obtained can lead to solutions to these problems.

In addition, we have not considered the split case in this thesis. If G is a finite nonabelian split metacyclic p-group where p is an odd prime, then the automorphism group $Aut(G)$ of G is no longer a p-group. Bidwell and Curran [3] found generators and a presentation of $Aut(G)$. Using similar methods to those used in this thesis, we expect to find the class of the Sylow p-subgroup of $Aut(G)$.

Bibliography

[1] J. E. Adney and T. Yen. 'Automorphisms of a p-group'. *Illinois J. Math.,* 9:137–143, 1965.

[2] B. G. Basmaji. 'On the isomorphisms of two metacyclic groups'. *Proc. Amer. Math. Soc.,* 22(1):175–182, 1969.

[3] J. N. S. Bidwell and M. J. Curran. 'The automorphism group of a split metacyclic p-group'. *Arch. Math. (Basel),* 87(6):488–497, 2006.

[4] N. Blackburn. 'On prime-power groups with two generators'. *Proc. Cambridge. Philos. Soc.,* 54:327–337, 1958.

[5] W. Bosma and J. J. Cannon. *Handbook of Magma functions* . Mathematics Department, University of Sydney, 1993.

[6] M. J. Curran. 'A Note on p-groups that are automorphism groups'. Proceedings of the Second International Group Theory Conference (Bressanone, 1989). *Rend. Circ. Mat. Palermo (2) Suppl.,* 23:57–61, 1990.

[7] M. J. Curran. 'The automorphism group of a nonsplit metacyclic p-group'. *Arch. Math. (Basel),* 90(6):483–489, 2008.

[8] M. J. Curran. 'The automorphism group of a split metacyclic 2-group'. *Arch. Math. (Basel),* 89(1):10–23, 2007.

[9] R. M. Davitt. 'The automorphism group of a finite metacyclic p-group'. *Proc. Amer. Math. Soc.,* 25(4):876–879, 1970.

[10] R. Faudree. 'A note on the automorphism group of a p-group'. *Proc. Amer. Math. Soc.,* 19(6):1379–1382, 1968.

[11] P. Hall. 'A contribution to the theory of groups of prime-power order'. *Proc. London Math. Soc.,* 36:29–95, 1933.

[12] C. E. Hempel. 'Metacyclic groups'. *Comm. Algebra,* 28(8):3865–3897, 2000.

[13] B. Huppert. 'Uber das Produkt von paarweise vertauschbaren zyklischen Gruppen'. *Math. Z.,* 58:243–264, 1953.

[14] B. W. King. 'Presentations of metacyclic groups'. *Bull. Austral. Math. Soc.,* 8:103–131, 1973.

[15] F. Menegazzo. 'Automorphisms of p-groups with cyclic commutator subgroup'. *Rend. Sem. Mat. Univ. Padova,* 90:81–101, 1993.

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

[17] E. A. Ormerod. 'The Wielandt subgroup of metacyclic p-groups'. *Bull. Austral. Math. Soc.,* 42:499–510, 1990.

[18] D. J. S. Robinson. *A Course in the Theory of Groups* . Springer-Verlag, New York, 1982.

[19] M. Schulte. 'Automorphisms of metacyclic p-groups with cyclic maximal subgroups'. *Rose-Hulman Undergraduate Research Journal,* 2(2), 2001.

[20] G. Silberberg. 'Finite equilibrated 2-generated 2-groups'. *Acta Math. Hungar.,* 110(1-2):23–35, 2006.

[21] Hyo-Seob Sim. 'Metacyclic groups of odd order'. *Proc. London Math. Soc. (3),* 69(1):47–71, 1994.