Automorphisms of non-Abelian p-groups

by

Kalina Mincheva

Submitted to

Central European University

Department of Department of Mathematics

In partial fulfulment of the requirements for the degree of Master of Science

Supervisor: Professor Pál Hegedűs

Budapest, Hungary

2010

Acknowledgments

I would like to express my gratitude to my advisor, Professor Pál Hegedűs, whose guidance, ideas and advice meant an indispensable help in writing the present thesis.

Table of Contents

Chapter 1

Introduction

The topic of p-groups with Abelian automorphism groups (Abelian $Aut(G)$) has interested researchers for years. One of the most significant fields of application and source of questions of group theory is cryptography. The security of a cryptosystem depends on the difficulty of the problem that the eavesdropper should solve in order to crack it, and group theory is a good source of such problems. Nilpotent and p-groups are very attractive for cryptographic purposes since they have nice presentation and computation in them is fast and easy. Researchers are working on protocols using non-Abelian groups for secret sharing or exchange of private keys over a non-secure channel.

The particular interest in the existence of a p-group with Abelian automorphism group is motivated by a cryptographic protocol proposed in [10].

Motivational Example

The protocol that Mahalanobis proposes in article [10] uses finite non-Abelian groups based on the Diffie-Hellman problem. It is the following: Let $G = \langle g \rangle$ be a cyclic group of order

n. We know $g,\ g^a,\ g^b$, where $a, b \in \mathbb{Z}$. Find g^{ab}. We can generalize the problem for a non-cyclic group. Let $\phi, \psi : G \to G\ \phi, \psi \in Aut(G)$ such that $\phi\psi = \psi\phi$ and let $a,\ \phi(a),\ \psi(a)$ be known. We want to find $\phi(\psi(a))$.

Using the generalized Deffie-Hellman problem one can construct the following protocol that can serve as a motivating example for studying p-groups and their automorphisms:

Two people - A and B - the left and the right column respectively agree on a group G.

Person A chooses a non-central element g, computes its image under the action of an automorphism of his/her choice and sends it to person B.

$g \in G \setminus Z(G)$, $\phi_A \in Aut(G) \quad \overrightarrow{\phi_A(g)} \quad \phi_A(g)$

Person B chooses another automorphism and sends the image of the received element to A. But A knows the initial automorphism ϕ_A therefore it knows its inverse and can compute $\phi_B(g)$.

${\phi_A}^{-1}\phi_B(\phi_A(g))$, $\phi_B(g) \quad \overleftarrow{\phi_B(\phi_A(g))} \quad \phi_B \in Aut(G)$

Person A chooses another automorphism ϕ_H and sends the image of $\phi_B(g)$ under it to B. Where B computes $\phi_H(g)$ because they know ϕ_B and therefore its inverse.

$\phi_H \in Aut(G),\ \phi_H(g) \quad \overrightarrow{\phi_H(\phi_B(g))} \quad \phi_H(g)$ via ϕ_B^{-1}

Note that the information they send to each other (middle column) is public so it can be "overheard". The private key is $\phi_H(g)$ and it should not be obtainable by the public information.

However there are cases when this problem is not difficult and the cryptosystem is not secure. Let ϕ_A and ϕ_B be such that $\phi(g) = gz_{\phi,g}$ for $z_{\phi,g} \in Z(G)$

As we will see later in the thesis this particular kind of automorphisms, that act by multiplication by a central element fix the derived subgroup G' pointwise. Thus if $Z(G) = G'$, we have that $\phi_B(gz_{\phi_A,g}) = gz_{\phi_B,g}z_{\phi_A,g}$. Thus we can compute $z_{\phi_B,g}$.

Since $\phi_H(\phi_B(g)) = gz_{\phi_B,g}z_{\phi_H,g}$ one can obtain $gz_{\phi_H,g} = \phi_H(g)$ which is the private key.

The automorphisms we consider in the above example, given by multiplication by a central element, constitute a subgroup of $Aut(G)$. The protocol proposed by Mahalanobis can work when this particular subgroup is Abelian. However the above example poses the question of the existence of a p-group whose whole automorphism group is Abelian but the center and the derived subgroup do not coincide.

In general very little is known about groups with Abelian automorphisms. There is no condition that ensures that a group has Abelian $Aut(G)$. It is well-known that apart from cyclic groups no commutative group has Abelian automorphism group. In the literature there are a few examples of non-Abelian p-groups with commutative $Aut(G)$. The first construction of such a group was given by G.A.Miller. This is why sometimes the p-groups with Abelian automorphism groups are referred to as Miller groups. The example he gave is listed under number 99 in the Hall-Senior tables [4] and it works only for $p = 2$. There are two more examples of Miller groups in the tables - number 91 and number 92 which are also 2-groups. There are a few generalizations of the above groups, some of which can be found in [10] and [7] but still the groups obtained have Abelian automorphism groups only for $p = 2$. Some of the most notable examples of families of Miller p-groups for arbitrary p, are given by Morigi [11], Jonah and Konvisser [8].

The groups from the Hall Senior table have the derived subgroup properly contained in the center. However for all known Miller groups, in the case when p is odd, the center and the derived subgroup coincide. It has been conjectured that all groups with Abelian automorphism groups for odd prime p have this property ($G' = Z(G)$).

In this thesis we give an example of a non-Abelian p-group, of order p^8, whose center properly contains the derived subgroup and has an Abelian automorphism group.

This thesis is structured in the following way. In chapter 2 we give some basic results from the theory of finite groups. We look at the necessary conditions for a group to have Abelian automorphism group focusing on both abelian and non-abelian p-groups in chapter 3 and 6 respectively. In chapter 4 we discuss the subgroup of automorphisms that act by multiplication by a central element. The existence of an automorphism which is not of this kind ensures that $Aut(G)$ is not Abelian. We show in chapter 5 a few ways to check if the group possesses such a "bad" automorphism. In the end we arrive at the counterexample for the conjecture proposed in [10] and investigate its minimality.

Chapter 2

Preliminaries on p-groups

In this section we give some basic definitions and well-known results from the theory of finite groups. We point out that by group we always understand a finite group.

2.1 Abelian p-groups

We will denote by C_k a cyclic group of order k. If G is an Abelian p-group there exists an integer $n \geq 1$ and integers $e_1, \ldots, e_n$ with $e_i \geq 1$ such that G is isomorphic to the direct product of the cyclic groups $C_{p^{e_i}}$. Moreover, the integer n and the integers e_i are uniquely determined (up to ordering) and we say that G is of type $p^{e_1}, \ldots, p^{e_n}$. An Abelian p-group is **homocyclic** of type p^e if $e_i = e$, for all $i = 1, \ldots, n$.

If an Abelian group G is homocyclic of type p, then G is called **elementary Abelian**. A p-group G is elementary Abelian if and only if G is Abelian and has exponent p. The **exponent** of a group G which we denote by $exp(G)$, is the least common multiple of the orders of all elements. An elementary Abelian group can always be seen as a vector space

over the field $\mathbb{F}_{\text{|}}$ with p elements.

2.2 Non-Abelian p-groups

In this section we introduce some random definitions and facts concerning non-Abelian p-groups.

If G is a group, we will denote by G' or $[G, G]$ its **derived subgroup**, the subgroup of G generated by all commutators $[x, y] = xyx^{-1}y^{-1}$, for $x, y \in G$. If z is a central element, $z \in Z(G)$, then $[xz, y] = [x, y] = [x, yz]$.

We denote by $Z(G)$ the **center** of G. The center of a p-group is non-trivial. Moreover if $G/Z(G)$ is cyclic, then G is Abelian.

Lemma 1. *In a non-Abelian p-group every maximal Abelian subgroup properly contains the center.*

P-groups are nilpotent. We call a group **nilpotent** when it has a finite central series. A **central series** is a sequence of normal subgroups

$$e = G_0 \leq G_1 \leq \cdots \leq G_n = G,$$

such that $[G, G_{i+1}] \subseteq G_i$, where $[G, H]$ denotes the commutator subgroup. The subgroups in a central series are always normal subgroups of G, so it makes sense to talk about G/G_i. A sequence G_i of normal subgroups of G is a central series if and only if $G_{i+1}/G_i \subseteq Z(G/G_i)$, where $Z(H)$ denotes the center of a group H.

As we noted, the central series is finite for a nilpotent group, in particular for a p-group, the number of steps in which it terminates is called the **nilpotency class** of G.

It is easy to see that the groups of nilpotency class 1 are the non-trivial Abelian groups. For

these groups we have $1 = [G, G, G] = [G', G]$ so that $G' \subseteq Z(G)$ or equivalently $G/Z(G)$ is Abelian.

For an arbitrary group G, the **Frattini subgroup** $\Phi(G)$ is defined as the intersection of all maximal subgroups of G. If G is a p-group, then the Frattini subgroup is the smallest normal subgroup of G with elementary Abelian quotient. This quotient is cyclic only when the group G is cyclic.

Lemma 2. $G' \subseteq \Phi(G)$

Proof. Since G' is the intersection of all normal subgroups with Abelian quotients, and $\Phi(G)$ is the intersection of all maximal subgroups, it suffices to show that any maximal subgroup is normal with Abelian quotient. Every maximal subgroup is normal, and hence maximal normal. The quotient is a simple p-group, moreover it is an Abelian group. Thus, every maximal subgroup is normal with Abelian quotient. □

Lemma 3. *Let G be a p-group of class two, and let G' have exponent p^e, then the exponent of $G/Z(G)$ divides p^e. In particular if G' is elementary Abelian then $G/Z(G)$ is elementary Abelian and $\Phi(G) \subseteq Z(G)$.*

Proof. Since the group G is class 2, then $G' \leq Z(G)$ and both G' and $G/Z(G)$ are Abelian. G' is elementary Abelian if and only if $e = 1$. To see that the central quotient is elementary Abelian it is enough to show that $exp(G/Z(G))$ divides p, and this is the assertion of the lemma when $e = 1$. Therefore since $\Phi(G)$ is the unique smallest normal subgroup having elementary Abelian factor, the lemma follows. □

Remark 1. *In fact we will see later in the thesis that when G is of class 2, $exp(G') = exp(G/Z(G))$.*

Definition 1. *A group is called **special** if $Z(G) = G' = \Phi(G)$. Furthermore if those subgroups are of order p then the group is **extra special**.*

We call a group G **purely non-Abelian (PN)** if it has no non-trivial Abelian direct factors.

We introduce the following piece of non-standard terminology, which Hegarty uses in [5].

Definition 2. *Two groups G and H will be called **hypomorphic** if*

$$G' \cong H',\ Z(G) \cong Z(H),\ G/G' \cong H/H',\ G/Z(G) \cong H/Z(H).$$

*We say that two groups are hypomorphic if they belong to the same **hypomorphism class**.*

2.3 Commutators

Before proceeding with the basic properties of commutators, observe that when G is of class 2, all commutators are central, that is

$$[xy, z] = [x, z]^y[y, z] = [x, z][y, z],$$

and thus the map $[\_, z]$ defines a homomorphism from G into G'.

Most of the computations in this thesis use the following basic properties of commutators:

Lemma 4. *Let G be a group and with $G' \leq Z(G)$, then*

- $[x_1x_2, y] = [x_1, y][x_2, y]$, *for all* $x_1, x_2, y \in G$;
- $[x, y_1y_2] = [x, y_1][x, y_2]$, *for all* $x, y_1, y_2 \in G$;

Proof. By elementary computation we get:

$$[x_1x_2, y] = x_1x_2yx_2^{-1}x_1^{-1}y^{-1} = x_1(x_2yx_2^{-1}y^{-1})yx_1^{-1}y^{-1} = [x_1, y][x_2, y]$$

and analogously for the second one. □

Lemma 5. *Let G is a group and let $x, y \in G$, such that $[x, y]$ commutes with x and y. Then*

- $[x, y]^k = [x^k, y] = [x, y^k]$;
- $(xy)^k = x^k y^k [y, x]^{\frac{1}{2}k(k-1)}$, *for all* $k \in \mathbb{Z}$

Remark 2. *Let G be a p-group of class at most 2 with p odd. If G' is elementary Abelian, then $(xy)^p = x^p y^p$, for all x, y in G.*

2.4 Automorphisms

Definition 3. *We call an automorphism σ of G **central** if σ commutes with every automorphism in $Inn(G)$, the group of inner automorphisms of G. Equivalently $g^{-1}\sigma(g)$ lies in $Z(G)$, for all $g \in G$. We denote the central automorphisms by $Aut_c(G)$. They fix the commutator subgroup G' of G pointwise and form a normal subgroup of the full automorphism group $Aut(G)$.*

Proposition 1. *If in a group G commutator subgroup and center coincide then every pair of central automorphisms commutes.*

Proof. Assume that the group is special. Then take $\phi, \psi \in Aut_c(G)$. Let $\phi(x) = xz_{\phi,x}$ and $\psi(x) = xz_{\psi,x}$, where $z_{\phi,x}$ and $z_{\psi,x}$ are central elements. Then by a simple calculation we see

$$\psi(\phi(x)) = \psi(xz_{\phi,x}) = \psi(x)z_{\phi,x} = xz_{\psi,x}z_{\phi,x} = xz_{\phi,x}z_{\psi,x} = \phi(\psi(x))$$

□

Definition 4. *A group G is called **Miller** if $Aut(G)$ is Abelian.*

Remark 3. *$Inn(G) \triangleleft Aut(G)$ and $G/Z(G) \simeq Inn(G)$*

Remark 4. *If G is non-Abelian Miller then G is nilpotent of class 2.*

($G/Z(G) \simeq Inn(G)$ and inner automorphism commute.)

Chapter 3

Automorphisms of Abelian groups

In this section we try to understand how the automorphism groups of Abelian groups look. We see that the only Abelian Miller groups are the cyclic ones. We conclude that the non-special Miller group we are interested in has to be a non-Abelian p-group.

3.1 Automorphisms of cyclic groups

Lemma 6. *If a group G is cyclic then the $Aut(G)$ is Abelian. Furthermore if G is cyclic of order n then $Aut(G)$ is cyclic of order $\phi(n)$, where ϕ is the Euler function.*

Proof. Let $G = \langle x \rangle$ and $|G| = n$. Take $\phi \in Aut(G)$, then $\phi(x)$ also has order n and $\phi(x) = x^k$ for some k such that $(n, k) = 1$. Conversely for every integer k, $(n, k) = 1$ the map $x^i \mapsto x^{ik}$ is an automorphism of G.

Furthermore, if $\phi_h, \phi_k \in Aut(G)$ then we have $\phi_k\phi_h(x) = (x^h)^k = x^{hk} = x^{\overline{hk}}$, where $\overline{hk}$ is $hk(mod\ n)$. Therefore $\phi_k\phi_h = \phi_{hk}$. From this we see that $Aut(G)$ is isomorphic to the multiplicative group of residue classes $(mod\ n)$ which is Abelian.

In the case when $n = p$ then $Aut(G)$ is isomorphic to the multiplicative group of a field of p elements, which is cyclic of order $p - 1$. □

3.2 Automorphisms of Abelian groups

Below we give a well-known result on the automorphism group of Abelian groups:

Theorem 1. *In the case when $G \cong H \times K$, where H and K are groups with relatively prime orders, then $Aut(G) \cong Aut(H) \times Aut(K)$.*

Proposition 2. *If G is a noncyclic Abelian group then, $Aut(G)$ is not Abelian.*

Proof. First let us assume that G has only two generators x and y. We may choose x and y in such a way so that the order m of x divides the order n of y, because we can write G as a direct product of cyclic groups in the form $G = C_1 \times C_2 \times \cdots \times C_r$, where the order h_i of C_i divides the order h_{i+1} of C_{i+1} for $i = 1, 2, \ldots m - 1$ and m is the smallest possible number of generators for G. Once we have chosen x and y we can define three mappings of G onto itself:

$$\alpha : x^s y^t \to x^{s+t} y^t$$

$$\beta : x^s y^t \to x^s y^{-t}$$

$$\gamma : x^s y^t \to x^t y^s$$

Because $m|n$, α is always well defined, non-trivial automorphism of G. If $n \neq 2$, then β is also a non-trivial automorphism of G and it does not commute with α. In the case when $n = 2$ we get β to be the identity map but in this case γ is a well defined automorphism that does not commute with α. Thus $Aut(G)$ is not commutative.

In the general case, we may assume again that G is product of cyclic subgroups, namely $G = C_1 \times C_2 \times \cdots \times C_r$ with each C_i dividing the order of the next. The $Aut(G)$ contains a

subgroup consisting of all automorphisms of G which leave the elements of $C_3 \times C_4 \times \cdots \times C_r$ fixed. This subgroup is isomorphic to $Aut(C_1 \times C_2)$ which is non-Abelian by the special case above. □

Proposition 3. *Let G be an Abelian group, then $|Aut(G)| \geq \phi(|G|)$, with equality if and only if G is (non-trivial) cyclic.*

Proof. If G is Abelian group, in particular if G is Abelian p-group, then by the structure theorem the $Aut(G)$ acts transitively on the elements of largest order. There are at least $\phi(|G|)$ such elements, because the elements of smaller order form a proper subgroup, of order at most $|G|/p$. Moreover if g is an element of largest order then provided that G is not cyclic, $G = \langle g \rangle \times B$, for some B subgroup of G and $|Aut(G)| \geq \phi(|G|)|Aut(B)| > \phi(|G|)$. □

Remark 5. *If G is Abelian and p^n divides $|G|$, for some prime p, then $p^{n-1}(p-1)$ divides $|Aut(G)|$.*

3.2.1 Automorphisms of elementary Abelian groups

Proposition 4. *If G is elementary Abelian p-group of order p^n, then $Aut(G)$ is isomorphic to the multiplicative group of all non singular $n \times n$ matrices with entries in the field of integers (mod p), in other words $Aut(G) \cong GL(n, p)$*

Proof. Since G is elementary Abelian then it is a direct product of n cyclic groups of order p. If V is a vector space of dimension n over $\mathbb{Z}_p$ - the field of integers (*mod* p), then V is additive Abelian group, which is clearly isomorphic to G. Therefore $Aut(G) \cong Aut(V)$. A

mapping α of V onto itself is an automorphism if it satisfies the following:

$$\alpha(u+v) = \alpha(u) + \alpha(v)$$
$$\alpha(mu) = m\alpha(u)$$

for each $u, v \in V$ and m integer. The two conditions above show us that α is a linear transformation of V. Thus $Aut(V)$ is the group of all invertible linear transformations of V onto itself. Therefore $Aut(V)$ is isomorphic to $GL(n, p)$. □

Chapter 4

The group of central automorphisms $Aut_c(G)$

As we already know the central automorphisms form a subgroup of $Aut(G)$. This section outlines results on how to compute the size of this subgroup and provides criteria for it to be commutative. In the search for a non-special Miller p-group, the following results are useful in eliminating certain hypomorphism classes of p-groups.

4.1 Criteria for central automorphisms to commute

As a subgroup of the group of automorphisms we need $Aut_c(G)$ to be Abelian. In [1] Adney and Yen give a criteria for a p-group G to have Abelian $Aut_c(G)$ based only on the hypomorphism class of G.

Let G be a purely non-Abelian group. Let $\sigma : G \to G$ be a central automorphism. Then $\forall x \in G$ the map $f_\sigma : x \mapsto x^{-1}x^\sigma$ is a homomorphism of G to $Z(G)$. The map $\sigma \mapsto f_\sigma$ is

a one to one map of $Aut_c(G)$ onto $Hom(G, Z(G))$. Conversely if $f \in Hom(G, Z(G))$ then $\sigma_f : x \mapsto xf(x)$ is endomorphism of G. Since

$$Ker(\sigma_f) = \{x \in G : f(x) = x^{-1}\},$$

it follows that σ_f is automorphism if and only if $f(x) \neq x^{-1}$, $\forall x \in G, x \neq 1$.

Theorem 2. *(Adney and Yen) The map $\sigma \to f_\sigma$ is a one to one map of $Aut_c(G)$ onto $Hom(G, Z(G))$, when G is purely non-Abelian (PN).*

Before giving the proof we need the following definition:

Definition 5. *The height of an element x in a finite Abelian p-group A is given by:*

$$height_A(x) = n \text{ if } x \in A^{p^n}, \text{ but } x \notin A^{p^{n+1}}.$$

Proof. Suppose that there exists a homomorphism $f \in Hom(G, Z(G))$, such that $f(z) = z^{-1}$, for some $z \in G, z \neq 1$. It follows that $z \in Z(G)$ from the definition of f. Assume that z is of order p, prime. Write $G/G' = G_{p'}/G' \times G_p/G'$, where G_p/G' is the p-primary component of G/G'. Then $zG' \in G_p/G'$ and $zG' \neq G'$, because G' is in the $Ker(f)$. Let the height of zG' in G_p/G' be p^k and let $z = x^{p^k}u$, for $x \in G_p$ and $u \in G'$. The we can write

$$z^{-1} = f(z) = f(x^{p^k}) = f(x)^{p^k}.$$

Set $y = f(x)^{-1}$. Then $z = y^{p^k}$, for $y \in Z \cap G_p$ and $\langle y \rangle \cap G' = 1$; Then yG' generates a direct factor of G_p/G', say $G_p/G' = \langle yG' \rangle \times H_p/G'$. Since $\langle y \rangle \cap G' = 1$, then $G = \langle y \rangle \times (H_p G_{p'})$ is a direct decomposition of G. Then it follows that G has an Abelian factor if the mapping $\sigma \mapsto f_\sigma$ is not onto. □

For any $f \in Hom(G, Z(G))$, there is a map $f' \in Hom(G/G', Z(G))$ since $f(G') = 1$. Furthermore, corresponding to $f' \in Hom(G/G', Z(G))$ there is a map $f : G \to Z(G)$, $f = \eta \circ f'$ where η is the natural epimorphism $G \to G/G'$.

Let G be of class 2, then by the fundamental theorem of Abelian groups we can decompose

$$G/G' = A_1 \times A_2 \times \cdots \times A_n \text{ where } A_i = \langle a_i \rangle$$

$$Z(G) = B_1 \times B_2 \times \cdots \times B_m \text{ where } B_i = \langle b_i \rangle.$$

If the cyclic component $A_k = \langle a_k \rangle$ has exponent greater or equal to the exponent of $B_j = \langle b_j \rangle$, then one can define a homomorphism $f : G/G' \to Z(G)$ in the following way:

$$f(a_i) = \begin{cases} b_j & \text{if } i = k, \\ 1 & \text{if } i \neq k. \end{cases}$$

We can see that $Im(f)$ of all $f \in Hom(G, Z(G))$, generates the subgroup

$$\begin{aligned} R(G) &= \langle Im(f) \mid f \in Hom(G, Z(G)) \rangle \\ &= \langle z \in Z(G) | o(x) \leq p^d \rangle, where p^d = min(exp(G/G'), Z(G)) \end{aligned}$$

Furthermore since G is of class 2, we have that

$$exp(G/G') \geq exp(G/Z(G)) = exp(G')$$

hence if $p^d = min(exp(G/G'), Z(G))$, then $p^d = exp(G')$ or $p^d > exp(G')$.

Denote the exponent of G' by p^b. If $height(xG') \geq b$, then $xG' = y^{p^b}G'$ for some $y \in G$. Then for any $F \in Hom(G, G')$ we have $F(yG')^{p^b} = 1$, hence $xG' \in Ker(F)$.

Conversely let $height(xG') < b$. Then from the previous discussion we know that there is a homomorphism $F \in Hom(G/G', G')$, such that xG' is not in the kernel, thus $\exists F \in Hom(G, G')$ such that $x \notin Ker(F)$.

Thus following [1] we define

$$K = \bigcap_{F \in Hom(G,G')} Ker(F) = \{x \in G, height(xG') \geq b\}.$$

Proposition 5. $K(G) \subseteq R(G)$.

Proof. Since $b = exp(G/Z(G))$ and $K \subseteq Z(G)$, an element $x \in K(G)$ has the form $x = y^{p^b}z$, for some $z \in G'$. denote $exp(G/G') = p^c$ Then since G is class 2, as we remarked earlier in the section $c \geq b$. Then $y^{p^c} \in G'$ and we have that $x^{p^c} = 1$ and $o(x) \leq min(exp(Z(G)), p^c)$. □

Proposition 6. *$R(G) \subseteq K(G)$, when G is PN and of class 2 with Abelian $Aut_c(G)$.*

Proof. We know from Theorem 2 that for PN group, $\sigma, \tau \in Aut_c(G)$ commute if the corresponding maps $f_\sigma, f_\tau \in Hom(G, Z(G))$ do. If follows that for any $f \in Hom(G, Z(G))$ and $F \in Hom(G, G')$, $f \circ F = F \circ f = 1$, as G' is contained in the $Ker(f)$. Thus $Im(f) \subseteq Ker(F)$, for any F any f. But by definition $K(G)$ is the intersection of $Ker(F)$, for all $F \in Hom(G, G')$ and $R(G)$ is generated by the set of all $f(G)$, $f \in Hom(G, Z(G))$. Thus we conclude that $R \subseteq K$. □

From the two propositions above we conclude that if G is PN, of class 2 and has Abelian central automorphism group, then $R(G) = K(G)$. In [1], Adney and Yen give necessary and sufficient condition that $Aut_c(G)$ is Abelian.

Lemma 7. *Let G be a class two p-group, and let $G/G' = \prod_{i=1}^{n} \langle G'x_i \rangle$. Define:*

$$K(G) = \langle x \in G | height_{G/G'}(G'x) \geq b \rangle, \text{ where } p^b = exp(G') \text{ and}$$
$$R(G) = \langle z \in Z(G) | o(x) \leq p^d \rangle, \text{where } p^d = min(exp(G/G'), exp(Z(G)))$$

Then $Aut_c(G)$ is Abelian iff $K(G) = R(G)$ and one of the following holds: either $b = d$ or $b < d$ and $R/G' = \langle G'x^{p^b} \rangle$, where x is chosen among $x_1, \ldots x_n$ such that $|x^{p^b}| = p^d$. In particular R/G' is cyclic.

Proof. In the above two propositions we saw that $R(G) = K(G)$ is a necessary condition. So assume that the conditions hold. Then as $R(G) = K(G)$, all elements of $R(G)$ are of the form $y^{p^b}z$, for some $z \in G'$. We look at the two cases:

If $b = d$, for every $f \in Hom(G, Z(G))$, we have that $f(y^{p^b}z) = 1$. Thus for any two homomorphisms $f, f' \in Hom(G, Z(G))$ we have that their composition is 1.

If $b < d$, Let $G/G' = \prod_{i=1}^{n} \{x_i G'\}$, then $R/G' = K/G' = \prod_{i=1}^{n} \{{x_i}^{p^b} G'\}$, then it is easy to check that R/G' is cyclic and is generated by ${x_1}^{p^b}$, where the exponent of R is attained at x_1. Then we can write $G/G' = \{x_1 G'\} \times G_1/G'$, where $exp(G_1/G') \leq p^b$.

Then for every $x \in G_1$, and $f \in Hom(G_1/G', R)$, we have that $f(x) = {x_1}^{sp^d}u$, where $u \in G'$ and $s = b + max(0, d - o(x_1 G'))$. Thus we have that for any two elements $f, f' \in Hom(G_1/G, R)$ we have $f'(f(x))$, for $x \in G_1$. Thus $Hom(G, Z(G)) = Hom(G, R(G))$ is commutative if $Hom(\{x_1 G'\}, R)$, which is, since R/G' is cyclic. □

4.2 On the size of $Aut_c(G)$

We can make an easy observation that if a group G has commutative $Aut(G)$ then every automorphism is central. This follows from the fact that the central automorphisms are by definition the the centralizer of the inner automorphisms of G. Thus if a group is Miller $Aut_c(G) = Aut(G)$.

In [14] Sanders provides a formula for computing the size of the group of central automorphisms. This information is useful in view of Hegarty's result in [5], which states that a Miller group has an automorphism group of size at least p^{12}. We will see later in the thesis that applying this result we can discard some hypomorphism classes for small powers of p. That is, if the size of the groups of central automorphisms is less than p^{12} we know that $Aut(G)$ cannot be Abelian.

Lemma 8. *(Sanders) Let G be a group with no-Abelian direct factors (PN group). Then*

$$|Aut_c(G)| = \prod_{i=1}^{k} |\Omega_i(Z(G))|^{r_i},$$

where p^k is the exponent of G/G', r_i are the invariants (direct factors) of G/G' and $\Omega_i(Z(G))$ is the subgroup of elements of the center whose order divides p^i.

Proof. From Theorem 2 we know that when G is PN there is a one-to-one map between $Aut_c(G)$ and $Hom(G, Z(G))$, given by $\sigma \mapsto f_\sigma$ in the terminology of the theorem. In particular $Aut_c(G) = Hom(G/G', Z(G))$. It is enough to compute the size of $Hom(G/G', Z(G))$. We remind that if K/G' is a direct factor of G/G', then any element of $Hom(K/G', Z(G))$ induces element on $Hom(G/G', Z(G))$ in a natural way, which is trivial on the complement of K/G'.

We decompose G/G' as a product of cyclic subgroups. Denote by C_{p^i} the cyclic group of order p^i. For each direct factor of G/G' of order p^i, we have the following

$$Hom(C_{p^i}, Z(G)) \cong \Omega_i(Z(G)).$$

Since G/G' has by definition r_i direct factors of order p^i, the result follows. □

Theorem 3. *(Hegarty) Let G be a finite non-cyclic p-group, p odd, for which Aut(G) is Abelian. Then p^{12} divides $|Aut(G)|$.*

Proof. We do not give the whole proof as it is very technical, we just give a brief sketch of author's approach. Hegarty looks at different hypomorphism classes of groups with Abelian $Aut_c(G)$ and $p^7 \leq |G| \leq p^{10}$. The author eliminates them one by one. We discuss the methods and constructions that he uses in detail in the following sections. □

Chapter 5

Some constructions of non-central automorphisms

As we remarked in the previous section when a group G has commutative $Aut(G)$ then every automorphism is central. Thus we can prove that the automorphism group of G is non-Abelian if we can construct a non-central automorphism. In the following section we present a few ways to construct (or show one cannot construct) a non-central automorphism.

The following Lemma proven by Earnley in [2] is central to the computations in this thesis. It gives a criterion for a group with homocyclic central quotient to posses a non-central automorphism.

Lemma 9. *Consider the extension* $1 \to Z \to G \to G/Z \to 1$ *where* G *is a* p*-group and* G/Z *is a direct product of* $n (n \geq 2)$ *copies of* C_{p^t} *for some fixed* t*. Let* $T : G/Z \to Z/Z^{p^t}$ *be the homomorphism given by* $(Zx)T = Z^{p^t}x^{p^t}$*. Also let* $[,] : G/Z \times G/Z \to Z$ *given by* $(Zx, Zy)[,] = [x, y]$ *and let* $\alpha \in Aut(G/Z)$ *and* $\beta \in Aut(Z)$*. Then* G *has an automorphism inducing* α *on* G/Z *and* β *on* Z *if and only if the following diagrams commute:*

$$\begin{array}{ccc} G/Z \times G/Z & \overset{[,]}{\to} & Z \\ \downarrow{\scriptstyle \alpha \times \alpha} & & \downarrow{\scriptstyle \beta} \\ G/Z \times G/Z & \overset{[,]}{\to} & Z \end{array} \qquad \begin{array}{ccc} G/Z & \xrightarrow{T} & Z/Z^{p^t} \\ \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \overline{\beta}} \\ G/Z & \xrightarrow{T} & Z/Z^{p^t} \end{array}$$

where $(Z^{p^t} z)\overline{\beta} = Z^{p^t}(z\beta)$.

Lemma 10. *Let N be a normal subgroup of group G such that G/N is cyclic of order n. Write $G/N = \langle Ng \rangle$. Let $x \in Z(N)$ such that $g^n = (gx)^n$. Then a map $\alpha : G \to G$ given by:*

$\alpha(n) = n$ *for every* $n \in N$

$\alpha(g) = gx$

can be extended to an automorphism of G.

Proof. First note that g and gx are on the same layer, as $g^n = (gx)^n$ Now we see how α extends to all elements of G. We know that $\alpha(gn) = (gx)n$, then $\alpha(g^k n) = g^k n x^{g^{k-1}+g^{k-2}+\cdots+1}$. It only remains to see that the extension of α is an automorphism - see that it preserves multiplication. Consider $\alpha((g^k n_1)(g^l n_2))$, that is

$$\alpha(g^{k+l} n_1 n_2) = (gx)^{k+l} n_1{}^{g^l} n_2.$$

On the other hand,

$$\alpha(g^k n_1)\alpha(g^k n_1) = g^k n_1 x^{g^{k-1}+g^{k-2}+\cdots+1} g^l n_2 x^{g^{l-1}+g^{l-2}+\cdots+1} = (gx)^{k+l} n_1{}^{(gx)^l} n_2.$$

But since $x \in Z(N)$ then these two are the same. □

Remark 6. *In the case when $x \in Z(N) \setminus Z(G)$, α extends to a non-central automorphism.*

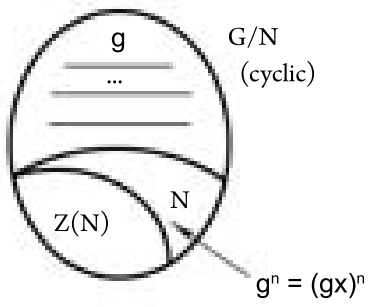

Figure 5.1: Illustration to the above lemma.

Remark 7. *Let N be a group and m be a positive integer, and $a \in N$ and let $\sigma \in Aut(N)$ such that $\forall x$ we have $a^\sigma = a$ and $x^{\sigma^m} = x^a$ then exists a group G up to isomorphism, such that N is a normal subgroup of G and with the following properties:*

$$(i)\ G/N = \langle gN \rangle \quad (ii)\ g^m = a \quad (iii)\ x^\sigma = x^g$$

The following two results are not used in the next sections, but we mention them without proofs for the sake of completeness.

Lemma 11. *Suppose a finite group G splits over an Abelian normal subgroup A. Then G has an automorphism of order 2, which inverts A elementwise.*

Lemma 12. *If $Aut(G)$ has an element of order 2, that leaves only the identity fixed, then G is Abelian of odd order.*

Chapter 6

Structure of a Miller group

In this section we make some final remarks on the necessary conditions for a group G to have Abelian $Aut(G)$. We discuss restrictions on the structure, the minimal number of generators of Miller group. We also show why the automorphism group of our Miller group should be a p-group.

Lemma 13. *$Aut(G)$ is non-Abelian if one of the following holds:*

- *$Z(G)$ is cyclic*
- *$exp(G) = p$*
- *the number of elements in a minimal generating system of G/Z is 2.*

Before mentioning the next results, we remind the reader that Miller groups are of class 2. The following result of Jafari can be found in [6].

Theorem 4. *(Jafari) Let p be an odd prime and let G be a finite purely non-Abelian (PN) group of class 2,*

- *$Aut_c(G)$ is elementary Abelian if and only if either $exp(Z(G)) = p$ or $exp(G/G') = p$.*
- *$Aut_c(G)$ is homocyclic of type $(p^n, \dots p^n)$ if and only if one of the following holds:*

  either $exp(Z(G)) = p^n$ and height $(xG') \geq p^n$ for all $x \in Z(G)$, and the invariants (direct factors) of the Abelian groups G/G' and $Z(G)$ have order greater than or equal to p^n

  or $exp(G/G') = p^n$ and $\Omega_n(Z(G)) \leq G'$ and the invariants (direct factors) of the Abelian groups G/G' and $Z(G)$ have order greater than or equal to p^n. Here $\Omega_n(Z(G))$ is the subgroup generated by the elements whose order is divisible by p^n

The above result is important for us, because in the case when G is Miller, we know that $Aut(G) = Aut_c(G)$. Thus the lemma provides a necessary condition for a group to have homocyclic and in particular elementary Abelian automorphism group.

Proof. It is enough to prove the homocyclic case as the first part of the theorem is just a special case. Assume that the group G is homocyclic of type p^n. Decompose $Z(G)$ and G/G' into (internal) direct product of cyclic subgroups.

$$G/G' = A_1/G' \times A_2/G' \times \cdots \times A_n/G',\ where A_i = \langle a_i \rangle$$
$$Z(G) = B_1 \times B_2 \times \cdots \times B_m,\ where B_i = \langle b_i \rangle.$$

Then as we saw in Lemma 8 that $|Aut_c(G)| = \prod_{i,j} |Hom(A_i/G', B_j)|$. Each $|Hom(A_i/G', B_j)| = p^n = gcd(|A_i/G'|, |B_j|)$, hence $|A_i/G'| \geq p^n$ and $|B_j| \geq p^n$. This means that both G/G' and $Z(G)$ have invariants of order greater than or equal p^n. They can not have both exponents exceeding p^n, as otherwise we have the following contradiction $p^n = |Hom(A_i/G', B_j)| = gcd(|A_i/G'|, |B_j|) > p^n$. We look at two cases

Case 1: $exp(G/G') = p^n$.

We write $G/G' = A_1/G' \times A/G'$, where $A_1/G' = \langle a_1 G' \rangle$, with $exp(A/G') = p^n$. Consider two homomorphisms $f \in Hom(A_1/G', Z(G))$ and $g \in Hom(A/G', Z(G))$. We have that $gf(a_i G') = fg(a_i G') = 1$, for every a_i. Thus we conclude

$$\Omega_n(Z(G)) = \bigcup_f Im(f) \leq \bigcap_g Ker(g) = \langle a_1 \rangle G'$$
$$\Omega_n(Z(G)) = \bigcup_g Im(g) \leq \bigcap_f Ker(f) = A$$

It follows that $\Omega_n(Z(G)) \leq A \cap \langle a_1 \rangle G' = G'$

Case 2: $exp(Z(G)) = p^n$.

We again write $G/G' = A_1/G' \times A/G'$ and consider the same automorphisms as in Case 1, $f \in Hom(A_1/G', Z(G))$ and $g \in Hom(A/G', Z(G))$.

$$Z(G) \leq \langle a_1 \rangle \{a \in A | height(aG') \geq p^n\}$$
$$Z(G) \leq A\{y \in \langle a_1 \rangle | height(yG') \geq p^n\}.$$

Hence $Z(G) \leq \{u \in G | height(uG') \geq p^n\}$.

For the reverse implication we again consider two cases:

Case 1: Assume $exp(G/G') = p^n$ and the conditions in the theorem hold and we want to see $Aut_c(G)$ is homocyclic of type p^n.

Take $f \in Hom(G/G', Z(G))$ and observe that $exp(Im(f)) \leq exp(G/G') = p^n$, as $Im(f) \leq G'$. It follows that $Aut_c(G)$ is Abelian. In particular it is easy to see that $Aut_c(G) = \prod_{i,j} \{\sigma_f | f \in Hom(A_i, B_j)\}$ and $|\{\sigma_f | f \in Hom(A_i, B_j)\}| = |Hom(A_i, B_j)| = p^n$. Thus $Aut_c(G)$ is homocyclic of type p^n.

Case 2: Assume $exp(G(Z)) = p^n$ and the conditions in the theorem hold and we want to see $Aut_c(G)$ is homocyclic of type p^n.

Take $f, g \in Hom(G/G', Z(G))$. If $x \in G$ then $\exists\ y \in G$ such that $y^{p^n}G' = f(x)G'$. Since $exp(G(Z)) = p^n$, we see that $gf(xG') = g(y^{p^n}G') = g(yG')^{p^n} = 1$. Hence $fg = gf = 0$ and thus $Aut_c(G)$.

□

Lemma 14. *Let G be a p-group of class 2. Then in the decomposition of $G/Z(G)$ as direct product of cyclic p-subgroups at least two factors of maximal order must occur, that is $exp(G/Z(G)) = p^c$, then $G/Z(G)$ has the form $C_{p^c} \times C_{p^c} \times C$, where C is some Abelian p-group, possibly trivial.*

Proof. Let $G/Z(G)$ be generated by $\{x_l, \ldots, x_n\}$, then G' is generated by $\{[x_i, x_j], i, j = 1, \ldots, n\}$. Let G' attain its exponent at some x. Then $[x, \_]$ has order equal to the order of x, by definition of commutator. As the group if of class 2 then $exp(G') = exp(G/Z(G))$. It is immediate to see that there are least two factors of maximal order. □

Remark 8. *In the above lemma C cannot be trivial if we want G to be Miller by Lemma* [13].

We continue with a few remarks on the minimal generating system of a Miller group. First result is found in [12].

Theorem 5. *(Morigi) For p an odd prime, there exists no finite non-Abelian three generator p-group having an Abelian automorphism group; thus the minimal number of generators for a p-group with this property is four.*

A previous weaker result on the size of the minimal generating set was given by Earnley in [2]. He claims that if the minimal generating set is 3 and G is special or has a derived subgroup of order p, it cannot be Miller.

We should point out that Morigi in [11] constructs the smallest example of a p-group

with Abelian automorphism group. She proves that there is no smaller non-Abelian Miller p-group. The group is of order p^7. It is special and is generated by 4 elements.

Proof. The proof of the theorem is very computational this is why we just give a brief sketch of the approach of the author. Let $exp(G) = p^m$ and $exp(G') = p^t$. Define a group

$$F = \langle x_1, x_2, x_3 | [x_i, x_j, x_k] = [x_i, x_j]^{p^t} = x_i^{p^{m+1}} = 1 \rangle.$$

Then there is a normal subgroup $N \triangleleft G$, such that $G \cong F/N$. Instead of considering all possible groups G, Morigi takes all pairs (F, N). For each pair she gives a matrix A, such that the corresponding automorphism of F normalizes N and induces non-central automorphism on F/N.

The author defines the following subgroup of F, $M = N \cap Z(F)$. Here $Z(F) = F' \times F^{p^t}$. Call the two projections be π_1 and π_2. Then $\pi_1(M) = V = M/M \cap F'$ and $\pi_2(M) = U = M/M \cap F^{p^t}$. It is easy to see that $V/M \cap F^{p^t} \cong U/M \cap F'$, which are Abelian groups (and we can express their automorphisms as matrices). The proof proceeds buy case by case analysis of cases depending on the number of direct factors of order p^t in the decomposition of $V/M \cap F^{p^t}$. □

We conclude this section with a few remarks on when $Aut(G)$ is a p-group.

An easy corollary from Lemma 8 is that if G is a p-group so is $Aut_c(G)$. Therefore if G has Abelian automorphism group, then $Aut(G)$ is a p-group.

A simple proposition from [14] tells us that when $Aut(G)$ a is p-group then G is PN.

Proposition 7. *If G is a group, such that the automorphism group is a p-group then G is either PN p-group G_p or $G \cong G_p \times C_2$.*

Proof. We are interested in the case when p is an odd prime. If G is Abelian then $|Aut(G)|$ is even, of course unless $|G| \leq 2$, then $|Aut(G)| = 1$.

Thus, assume that G is non-Abelian. Since $Aut(G)$ is p-group, so is $Inn(G)$ as a subgroup, but $Inn(G) \cong G/Z(G)$, so we conclude that the central quotient is nilpotent and so is G. Hence we can write G as product of nilpotent groups $G = G_p \times A$, where G_p is a Sylow p-group and A is Abelian p-group, but the order of A is not divisible by p. Thus by Theorem 1 $Aut(G) \cong Aut(G_p) \times Aut(A)$. G has an automorphism of order 2 unless $|A| \leq 2$. Thus $G = G_p$ or $G = G_p \times C_2$. G_p is PN, because otherwise $|Aut(G)|$ is even and we get a contradiction. □

Remark 9. *Furthermore in* [5] *the author shows that* $|G|$ *properly divides* $|Aut(G)|$ *when* G *is Miller.*

Chapter 7

The counterexample

In this section we present a counterexample of order p^8 to the conjecture in [10], by showing that there exists a Miller p-group that is not special. In next section we would investigate the minimality of the counterexample.

Consider a group G of order p^8 and class 2 such that

$$Z(G) \cong C_p \times C_p \times C_p \times C_p$$
$$G' \cong C_p \times C_p \times C_p$$
$$G/Z(G) \cong C_p \times C_p \times C_p \times C_p$$
$$G/G' \cong C_{p^2} \times C_p \times C_p \times C_p$$

It is generated by four elements $\{a, b, c, d\}$ which satisfy the following relations:

$$[a, b] = [c, d] \qquad b^p = 1$$
$$[b, c] = [a, d] \qquad c^p = [a, b][a, c][a, d]$$
$$[b, d] = [a, c] \qquad d^p = [a, c]$$

We first see that this group has Abelian $Aut_c(G)$ and then we prove that there are no non-central automorphisms, concluding that $Aut(G)$ is Abelian.

To verify that all central automorphisms commute we return to Lemma 7. We have to check that $K(G) = R(G)$, where

$$K(G) = \langle x \in G | height_{G/G'}(G'x) \geq b \rangle, \ where\ p^b = exp(G')\ and$$
$$R(G) = \langle z \in Z(G) | o(x) \leq p^d \rangle, \ where\ p^d = min(exp(G/G'), Z(G))$$

Here $exp(G/G') = p^2$ and $exp(Z(G)) = p \Rightarrow d = 1$. Since the center is elementary Abelian it is clear that $R(G) = Z(G)$.

To calculate $K(G)$ we look at

$$G/G' \cong C_{p^2} \times C_p \times C_p \times C_p = \langle aG' \rangle \times \langle bG' \rangle \times \langle cG' \rangle \times \langle dG' \rangle.$$

Then $K(G) = \langle x \in G | G'x = G'a^{pi}, \ for\ some\ i \rangle = \langle a^p \rangle G' = G^pG' = \Phi(G)$. But $\Phi(G) = Z(G)$ as the central quotient is elementary Abelian.

We also compute the size of $Aut_c(G)$. By Lemma 8 we know that

$$|Aut_c(G)| = \prod_{i=1}^{k} |\Omega_i(Z(G))|^{r_i} = (p^4)^3(p^4)^1 = p^{16}.$$

Since $|Aut_c(G)| > p^{12}$, we know that the subgroup of central automorphisms is big enough so that all automorphisms commute.

Since G' is elementary Abelian we can view it as a three dimensional vector space over the field $\mathbb{Z}_p$ by Proposition 4. Since the three commutators $[a, b]$, $[a, c]$ and $[a, d]$ are obviously independent, without loss of generality we can choose them as basis of G'. We denote them by x_1, x_2 and x_3 respectively. Thus

$$G' = \langle x_1 \rangle \times \langle x_2 \rangle \times \langle x_3 \rangle.$$

Similarly we can regard $Z(G)$ as a four dimensional vector space over $\mathbb{Z}_p$. We know that $G' \leq Z(G)$ and the hypomorphism class tells us that $Z(G)/G' = C_p$. So by the choosing $x_0 = a^p$ we have

$$Z(G) = \langle x_0 \rangle \times \langle x_1 \rangle \times \langle x_2 \rangle \times \langle x_3 \rangle = \langle x_0 \rangle \times G'.$$

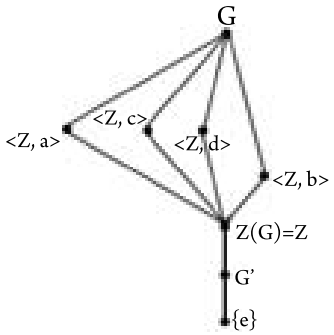

Figure 7.1: Part of the lattice of subgroups.

Suppose we have an automorphism σ on G. Then σ induces an automorphism α on $G/Z(G)$ and an automorphism β on $Z(G)$ which satisfy the conditions of Lemma 9. We prove that matrices associated to the automorphisms α and β are the identity matrices. Hence we conclude that every $\sigma \in Aut(G)$ is central.

Consider an automorphism $\alpha : G/Z(G) \longrightarrow G/Z(G)$. Since $G/Z(G)$ is elementary Abelian as before we can view it as a four dimensional vector space over the field $\mathbb{Z}_p$.

Similarly let β be the automorphism $\beta : Z(G) \longrightarrow Z(G)$. It can also be represented as a 4×4 matrix, as the center is elementary Abelian.

In view of Lemma 9 we are looking at α and β such that for all $g, h \in G$

$$[g^\alpha, h^\alpha] = [g, h]^\beta$$

$$(x^\alpha)^p = (x^p)^\beta$$

Observe that $(b^\alpha)^p = (b^p)^\beta = 1$. Thus we can write α by the following matrix

$$\alpha = \begin{pmatrix} i & j & k & m \\ 0 & e & 0 & 0 \\ q & f & n & r \\ s & w & t & y \end{pmatrix}$$

It is enough to see how these two automorphisms act on the four generators of G. We calculate the images of the generators of G under the two automorphisms

$$\begin{aligned}
[a^\alpha, b^\alpha] &= [a, b]^\beta = x_1^\beta \\
&= [a^i b^j c^k d^m, b^e] = [a^i, b^e][b^j, b^e][c^k, b^e][d^m, b^e] = x_1^{ie} x_2^{-me} x_3^{-ke} && (7.1) \\
[b^\alpha, c^\alpha] &= [b, c]^\beta = x_3^\beta \\
&= [b^e, a^q b^f c^n d^r] = [b^e, a^q][b^e, b^f][b^e, c^n][b^e, d^r] = x_1^{-qe} x_2^{er} x_3^{en} && (7.2) \\
[b^\alpha, d^\alpha] &= [b, d]^\beta = x_2^\beta \\
&= x_1^{-se} x_2^{ye} x_3^{te} && (7.3)
\end{aligned}$$

$$\begin{aligned}
(a^\alpha)^p &= (a^p)^\beta = x_0^\beta \\
&= (a^i c^k d^m)^p = (a^p)^i (c^p)^k (d^p)^m = x_0^i x_1^k x_2^k x_3^k x_2^m = x_0^i x_1^k x_2^{k+m} x_3^k && (7.4) \\
(c^\alpha)^p &= (c^p)^\beta = x_1^\beta x_2^\beta x_3^\beta \\
&= (a^q c^n d^r)^p = (a^p)^q (c^p)^n (d^p)^r = x_0^q x_1^n x_2^{n+r} x_3^n && (7.5) \\
(d^\alpha)^p &= (d^p)^\beta = x_2^\beta \\
&= (a^s c^t d^y)^p = x_0^s x_1^t x_2^{t+y} x_3^t && (7.6)
\end{aligned}$$

From (3) and (6) we get

$$x_2^\beta = x_0^s x_1^t x_2^{t+y} x_3^t = x_1^{-se} x_2^{ey} x_3^{te}$$

From here it follows that $s = 0$ and $t = 0$. We want to make a note that all computations are *mod p*. Therefore by $s = 0$ we actually mean $s \equiv 0(mod\ p)$. And since $y = ey$ we get that $e = 1$.

If we consider equations(1),(2),(3) and (5) and plug in the value we got for t, s and e we get

$$x_1^\beta x_2^\beta x_3^\beta = x_1^i x_2^{-m} x_3^{-k} x_1^{-q} x_2^r x_3^n x_2^y = x_0^q x_1^n x_2^{n+r} x_3^n$$

We can see that $q = 0$, $k = 0$ and $i = n = y - m$.

With these new results we see that the automorphism α looks like this

$$\alpha = \begin{pmatrix} i & j & 0 & m \\ 0 & 1 & 0 & 0 \\ 0 & f & n & r \\ 0 & w & 0 & y \end{pmatrix}$$

and we arrive at the following relations for β

$$x_0^\beta = x_0^i x_2^m, \qquad x_2^\beta = x_2^y$$
$$x_1^\beta = x_1^i x_2^{-m}, \qquad x_3^\beta = x_2^r x_3^{y-m}$$

We can rewrite these in matrix form corresponding to β

$$\beta = \begin{pmatrix} i & 0 & m & 0 \\ 0 & i & -m & 0 \\ 0 & 0 & i+m & 0 \\ 0 & 0 & r & i \end{pmatrix}$$

Now we look at the remaining relations

$$\begin{aligned}
[a^\alpha, d^\alpha] &= [a,d]^\beta = x_3^\beta \\
&= [a^i b^j c^k d^m, b^w c^t d^y] = x_1^{iw} x_2^{jy-mw} x_3^{iy} \qquad (7.7)\\
[c^\alpha, d^\alpha] &= [c,d]^\beta = x_1^\beta \\
&= [b^f c^n d^r, b^w c^t d^y] = x_1^{ny} x_2^{fy-rw} x_3^{-nw} \qquad (7.8)\\
[a^\alpha, c^\alpha] &= [a,c]^\beta = x_2^\beta \\
&= [a^i b^j c^k d^m, b^f c^n d^r] = x_1^{if-mn} x_2^{in+jr-mf} x_3^{ir+jn} \qquad (7.9)
\end{aligned}$$

From (7) we see that $iw = 0$ since x_3^β does not have x_1 component. But i cannot be 0, because the matrix corresponding to β has to be invertible. Therefore $w = 0$.

Still from (7) we see that $iy = y$. By the same argument as above, we cannot have a row of zeros in the matrix corresponding to an automorphism we conclude that $y \neq 0$ and $i = 1 \Rightarrow n = 1$.

From (8) we see that $ny = i = 1 \Rightarrow y = 1$; $fy = f = -m$ and $if - mn = f - m = 0 \Rightarrow f = m$ We can conclude that $f = m = 0$.

From (9) $r + j = 0 \Rightarrow r = -j$, but $in + jr = y = 1 \Rightarrow j^2 = 0 \Rightarrow j = r = 0$

When we plug these values in the matrices associated to α and β we see that both are the identity matrix. Thus in view of Lemma 9 all automorphisms of G are central, that is $Aut_c(G) = Aut(G)$. $Aut(G)$ is elementary Abelian, as $exp(Z(G)) = p$ and $|Aut(G)| = p^{16} (= |Aut_c(G)|)$.

Chapter 8

On the minimality of the counter-example

8.1 On the smallest non-Abelian with cyclic $Aut(G)$

Before discussing the existence of a group with smaller elementary Abelian $Aut(G)$ than the one proposed in the previous section we look at the groups with cyclic automorphism group. In fact we will see that the only p-groups for p odd, with cyclic $Aut(G)$ are the cyclic groups.

We refer to a simple observation of Flannery and MacHale in [3]:

Proposition 8. *The automorphism group of G is cyclic if and only if G is cyclic of order $1, 2, 4, p^r$ or $2p^r$, where p is an odd prime and r is a positive integer. In particular $Aut(G)$ is of prime power order if and only if $G \cong C_s$, where $s = 1, 2, 4, k, 2k$, where k is a Fermat prime.*

Proof. If $Aut(G)$ is cyclic, then $Inn(G)$ is cyclic and so is the central quotient as $Inn(G) \cong G/Z(G)$ by Remark 3. But then G has to be Abelian. Then by Lemma 6 G is cyclic of order n, for some n. $Aut(G)$ has order $\phi(n)$ and since it is cyclic, there exists a primitive root mod n. Hence $n = 1, 2, 4, p^r$ or $2p^r$, for p odd and $r \in \mathbb{N}$. □

So we see that there is no non-Abelian p-group, with p odd that has cyclic $Aut(G)$.

8.2 On the smallest non-special with elementary Abelian $Aut(G)$

The conditions that a group should satisfy to have an elementary Abelian $Aut(G)$ make it very easy to work with different hypomorphism classes of groups. For small powers of p it is fairly easy to construct a non-central automorphism. In this section we will check if the counterexample in the previous conjecture is indeed the smallest that has an elementary Abelian automorphism group such that the center properly contains the derived subgroup. We proceed by constructing a non-central automorphism for each of the hypomorphism classes corresponding to groups of order p^7.

Before going into computations we make an observation. Groups that we consider fall in one of the two major categories:

1. In the case where $G', Z(G), G/Z(G), G/G'$ are elementary Abelian we have $R(G) = Z(G)$ and $K(G) = G'$. Since we require Abelian central automorphisms by Lemma 7 we need $Z(G) = K(G) = R(G) = G'$. So in this case the group should be special. Of course even if a group satisfies the above conditions it does not mean it is Miller (see examples bellow).

2. In the case when $G', Z(G), G/Z(G)$ are elementary Abelian, we can have $R(G) =$

$Z(G) = K(G) > G'$. We want to see if the group can have elementary Abelian $Aut(G)$ for $|G| < p^8$.

To illustrate (1) we give the following two examples of groups from the literature, from [11] and [5] respectively:

Example 1. *Take G of order p^7 with the following structure:*

$G' = Z(G) = C_p \times C_p \times C_p$

$G/G' = G/Z(G) = C_p \times C_p \times C_p \times C_p$

from the lemma $b = d = 1$ and $R(G) = Z(G)$ and $K(G) = G'$. We have that $Aut_c(G)$ is Abelian. We also know that the group is Miller by Morigi's paper.

Example 2. *Take G of order p^7 with the following structure:*

$G' = Z(G) = C_p \times C_p$

$G/G' = G/Z(G) = C_p \times C_p \times C_p \times C_p \times C_p$

from the lemma $b = d = 1$ and $R(G) = Z(G)$ and $K(G) = G'$. We have that $Aut_c(G)$ is Abelian. We also know that the group is not Miller by Hegarty's paper.

In general the restriction on the exponent of the center and on the quotient by the derived subgroups gives us two hypomorphism classes:

Case 1: $exp(G/G') = p$

- If $G/G' \cong C_p$ then $|G/G'| = p$ which implies that G' is maximal Abelian group and since $G' \subseteq Z(G)$ then $G' = Z(G)$ and we get that $G/Z(G)$ is cyclic, hence G is Abelian. Therefore

  $G/G' \cong C_p \times \cdots \times C_p = {C_p}^k$, for $k > 1$.

- $G/Z(G) \cong C_p \times \cdots \times C_p = {C_p}^l$, for $l \leq k$, since $G/Z(G) \cong G/G'/Z(G)/G'$

- $G' \cong C_p \times \cdots \times C_p$ since $exp(G') = exp(G/Z(G)) = p$

The restriction on the size of the central quotient, namely it needs to have at least tree direct factors by Lemma 14, and the fact that the exponent of the derived subgroup should be the same as the one of the central quotient, give rise to only two hypomorphism classes:

Case 1.1

$$G/G' \cong C_p \times C_p \times C_p \times C_p$$
$$G/Z(G) \cong C_p \times C_p \times C_p$$
$$G' \cong C_p \times C_p \times C_p$$
$$Z(G) \cong C_{p^2} \times C_p \times C_p$$

Here $|Aut_c(G)| = \prod_{i=1}^{k} |\Omega_i(Z(G))|^{r_i} = (p^3)^4 = p^{12}$. We discuss this case at the end of the section.

Case 1.2

$$G/G' \cong C_p \times C_p \times C_p \times C_p \times C_p$$
$$G/Z(G) \cong C_p \times C_p \times C_p \times C_p$$
$$G' \cong C_p \times C_p$$
$$Z(G) \cong C_{p^2} \times C_p$$

However here $|Aut_c(G)| = \prod_{i=1}^{k} |\Omega_i(Z(G))|^{r_i} = (p^2)^5$. By Theorem 3 we know that the automorphism group is not Abelian.

Case 2: $exp(Z(G)) = p$

- $Z(G) \cong C_p \times \cdots \times C_p = {C_p}^k$ for $k > 1$, since cyclic center implies non-Abelian automorphism group.
- $G' \cong C_p \times \cdots \times C_p = {C_p}^{k-r}$ for some $r < k$, since $G' \leq Z(G)$
- $G/Z(G) \cong C_p \times \cdots \times C_p = {C_p}^m$, for $m > 2$, since $p = exp(G') = exp(G/Z(G))$

In this case since we need our $Aut_c(G)$ group to be Abelian we have a constraint on the way G' and $Z(G)$ relate to each other. We are left with two hypomorphism classes were $Aut_c(G)$ is Abelian - namely $K(G) = R(G)$ and $exp(G') = min(exp(G/G'), Z(G)) = p$ and has size p^{12}. We will show that in both cases we can construct a non-central automorphism.

Case 2.1

The first hypomorphism class is the following:

$$G' \cong C_p \times C_p \times C_p$$
$$Z(G) \cong C_p \times C_p \times C_p \times C_p$$
$$G/G' \cong C_{p^2} \times C_p \times C_p$$
$$G/Z(G) \cong C_p \times C_p \times C_p$$

Here $Z(G) = \Phi(G)$. We see that G is generated by at most 3 elements as the central quotient has three direct factors. Thus by Theorem 5 we conclude that the $Aut(G)$ is not Abelian. We can also proceed here by directly constructing a non-central automorphism using Lemma 9.

Case 2.2

The second hypomorphism class:

$$G' \cong C_p \times C_p$$
$$Z(G) \cong C_p \times C_p \times C_p$$
$$G/G' \cong C_{p^2} \times C_p \times C_p \times C_p$$
$$G/Z(G) \cong C_p \times C_p \times C_p \times C_p$$

By the same argument as in the previous case the size of the maximal Abelian group cannot be p^7 or p^6. And again since A properly contains the center $|A| = p^4$ or $|A| = p^5$.

In the case $|A| = p^4$, $A = \langle Z(G), a\rangle$, for some $a \in G \setminus Z(G)$. We have

$$|[a, G]| \leq |G'| = p^2, \text{ in other words } |G : C_G(a)| \leq p^2$$

but we have that $|G : C_G(a)| = p^3$, so $|A| \neq p^4$.

We conclude that $|A| = p^5$. As $|G'| = p^2$, then $|[A, g]| \leq p^2$, for all $g \in G$. Moreover $[A, g] \neq 1$, for all $g \in G \setminus A$. Here we have to look at two cases again:

1. Assume that A is elementary Abelian, i.e $A \cong C_p \times C_p \times C_p \times C_p \times C_p$.

   (a) Assume that $\exists\ b_1 \in G \setminus A$ such that $|[A, b_1]| = p$. Then

   $|A : C_A(b_1)| = p$, hence $\exists\ a_1 \in A \setminus Z(G)$ such that $[a_1, b_1] = 1$.

   We conclude that $A = \langle a_1, a_2, Z(G)\rangle$, where $[a_2, b_1] \neq 1$ by maximality of A and $G = \langle a_1, a_2, b_1, b_2\rangle$.

   We can construct automorphisms α and β on $G/Z(G)$ and $Z(G)$ respectively such that α is not the identity. By Lemma 9 exists a non-central automorphism of G which induces α and β. Take β to be the identity matrix and

$$\alpha = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$

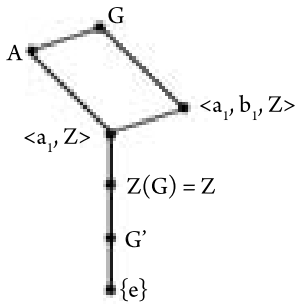

Figure 8.1: Part of the lattice of subgroups.

They satisfy the conditions of the lemma so we conclude that $Aut(G)$ is not Abelian.

(b) Assume that $\forall b \in G \setminus A$ such that $|[A, b]| = p^2$, i.e. $[A, b] = G'$.

Take $b_1 \in G \setminus A$, then $C_G(b_1) \cap A = Z(G)$ and $|G : C_G(b_1)| = p^2$. Note that $|C_G(b_1)| = p^5$ by the same argument as for the size of A. Then we get that $C_G(b_1) = \langle b_1, b_2, Z(G)\rangle$ and $G = \langle A, b_1, b_2\rangle$.

As remarked above $[A, b_1] = [A, b_2] = G'$, therefore $\exists\ a_1, a_2 \in A$ such that $[a_2, b_1] = [a_1, b_2]$. We would like to see that $a_2 \notin \langle a_1, Z(G)\rangle$. Assume the opposite, then $a_2 = a_1 z$, for some central element z. Then $[a_2, b_1] = [a_1 z, b_1] = [a_1, b_1] \Rightarrow [a_1, b_1 {b_2}^{-1}] = 1$. But this means that $|[A, b_1 {b_2}^{-1}]| \leq p$, contrary to the initial assumption. Therefore $a_2 \notin \langle a_1, Z(G)\rangle$ and $G = \langle a_1, a_2, b_1, b_2\rangle$.

As in the previous case wse use Lemma 9 to construct automorphisms α and β on $G/Z(G)$ and $Z(G)$ respectively induced by a non-central automorphism of G. Take β to be the identity matrix and

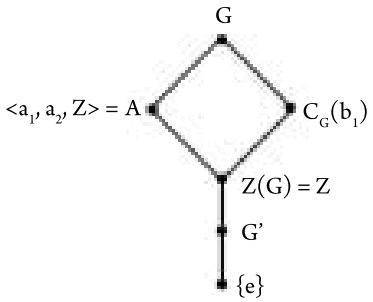

Figure 8.2: Part of the lattice of subgroups.

$$\alpha = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

They satisfy the conditions of the lemma so we conclude that $Aut(G)$ is not Abelian.

2. Assume that A is not elementary Abelian and $exp(A) \geq p^2$, i.e $A \cong C_{p^2} \times C_p \times C_p \times C_p$.

   In the case when $A \cong C_{p^2} \times Z(G)$, then G is generated by at most 3 elements and thus $Aut(G)$ is not Abelian by Theorem 5.

   Otherwise $Z(G) \cong \langle a_1^p \rangle \times \langle z_1 \rangle \times \langle z_2 \rangle$ and $A \cong \langle a_1, a_2, Z(G) \rangle$, where $o(a_2) = p$.

   As before we look at two cases:

   If $|[A, b_1]| = p$, for some $b_1 \in G \setminus A$, $\exists a_i \in A$ such that $[a_i, b_1] = 1$.

   If $[a_2, b_2] = 1$, then we can construct an automorphism on $G/Z(G)$, which by Lemma 9 is induced by a non-central automorphism on G.

$$\alpha = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

In fact the same argument as for $A \cong C_p \times C_p \times C_p \times C_p \times C_p$ works if $[b_1, b_2] = 1$.

If $[a_1, b_2] = 1$, it is easily seen that if $o(a_1) = p^2$ then $o(a_2) = o(b_1) = p$ by maximality of A. Furthermore $[a_2, b_1] \neq 1$ by the same argument. Let $[a_2, b_1] = u$. Consider the subgroup $A' = \langle x, y, Z(G) \rangle$, where $x, y \in \Omega_1 \setminus Z(G)$ and $[x, y] \neq 1$ and $B = \langle a_2, b_1, u \rangle$. Then $A' = B \times \langle z \rangle$, for $z \in Z$ and $G \cong \langle A', a_1, b_2 \rangle$. Then we can choose r_1, r_2, s_1, s_2 such that $b_1^{b_2} = b_1 u^{r_1} z^{s_1}$ and $a_2^{b_2} = a_2 u^{r_2} z^{s_2}$

if $s_1 \neq 0$ we may assume $s_2 = 0$, take $s_2 = s_1 k$. Replace b_1, a_2 and u in the following way $b_1' = b_1$, $a_2' = a_2 b_1^{-k}$ and $u' = [b_1', a_2']$. In this new basis consider $\beta = id$ and

$$\alpha = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & -r_2 & 0 & 1 \end{pmatrix}$$

in the case when $s_1 = 0$ then β is the identity matrix and

$$\alpha = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ r_1 & 0 & 0 & 1 \end{pmatrix}$$

$|[A, g]| = p^2 = |G'|$ In this case nothing outside the group commutes. Here like in case 1.1 deeper understanding about the group structure is needed to present a non-

central automorphism or show that such a construction is impossible. We note that unlike in the cases discussed until now β is not the identity matrix.

8.3 On the smallest non-special with homocyclic $Aut(G)$

In the case when $|G| = p^7$ there is one hypomorphism class that satisfies the necessary conditions for a group to have homocyclic $Aut_c(G)$.

$$G' \cong C_p$$
$$Z(G) \cong C_{p^2} \times C_{p^2}$$
$$G/Z(G) \cong C_p \times C_p \times C_p$$
$$G/G' \cong C_{p^2} \times C_{p^2} \times C_{p^2}$$

But we will see that central automorphisms do not commute. By Lemma 7. We have to check that $K(G) \neq R(G)$, where

$$K(G) = \langle x \in G | height_{G/G'}(G'x) \geq b \rangle, \ where\ p^b = exp(G')\ and$$
$$R(G) = \langle z \in Z(G) | o(x) \leq p^d \rangle, where\ p^d = min(exp(G/G'), Z(G))$$

We see that $R(G) = Z(G)$. However $1 = b < d = 2$, so we are in the second case of the lemma, and we have to see that $R(G)/G'$ is cyclic, but it's obviously not. So we conclude that the central automorphisms do not commute and therefore the group with this hypomorphism class is not Miller.

Chapter 9

Conclusion

In this thesis we presented a counterintuitive result, by constructing an example disproving the conjecture that for p odd every Miller group is special.

A natural direction for future research is to generalize the given example. In general there are three different ways in which one can do this, in either of the three "degrees of freedom" - number of generators, exponent of center and the prime.

In [7] Jamali gives an interesting construction. He generalizes the groups n. 91 and 92 from the Hall Senior tables [4] in two directions - size of exponent and number of generators. Other interesting generalizations can be found in [10] and [2]. The latter gives a generalization of the result of Jonah and Konvisser to $n + 2$ generators.

Bibliography

[1] J.E. Adney, Ti Yen *Automorphisms of p-groups*. Illinois J. Math. 9 (1965), 137-143

[2] B. E. Earnley, *On finite groups whose automorphism group is Abelian*. PhD thesis Wayne State University, 1975

[3] D. Flannery, D. MacHale *Some Finite Groups that are rarely automorphism groups - I*. Proc. of the Royal Irish Academy Vol 81A No.2, 209-215(1983)

[4] M. Hall, J.K. Senior *The groups of order* 2^n. The Macmillian Co., New York, 1964

[5] P. Hegarty, *Minimal Abelian automorphism groups of finite groups*. Rend. Sem. Mat. Univ. Padova, Vol 94, (1995) 121-135

[6] M.H. Jafari *Elementary Abelian p-Groups as Central Automorphism Groups* . Communications in Algebra, Volume 34, Issue 2 January 2006 , pages 601 - 607

[7] A. R. Jamali *Some new non-Abelian* 2*-groups with Abelian automorphism groups*. Journal of Group Theory, 5 (2002), 53-57

[8] D. Jonah, M. Konvisser *Some non-Abelian p-groups with Abelian automorphism groups*. Arch. Math. (Basel), 26 (1975), 131-133.

[9] D. MacHale *Some Finite Groups that are rarely automorphism groups - II*. Proc. of the Royal Irish Academy Vol 83A No.2, 189-196 (1983)

[10] A. Mahalanobis, *Diffie-Hellman key exchange protocol and non-Abelian nilpotent groups*. Israel Journal of Mathematics, 165, (2008), 161-187

[11] M. Morigi, *On p-groups with Abelian automorphism groups*. Rend. Sem. Mat. Univ. Padova, Vol 92, (1994), 47-58

[12] M. Morigi *On the minimal number of generators of finite non-Abelian p-groups having an Abelian automorphism group*. Communications in Algebra, Volume 23, Issue 6 1995 , pages 2045 - 2065.

[13] J. J. Rotman, *An introduction to the theory of groups*. Springer-Verlag, 1994.

[14] P. R. Sanders *Central Automorphisms of a finite group* J. London Math. Soc., 44 (1969), 225-228.