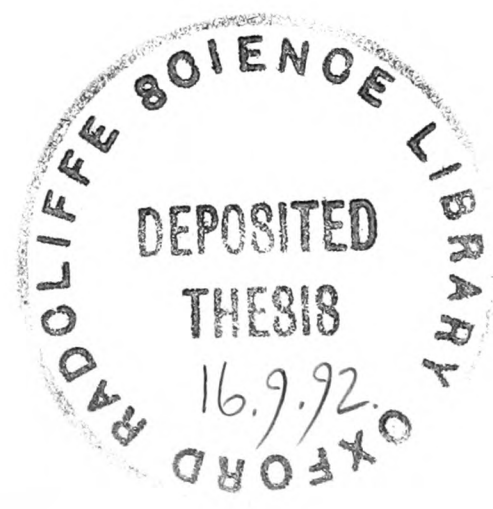
Group Enumeration

Simon Robert Blackburn
Lady Margaret Hall
Oxford

A Thesis submitted for the degree of
Doctor of Philosophy
Trinity Term 1992



Abstract

Group Enumeration

A Thesis submitted for the degree of Doctor of Philosophy

Simon Robert Blackburn
Lady Margaret Hall

Trinity Term 1992

The thesis centres around two problems in the enumeration of p-groups. Define $f_\Phi(p^m)$ to be the number of (isomorphism classes of) groups of order p^m in an isoclinism class Φ. We give bounds for this function as Φ is fixed and m varies and as m is fixed and Φ varies. In the course of obtaining these bounds, we prove the following result. We say a group is *reduced* if it has no non-trivial abelian direct factors. Then the rank of the centre $Z(P)$ and the rank of the derived factor group P/P' of a reduced p-group P are bounded in terms of the orders of $P/Z(P)P'$ and $P' \cap Z(P)$.

A long standing conjecture of Charles C. Sims states that the number of groups of order p^m is

$$p^{\frac{2}{27}m^3+O(m^2)}. \tag{1}$$

We show that the number of groups of nilpotency class at most 3 and order p^m satisfies (1). We prove a similar result concerning the number of graded Lie rings of order p^m generated by their first grading.

Acknowledgements

First and foremost, I would like to thank my supervisor Dr Peter M. Neumann. He has suggested many interesting problems to work on and his constant enthusiasm has made the time spent on trying to find their solution a great pleasure. Thanks are also due to my supervisor throughout my first year, Dr Martin Powell, who directed my interests towards group enumeration and to whom I owe the solid grounding in group theory that I have absorbed while at Oxford.

Thanks to all the Algebra graduate students for providing such a friendly atmosphere in which to work. Special mention is due to Geetha, John, Julia and Meenaxi for having to put up with sharing the same room as me for all these months.

On a less directly mathematical note, I would like to thank the members of Lady Margaret Hall – Middle Common Room members, Fellows and staff – for providing me with such an enjoyable social life during the last three years.

I am grateful to the Science and Engineering Research Council for providing me with the funding which enabled me to study for a D.Phil.

Contents

Chapter 1

Introduction

This introductory chapter is divided into two sections. The first section gives an outline of the history of group enumeration. The second section lists and gives motivation for the new results included in the later chapters.

Throughout, p will denote a prime. All groups are finite unless specified otherwise.

1.1 Enumeration of Groups: A History

If n is a positive integer, define $f(n)$ to be the number of (isomorphism classes of) groups of order n. We will concentrate on those papers within group enumeration which investigate this function. Papers which do not address this subject but nevertheless fall within the demesne of group enumeration include [2, 4, 12, 14, 15, 17, 18, 19, 22].

The first substantial progress in group enumeration came with Graham Higman's 1960 paper [11], in which he shows that the number $f(p^m)$ of groups

of order p^m satisfies

$$p^{(\frac{2}{27}-\epsilon_m)m^3} \leq f(p^m) \leq p^{(\frac{2}{15}+\epsilon_m)m^3}$$

where ϵ_m depends only on m and tends to 0 as m tends to ∞. Higman obtains the lower bound by counting a certain class $\mathcal{H}_p$ of groups of nilpotency class 2. In 1965, Charles Sims [24] showed that the groups in $\mathcal{H}_p$ provide the leading term for $f(p^m)$ when he proved that

$$f(p^m) = p^{\frac{2}{27}m^3+O(m^{8/3})}.$$

I hear from Mike Newman that the error term has been brought down to $O(m^{5/2})$ in joint work by Craig Seeley and himself.

Inspired by Sims' beautiful theorem, a clutch of papers appeared in the late sixties ([5, 8, 21]) which attempted to generalise the result to groups of arbitrary order. These results were sharpened in McIver and Neumann's 1987 paper [16] in which, amongst other things, they show that

$$f(n) \leq n^{\mu^2+\mu+2}$$

where μ is the largest integer such that p^μ divides n for some prime p. More recently, Pyber shows [23] that the number of groups of order n with specified Sylow subgroups is at most

$$n^{75\mu+16}.$$

This theorem has the corollary, when taken together with Sims' Theorem, that

$$f(n) \leq n^{\frac{2}{27}\mu^2+O(\mu^{5/3})}.$$

1.2 An Overview of the Thesis

The remainder of the work is divided into seven chapters and two appendices.

Chapter 2 contains some background material: All the results and methods contained in this chapter are either contained in [11] or are trivial modifications of the work there. The construction of groups of Φ-class 2 is used in Chapter 4, the results concerning enumeration of 'small' varieties of p-groups are used in Chapter 8.

Chapter 3 concerns itself with the proof of the following theorem concerning reduced groups:

Definition 1 *A group P is* reduced *if whenever there exist groups Q and D such that D is abelian and $P = Q \times D$, then D is trivial.*

Theorem 1 *Let P be a reduced p-group and suppose that $|P' \cap Z(P)| = p^n$ and $|P/P'Z(P)| = p^a$. Then:*

(i) *The rank of $Z(P)$ is at most $a + n$.*

(ii) *The rank of P/P' is at most $a + n$.*

We include this theorem both because it is of interest in its own right and because we use part (i) in Chapter 4.

Chapter 4 contains results concerning enumeration of isoclinism classes of p-groups. Two groups P_1 and P_2 are said to be *isoclinic* if there exist isomorphisms $\phi : P_1/Z(P_1) \longrightarrow P_2/Z(P_2)$ and $\psi : P_1' \longrightarrow P_2'$ such that the

diagram

$$\begin{array}{ccccc} & & P_1/Z(P_1) \times P_1/Z(P_1) & \xrightarrow{[,]} & P_1' & \\ \phi \times \phi & & \downarrow & & \downarrow & \psi \\ & & P_2/Z(P_2) \times P_2/Z(P_2) & \xrightarrow{[,]} & P_2' & \end{array}$$

commutes, where the horizontal maps are induced in the natural way from the commutator maps in P_1 and P_2. The relation of being isoclinic is an equivalence relation: We will call equivalence classes under this relation *isoclinism classes*. Isoclinism was introduced by Philip Hall in [10] in order to simplify the classification of p-groups (he calls isoclinism classes *families* of groups). There are two very natural questions to ask concerning isoclinsm which we address here.

Question 1 *Suppose we fix a prime p and a positive integer m and consider groups of order p^m. How large can we expect a single isoclinism class of groups of order p^m to be?*

We prove:

Theorem 2 *Given any isoclinism class Φ, the number of groups of order p^m in Φ is at most*

$$p^{\frac{1}{3}m^2} f_{\mathrm{ab}}(p^m), \tag{1.1}$$

where $f_{\mathrm{ab}}(p^m)$ is defined to be the number of abelian groups of order p^m.

It is known (see [1, Chapter 6]) that

$$f_{\mathrm{ab}}(p^m) \sim \frac{1}{4m\sqrt{3}} e^{\pi\sqrt{\frac{2}{3}}\sqrt{m}}$$

so Theorem 2 says that the number of groups of order p^m in Φ is at most $p^{\frac{1}{3}m^2+O(m^{1/2})}$. We will give an example of an isoclinism class Φ (depending on m) which contains at least $p^{\frac{1}{8}(m^2-9)}$ groups, so Theorem 2 is reasonable. By the Higman–Sims result that $f(p^m) = p^{\frac{2}{27}m^3+O(m^{8/3})}$, Theorem 2 has the corollary that

Corollary 1 *The number of isoclinism classes of p-groups of order p^m is*

$$p^{\frac{2}{27}m^3+O(m^{8/3})}.$$

Question 2 *Suppose we fix a prime p and an isoclinism class of p-groups Φ. What can we say about the number of groups of order p^m in Φ as m varies ?*

We prove:

Theorem 3 *Let Φ be an isoclinism class. Define $f_\Phi(p^m)$ to be the number of groups of order p^m in Φ. Then*

$$\frac{f_\Phi(p^m)}{f_{\mathrm{ab}}(p^m)} \leq cm^k$$

where c and k are constants depending only on Φ.

In fact, if in the above theorem we have $P \in \Phi$ with $|P/(Z(P)P')| = p^a$ and $|P' \cap Z(P)| = p^n$, then we show we may take c and k to be

$$c = (a+n+1)2^{\frac{1}{2}(a+n)}p^{(a+n)^2}$$

and

$$k = \frac{1}{2}(a+n).$$

The theorem has the following simple corollary.

Corollary 2 *Let Φ be an isoclinism class. Then*

$$f_\Phi(p^m) = e^{\pi\sqrt{\frac{2}{3}}\sqrt{m}+O(\log m)}.$$

The proof of Theorem 3 shows that the leading term in $f_\Phi(p^m)$ is provided by the variety of abelian groups which can be chosen for the centre of a group in Φ, rather than by the number of groups in Φ having a given centre, when we consider large values of m.

My D.Phil Examiners have kindly pointed out that the results contained in Chapter 4 may be proved more slickly using the Universal Coefficients Theorem (See [3, page 34]). This method of proof still relies on the results contained in Chapter 3.

The results contained in Chapters 5,6 and 7 surround a conjecture — now more than 27 years old — published by Sims in [24]:

Conjecture 1 (Sims) *The number of groups of order p^m is*

$$p^{\frac{2}{27}m^3+O(m^2)}.$$

If this conjecture is true, Pyber's Theorem would imply that

$$f(n) = n^{\frac{2}{27}\mu^2+O(\mu)}.$$

We prove two results, both strongly suggesting that Sims' conjecture is true. In Chapter 5 we prove:

Theorem 4 *Let $p > 2$. The number of groups of exponent p, nilpotency class at most 3 and order p^m is*

$$p^{\frac{2}{27}m^3+O(m^2)}.$$

This is a weaker result than that contained in Chapter 7: It is included because the proof contains all of the essential ideas developed in full in Chapters 6 and 7, without many of the obscuring details.

Chapter 6 is concerned with proving:

Theorem 5 *The number of graded Lie rings*

$$L = L_1 \oplus \cdots \oplus L_c$$

of order p^m *and where* L *is generated by* L_1 *is at most*

$$p^{\frac{2}{27}m^3+O(m^2)}.$$

This theorem is proved by a straightforward extension of the methods developed in the proof of Theorem 4.

Chapter 7 proves the extension of Theorem 4:

Theorem 6 *The number of groups of class at most 3 and order* p^m *is*

$$p^{\frac{2}{27}m^3+O(m^2)}.$$

An extension of Theorem 6 to groups of nilpotency class more than 3 or of Theorem 5 to arbitary nilpotent Lie rings by a naive generalisation of their methods has proved difficult, although it is quite possible that a small improvement in these methods might provide a proof of the Sims conjecture. This is a project for the future.

Chapter 8 investigates the enumeration functions of the two smallest non-abelian varieties of p-groups when $p > 2$. Define $\mathcal{B}_{p,k}$ to be the variety of

groups of exponent p and nilpotency class at most k. Define $\mathcal{H}_p$ to be the variety of groups whose Frattini subgroup is central and of exponent p. For a variety $\mathcal{U}$, define $\mathcal{U}(m)$ to be the set of groups in $\mathcal{U}$ of order p^m. We prove that

Theorem 7 *If p is odd, then*

$$\frac{|\mathcal{H}_p(m)|}{|\mathcal{B}_{p,2}(m)|} \leq p^{\frac{2}{9}m^2+O(m^{3/2})}.$$

It is to be hoped that more results of this type — concerning the ratios of enumeration functions of varieties of p-groups — could be proved once Sims' conjecture is settled.

The two appendices contain results used in earlier chapters which have been postponed to an appendix due to a combination of their length and their comparative lack of depth. Appendix A contains the proof, deferred from Chapter 3, that a function $\hat{\alpha}$ is a homomorphism. Appendix B contains the proof that a binary operation defined in Chapter 4 is, in fact, a group operation.

Any background material concerning p-groups which we use (such as properties of the Frattini subgroup and construction of the associated Lie ring of a group) can be found in [9]. The basic theory of varieties can be found in the early chapters of [20]. All the work that follows is original, excepting Chapter 2.

Chapter 2

Background Material

2.1 Enumeration of p-Groups of Class 2

All the results in this section are either contained in G. Higman's paper [11] on the enumeration of groups of order p^m or are obtained by trivial modifications of his methods. We begin by reproducing the bounds given in [11] for the number of groups of order p^m with a central, elementary abelian Frattini subgroup. Higman derives these bounds from estimating the number of a certain class of p-groups, namely groups of 'Φ-complexion (r, s)'.

Definition 2 *A p-group G is of Φ-complexion (r, s) if $\Phi(G)$ is central, elementary abelian of order p^s and has index p^r in G.*

Let p^m be a prime power. Define $f_{r,s}(p^m)$ to be the number of (isomorphism classes of) groups of order p^m and of Φ-complexion (r, s). The next theorem gives bounds for $f_{r,s}(p^m)$.

Theorem 8 *If $s + r = m$ and $s \leq \frac{1}{2}r(r+1)$ then*

$$p^{\frac{1}{2}rs(r+1)-r^2-s^2} \leq f_{r,s}(p^m) \leq p^{\frac{1}{2}rs(r+1)-s(s-1)}.$$

Proof: Let X_r be the free group on r generators $x_1, \ldots, x_r$ and let R be the subgroup of X_r generated by $x^{p^2}, [x,y]^p$, $[x^p, y]$ and $[x,y,z]$ for all $x, y, z \in X_r$. Define $H = X_r/R$. Note that a group P can be expressed as a quotient of H if and only if it is a p-group generated by at most r elements and $\Phi(P)$ is both central and elementary abelian.

Let G be a p-group of Φ-complexion (r,s). Since $|G/\Phi(G)| = p^r$, G is generated by r elements. Since $\Phi(G)$ is central and elementary abelian, G is a quotient of H: Let $G \cong H/N$, say. Since a generating set of G containing r elements is irredundant, N is contained in $\Phi(H)$.

Since all the groups that we are counting correspond to quotients of H by subgroups of $\Phi(H)$, we investigate the structure of $\Phi(H)$. We have that $\Phi(H)$ is elementary abelian by definition of R, and so it remains to find the dimension of $\Phi(H)$. Suppose $h_1, \ldots, h_r$ is a free generating set of H. We have that $\Phi(H)$ is generated by $h_1^p, \ldots, h_r^p$ together with the derived group H'. Now H' is generated by the elements $[h_i, h_j]$ where $1 \leq i < j \leq r$ and their conjugates, i.e. by these elements themselves since H' is central. Hence $\Phi(H)$ is generated by the $\frac{1}{2}r(r+1)$ elements:

$$h_i^p \text{ where } 1 \leq i \leq r \text{ and } [h_i, h_j] \text{ where } 1 \leq i < j \leq r.$$

Suppose that this generating set is not minimal. Then there exists a non-trivial relation:

$$\prod h_i^{p\alpha_i} \prod [h_i, h_j]^{\beta_{ij}} = 1 \tag{2.1}$$

for some integers $0 \leq \alpha_i, \beta_{ij} < p$ not all 0. Since this is a relation between free generators of H,

$$\prod g_i^{p\alpha_i} \prod [g_i, g_j]^{\beta_{ij}} = 1$$

for any elements g_i in a p-group which is a quotient of H. But putting g_i generating a cyclic group of order p^2 and $g_j = 1$ for $j \neq i$ gives $\alpha_i = 0$, and then taking g_i and g_j generating a non-abelian group of order p^3 gives $\beta_{ij} = 0$. Hence no non-trivial relation (2.1) holds and so $\Phi(H)$ is of order $p^{\frac{1}{2}r(r+1)}$.

Consider a subgroup N of $\Phi(H)$ such that H/N is of Φ-complexion (r, s) and hence of order p^{r+s}. Then since $|H/\Phi(H)| = p^r$, we have the index of N in $\Phi(H)$ is p^s. Conversely, if N is a subgroup of $\Phi(H)$ of index p^s then H/N is a group of Φ-complexion (r, s). The number of subgroups of $\Phi(H)$ of index p^s is equal to the number of subgroups of $\Phi(H)$ of order p^s, by duality (since we may regard $\Phi(H)$ as a vector space over $\mathbb{F}_p$). Hence the number of such subgroups is:

$$\frac{(p^{\frac{1}{2}r(r+1)} - 1)(p^{\frac{1}{2}r(r+1)} - p) \ldots (p^{\frac{1}{2}r(r+1)} - p^{s-1})}{(p^s - 1)(p^s - p) \ldots (p^s - p^{s-1})}.$$

Since any p-group of Φ-complexion (r, s) occurs as a quotient of H by one of these subgroups, there are at most

$$\frac{(p^{\frac{1}{2}r(r+1)} - 1)(p^{\frac{1}{2}r(r+1)} - p) \ldots (p^{\frac{1}{2}r(r+1)} - p^{s-1})}{(p^s - 1)(p^s - p) \ldots (p^s - p^{s-1})} \leq p^{\frac{1}{2}rs(r+1) - s(s-1)}$$

p-groups of Φ-complexion (r, s) and the upper bound follows. If we can put an upper bound on the maximum number of subgroups of index p^s in $\Phi(H)$

that produce isomorphic quotients of H, then we have found a lower bound for the number of p-groups of Φ-complexion (r, s).

Let N_1 and N_2 be subgroups of $\Phi(H)$ of index p^s and suppose

$$\alpha : H/N_1 \longrightarrow H/N_2$$

is an isomorphism which maps h_iN_1 to k_iN_2, say. Since the h_i are a free generating set, the map $h_i \mapsto k_i$ can be extended to an endomorphism β of H. The k_i generate H modulo N_2, so certainly they generate H modulo $\Phi(H)$. Hence the k_i generate the whole of H and β is an isomorphism. Trivially, if $\beta \in \mathrm{Aut}(H)$ then $H/N \cong H/\beta(N)$, so there is a 1–1 correspondence between groups of Φ-complexion (r,s) and orbits of the set of subgroups of $\Phi(H)$ of index p^s under the action of $\mathrm{Aut}(H)$. If we can find an upper bound for the length of an orbit, then we can find a lower bound for p-groups of Φ-complexion (r, s).

The length of any given orbit is at most $|\mathrm{Aut}(H)/X|$ where we define X to be the set

$$\{\beta \in \mathrm{Aut}(H) : \beta \text{ is the identity on } \Phi(H)\}$$

Hence the number of p-groups of Φ-complexion (r, s) is at least:

$$\frac{\text{the number of subgroups of } \Phi(H) \text{ of index } p^s}{|\mathrm{Aut}(H)/X|}$$

We show that $|\mathrm{Aut}(H)/X| \leq |\mathrm{Aut}(H/\Phi(H))|$. Define the natural map $\phi : \mathrm{Aut}(H) \longrightarrow \mathrm{Aut}(H/\Phi(H))$. Then if $\beta \in \ker \phi$ we have $\beta h_i = h_i x_i$ for some $x_i \in \Phi(H)$. Hence β is the identity on $\Phi(H)$ (as it is the identity on

h_i^p, $1 \leq i \leq r$ and $[h_i, h_j]$, $1 \leq i < j \leq r$). Therefore $\ker \phi \leq X$,so:

$$\begin{aligned}\left|\frac{\mathrm{Aut}(H)}{X}\right| &\leq \left|\frac{\mathrm{Aut}(H)}{ker\phi}\right| \\ &\leq |\mathrm{Aut}(H/\Phi(H))| \\ &= (p^r-1)(p^r-p)\ldots(p^r-p^{r-1}).\end{aligned}$$

Hence we have that the number of p-groups of Φ-complexion (r,s) is at least:

$$\frac{(p^{\frac{1}{2}r(r+1)}-1)(p^{\frac{1}{2}r(r+1)}-p)\ldots(p^{\frac{1}{2}r(r+1)}-p^{s-1})}{(p^s-1)(p^s-p)\ldots(p^s-p^{s-1})(p^r-1)(p^r-p)\ldots(p^r-p^{r-1})}$$

which is greater than $p^{\frac{1}{2}r(r+1)s-r^2-s^2}$ and the result follows. □

We use the bounds given above to enumerate groups with a central, elementary abelian Frattini subgroup.

Theorem 9 *Let p^m be a prime power. If we define $\mathcal{H}_p(m)$ to be the number of (isomorphism classes of) groups of order p^m with a central, elementary abelian Frattini subgroup, then*

$$p^{\frac{2}{27}(m^3-6m^2)} \leq \mathcal{H}_p(m) \leq (m-1)p^{\frac{2}{27}m^3+\frac{11}{24}m}$$

if $m \geq 2$.

Proof: The lower bound is trivially true for $m \leq 6$, so we may assume $m \geq 6$. Obviously, $\mathcal{H}_p(m) \geq f_{r,s}(p^m)$ for any r, s such that $r+s=m$. If we put $r = (2m-\delta)/3$ and $s = (m+\delta)/3$ where δ is one of 0,1 or 2 chosen so as to make r and s integral then since $s \leq \frac{1}{2}r(r+1)$ we can apply the previous

theorem to obtain:

$$f_{r,s}(p^m) = \begin{cases} p^{\frac{2}{27}(m^3-6m^2)} & \text{if } \delta = 0 \\ p^{\frac{2}{27}(m^3-6m^2)+\frac{2}{9}(m-\frac{7}{6})} & \text{if } \delta = 1 \\ p^{\frac{2}{27}(m^3-6m^2)+\frac{1}{3}(m-\frac{26}{9})} & \text{if } \delta = 2 \end{cases}$$

and the lower bound follows since we are assuming that $m \geq 6$.

We turn our attention to the upper bound. We have that

$$\mathcal{H}_p(m) = \sum_{r=1}^{m-1} f(r, m-r) \leq (m-1)p^M$$

where M is the maximum of $\frac{1}{2}rs(s+1) - s(s-1)$, $s = m - r$ such that $0 < r \leq m$. It is easy to show that the maximum occurs when $r = \frac{2}{3}m + \delta$ where $0 < \delta < \frac{1}{2}$, hence that $M \leq \frac{2}{27}m^3 + \frac{11}{24}m$.□

The methods used above can be used, with virtually no modification, to prove the following results.

Theorem 10 *Let p be an odd prime. If $\mathcal{B}_{p,2}(r,s)$ is the number of groups of Φ-complexion (r,s) and exponent p, then*

$$p^{\frac{1}{2}r(r-1)s-s^2-r^2} \leq \mathcal{B}_{p,2}(r,s) \leq p^{\frac{1}{2}r(r-1)s-s(s-1)}.$$

Theorem 11 *Let p be an odd prime. The number of groups of exponent p and order p^m with a central, elementary abelian Frattini subgroup is*

$$p^{\frac{2}{27}m^3+O(m^2)}.$$

Chapter 3

Reduced Groups

3.1 An Overview of the Chapter

This chapter is divided into two sections. In the first, we prove two lemmas which concern themselves with the structure of abelian p-groups. In the second, we use these lemmas to prove Theorem 1.

3.2 Some Abelian p-Group Theory

Lemma 1 *Let A be an abelian p-group. Suppose $H \leq A$ such that $|H| = p^n$. Then $A = A_1 \oplus A_2$ where $H \leq A_1$ and where A_1 has rank at most n.*

Proof: We use induction on n: the case $n = 0$ is trivial.

Assume the result holds for subgroups of order strictly less than p^n. Let $x \in H$ be an element of order p. Any element of order p is contained in a cyclic direct summand of A (this is a special case of [13, Lemma 10, Page 23]). Hence there exists $h \in A$ such that $x \in \langle h \rangle$ and

$$A = \langle h \rangle \oplus B$$

for some $B \leq A$. Let $H_1 \leq B$ be the projection of H onto B. We have that $H \leq \langle h \rangle \oplus B$. Since $x \in H \cap \langle h \rangle$, $|H_1| < |H|$. By our inductive hypothesis, $B = B_1 \oplus B_2$ where $H_1 \leq B_1$ and where $\mathrm{rk}(B_1) \leq n-1$. Setting $A_1 = \langle h \rangle \oplus B_1$ and $A_2 = B_2$, we have that $A = A_1 \oplus A_2$ where $H \leq A_1$ and $\mathrm{rk}(A_1) \leq n$, as required.□

Lemma 2 *Let A be an abelian p-group. Suppose that $H \leq A$ such that $|A/H| = p^a$. Then $A = A_1 \oplus A_2$ where $A_2 \leq H$ and A_1 has rank at most a*

Proof: The lemma follows by duality of finite abelian p-groups. (See [7, pages 311-312]).□

3.3 The Rank of the Centre of a Reduced Group

We are now in a position to prove the main result of the chapter. The definition of 'reduced' is given in the introduction.

Theorem 1 *Let P be a reduced p-group and suppose that $|P' \cap Z(P)| = p^n$ and $|P/P'Z(P)| = p^a$. Then:*

(i) *The rank of $Z(P)$ is at most $a + n$.*

(ii) *The rank of P/P' is at most $a + n$.*

Proof: We prove part (i). By Lemma 1, $Z(P) = A_1 \times A_2$ where $P' \cap Z(P) \leq A_1$ and $\mathrm{rk}(A_1) \leq n$. Set

$$B := P/P'A_1.$$

Consider $\pi : A_2 \longrightarrow B$ given by restricting the natural map from P to B. Since

$$\pi(A_2) = P'A_1A_2/P'A_1 = P'Z(P)/P'A_1,$$

we have that

$$|B/\pi(A_2)| = \left|\frac{P/P'A_1}{P'Z(P)/P'A_1}\right| = |P/P'Z(P)| = p^a.$$

Hence, by Lemma 2, we have that $B = B_1 \times B_2$ where $\pi(A_2) \geq B_2$ and where B_1 has rank at most a. Set $D := \pi^{-1}(B_2)$. Set Q to be equal to the inverse image of B_1 under the natural map from P to B. We claim that $P = Q \times D$. Now Q is normal as it contains P' and D is normal as it is central. Suppose that $x \in Q \cap D$. Then $x \in D \leq Z(P)$, so

$$x \in (P'A_1) \cap Z(P) = (P' \cap Z(P))A_1 = A_1.$$

But $x \in D \leq A_2$, so $x \in A_1 \cap A_2 = 1$. Hence $Q \cap D = 1$ and so $P = Q \times D$.

Since P is reduced, we may deduce that $D = 1$, hence that $B_2 = 1$. But in this case,

$$\begin{aligned} \mathrm{rk}(Z(P)) \leq \mathrm{rk}(A_1) + \mathrm{rk}(Z(P)/A_1) &\leq \mathrm{rk}(A_1) + \mathrm{rk}(B) \\ &= \mathrm{rk}(A_1) + \mathrm{rk}(B_1) \\ &\leq a + n. \end{aligned}$$

So the rank of $Z(P)$ is at most $a + n$, as required.

We now turn our attention to part (ii) of the theorem. The proof is similar to part (i). Let P be a reduced p-group as in the statement of the

theorem. Applying Lemma 2 to the image of $Z(P)$ in P/P', we find that there exist subgroups A_1 and A_2 of P such that $P = A_1A_2$, $A_1 \leq Z(P)$, $P' \leq A_2$, $A_1 \cap A_2 \leq P' \cap Z(P)$ and $rk(A_2/P') \leq a$. Applying Lemma 1 to A_1, we find that $A_1 = B_1 \times B_2$ where $P' \cap Z(P) \leq B_2$ and such that B_2 has rank at most n. Set $Q = B_2A_2$ and $D = B_1$. As in part (i), we have that D is a direct factor of P, hence that $D = 1$. But now

$$\mathrm{rk}(P/P') \leq \mathrm{rk}(A_2/P') + \mathrm{rk}(B_2P'/P') \leq a + \mathrm{rk}(B_2) \leq a + n,$$

and so part (ii) of the theorem follows.□

Corollary 3 *Let Φ be an isoclinism class of p-groups and suppose that $S \in \Phi$ with $|S' \cap Z(S)| = p^n$ and $|S/S'Z(S)| = p^a$. Then for any reduced group $P \in \Phi$, the rank of $Z(P)$ and the rank of P/P' are at most $a + n$.*

Proof: This follows from part (i) of the previous theorem once we note that the orders of $P' \cap Z(P)$ and of $P/P'Z(P)$ are invariants of the isoclinism class. □

Chapter 4

Enumeration within Isoclinism Classes

4.1 An Overview of the Chapter

The object of this chapter is to prove the enumeration results concerning isoclinism stated in Chapter 1: namely Theorems 2 and 3 and their corollaries. In order to prove Theorems 2 and 3, we need to know something about the structure of a group in an isoclinism class Φ. In Section 4.2, we associate several triples $(A, \mu, \underline{v})$ with $P \in \Phi$, and prove that any one of these triples defines the isomorphism class of P uniquely. Counting triples of the appropriate type gives an upper bound for the number of groups of order p^m in Φ. Section 4.3 proves Theorem 2 using this method. The section also contains an example which shows that Theorem 2 gives a reasonable bound. Section 4.4 uses the triples defined in Section 4.2 to prove Theorem 3 and its corollary. Finally, Section 4.5 contains a shorter proof of Theorem 3, which produces slightly cruder bounds than the proof contained in Section 4.4.

4.2 The structure of isoclinic groups

Let p be a fixed prime number and let Φ be a fixed isoclinism class. We associate several triples $(A, \mu, \underline{v})$ with each group in this isoclinism class, and then prove that a triple defines the isomorphism class of a unique group in Φ.

We require a standard p-group in Φ which we will use to define triples associated with each member of Φ. Let S be a fixed p-group in Φ. Set $L = S/Z(S)$, $M = S'$ and $N = S' \cap Z(S)$. Let

$$\gamma : L \times L \longrightarrow M$$

be the map induced by forming commutators in S. Suppose that L/L' has rank d and order p^a. Choose elements $s_1, \ldots, s_d \in L$ such that

$$L/L' = \langle s_1 L' \rangle \times \cdots \times \langle s_d L' \rangle .$$

Set $\underline{s}$ to be the d-tuple $(s_1, \ldots s_d)$. For i such that $1 \leq i \leq d$, let ϵ_i be the least integer such that $s_i^{p^{\epsilon_i}} \in L'$. Then $\sum_{i=1}^{d} \epsilon_i = a$. We will fix all the above notation for the rest of the chapter.

Definition 3 *We say the triple $(A, \mu, \underline{v})$ is an* $\underline{s}$-triple *if A is an abelian group, μ is an injective homomorphism mapping N into A and*

$$\underline{v} = (v_1, v_2, \ldots, v_d)$$

where $v_i \in A/p^{\epsilon_i}A$ for $1 \leq i \leq d$ (here we are writing A additively).

Two $\underline{s}$-triples $(A_1, \mu_1, (v_1, \ldots, v_d))$ and $(A_2, \mu_2, (w_1, \ldots, w_d))$ are isomorphic if there exists an isomorphism $\theta : A_1 \longrightarrow A_2$ of abelian groups such that $\mu_2 = \theta\mu_1$ and such that $\theta(v_i) = w_i$ for $1 \leq i \leq d$.

Fix a transversal $\{\tau_\lambda\}_{\lambda\in\Lambda}$ of N in M. Note that there is a natural identification of the elements τ_λ with elements of L': Set $\overline{\tau}_\lambda = \tau_\lambda Z(S) \in L'$ for all $\lambda \in \Lambda$. The following lemma consists of results concerning the structure of a p-group isoclinic to S.

Lemma 3 *Let P be a p-group in Φ. Let ϕ and ψ be isomorphisms such that the following square commutes:*

$$\begin{array}{ccccc} & & L \times L & \xrightarrow{\gamma} & M \\ \phi \times \phi & & \downarrow & & \downarrow \ \psi \\ & & P/Z(P) \times P/Z(P) & \xrightarrow{[,]} & P' \end{array} \tag{4.1}$$

Then

(i) $\psi(N) = P' \cap Z(P)$

(ii) $\psi(\tau_\lambda)Z(P) = \phi(\overline{\tau}_\lambda)$ *for any* $\lambda \in \Lambda$.

(iii) *if we pick $x_i \in P$ such that*

$$x_i Z(P) = \phi(s_i)$$

for $1 \leq i \leq d$ then every element of P can be uniquely expressed in the form

$$x_1^{\beta_1} \ldots x_d^{\beta_d} \psi(\tau_\lambda) z$$

where $0 \leq \beta_i < p^{\epsilon_i}$, $\lambda \in \Lambda$ and $z \in Z(P)$.

Proof: We first prove a stronger version of part (ii), namely that for any $c \in S'$,

$$\psi(c)Z(P) = \phi(cZ(S)). \tag{4.2}$$

Since ψ and ϕ are homomorphisms, it is sufficient to prove the result for $c = [g_1, g_2]$ where $g_1, g_2 \in S$. By commutivity of Diagram (4.1), we have that

$$\psi([g_1Z(S), g_2Z(S)]) = [\phi(g_1Z(S)), \phi(g_2Z(S))]$$

in P and hence that

$$\psi([g_1Z(S), g_2Z(S)])Z(P) = \phi([g_1Z(S), g_2Z(S)])$$

in $P/Z(P)$. So

$$\begin{aligned} \phi(cZ(S)) &= \phi([g_1, g_2]Z(S)) \\ &= \phi([g_1Z(S), g_2Z(S)]) \\ &= \psi([g_1Z(S), g_2Z(S)])Z(P) \\ &= \psi([g_1, g_2])Z(P) \\ &= \psi(c)Z(P) \end{aligned}$$

and hence (4.2) follows. Part (ii) of the lemma now follows immediately, since $\tau_\lambda \in S'$ and $\overline{\tau}_\lambda = \tau_\lambda Z(S)$ for any $\lambda \in \Lambda$.

We now prove part (i). We have that

$$N = \{c \in S' \mid cZ(S) = Z(S)\}.$$

Since $cZ(S) = Z(S)$ if and only if $\psi(c)Z(P) = Z(P)$, by (4.2), we have

$$\psi(N) = \{\psi(c) \in P' \mid cZ(S) = Z(S)\}$$

$$
\begin{aligned}
&= \{\psi(c) \in P' \mid \psi(c)Z(P) = Z(P)\} \\
&= \{c \in P' \mid cZ(P) = Z(P)\} \\
&= P' \cap Z(P)
\end{aligned}
$$

and part (i) follows.

We prove part (iii). Every element of L/L' can be uniquely expressed in the form

$$s_1^{\beta_1} \dots s_d^{\beta_d} L'$$

where $0 \leq \beta_i < p^{\epsilon_i}$, by definition of the s_i. Hence every element of $P/Z(P)P'$ can be uniquely expressed in the form

$$x_1^{\beta_1} \dots x_d^{\beta_d} x$$

for some $x \in Z(P)P'$. Since $\{\tau_\lambda\}_{\lambda \in \Lambda}$ is a transversal of N in S', we have, by part (i), that $\{\psi(\tau_\lambda)\}_{\lambda \in \Lambda}$ is a transversal of $P' \cap Z(P)$ in P', hence a transversal of $Z(P)$ in $Z(P)P'$. So x can be written uniquely in the form

$$x = \psi(\tau_\lambda) z$$

where $\lambda \in \Lambda$ and $z \in Z(P)$. Hence the result follows. □

We now explain how we associate an $\underline{s}$-triple with a group in Φ. Let $P \in \Phi$, and let ϕ, ψ be isomorphisms such that diagram (4.1) commutes. Let $x_1, \dots, x_d$ be chosen in P such that $x_i Z(P) = \phi(s_i)$. We define an $\underline{s}$-triple $(A, \mu, \underline{v})$ as follows.

Set $A = Z(P)$. Define μ as the restriction of ψ to N. We have

$$x_i^{p^{\epsilon_i}} = \psi(\tau_{\lambda_i}) z_i$$

for some unique λ_i and z_i where $\lambda_i \in \Lambda$ and $z_i \in Z(P)$. Writing $Z(P)$ additively, set $v_i = z_i + p^{e_i}Z(P)$. We say that $(A, \mu, \underline{v})$ is the $\underline{s}$-triple induced from P via (ϕ, ψ). Note that the definition of this triple depends upon the choice of ϕ, ψ and the x_i, so a given group may give rise to more than one triple. However, as the following will show, a given isomorphism class of triples is induced by at most one group in Φ.

Lemma 4 *Let P_1 and P_2 be p-groups isoclinic to S that induce $\underline{s}$-triples isomorphic to $(A, \mu, \underline{v})$. Then $P_1 \cong P_2$.*

Proof: Let P_1 and P_2 be as above, and suppose they induce triples isomorphic to $(A, \mu, \underline{v})$ via the isomorphisms (ϕ_1, ψ_1) and (ϕ_2, ψ_2) respectively. We have that the diagram

$$\begin{array}{ccccc} P_1/Z(P_1) \times P_1/Z(P_1) & \xrightarrow{[,]} & P_1' & & \\ \phi_1 \times \phi_1 \uparrow & & \uparrow & \psi_1 & \\ L \times L & \xrightarrow{\gamma} & M & & \\ \phi_2 \times \phi_2 \downarrow & & \downarrow & \psi_2 & \\ P_2/Z(P_2) \times P_2/Z(P_2) & \xrightarrow{[,]} & P_2' & & \end{array} \tag{4.3}$$

commutes. For $i = 1, 2$, let $\theta_i : Z(P_i) \longrightarrow A$ be the isomorphism between the $\underline{s}$-triple induced by P_i and the $\underline{s}$-triple $(A, \mu, \underline{v})$. We have that

$$\psi_i(x) = \theta_i^{-1}\mu(x) \tag{4.4}$$

for any $x \in N$, by definition of the $\underline{s}$-triple induced by P_i.

Clearly we have that $P_1' \cong P_2'$ via the isomorphism $\psi_2\psi_1^{-1}$, and $Z(P_1) \cong Z(P_2)$ via the isomorphism $\theta_2^{-1}\theta_1$. We will first extend these isomorphisms to an isomorphism α between $Z(P_1)P_1'$ and $Z(P_2)P_2'$.

Define $\alpha : Z(P_1)P_1' \longrightarrow Z(P_2)P_2'$ by

$$\alpha(zc) = \theta_2^{-1}\theta_1(z)\psi_2\psi_1^{-1}(c)$$

for an element $zc \in Z(P_1)P_1'$ where $z \in Z(P_1)$ and $c \in P_1'$. We check that α is well defined. Let $x \in Z(P_1)P_1'$ and suppose that $x = z_1c_1 = z_2c_2$ for some $z_1, z_2 \in Z(P_1)$ and $c_1, c_2 \in P_1'$. Clearly there exists $z \in Z(P_1) \cap P_1'$ such that $z_1 = z_2z$ and $c_1 = z^{-1}c_2$. Then we have

$$\begin{aligned}
\alpha(z_1c_1) &= \theta_2^{-1}\theta_1(z_1)\psi_2\psi_1^{-1}(c_1) \\
&= \theta_2^{-1}\theta_1(z_2z)\psi_2\psi_1^{-1}(z^{-1}c_2) \\
&= \theta_2^{-1}\theta_1(z_2)\theta_2^{-1}\mu\mu^{-1}\theta_1(z)\psi_2\psi_1^{-1}(z^{-1})\psi_2\psi_1^{-1}(c_2) \\
&= \theta_2^{-1}\theta_1(z_2)\psi_2\psi_1^{-1}(z)\psi_2\psi_1^{-1}(z^{-1})\psi_2\psi_1^{-1}(c_2) \\
&= \theta_2^{-1}\theta_1(z_2)\psi_2\psi_1^{-1}(c_2) \\
&= \alpha(z_2c_2).
\end{aligned}$$

Hence α is well defined. We check that α is a homomorphism. Let $z_1, z_2 \in Z(P_1)$ and let $c_1, c_2 \in P_1'$. Then since $\theta_2^{-1}\theta_1(z_2) \in Z(P_2)$ we have

$$\begin{aligned}
\alpha(z_1c_1)\alpha(z_2c_2) &= \theta_2^{-1}\theta_1(z_1)\psi_2\psi_1^{-1}(c_1)\theta_2^{-1}\theta_1(z_2)\psi_2\psi_1^{-1}(c_2) \\
&= \theta_2^{-1}\theta_1(z_1)\theta_2^{-1}\theta_1(z_2)\psi_2\psi_1^{-1}(c_1)\psi_2\psi_1^{-1}(c_2) \\
&= \theta_2^{-1}\theta_1(z_1z_2)\psi_2\psi_1^{-1}(c_1c_2) \\
&= \alpha(z_1z_2c_1c_2) \\
&= \alpha((z_1c_1)(z_2c_2))
\end{aligned}$$

and thus $\alpha : Z(P_1)P_1' \longrightarrow Z(P_2)P_2'$ is a homomorphism. Clearly, $Z(P_2)$ is the image of $Z(P_1)$, and P_2' is the image of P_1' under α. Since $Z(P_2)P_2'$

is generated by $Z(P_2)$ and P_2', we have that α is onto. To prove that α is an isomorphism, it is sufficient to show that $|Z(P_1)P_1'| = |Z(P_2)P_2'|$, for then α is an onto homomorphism between finite sets of the same size. Since $P_1/Z(P_1) \cong P_2/Z(P_2)$ and $Z(P_1) \cong Z(P_2)$, we have that $|P_1| = |P_2|$. Since $P_i/Z(P_i)P_i' \cong (P_i/Z(P_i)/(P_i/Z(P_i))' \cong L/L'$, we have $|Z(P_1)P_1'| = |Z(P_2)P_2'|$ and hence α is an isomorphism as required.

It remains to extend α to an isomorphism from P_1 to P_2. Let $x_1, \ldots, x_d \in P_1$ be fixed such that $x_i Z(P_1) = \phi_1(s_i)$ for $1 \leq i \leq d$. Define $z_i \in Z(P_1)$ and $\lambda_i \in \Lambda$ where $1 \leq i \leq d$ by

$$x_i^{p^{e_i}} = \psi_1(\tau_{\lambda_i}) z_i.$$

We know that $x_i^{p^{e_i}}$ can be written in this form because of Lemma 3 (iii) together with the definition of the elements s_i. By the definition of the $\underline{s}$-triple induced by P_1, we may specify in addition that

$$\theta_1(z_i) + p^{e_i} A = v_i$$

for $1 \leq i \leq d$. We show that we can find $y_i \in P_2$ where $1 \leq i \leq d$ such that $y_i Z(P_2) = \phi_2(s_i)$ and such that

$$y_i^{p^{e_i}} = \psi_2(\tau_{\lambda_i}) \alpha(z_i) \tag{4.5}$$

Consider, for $1 \leq i \leq d$, an arbitrary $u_i \in P_2$ such that $u_i Z(P_2) = \phi_2(s_i)$. Then

$$u_i^{p^{e_i}} Z(P_2) \;=\; \phi_2(s_i^{p^{e_i}})$$

$$
\begin{aligned}
&= \phi_2\phi_1^{-1}\phi_1(s_i)^{p^{\epsilon_i}} \\
&= \phi_2\phi_1^{-1}(x_i^{p^{\epsilon_i}} Z(P_1)) \\
&= \phi_2(\overline{\tau}_{\lambda_i}) \\
&= \psi_2(\tau_{\lambda_i})Z(P_2).
\end{aligned}
$$

By the definition of the $\underline{s}$-triple induced by P_2, we may pick $u_1, \ldots, u_d$ such that $u_i Z(P_2) = \phi_2(s_i)$ and such that

$$u_i^p = \psi_2(\tau_{\lambda_i})t_i$$

where $t_i \in Z(P_2)$ and $\theta_2(t_i) + p^{\epsilon_i}A = v_i$. Now

$$\theta_1(z_i) + p^{\epsilon_i}A = v_i = \theta_2(t_i) + p^{\epsilon_i}A.$$

Hence $\theta_1(z_i) - \theta_2(t_i) \in p^{\epsilon_i}A$, so $\theta_2^{-1}(\theta_1(z_i) - \theta_2(t_i)) \in p^{\epsilon_i}Z(P_2)$. Set $w_i \in Z(P_2)$ to be an element such that

$$p^{\epsilon_i}w_i = \theta_2^{-1}(\theta_1(z_i) - \theta_2(t_i)) = \alpha(z_i) - t_i.$$

Set $y_i = u_i w_i$. Then

$$y_i^{p^{\epsilon_i}} = u_i^{p^{\epsilon_i}} w_i^{p^{\epsilon_i}} = \psi_2(\tau_{\lambda_i})t_i\alpha(z_i)t_i^{-1} = \psi_2(\tau_{\lambda_i})\alpha(z_i).$$

Hence $y_1, \ldots, y_d$ satisfy (4.5), as required.

We are now in a position to define the candidate for our isomorphism between P_1 and P_2. Define $\hat{\alpha} : P_1 \longrightarrow P_2$ by

$$\hat{\alpha}(x_1^{\beta_1} \ldots x_d^{\beta_d} c) = y_1^{\beta_1} \ldots y_d^{\beta_d}\alpha(c)$$

where $0 \leq \beta_i < p^{\epsilon_i}$ for $1 \leq i \leq d$ and where $c \in Z(P_1)P_1'$. Clearly $\hat{\alpha}$ is well defined and is a bijection. It is immediate from the definition of $\hat{\alpha}$ that

$$\hat{\alpha}(x_i^{\beta} x) = \hat{\alpha}(x_i^{\beta})\hat{\alpha}(x) \tag{4.6}$$

where $0 \leq \beta < p^{\epsilon_i}$ and $x \in \langle x_{i+1}, \ldots, x_d \rangle Z(P_1)P_1'$. It is also clear that

$$\hat{\alpha}(x_i^{\beta+\beta'}) = \hat{\alpha}(x_i^{\beta})\hat{\alpha}(x_i^{\beta'}) \tag{4.7}$$

where $0 \leq \beta, \beta' < p^{\epsilon_i}$ and $\beta + \beta' < p^{\epsilon_i}$. We also have that

$$\hat{\alpha}(x_i^{p^{\epsilon_i}}) = \hat{\alpha}(x_i)^{p^{\epsilon_i}} \tag{4.8}$$

for $1 \leq i \leq d$ by (4.5). We now check that

$$\hat{\alpha}([x, x_i^{\beta}]) = [\hat{\alpha}(x), \hat{\alpha}(x_i^{\beta})] \tag{4.9}$$

where $x \in P_1$, $0 \leq \beta < p^{\epsilon_i}$ and $1 \leq i \leq d$.

Let $x \in P_1$ and let β be an integer such that $0 \leq \beta < p^{\epsilon_i}$. Then

$$x = x_1^{\beta_1} \ldots x_d^{\beta_d} \psi_1(\tau_\lambda) z$$

where $0 \leq \beta_i < p^{\epsilon_i}$, $\lambda \in \Lambda$ and $z \in Z(P_1)$. Then

$$\begin{aligned} \hat{\alpha}([x, x_i^{\beta}]) &= \hat{\alpha}([xZ(P_1), x_i^{\beta} Z(P_1)]) \\ &= \hat{\alpha}(\psi_1 \psi_2^{-1}[\phi_2 \phi_1^{-1}(xZ(P_1)), \phi_2 \phi_1^{-1}(x_i^{\beta} Z(P_1))]) \end{aligned}$$

since P_1 and P_2 are isoclinic. Since $y_i^{\beta} Z(P_2) = \phi_2 \phi_1^{-1}(x_i^{\beta} Z(P_1))$ and

$$\begin{aligned} \phi_2 \phi_1^{-1}(xZ(P_1)) &= \phi_2 \phi_1^{-1}(x_1^{\beta_1} \ldots x_d^{\beta_d} \psi_1(\tau_\lambda) Z(P_1)) \\ &= y_1^{\beta_1} \ldots y_d^{\beta_d} \alpha(\psi_1(\tau_\lambda)) Z(P_2) \end{aligned}$$

we have that

$$\begin{aligned}\hat{\alpha}([x, x_i^{\beta}]) &= \hat{\alpha}(\psi_1\psi_2^{-1}([y_1^{\beta_1}\dots y_d^{\beta_d}\alpha(\psi_1(\tau_\lambda)), y_i^{\beta}])) \\ &= \hat{\alpha}(\psi_1\psi_2^{-1}([\hat{\alpha}(x), \hat{\alpha}(x_i)^{\beta}])) \\ &= [\hat{\alpha}(x), \hat{\alpha}(x_i)^{\beta}]\end{aligned}$$

since $\hat{\alpha} = \psi_2\psi_1^{-1}$ on P_1', as required.

Define

$$H_k = \langle x_{d-k+1}, \dots, x_d \rangle\, Z(P_1)P_1'$$

for $1 \leq k \leq d$ and define $H_0 = Z(P_1)P_1'$. Using the properties (4.6), (4.7), (4.8) and (4.9) of $\hat{\alpha}$, it is an easy exercise to prove that $\hat{\alpha}$ is an isomorphism on P_1 by using induction on k to show that $\hat{\alpha}$ restricted to H_k is an injective homomorphism: We do this in Appendix A. Since we have constructed an isomorphism between P_1 and P_2, the result follows.□

4.3 Proof of Theorem 2

Theorem 2 *Given any isoclinism class Φ, the number of groups of order p^m in Φ is at most*

$$p^{\frac{1}{3}m^2} f_{\mathrm{ab}}(p^m),$$

where $f_{\mathrm{ab}}(p^m)$ is defined to be the number of abelian groups of order p^m.

Proof: Let Φ be an isoclinism class containing a group S. Let $S/Z(S)S'$ have rank d and order p^a, let $|S/Z(S)| = p^l$ and suppose $|S' \cap Z(S)| = p^n$. Set $N = S' \cap Z(S)$. Let $P \in \Phi$ with $|P| = p^m$. Since $|P/Z(P)| = |S/Z(S)|$,

we have that $|Z(P)| = p^{m-l}$. Hence P will give rise to an $\underline{s}$-triple $(A, \mu, \underline{v})$ where $|A| = p^{m-l}$. Counting the number of isomorphism classes of triples of this form gives an upper bound for the number of groups of order p^m in Φ, by Lemma 4.

We first consider the number of possibilities for A. If we identify N with its image in A under μ, A is an abelian group which is an extension of N by a group A/N of order p^{m-l-n}. The number of possibilities for A/N is at most $f_{\mathbf{ab}}(p^{m-l-n})$. Suppose that A/N has presentation

$$\langle a_1, \ldots, a_k \mid a_i^{m_i} = 1, [a_i, a_j] = 1 \rangle$$

for some integers $k, m_1, \ldots, m_k$ and that N has presentation $\langle X \mid R \rangle$. Then A has a presentation of the form

$$\langle X, a_1, \ldots, a_k \mid R, a_i^{m_i} = b_i, [a_i, a_j] = 1, [a_i, X] = 1 \rangle$$

where the $b_i \in N$. Hence the number of possibilities for A as an extension of N once A/N has been chosen is at most $p^{n(m-l-n)}$ corresponding to the number of choices for the b_i. Once A has been fixed as a particular extension of N, μ is determined as the inclusion map $\mu : N \longrightarrow A$. The number of possibilities for each $v_i \in A/p^{\epsilon_i}A$ is at most p^{m-l}. Hence the number of possibilities for $\underline{v}$ is at most $p^{d(m-l)}$. Therefore we have that the number of possibilities for triples of the form $(A, \mu, \underline{v})$ with $|A| = p^{m-l}$ is at most

$$\begin{aligned} p^{d(m-l)+n(m-l-n)} f_{\mathbf{ab}}(p^{m-l-n}) &\leq p^{n(m-l-n)+a(m-l-n+n)} f_{\mathbf{ab}}(p^m) \\ &\leq p^{\frac{1}{3}m^2} f_{\mathbf{ab}}(p^m) \end{aligned}$$

and Theorem 2 follows.□

We now give an example to show that Theorem 2 gives a reasonable bound. Let X_r be the free group on r generators $x_1, \ldots, x_r$ and let R be the subgroup of X_r generated by all elements of the form $x^{p^2}, [x,y]^p, [x^p, y]$ and $[[x,y],z]$ where x, y and z range over all the elements of F. Set $H = X_r/R$. Define $h_i := x_i R$. One may show (see the proof of Theorem 8) that $|H/\Phi(H)| = p^r$ and that $\Phi(H)$ is elementary abelian of order $p^{\frac{1}{2}r(r+1)}$ and generated by the elements

$$h_i^p$$

for $1 \leq i \leq r$ together with

$$[h_i, h_j]$$

for $1 \leq i < j \leq r$. If N is a subgroup of $\Phi(H)$ of index p^s, H/N is a group of order p^{r+s}. It is shown in the proof of Theorem 8 that at most p^{r^2} quotients of this form are isomorphic to any given group.

We construct a number of isoclinic groups of order p^{r+s}. Define $V \leq \Phi(H)$ by

$$V = \langle [h_i, h_j] \mid 1 \leq i < j \leq r \rangle .$$

Let K be a subgroup of V of index p^s in V. For $v_1, \ldots, v_r \in V$, define

$$N(v_1, \ldots v_r) = \langle K, h_1^p v_1, h_2^p v_2, \ldots h_r^p v_r \rangle .$$

It is clear that $N(v_1, \ldots v_r) = N(v_1', \ldots v_r')$ if and only if $v_i \in v_i' K$ for $1 \leq i \leq r$. Hence we have a collection of p^{sr} subgroups of $\Phi(H)$, all of index p^s in $\Phi(H)$. Define

$$G(v_1, \ldots v_r) = H/N(v_1, \ldots v_r).$$

Since at most p^{r^2} quotients of H of this form are isomorphic, we have a collection of at least p^{sr-r^2} distinct isomorphism classes of groups. We show that any two of these groups are isoclinic.

Let $v_1, \ldots, v_r, v_1', \ldots, v_r' \in K$. We show that $G(v_1, \ldots, v_r)$ is isoclinic to $G(v_1', \ldots, v_r')$. Consider the subgroup $Z(v_1, \ldots, v_r)$ of H corresponding to the centre of $G(v_1, \ldots, v_r)$. Then

$$\begin{aligned} Z(v_1, \ldots, v_r) &= \{h \in H \mid [h, x] \in N(v_1, \ldots, v_r) \text{ for all } x \in H\} \\ &= \{h \in H \mid [h, x] \in N(v_1, \ldots, v_r) \cap H' \text{ for all } x \in H\} \\ &= \{h \in H \mid [h, x] \in K \text{ for all } x \in H\}. \end{aligned}$$

Hence $Z(v_1, \ldots, v_r)$ is independent of $v_1, \ldots, v_r$ and so the identity map on H induces a map ϕ between the central quotients of $G(v_1, \ldots, v_r)$ and $G(v_1', \ldots, v_r')$. Since $G(v_1, \ldots, v_r)'$ corresponds to $H'/(N(v_1, \ldots, v_r) \cap H') = H'/K$, the identity map on H also induces a map ψ between the derived subgroups of $G(v_1, \ldots, v_r)$ and $G(v_1', \ldots v_r')$. It is clear that $G(v_1, \ldots, v_r)$ and $G(v_1', \ldots, v_r')$ are isoclinic via the isomorphism pair (ϕ, ψ).

We have found p^{sr-r^2} distinct isoclinic groups of order p^{r+s}. Setting $r = \frac{1}{4}m + \delta$ and $s = \frac{3}{4}m - \delta$, where δ is chosen from the set $\{0, \frac{1}{4}, \frac{1}{2}, \frac{3}{4}\}$ so as to make r and s integers, we find there are at least

$$p^{\frac{1}{8}m^2 - 2\delta^2} \geq p^{\frac{1}{8}(m^2-9)}$$

groups of order p^m which are contained in the same isoclinism class.

4.4 Proof of Theorem 3

We are now in a position to prove:

Theorem 3 *Let Φ be an isoclinism class. Define $f_\Phi(p^m)$ to be the number of groups of order p^m in Φ. Then*

$$\frac{f_\Phi(p^m)}{f_{\mathrm{ab}}(p^m)} \leq cm^k$$

where c and k are constants depending only on Φ.

Proof: Let Φ be a fixed isoclinism class, let $S \in \Phi$ and suppose that $|S/Z(S)| = p^l$ and that $S/S'Z(S)$ is of rank d and order p^a. Set $N = Z(S) \cap S'$ and suppose $|N| = p^n$. Choose $s_1, \ldots, s_d \in S/Z(S)$ as in Section 4.2.

The theorem is trivial if $m \leq l$, so we may assume $m > l$. Let $P \in \Phi$ be a group of order p^m. Then $P = Q \times D$ where Q is reduced and D is abelian. Now by Corollary 3, $Z(P) = Z(Q) \times D$, where $\mathrm{rk}(Z(Q)) \leq a + n$. The isomorphism class of P is, by Lemma 4, determined by the isomorphism class of $Z(P)$, the isomorphism class of a direct summand $Z(Q)$ of $Z(P)$ and the isomorphism class of an $\underline{s}$-triple $(Z(Q), \mu, \underline{v})$.

The number of possibilities for $Z(P)$ is at most $f_{\mathrm{ab}}(p^{m-l})$. Let $Z(P)$ be fixed. We determine the number of possibilities for $Z(Q)$ as a direct summand of $Z(P)$.

We have that

$$Z(Q) = \langle g_1 \rangle \oplus \cdots \oplus \langle g_r \rangle$$

for some elements g_i and for some $r \leq a + n$. Suppose that $|g_i| = p^{k_i}$ for $1 \leq i \leq r$. The isomorphism class of $Z(Q)$ is determined by the r-tuple

$(k_1, \ldots, k_r)$. The number of choices for each k_i is at most f where f is the number of distinct orders of non-trivial cyclic direct summands of $Z(P)$. But for $Z(P)$ to have f distinct orders of this kind,

$$|Z(P)| \geq pp^2 \ldots p^f = p^{\frac{1}{2}f(f+1)}.$$

Hence $\frac{1}{2}f(f+1) \leq m - l$. Since in this case, $\frac{1}{2}f^2 \leq m - l$ and so $f \leq \sqrt{2(m-l)}$, the number of choices for each k_i is at most $\sqrt{2(m-l)}$. Hence there are at most

$$2^{\frac{1}{2}r}(m-l)^{\frac{1}{2}r} \leq 2^{\frac{1}{2}(a+n)}(m-l)^{\frac{1}{2}(a+n)}$$

possibilities for $Z(Q)$ once r is fixed. Since there are at most $a+n+1$ choices for r, there are at most

$$(a+n+1)2^{\frac{1}{2}(a+n)}(m-l)^{\frac{1}{2}(a+n)}$$

possibilities for $Z(Q)$.

Let $Z(P)$ and $Z(Q)$ be fixed. We now find the number of isomorphism classes of $\underline{s}$-triples of the form $(Z(Q), \mu, \underline{v})$. We determine the number of possibilities for μ. Since $|N| = p^n$, we may write

$$N = \langle h_1 \rangle \oplus \cdots \oplus \langle h_r \rangle$$

for some elements h_i and some $r \leq n$. If h_i has order p^{k_i}, then $\sum_{i=1}^{r} k_i = n$. Now μ is determined by the elements $\mu(h_i)$ where $1 \leq i \leq r$. We have

$$\mu(h_i) \leq Z(Q)[p^{k_i}]$$

where $Z(Q)[p^{k_i}] = \{x \in Z(Q) \mid p^{k_i}x = 0\}$. Now $\left|Z(Q)[p^{k_i}]\right| \leq (p^{k_i})^{a+n}$, since it is generated by at most $a+n$ elements of order at most p^{k_i}. Hence there are at most $p^{k_i(a+n)}$ choices for each $\mu(h_i)$ and so there are at most

$$p^{\sum_{i=1}^{r} k_i(a+n)} = p^{n(a+n)}$$

choices for μ.

Let $Z(P)$, $Z(Q)$ and μ be fixed. We find the number of possibilities for $\underline{v}$. We have that the number of possibilities for each v_i is at most $|Z(Q)/p^{\epsilon_i}Z(Q)|$ and that

$$|Z(Q)/p^{\epsilon_i}Z(Q)| \leq p^{\epsilon_i(a+n)}.$$

Hence the number of possibilities for $\underline{v}$ is at most

$$p^{\sum_{i=1}^{d} \epsilon_i(a+n)} = p^{a(a+n)}.$$

The number of possibilities for $P \in \Phi$ of order p^m is therefore at most

$$f_{\mathrm{ab}}(p^{m-l})(a+n+1)2^{\frac{1}{2}(a+n)}p^{(a+n)^2}(m-l)^{\frac{1}{2}(a+n)}.$$

Since a and n are invariants of Φ, we have that

$$\frac{f_\Phi(p^m)}{f_{\mathrm{ab}}(p^m)} \leq \frac{f_{\mathrm{ab}}(p^{m-l})}{f_{\mathrm{ab}}(p^m)}c(m-l)^k \leq cm^k$$

where $c = (a+n+1)2^{\frac{1}{2}(a+n)}p^{(a+n)^2}$ and $k = \frac{1}{2}(a+n)$ are constants depending only on Φ, so Theorem 3 follows. □

We now prove the corollary to Theorem 3 (see the introduction). Suppose that Φ is an isoclinism class and that $P \in \Phi$ with $|P' \cap Z(P)| = p^n$ and with

$|P/P'| = p^l$. It is shown in [10] that there exists a group S in Φ of order p^{n+l} where S is of minimal order subject to being in Φ. Clearly, S does not have any non-trivial abelian direct factors, so by the Remak–Krull–Schmidt Theorem, if A and B are abelian groups the groups $S \times A$ and $S \times B$ are isomorphic if and only if the groups A and B are isomorphic. Since $S \times A \in \Phi$ for any abelian group A, the set of groups

$$\{S \times A \mid A \text{ is an abelian group of order } p^{m-n-l}\}$$

is a collection of $f_{\mathrm{ab}}(p^{m-n-l})$ groups in Φ of order p^m, provided that $m \geq n+l$. Hence

$$f_{\mathrm{ab}}(p^{m-n-l}) \leq f_\Phi(p^m) \leq f_{\mathrm{ab}}(p^m) c m^k.$$

By the asymptotic formula (1.2) for the number of abelian groups of order p^m, we have

$$f_\Phi(p^m) = e^{\pi\sqrt{\frac{2}{3}}\sqrt{m}+O(\log m)}$$

and the corollary follows.□

4.5 A Short Proof

This section gives a sketch of a short proof of Theorem 3. The bound that this shorter proof gives is not quite as good as that in Section 4.4, and the proof is not as amenable to the alterations required to prove Theorem 2.

Let Φ be an isoclinism class of p-groups. Let $S \in \Phi$ be fixed. As in Section 4.2, define a, n, l, and M by $|S' \cap Z(S)| = p^n$, $|S/Z(S)| = p^l$, $|S/S'Z(S)| = p^a$ and $M = S'$. Define t by $|S'| = p^t$.

Let $P \in \Phi$ be of order p^m. Then $P = Q \times D$ where Q is reduced and where D is abelian. Clearly, $P' = Q'$ and, since P, Q and S are isoclinic, $Q' \cong M$. Let $x_1, \ldots x_r$ be elements of Q such that

$$Q/Q' = \langle x_1 \rangle \times \cdots \times \langle x_r \rangle Q'.$$

By Corollary 3, we have that $r \leq a + n$. For i such that $1 \leq i \leq r$, define ϵ_i to be the smallest integer such that $x_i^{p^{\epsilon_i}} \in Q'$. Then the isomorphism class of $P \in \Phi$ is determined by the isomophism class of P/P', the isomorphism class of Q/Q' as a direct summand of P/P' and the extension of Q' by Q/Q' corresponding to Q. The extension of Q' by Q/Q' is in turn determined by the powers $x_i^{p^{\epsilon_i}} \in Q'$ where $1 \leq i \leq r$, the commutator relations $[x_i, c]$ where $1 \leq i \leq r$ and where $c \in Q'$ together with commutators of the form $[x_i, x_j]$ where $1 \leq i < j \leq r$.

We find an upper bound for the number of possibilities for P as follows. Since $|P'| = p^t$, P/P' has order p^{m-t}. We may argue just as in Section 4.4 to show that the number of possibilities for P/P' together with the number of possibilities for Q/Q' as a direct summand of P/P' is at most

$$f_{\mathrm{ab}}(p^{m-t})(a+n+1)2^{\frac{1}{2}(a+n)}(m-t)^{\frac{1}{2}(a+n)}.$$

It remains to determine the number of possibilities for the p^{ϵ_i}-powers and the commutators given above. The number of possibilities for the p^{ϵ_i}-powers is at most

$$p^{lr} \leq p^{t(a+n)}$$

since there are at most $|Q'| = p^t$ possibilities for each $x_i^{\epsilon_i}$ where $1 \leq i \leq r$.

We now give a rather crude upper bound for the number of possibilities for the commutator relations given above. The number of possibilities for the value of each commutator is at most $|Q'| = p^t$. Since there are $\frac{1}{2}r(r-1)$ commutators of the form $[x_i, x_j]$ where $1 \leq i < j \leq r$ and $p^t r$ commutators of the form $[x_i, c]$ where $1 \leq i \leq r$ and $c \in Q'$, there are at most

$$p^{trp^t + \frac{1}{2}tr(r-1)}$$

possibilities for the commutators we are seeking. Hence there are at most

$$(a+n+1)2^{\frac{1}{2}(a+n)}p^{t(a+n)}p^{\frac{1}{2}(a+n)(a+n-1)t}p^{t(a+n)p^t}(m-t)^{\frac{1}{2}(a+n)}f_{\mathrm{ab}}(p^{m-t})$$

choices for P. Hence Theorem 3 follows:

$$\frac{f_\Phi(p^m)}{f_{\mathrm{ab}}(p^m)} \leq cm^k$$

where we may take c and k to be $k = \frac{1}{2}(a+n)$ and

$$c = (a+n+1)2^{\frac{1}{2}(a+n)}p^{t(a+n)+\frac{1}{2}(a+n)(a+n-1)t}p^{t(a+n)p^t}.$$

Our constant c is considerably worse than that given in the first proof of Theorem 3. This is mainly due to our having made virtually no use of the commutator information given by the isoclinism class. With some extra work, we may show that we may take c to be

$$(a+n+1)2^{\frac{1}{2}(a+n)}p^{(l+t)(a+n)}.$$

Chapter 5

Enumeration of Groups of Exponent p and Class 3

5.1 An Overview of the Chapter

This chapter concerns itself with the proof of Theorem 4 referred to in the introduction. Section 5.2 reduces the enumeration of groups of exponent p and class at most 3 to the enumeration of graded Lie algebras. Section 5.3 provides an upper bound for the number of Lie algebras of dimension m and class 3. Section 5.4 draws on the results contained in the previous two sections to prove Theorem 4.

5.2 The Number of Groups of Exponent p and Class 3 Associated with a Given Lie Algebra

Recall from the introduction that we denote the variety of groups of exponent p and class at most 3 by $\mathcal{B}_{p,3}$. In this section we aim to prove the following

result.

Theorem 12 *Let p be an odd prime. Let $P \in \mathcal{B}_{p,3}$ be a fixed group of order p^m. If we denote the i th term in the lower central series of P by $\gamma_i(P)$. Define integers r, s and t by*

$$\begin{aligned} |P/(\gamma_2(P))| &= p^r \\ |(\gamma_2(P)/\gamma_3(P))| &= p^s \text{ and} \\ |\gamma_3(P)| &= p^t. \end{aligned}$$

Let L be the associated graded Lie algebra of P. Then the number of groups in $\mathcal{B}_{p,3}$ with associated Lie algebra L is p^M where

$$\frac{1}{2}tr(r-1) - st - r(m-t) \leq M \leq \frac{1}{2}tr(r-1).$$

The proof of the theorem is contained in the following two lemmas.

Lemma 5 *In the notation of Theorem 12, there are at most $p^{\frac{1}{2}tr(r-1)}$ members of $\mathcal{B}_{p,3}$ with associated Lie algebra L.*

Proof: Since L is associated with P, L has a grading of the form $L = L_1 \oplus L_2 \oplus L_3$ where the dimensions of L_1, L_2 and L_3 are r, s and t respectively. Pick a basis $e_1, \ldots, e_m$ for L such that

$$\begin{aligned} L_1 &= \langle e_1, \ldots, e_r \rangle \\ L_2 &= \langle e_{r+1}, \ldots, e_{r+s} \rangle \\ L_3 &= \langle e_{r+s+1}, \ldots, e_m \rangle . \end{aligned}$$

Define $\lambda_{ijk} \in \mathbb{F}_p$ by

$$e_i e_j = \sum \lambda_{ijk} e_k.$$

Suppose that $Q \in \mathcal{B}_{p,3}$ has associated Lie algebra L. There exist elements x_i in Q which map to the elements e_i under the natural map

$$\begin{aligned} Q/(\gamma_2(Q)) &\longrightarrow L_1 && \text{if } 1 \leq i \leq r \\ (\gamma_2(Q))/(\gamma_3(Q)) &\longrightarrow L_2 && \text{if } r+1 \leq i \leq r+s \\ \gamma_3(Q) &\longrightarrow L_3 && \text{if } r+s+1 \leq i \leq m. \end{aligned}$$

Every element of Q is uniquely expressible in the form

$$x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_m^{\alpha_m}$$

where $0 \leq \alpha_i < p$. Since we are assuming that Q is of exponent p, we know that $x_i^p = 1$ for all i. The Lie algebra structure determines the commutators $[x_i, x_j]$ when $1 \leq j \leq r$ and $r+1 \leq i \leq m$ and also when $r+1 \leq j < i \leq m$. In addition, the Lie algebra determines $[x_i, x_j]$ modulo $\gamma_3(Q) = \langle x_{r+s+1}, \ldots, x_m \rangle$ when $1 \leq j < i \leq r$. Hence $x_1, \ldots, x_m$ satisfy the relations

$$\left.\begin{aligned} x_i^p &= 1 \text{ where } 1 \leq i \leq m \\ [x_i, x_j] &= \textstyle\prod x_k^{\lambda_{ijk}} \text{ where } 1 \leq j \leq r \text{ and } r+1 \leq i \leq m \\ [x_i, x_j] &= \textstyle\prod x_k^{\lambda_{ijk}} \text{ where } r+1 \leq j < i \leq m \\ [x_i, x_j] &= \textstyle\prod_{k=r+1}^{r+s} x_k^{\lambda_{ijk}} \prod_{k=1}^{t} x_{r+s+k}^{\beta_{ijk}} \text{ where } 1 \leq j < i \leq r \end{aligned}\right\} \quad (5.1)$$

for some elements $\beta_{ijk} \in \mathbb{F}_p$ and furthermore these generators and relations give a presentation for Q. The power and commutator information given above uniquely determines the isomorphism class of Q once we specify the $\frac{1}{2}r(r-1)t$ elements $\beta_{ijk} \in \mathbb{F}_p$ where $1 \leq j < i \leq r$ and $1 \leq k \leq t$. There

are at most p choices for the value of each β_{ijk}, hence there are at most $p^{\frac{1}{2}tr(r-1)}$ choices for a presentation of the form (5.1). Since any $Q \in \mathcal{B}_{p,3}$ with associated Lie algebra L must have a presentation of the form (5.1), the lemma follows. □

Lemma 6 *In the notation of Theorem 12, the number of members of $\mathcal{B}_{p,3}$ with associated Lie algebra L is at least $p^{\frac{1}{2}tr(r-1)-r(m-t)-st}$.*

Proof: We will first show that all choices for the $\frac{1}{2}r(r-1)$ commutators of the form $[x_i, x_j]$ where $1 \leq j < i \leq r$ give members of $\mathcal{B}_{p,3}$ with associated Lie algebra L. We pick elements $x_1, \ldots, x_m \in P$ as in Lemma 5. We will use these elements to define the $p^{\frac{1}{2}tr(r-1)}$ groups in $\mathcal{B}_{p,3}$ with associated Lie algebra L that we require. To this end, suppose that β_{ijk} is an element of $\mathbb{F}_p$ for $1 \leq j < i \leq r$ and $1 \leq k \leq t$. We define a group $P_{\{\beta_{ijk}\}}$ as follows. The underlying set of our group is the set of m-tuples $(\alpha_1, \ldots, \alpha_m)$ of elements of $\mathbb{F}_p$. If we have that

$$(x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_m^{\alpha_m})(x_1^{\alpha'_1} x_2^{\alpha'_2} \ldots x_m^{\alpha'_m}) = (x_1^{\gamma_1} x_2^{\gamma_2} \ldots x_m^{\gamma_m})$$

in P, we define

$$(\alpha_1, \ldots, \alpha_m) * (\alpha'_1, \ldots, \alpha'_m) = (\gamma_1, \ldots, \gamma_{r+s}, \delta_1, \ldots, \delta_t)$$

in $P_{\{\beta_{ijk}\}}$ where

$$\delta_k = \gamma_k + \sum_{j=1}^{r} \sum_{i=j+1}^{r} \alpha_i \alpha'_j \beta_{ijk}.$$

It is an easy, but rather long, exercise to show that this binary operation on the set of all m-tuples of elements from $\mathbb{F}_p$ is in fact a group operation: We

relegate the work required for this to Appendix B. Suppose that $x_1, \ldots, x_m \in P$ are subject to the relations

$$\begin{aligned} x_i^p &= 1 \text{ where } 1 \leq i \leq m \\ [x_i, x_j] &= \prod_{k=1}^{m} x_k^{\gamma_{ijk}} \text{ where } 1 \leq j < i \leq m. \end{aligned}$$

Then we prove in the appendix that $P_{\{\beta_{ijk}\}}$ has a presentation consisting of generators $y_1, \ldots, y_m$ and relations

$$\left.\begin{aligned} y_i^p &= 1 \text{ where } 1 \leq i \leq m \\ [y_i, y_j] &= \textstyle\prod_{k=1}^{m} y_k^{\gamma_{ijk}} \text{ where } 1 \leq j < i \leq m \text{ and } i \geq r+1 \\ [y_i, y_j] &= \textstyle\prod_{k=1}^{r+s} y_k^{\gamma_{ijk}} \prod_{k=1}^{t} y_k^{\gamma_{ij(r+s+k)}+\beta_{ijk}} \text{ where } 1 \leq j < i \leq r. \end{aligned}\right\} \quad (5.2)$$

In order to prove the lemma, it remains to show that at most $p^{st+r(m-t)}$ of these groups fall into a single isomorphism class. It suffices to show that, for a group $Q \in \mathcal{B}_{p,3}$, there are at most $p^{st+r(m-t)}$ ways of choosing $y_1, \ldots, y_m \in Q$ such that the y_i satisfy commutator relations of the form (5.2) for distinct sets of elements $\{\beta_{ijk}\}$. Suppose that we choose the elements $y_1, \ldots, y_r$ modulo $\gamma_3(Q)$: there are at most

$$p^{r(m-t)}$$

ways of doing this. Since the elements y_i must satisfy commutator relations of the form (5.2), we find that the elements $y_{r+1}, \ldots, y_{r+s}$ are determined modulo $\gamma_3(Q)$ and the elements $y_{r+s+1}, \ldots, y_m$ are completely determined, once we have specified $y_1, \ldots, y_r$ modulo $\gamma_3(Q)$. We now choose the elements $y_{r+1}, \ldots, y_{r+s}$. Since they are already specified modulo $\gamma_3(Q)$, there are at most

$$p^{st}$$

ways of choosing these elements. Since the power-commutator presentation for Q depends only on the choice of $y_1, \ldots, y_r$ modulo $\gamma_3(Q)$, we have shown that there are at most

$$p^{st+r(m-t)}$$

possibilities for presentations of Q of the form (5.2). Hence the result follows. □

5.3 Graded Lie Algebras of Class 3

Let X, Y and Z be vector spaces over some field and let

$$\gamma : Y \times X \longrightarrow Z$$

be a bilinear map. For $x \in X$, we define the *breadth* $b(x)$ of x to be

$$b(x) = \dim((Y, x)\gamma).$$

Define $b(\gamma)$ by

$$b(\gamma) = \max\{b(x) \mid x \in X\}.$$

Then we have the following result.

Lemma 7 *Let b be a positive integer. Let X, Y and Z be vector spaces over $\mathbb{F}_p$ of dimensions r, s and t respectively. Then the number of bilinear maps γ defined as above with $b(\gamma) \leq b$ is at most*

$$p^{br(s+t-b+1)}.$$

Proof: Let $\{x_1, \ldots, x_r\}$ be a basis for X and let $\{y_1, \ldots, y_s\}$ be a basis for Y. Since γ is bilinear, γ is determined by the images

$$(y_i, x_j)\gamma \text{ where } 1 \leq i \leq s,\ 1 \leq j \leq r.$$

Since $b(\gamma) \leq b$, we have that

$$\dim(Y, x_j)\gamma \leq b$$

for $1 \leq j \leq r$. We choose r subspaces W_j of Z of dimension b in which the subspaces $(Y, x_j)\gamma$ are to be contained. There are at most

$$\frac{(p^t - 1)(p^t - p)\ldots(p^t - p^{b-1})}{(p^b - 1)(p^b - p)\ldots(p^b - p^{b-1})} \leq p^{(t-(b-1))b}$$

choices for each of the W_j, hence at most

$$p^{br(t-b+1)}$$

choices for all the W_j. Once the W_j have been chosen, there are at most p^b choices for the value of each of the elements $(y_i, x_j)\gamma$, so there are at most

$$p^{brs}$$

choices for the elements $(y_i, x_j)\gamma$ once the W_j are fixed. Hence there are at most

$$p^{br(t-b+1)+brs} = p^{br(s+t-b+1)}$$

choices for γ.□

We are now in a position to prove the main result of the section.

Lemma 8 *The number of graded Lie algebras* $L = L_1 \oplus L_2 \oplus L_3$ *over* $\mathbb{F}_p$ *generated by* L_1 *and such that the dimensions of* L_1, L_2 *and* L_3 *are equal to* r, s *and* t *respectively is at most*

$$sp^F$$

where

$$F = \max_{0 \leq b \leq \min\{s,t\}} \{br(s+t-b+1) + s(r-1) + \frac{1}{2}(s-b)(r-1)(r-2)\}.$$

Proof: Let L be a graded Lie algebra of the form above. Then L is determined by the two bilinear maps

$$\alpha : L_1 \times L_1 \longrightarrow L_2$$

and

$$\gamma : L_2 \times L_1 \longrightarrow L_3$$

which are induced by the Lie multiplication on L. These maps satisfy

$$(x,x)\alpha = 0 \tag{5.3}$$

for all $x \in L_1$ and (since the Lie multiplication in L satisfies the Jacobi identity)

$$((u,v)\alpha, x)\gamma = ((x,v)\alpha, u)\gamma - ((x,u)\alpha, v)\gamma. \tag{5.4}$$

If we can find an upper bound for the number of maps α and γ which satisfy the conditions (5.3) and (5.4), then we have found an upper bound for the

number of graded Lie algebras of the type we are considering. Suppose that $b(\gamma) = b$. By Lemma 7, there are at most

$$p^{br(s+t-b+1)}$$

possibilities for γ. Suppose we have chosen b and γ such that $b(\gamma) = b$. We estimate the number of possibilities for α such that (5.3) and (5.4) are satisfied. Since $b(\gamma) = b$, there exists $x_1 \in L_1$ such that $b(x_1) = b$. Extend $\{x_1\}$ to a basis $\{x_1, \ldots, x_r\}$ of L_1. Since we require α to be bilinear and to satisfy (5.3), it is determined by the elements

$$(x_i, x_j)\alpha$$

for $1 \leq i < j \leq r$. We next pick $r - 1$ elements of L_2 which correspond to the elements

$$(x_1, x_j)\alpha$$

where $2 \leq j \leq r$. There are at most

$$p^{s(r-1)}$$

choices for these elements. Once these elements have been chosen, since we have already chosen γ, the elements of L_3 given by

$$((x_1, x_k)\alpha, x_j)\gamma - ((x_1, x_j)\alpha, x_k)\gamma$$

are determined for all $2 \leq j < k \leq r$. Since we require that α and γ satisfy (5.4), the elements

$$((x_j, x_k)\alpha, x_1)\gamma$$

have been determined for all $2 \leq j < k \leq r$. Hence, since $b(x_1) = b$, there are at most p^{s-b} choices for each of the elements $(x_j, x_k)\alpha$ once b, γ and the elements $(x_1, x_j)\alpha$ have been chosen.Since there are $\frac{1}{2}(r-1)(r-2)$ pairs of the form (j,k) where $2 \leq j < k \leq r$, there are at most

$$p^{\frac{1}{2}(s-b)(r-1)(r-2)}$$

choices for the $(x_j, x_k)\alpha$ where $2 \leq j < k \leq r$. Once these elements have been picked, we have completely determined α and γ. Hence the number of bilinear maps α and γ satisfying (5.3) and (5.4) and with $b(\gamma) = b$ is at most

$$p^{br(s+t-b+1)+s(r-1)+\frac{1}{2}(s-b)(r-1)(r-2)}.$$

Since $0 \leq b \leq \min\{s,t\}$, the result follows.□

5.4 Proof of Theorem 4

Theorem 4 *Let $p > 2$. The number of groups of exponent p, nilpotency class at most 3 and order p^m is*

$$p^{\frac{2}{27}m^3+O(m^2)}.$$

Proof: The following result is the upper bound of Theorem 12.

Lemma 9 *Let $L = L_1 \oplus L_2 \oplus L_3$ be a graded Lie algebra over the field of p elements where the dimensions of L_1, L_2 and L_3 are r, s and t respectively. Then the number of groups in $\mathcal{B}_{p,3}$ with associated Lie algebra L is at most*

$$p^{\frac{1}{2}tr(r-1)}.$$

We use this result and Lemma 8 to prove Theorem 4. These two results clearly imply that the number of groups in $\mathcal{B}_{p,3}$ with an associated Lie algebra whose first, second and third gradings are dimensions r, s and t respectively is at most

$$sp^{F+\frac{1}{2}tr(r-1)}.$$

Hence we have that $\mathcal{B}_{p,3}(p^m)$ is at most

$$m^3 p^G$$

where G is the maximum of the function $H(r,s,t,b)$ defined by

$$H(r,s,t,b) = br(s+t-b+1) + s(r-1) + \frac{1}{2}(s-b)(r-1)(r-2) + \frac{1}{2}tr(r-1)$$

where r, s, t and b are positive integers subject to

$$r+s+t = m$$

and

$$0 \leq b \leq \min\{s,t\}.$$

Clearly, since $r,s,t \leq m$, we may write

$$H(r,s,t,b) = br(s+t-b) + \frac{1}{2}(s+t)r^2 - \frac{1}{2}br^2 + O(m^2).$$

Hence Theorem 4 follows if we can show that $M(r,s,t,b) \leq \frac{2}{27}m^3$ where

$$M(r,s,t,b) = r\left[b(s+t) - b^2 + \frac{1}{2}(s+t)r - \frac{1}{2}br\right]$$

subject to

$$r+s+t = m \tag{5.5}$$

and

$$0 \leq b \leq \min\{s, t\}. \tag{5.6}$$

In fact, we will weaken condition (5.6) to $0 \leq b$. Setting $s + t = m - r$ in the above expression for $M(r, s, t, b)$ gives that

$$M(r, s, t, b) = r[b(m - r) - b^2 + \frac{1}{2}(m - r)r - \frac{1}{2}br]. \tag{5.7}$$

We first check the values of any internal maxima of M. We have that $\frac{\partial M}{\partial b} = 0$ when

$$b = \frac{1}{2}(m - r) - \frac{1}{4}r.$$

Substituting this value of b into (5.7) gives that

$$M(r, s, m - r - s, \frac{1}{2}(m - r) - \frac{1}{4}r) = \frac{r}{4}\left[(m - r)^2 + (m - r)r + \frac{1}{4}r^2\right].$$

Setting $r = cm$ for some c such that $0 \leq c \leq 1$ we have that the value of M when $\frac{\partial M}{\partial b} = 0$ is

$$\frac{1}{4}\left[c - c^2 + \frac{1}{4}c^3\right]m^3.$$

This maximises when $c = \frac{2}{3}$, and substituting this value of c into our formula for M gives that

$$M \leq \frac{2}{27}m^3$$

when $\frac{\partial M}{\partial b} = 0$ as required. We now need to check that M is at most $\frac{2}{27}m^3$ on the boundary of its range. When $r = 0$, $M = 0 < \frac{2}{27}$ as required. When $r = m$,

$$M = m(-b^2 - \frac{1}{2}bm) \leq 0.$$

Finally, setting $b = 0$ in (5.7) gives that

$$M(r, s, t, 0) = \frac{1}{2}(m - r)r^2.$$

This maximises when $r = \frac{2}{3}m$ at $\frac{2}{27}m^3$ as required. Hence Theorem 4 follows.

□

Chapter 6

Graded Lie Rings

We aim to prove:

Theorem 5 *The number of graded Lie rings*

$$L = L_1 \oplus \cdots \oplus L_c$$

of order p^m *and where* L *is generated by* L_1 *is at most*

$$p^{\frac{2}{27}m^3+O(m^2)}.$$

The bulk of the proof of this theorem is contained in the following four lemmas.

Lemma 10 *Let* $L = L_1 \oplus L_2 \oplus \cdots \oplus L_c$, *where* L *is generated by* L_1. *Then* L *is determined by*

1. *the groups* L_i *where* $1 \leq i \leq c$.

2. *the map* $\gamma : L \otimes L_1 \longrightarrow L_2 \oplus \cdots \oplus L_c$ *induced by the Lie operation in* L.

Proof: Clearly the structure of L as an abelian group is determined by the L_i. It remains to prove that the Lie operation in L is determined by γ. It is sufficient to show that ab is determined by γ for all $a \in L_i$ and $b \in L_j$. We prove this by induction on j: for $j = 1$, $ab = (a \otimes b)\gamma$ as required.

Suppose now that $j > 1$ and that xy is determined by γ for all $x \in L$,$y \in L_k$ where $k < j$. Since $b \in L_j = L_{j-1}L_1$, we have that

$$b = \sum_{\alpha} c_\alpha d_\alpha$$

for some $c_\alpha \in L_{j-1}$, $d_\alpha \in L_1$. But now, using the Jacobi identity, we have that

$$ab = \sum_{\alpha} a(c_\alpha d_\alpha) = -\sum_{\alpha}(c_\alpha d_\alpha)a = \sum_{\alpha}(d_\alpha a)c_\alpha + \sum_{\alpha}(ac_\alpha)d_\alpha.$$

But $(d_\alpha a)c_\alpha$ and $(ac_\alpha)d_\alpha$ are determined by γ since $c_\alpha \in L_{j-1}$, $d_\alpha \in L_1$, and so ab is determined by γ as required.□

We define *the ith grading breadth* $b_i(L)$ of a graded Lie ring $L_1 \oplus \cdots \oplus L_c$ to be

$$\max\{\alpha \mid |L_i x| = p^\alpha \text{ for some } x \in L_1\}.$$

If $|L_i| = p^{r_i}$, it is clear that

$$0 \leq b_i(L) \leq \min\{r_i, r_{i+1}\}.$$

We will use the concept of second grading breadth to enumerate graded Lie rings of the type we are considering.

Lemma 11 *Let L be a graded Lie ring such that $b_i(L) = b_i$. Let*

$$\gamma_i : L_i \otimes L_1 \longrightarrow L_{i+1}$$

be the map induced by the Lie operation in L. Then there are at most

$$p^{r_1 b_i(r_i + r_{i+1} - b_i + 1)}$$

possibilities for γ_i, where $|L_i| = p^{r_i}$.

Proof: The proof of this lemma is exactly the same as that of Lemma 7, after noting that the number of subgroups of an abelian group of order p^r is at most the number of subspaces of a vector space over $\mathbb{F}_p$ of dimension r. □

Lemma 12 *Let M be the number of graded Lie rings*

$$L = L_1 \oplus L_2 \oplus \cdots \oplus L_c$$

generated by L_1 such that $b_2(L) = u$ and such that $|L_i| = p^{r_i}$. Then

$$M \leq p^{\frac{1}{2}(r_2 - u)r_1^2 + r_1 u(r_2 + r_3 - u) + \sum_{i=3}^{c-1} r_1 r_i r_{i+1} + O((r_1 + \cdots + r_c)^2)}$$

Proof: By Lemma 10, we need only specify the isomorphism classes of the L_i and the maps

$$\gamma_i : L_i \otimes L_1 \longrightarrow L_{i+1}$$

where $1 \leq i \leq c - 1$ in order to specify L completely.

The number of abelian groups of order p^{r_i} is, using a very crude estimate, at most p^{r_i}. Hence the number of choices for the isomorphism class of each

L_i is at most p^{r_i}, so the number of choices for the isomorphism classes of the L_i is at most

$$p^{r_1+r_2+\cdots+r_c}.$$

The number of choices for each γ_i where $i \geq 3$ is at most $p^{r_i r_{i+1} r_1}$ since γ_i is determined by the images in L_{i+1} of the $r_i r_1$ elements of a generating set of $L_i \otimes L_1$.

The number of choices for γ_2 is at most

$$p^{r_1 u(r_2+r_3-u+1)}$$

by Lemma 11.

Suppose now that the γ_i are fixed for $i \geq 2$. We find the number of possibilities for γ_1. Since γ_1 is induced from a Lie operation, it satisfies

$$(x,x)\gamma_1 = 0 \tag{6.1}$$

and also the Jacobi identity, namely

$$((x \otimes y)\gamma_1 \otimes z)\gamma_2 + ((y \otimes z)\gamma_1 \otimes x)\gamma_2 + ((z \otimes x)\gamma_1 \otimes y)\gamma_2 = 0 \tag{6.2}$$

for all $x, y, z \in L_1$.

Choose a subset $\{x_1, \ldots, x_{r_1}\}$ of L_1 such that the set generates L_1 and such that

$$|(L_2 \otimes x_1)\gamma_2| = p^u.$$

This element exists since $b_2(L) = u$. Choose the elements $(x_1 \otimes x_j)\gamma_1$ for $2 \leq j \leq r_1$: There are at most $p^{r_2(r_1-1)}$ choices for these elements. Once

these elements are chosen, we have severely restricted our choice of γ_1 since we know, by (6.2), that

$$((x_i \otimes x_j)\gamma_1 \otimes x_1)\gamma_2 = ((x_1 \otimes x_j)\gamma_1 \otimes x_i)\gamma_2 - ((x_1 \otimes x_i)\gamma_1 \otimes x_j)\gamma_2.$$

Hence, once the $(x_1 \otimes x_i)\gamma_1$ have been chosen, there are at most p^{r_2-u} choices for each of the elements $(x_i \otimes x_j)\gamma_1$ where $2 \leq i < j \leq r_1$. Hence there are at most

$$p^{r_2(r_1-1)+\frac{1}{2}(r_1-1)(r_1-2)(r_2-u)}$$

choices for the elements $(x_i \otimes x_j)\gamma_1$ where $1 \leq i < j \leq r_1$. Since γ_1 satisfies (6.1), the images of these elements define γ_1 completely and so we have found the maximum number of possibilities for γ_1.

In summary, there are at most

$$\begin{aligned} & p^{\frac{1}{2}(r_2-u)(r_1-1)(r_1-2)+r_2(r_1-1)+r_1u(r_2+r_3-u+1)+\left(\sum_{i=3}^{c-1} r_1r_ir_{i+1}\right)+r_1+\cdots+r_c} \\ \leq \quad & p^{\frac{1}{2}(r_2-u)r_1^2+r_1u(r_2+r_3-u)+(\sum_{i=3}^{c-1} r_1r_ir_{i+1})+O((r_1+\cdots+r_c)^2)} \end{aligned}$$

choices for the isomorphism classes of the L_i and the maps γ_i, hence the result follows.□

Lemma 13 *Define* $M_c(r_1, \ldots, r_c, u)$ *by*

$$M_c(r_1, \ldots, r_c, u) = \frac{1}{2}(r_2 - u)r_1^2 + ur_1(r_2 + r_3 - u) + \sum_{i=3}^{c-1} r_1r_ir_{i+1}.$$

Then $M_c(r_1, \ldots, r_c, u) \leq \frac{2}{27}$ *on the region defined by* $r_i \geq 0$, $u \geq 0$, $u \leq r_2$, $u \leq r_3$ *and* $r_1 + r_2 + \cdots + r_c = 1$.

Proof: We prove the assertion for the cases $c \leq 5$ individually, and then use induction to prove the general assertion.

The case $c \leq 3$ follows by the same argument as that in the proof of Theorem 4.

Assume $c = 4$. We must maximise

$$M_4 = \frac{1}{2}(r_2 - u)r_1^2 + ur_1(r_2 + r_3 - u) + r_1 r_3 r_4$$

where $r_1 + r_2 + r_3 + r_4 = 1$, $r_i \geq 0$, $u \geq 0$, $u \leq r_2$ and $u \leq r_3$.

We check for internal local maxima. By using Lagrange multipliers (see, for example, [25, Section 7H]), at an internal local maximum there exists λ such that

$$\frac{\partial M_4}{\partial r_1} = r_1(r_2 - u) + u(r_2 + r_3 - u) + r_3 r_4 = \lambda \tag{6.3}$$

$$\frac{\partial M_4}{\partial r_2} = \frac{1}{2}r_1^2 + ur_1 = \lambda \tag{6.4}$$

$$\frac{\partial M_4}{\partial r_3} = ur_1 + r_1 r_4 = \lambda \tag{6.5}$$

$$\frac{\partial M_4}{\partial r_4} = r_1 r_3 = \lambda \tag{6.6}$$

$$\frac{\partial M_4}{\partial u} = -\frac{1}{2}r_1^2 + r_1(r_2 + r_3) - 2ur_1 = 0 \tag{6.7}$$

Equations (6.4) and (6.5) imply that

$$\frac{1}{2}r_1 = r_4$$

and equations (6.5) and (6.6) imply that

$$u + r_4 = r_3.$$

Equalities (6.6) and (6.3) give that

$$r_1(r_2 - u) + u(r_2 + r_4) - \frac{1}{2}r_1 r_3 = 0$$

or, substituting our values for r_3 and r_4 into this equation, that

$$r_1(r_2 - u) + ur_2 - \frac{1}{4}r_1^2 = 0. \tag{6.8}$$

Now (6.7) implies that

$$r_2 = 2u - r_3 + \frac{1}{2}r_1 = u$$

and substituting this value of r_2 into (6.8) we get that $r_2^2 = \frac{1}{4}r_1^2$ or that $r_2 = \frac{1}{2}r_1$. Hence we have that $r_3 = \frac{1}{2}r_1 + \frac{1}{2}r_1 = r_1$. We know that

$$r_1 + r_2 + r_3 + r_4 = r_1 + \frac{1}{2}r_1 + r_1 + \frac{1}{2}r_1 = 3r_1 = 1$$

and hence that $r_1 = \frac{1}{3}$ and $\lambda = \frac{1}{9}$. This implies, by Euler's formula for homogeneous equations, that

$$M_4 = \frac{1}{3}\sum_{i=1}^{4} r_i \frac{\partial M_4}{\partial r_i} = \frac{1}{3}\lambda = \frac{1}{27}$$

at this local maximum. In summary, we have shown that if M_4 has an internal local maximum, then M_4 is strictly less than $\frac{2}{27}$ at this point. It remains to check the values of M_4 on its boundary.

When $r_1 = 0$, $M_4 = 0$. If $r_2 = 0$, then $u = 0$ and $M = r_1 r_3 r_4 \leq \frac{1}{27}$. If $r_3 = 0$, then $u = 0$ and $M = \frac{1}{2}r_2 r_1^2 \leq \frac{2}{27}$. If $r_4 = 0$, the result follows by the $c = 3$ case. If $u = r_2$, then $M = r_1 r_3(r_2 + r_4) \leq \frac{1}{27}$. If $u = r_3$ then

$$M = \frac{1}{2}(r_2 - r_3)r_1^2 + r_1 r_3(r_2 + r_4).$$

But in this case, replacing r_2 by $r_2 + r_4$ and r_4 by 0, we always obtain a larger value for M. Hence the maximum occurs when $r_4 = 0$ and the result follows by the $c = 3$ case. We are left with the case where $u = 0$. In this case we have to maximise

$$M = \frac{1}{2} r_2 r_1^2 + r_1 r_3 r_4$$

subject to the $r_i \geq 0$ and $r_1 + r_2 + r_3 + r_4 = 1$. We know that $M \leq \frac{2}{27}$ on the boundary of this region, by the above cases, so it remains to check for internal local maxima. By Lagrange multiplier theory, an internal local maximum occurs when the following equalities hold.

$$\frac{\partial M}{\partial r_1} = r_2 r_1 + r_3 r_4 = \lambda \tag{6.9}$$

$$\frac{\partial M}{\partial r_2} = \frac{1}{2} r_1^2 = \lambda \tag{6.10}$$

$$\frac{\partial M}{\partial r_3} = r_1 r_4 = \lambda \tag{6.11}$$

$$\frac{\partial M}{\partial r_4} = r_1 r_3 = \lambda \tag{6.12}$$

Equalities (6.11) and (6.12) imply that $r_3 = r_4$. Equalities (6.10) and (6.11) imply that $\frac{1}{2} r_1 = r_4$, hence that $r_3 r_4 = \frac{1}{4} r_1^2$. Equalities (6.9) and (6.10) now imply that

$$\frac{1}{4} r_1^2 = r_2 r_1$$

hence $\frac{1}{4} r_1 = r_2$. We have that

$$r_1 + r_2 + r_3 + r_4 = r_1 \left(1 + \frac{1}{4} + \frac{1}{2} + \frac{1}{2}\right) = 1$$

hence $r_1 = \frac{4}{9}$, $r_2 = \frac{1}{9}$ and $r_3 = r_4 = \frac{2}{9}$. Putting these values of the r_i into (6.12) we have, by Euler's formula, that

$$M = \frac{1}{3}\lambda = \frac{1}{3}\frac{4}{9}\frac{2}{9} < \frac{2}{27}.$$

This completes our result for the case $c = 4$.

Now consider the case $c = 5$. We need to maximise

$$M_5 = \frac{1}{2}(r_2 - u)r_1^2 + ur_1(r_2 + r_3 - u) + r_1r_3r_4 + r_1r_4r_5$$

subject to $r_1 + r_2 + r_3 + r_4 + r_5 = 1$, the $r_i \geq 0$, $u \geq 0$, $u \leq r_2$ and $u \leq r_3$. Lagrange multiplier theory gives that $\frac{\partial M_5}{\partial r_3} = \frac{\partial M_5}{\partial r_5}$ at an internal local maximum, i.e. that

$$ur_1 + r_1r_4 = r_1r_4.$$

This implies that $u = 0$ or $r_1 = 0$, i.e. that the maxima occur on the boundary of M_5. We now check the values of M_5 on the boundary. When $r_1 = 0$, $M_5 = 0$. When $r_2 = 0$, we have that $u = 0$ hence that

$$M_5 = r_1(r_3r_4 + r_4r_5) = r_1r_4(r_3 + r_5) \leq \frac{1}{27} < \frac{2}{27}.$$

When $r_3 = 0$, then $u = 0$ so we have

$$M_5 = \frac{1}{2}r_2r_1^2 + r_1r_4r_5 = M_4(r_1, r_2, r_5, r_4, 0) \leq \frac{2}{27}$$

by the case when $c = 4$. When $r_4 = 0$, we have that

$$M_5(r_1, r_2, r_3, 0, r_5, u) \leq M_4(r_1, r_2, r_3, r_5, u) \leq \frac{2}{27},$$

again by the case when $c = 4$. When $r_5 = 0$, the case $c = 4$ shows that $M_5 \leq \frac{2}{27}$. It remains to check the cases $u = 0, r_2$ or r_3. Suppose now that $u = 0$. Then

$$M_5 = \frac{1}{2}r_2 r_1^2 + r_1 r_3 r_4 + r_1 r_4 r_5 = M_4(r_1, r_2, r_4, r_3 + r_5, 0) \leq \frac{2}{27}$$

by the case $c = 4$. Now suppose that $u = r_2$. We need to maximise

$$M = r_2 r_1 r_3 + r_1 r_3 r_4 + r_1 r_4 r_5.$$

At an internal maximum, we must have that $\frac{\partial M}{\partial r_2} = \frac{\partial M}{\partial r_4}$, hence

$$r_1 r_3 = r_1 r_3 + r_1 r_5.$$

This implies that $r_1 = 0$ or $r_5 = 0$, hence our function has no internal maxima. We have dealt with the case $r_i = 0$ for some i above, hence we have that $M_5 \leq \frac{2}{27}$ in this case. Finally we consider the case when $u = r_3$. We need to maximise

$$\frac{1}{2}(r_2 - r_3)r_1^2 + r_3 r_1 r_2 + r_1 r_3 r_4 + r_1 r_4 r_5$$

subject to $r_1 + r_2 + r_3 + r_4 + r_5 = 1$ and the $r_i \geq 0$. Using Lagrange multiplier theory we have that the following equations hold at an internal maximum.

$$\frac{\partial M_5}{\partial r_1} = r_1 r_2 - r_1 r_3 + r_2 r_3 + r_3 r_4 + r_4 r_5 = \lambda \tag{6.13}$$

$$\frac{\partial M_5}{\partial r_2} = \frac{1}{2}r_1^2 + r_1 r_3 = \lambda \tag{6.14}$$

$$\frac{\partial M_5}{\partial r_3} = -\frac{1}{2}r_1^2 + r_1 r_2 + r_1 r_4 = \lambda \tag{6.15}$$

$$\frac{\partial M_5}{\partial r_4} = r_1 r_5 + r_1 r_3 = \lambda \tag{6.16}$$

$$\frac{\partial M_5}{\partial r_5} = r_1 r_4 = \lambda \tag{6.17}$$

We have that (6.17) and (6.15) imply that

$$r_2 = \frac{1}{2} r_1.$$

Also (6.17) and (6.16) imply that

$$r_4 = r_5 + r_3.$$

Equalities (6.16) and (6.14) give that

$$r_5 = \frac{1}{2} r_1$$

and (6.14) and (6.13) imply that

$$2r_1 r_3 = r_2 r_3 + r_3 r_4 + r_4 r_5.$$

Setting $r_4 = \frac{1}{2} r_1 + r_3$ and $r_2 = r_5 = \frac{1}{2} r_1$ in the above equation gives that

$$\frac{1}{2} r_1 r_3 = r_3^2 + \frac{1}{4} r_1^2. \tag{6.18}$$

We also have that

$$r_1 + r_2 + r_3 + r_4 + r_5 = \frac{5}{2} r_1 + 2r_3 = 1$$

hence that $r_3 = \frac{1}{2} - \frac{5}{4} r_1$. Substituting this value for r_3 into (6.18), we find that

$$\frac{1}{4} r_1 - \frac{5}{8} r_1^2 = \frac{1}{4} - \frac{5}{4} r_1 + \frac{25}{16} r_1^2 + \frac{1}{4} r_1^2$$

or that

$$\frac{39}{4} r_1^2 - 6r_1 + 1 = 0.$$

But this equation has no real solutions, hence our equation has no internal local maxima. $M_5 \leq \frac{2}{27}$ when any of the $r_i = 0$ by the work above, hence our equation maximises to a value at most $\frac{2}{27}$. Hence the case $c = 5$ follows.

We now consider the case $c > 5$. We prove that $M_c \leq \frac{2}{27}$ by induction on c. By the work above, the result holds for $c = 1, 2, 3, 4$ and 5, so we may assume, by induction, that $M_{c-1} \leq \frac{2}{27}$ and that $c > 5$. If M_c has an internal local maximum, we have in particular that

$$\frac{\partial M_c}{\partial r_{c-2}} = \frac{\partial M_c}{\partial r_c}.$$

Hence

$$r_1 r_{c-3} + r_1 r_{c-1} = r_1 r_{c-1}$$

or that $r_1 r_{c-3} = 0$. Hence M_c has no internal local maxima. We now check that $M_c \leq \frac{2}{27}$ on the boundary. If $r_1 = 0$, then $M_c = 0$ and we are done. If $r_c = 0$, then $M_c \leq \frac{2}{27}$ by induction. If $r_i = 0$ for $i \geq 3$ then

$$M_c(r_1, r_2, \ldots, r_{i-1}, 0, r_{i+1}, \ldots r_c, u) \leq M_c(r_1, r_2, \ldots, r_{i-1}, r_{i+1}, \ldots r_c, 0, u)$$

which is less than $\frac{2}{27}$ by induction. If r_2 or u are at the extreme of their range, the same argument as above implies that this equation maximises on the boundary, hence the result follows. □

We are now in a position to prove the theorem:

Proof of Theorem 5*:* Let c and u be fixed integers such that $0 \leq c, u \leq m$. Then we have, by Lemma 12, that the number of graded Lie rings of class c and second graded breadth u is at most

$$p^{km^3 + O(m^2)}$$

where k is the maximum value of M_c as defined in Lemma 13. Hence, by Lemma 13, $k = \frac{2}{27}$ and the result follows. □

Chapter 7

Enumeration of Groups of Class 3

In the introduction, we stated that it was possible to extend Theorem 4 to prove:

Theorem 6 *The number of groups of class at most* 3 *and order* p^m *is*

$$p^{\frac{2}{27}m^3+O(m^2)}.$$

The aim of this chapter is to give the proof of this extended theorem. We first prove an analogue of Lemma 5, which gives an upper bound on the number of groups associated with a given Lie ring.

Lemma 14 *Let* $L = L_1 \oplus L_2 \oplus L_3$ *be a graded Lie ring of order* p^m *such that*

$$\begin{aligned} |L_1| &= p^r \\ |L_2| &= p^s \text{ and} \\ |L_3| &= p^t. \end{aligned}$$

Then L is the associated graded Lie ring of at most

$$p^{\frac{1}{2}tr^2+O(m^2)}$$

groups.

Proof: Pick elements $e_1, \ldots, e_m \in L$ such that

$$\begin{aligned} L_1 &= \langle e_1, \ldots, e_r \rangle \\ L_2 &= \langle e_{r+1}, \ldots, e_{r+s} \rangle \text{ and} \\ L_3 &= \langle e_{r+s+1}, \ldots, e_m \rangle \end{aligned}$$

and such that

$$pe_i \in \langle e_{i+1}, \ldots, e_m \rangle$$

where $1 \leq i \leq m$. Then every element of L can be expressed uniquely in the form

$$\alpha_1 e_1 + \cdots + \alpha_m e_m$$

where $0 \leq \alpha_i < p$. Define $\lambda_{ijk} \in \{0, 1, \ldots, p-1\}$ by

$$e_i e_j = \sum \lambda_{ijk} e_k.$$

Suppose P has associated Lie ring L. Then there exist elements $x_1, \ldots, x_m \in P$ such that x_i maps to e_i under the natural maps

$$\begin{aligned} P/\gamma_2(P) &\longrightarrow L_1 \qquad \text{if } 1 \leq i \leq r \\ \gamma_2(P)/\gamma_3(P) &\longrightarrow L_2 \qquad \text{if } r+1 \leq i \leq r+s \\ \gamma_3(P) &\longrightarrow L_3 \qquad \text{if } r+s+1 \leq i \leq m. \end{aligned}$$

Every element of P can be uniquely expressed in the form

$$x_1^{\alpha_1} \ldots x_m^{\alpha_m}$$

where $0 \leq \alpha_i < p$.

By our choice of the elements e_i, we know that

$$x_i^p = x_{i+1}^{\alpha_{i,i+1}} \dots x_m^{\alpha_{i,m}}$$

where $0 \leq \alpha_{i,j} < p$. The Lie ring structure determines $[x_i, x_j]$ where $1 \leq j \leq r$ and $r+1 \leq i \leq m$ and also when $r+1 \leq j < i \leq m$. In addition, the Lie ring also determines $[x_i, x_j]$ modulo $\gamma_3(P) = \langle x_{r+s+1}, \dots, x_t \rangle$ when $1 \leq j < i \leq r$. Hence $x_1, \dots, x_m$ satisfy the relations

$$\left.\begin{array}{rcl} x_i^p & = & x_{i+1}^{\alpha_{i,i+1}} \dots x_m^{\alpha_{i,m}} \text{ where } 1 \leq i \leq m \\ [x_i, x_j] & = & \prod x_k^{\lambda_{ijk}} \text{ where } 1 \leq j \leq r \text{ and } r+1 \leq i \leq m \\ [x_i, x_j] & = & \prod x_k^{\lambda_{ijk}} \text{ where } r+1 \leq j < i \leq m \\ [x_i, x_j] & = & \prod_{k=r+1}^{r+s} x_k^{\lambda_{ijk}} \prod_{k=1}^{t} x_{r+s+k}^{\beta_{ijk}} \text{ where } 1 \leq j < i \leq r \end{array}\right\} \quad (7.1)$$

for some elements $\alpha_{i,j}, \beta_{ijk} \in \mathbb{F}_p$, and furthermore these generators and relations give a presentation for P. The number of choices for relations of the form (7.1) is equal to the number of choices for the $\frac{1}{2}r(r-1)t$ elements β_{ijk} when $1 \leq j < i \leq r$ and $1 \leq k \leq t$ together with the $\frac{1}{2}m(m-1)$ elements $\alpha_{i,j}$ where $1 \leq i < j \leq m$. The number of possibilities for each β_{ijk} or each $\alpha_{i,j}$ is at most p, hence there are at most

$$p^{\frac{1}{2}tr(r-1)+\frac{1}{2}m(m-1)} = p^{\frac{1}{2}tr^2+O(m^2)}$$

choices for a presentation of the form (7.1). Since any group P with associated Lie ring L must have a presentation of the form (7.1), the result follows.□

We may now use Lemma 12 in the case $c = 3$ which states that the number of graded Lie rings $L = L_1 \oplus L_2 \oplus L_3$ of order p^m, generated by L_1,

such that $b_2(L) = b$ and such that

$$\begin{aligned} |L_1| &= p^r \\ |L_2| &= p^s \text{ and} \\ |L_3| &= p^t \end{aligned}$$

is at most

$$p^{\frac{1}{2}(s-b)r^2+rb(s+t-b)+O(m^2)}.$$

Our proof of the extended version of Theorem 4 now goes as follows. Let P be a group of order p^m of class at most 3. Suppose that r, s and t are defined by $|P/\gamma_2(P)| = p^r$, $|\gamma_2(P)/\gamma_3(P)| = p^s$ and $|\gamma_3(P)| = p^t$. Let L be the associated graded Lie ring of P. Since L, to be an associated graded Lie ring of P, must be generated by its first grading we have, by Lemma 12, that there are at most

$$p^{\frac{1}{2}(s-b)r^2+rb(s+t-b)+O(m^2)}$$

possibilities for L, where $b_2(L) = b$. Hence, by Lemma 14, there are at most

$$p^{\frac{1}{2}(s+t-b)r^2+rb(s+t-b)+O(m^2)}$$

possibilities for P for a particular choice of r, s, t and b. Hence there are at most

$$p^{M+O(m^2)}$$

possibilities for P, where M is the maximum of the function

$$M(r,s,t,b) := r[b(s+t) - b^2 + \frac{1}{2}(s+t)r - \frac{1}{2}br]$$

subject to $r, s, t \geq 0$, $r + s + t = m$ and $0 \leq b \leq \min\{s, t\}$. But now $M = \frac{2}{27}m^3$, by the work in Section 5.4, and so Theorem 6 follows.□

Chapter 8

Small Varieties of p-Groups

We aim to prove Theorem 7 of Chapter 1.

Let p be an odd prime. Let $\mathcal{H}_p$ be the variety defined by the set of laws $\{[x,y,z],[x^p,y],[x,y]^p,x^{p^2}\}$ i.e. the variety of p-groups with an elementary abelian, central Frattini subgroup. Let $\mathcal{B}_{p,2}$ be the variety defined by the set of laws $\{[x,y,z],x^p\}$. We have that $\mathcal{B}_{p,2}$ is the variety of groups of exponent p and nilpotency class at most 2, and that $\mathcal{B}_{p,2}$ is a subvariety of $\mathcal{H}_p$.

Let $\mathcal{U}$ be any variety, and let m be a positive integer. We will denote by $\mathcal{U}(m)$ the set of groups of order p^m in $\mathcal{U}$. Our object is to prove:

Theorem 7 *If p is odd, then*

$$\frac{|\mathcal{H}_p(m)|}{|\mathcal{B}_{p,2}(m)|} \leq p^{\frac{2}{9}m^2+O(m^{3/2})}.$$

We use the following notation. If $\mathcal{U}$ is any variety, we denote the set of all members of $\mathcal{U}$ that have order p^{r+s} and possess a minimal generating set of r elements by $\mathcal{U}(r,s)$. So we have, in particular, that

$$|\mathcal{H}_p(m)| = \sum_{r=1}^{m} |\mathcal{H}_p(r,m-r)|. \tag{8.1}$$

Define $S_{r,s}$ to be the set of isomorphism classes of antisymmetric bilinear maps from $V \times V \to W$, where V and W are vector spaces over $\mathbb{F}_p$ of dimension r and s respectively.

Lemma 15 *Let p be an odd prime and let r, s be positive integers. Then*

$$|S_{r,s}| = \sum_{i=0}^{s} |\mathcal{B}_{p,2}(r,i)| .$$

Proof: We define a series of maps $\psi_i : \mathcal{B}_{p,2}(r,i) \to S_{r,s}$ for $0 \leq i \leq s$. The lemma follows if we can show these maps are injective, that their images are disjoint and that any element of $S_{r,s}$ is in the image of some ψ_i.

We define the ψ_i as follows. Let $P \in \mathcal{B}_{p,2}(r,i)$. Then the commutator map from $P/\Phi(P) \times P/\Phi(P)$ onto $\Phi(P)$ gives an antisymmetric bilinear map from $V \times V$ to W_0 where V and W_0 are vector spaces of dimension r and i respectively. If we define W_1 to be a vector space of dimension $s-i$, then the commutator map induces a map α from $V \times V$ to $W_0 \oplus W_1$ in the obvious way. We define $\psi_i(P) = \alpha$. This map is well defined since P determines the isomorphism class of the commutator map $[,] : P/\Phi(P) \times P/\Phi(P) \to \Phi(P)$ uniquely.

The maps ψ_i are injective, since the commutator map completely determines the isomorphism class of a group in $\mathcal{B}_{p,2}(r,i)$. Since the image of every $\alpha \in \mathrm{im}(\psi_i)$ is of dimension i, the images of the ψ_i are disjoint. Finally, if $\alpha \in S_{r,s}$ maps $V \times V \to W$, then $W = \mathrm{im}(\alpha) \oplus W_1$ for some W_1 of dimension $s-i$ for some i. Then α is the image of $P \in \mathcal{B}_{p,2}(r,i)$ where the commutator map of P is determined by the map $\alpha : V \times V \to \mathrm{im}(\alpha)$. Hence every element of $S_{r,s}$ is in the image of some ψ_i and the lemma follows. □

Lemma 16 *Let p be an odd prime and let r and s be positive integers. Then*

$$|\mathcal{H}_p(r,s)| \leq p^{rs} |S_{r,s}| .$$

Proof: We define a map $\psi : \mathcal{H}_p(r,s) \to S_{r,s}$ by mapping $P \in \mathcal{H}_p$ to the map from $P/\Phi(P) \times P/\Phi(P)$ to $\Phi(P)$ given by forming commutators. Since the isomorphism class of $P \in \mathcal{H}_p$ is determined by the commutator map together with the linear map from $P/\Phi(P)$ to $\Phi(P)$ given by $x \mapsto x^p$ for all $x \in P$, the number of elements of $\mathcal{H}_p(r,s)$ which map under ψ to the same element of $S_{r,s}$ is at most the number of linear maps from a vector space of dimension r to a vector space of dimension s. Since the number of such maps is p^{rs}, at most p^{rs} members of $\mathcal{H}_p(r,s)$ correspond to each member of $S_{r,s}$ under ψ. Hence the result follows. □

Lemma 17 *Let p be an odd prime, and let m be a positive integer. Define*

$$f(r,i) = p^{r(m-r)} |\mathcal{B}_{p,2}(r,i)|$$

for any integers r and i. Let the maximum value of f when $1 \leq r \leq m$ and $0 \leq i \leq m-r$ be attained when $r = r_0$, say. Then

$$\frac{|\mathcal{H}_p(m)|}{|\mathcal{B}_{p,2}(m)|} \leq m^2 p^{r_0(m-r_0)}.$$

Proof: We have

$$\begin{aligned} |\mathcal{H}_p(m)| &= \sum_{r=1}^{m} |\mathcal{H}_p(r, m-r)| \text{ by (8.1)} \\ &\leq \sum_{r=1}^{m} p^{r(m-r)} |S_{r,m-r}| \text{ by Lemma 16} \end{aligned}$$

$$
\begin{aligned}
&= \sum_{r=1}^{m} \sum_{i=0}^{m-r} p^{r(m-r)} \, |\mathcal{B}_{p,2}(r,i)| \text{ by Lemma 15} \\
&\leq m^2 p^{r_0(m-r_0)} \, |\mathcal{B}_{p,2}(r_0,i)| \text{ for some } i \\
&\leq m^2 p^{r_0(m-r_0)} \, |\mathcal{B}_{p,2}(m)|
\end{aligned}
$$

□

The above lemma already gives

$$\frac{|\mathcal{H}_p(m)|}{|\mathcal{B}_{p,2}(m)|} \leq m^2 p^{\frac{1}{4}m^2}$$

using none of our knowledge of $|\mathcal{B}_{p,2}(r,i)|$. We give a better bound than this by using the fact that

$$p^{\frac{1}{2}r(r-1)i-i^2-r^2} \leq |\mathcal{B}_{p,2}(r,i)| \leq p^{\frac{1}{2}r(r-1)i-i(i-1)} \tag{8.2}$$

(see Theorem 10) to estimate r_0.

Proof of Theorem 7: We use the notation given in the statement of Lemma 17. If we can show that $r_0 = \frac{2}{3}m + \delta$ where $|\delta| \leq \sqrt{m}$ for sufficiently large m the result follows by Lemma 17. By (8.2) we have

$$p^{\frac{1}{2}r(r-1)i-i^2-r^2+r(m-r)} \leq p^{r(m-r)} \, |\mathcal{B}_{p,2}(r,i)| = f(r,i) \leq p^{\frac{1}{2}r(r-1)i-i(i-1)+r(m-r)}$$

where $1 \leq r \leq m$ and $0 \leq i \leq m-r$. Let ϵ be chosen such that $0 \leq \epsilon < 1$ and so as to make $\frac{2}{3}m+\epsilon$ an integer. Then putting $r = \frac{2}{3}m+\epsilon$ and $i = \frac{1}{3}m-\epsilon$ into the lower bound given above shows that the maximum value of $f(r,i)$ is at least

$$
\begin{aligned}
& p^{\frac{1}{2}(\frac{2}{3}m+\epsilon)(\frac{1}{3}m-\epsilon)-(\frac{1}{3}m-\epsilon)^2-(\frac{2}{3}m+\epsilon)^2+(\frac{2}{3}m+\epsilon)(\frac{1}{3}m-\epsilon)} \\
= \; & p^{\frac{2}{27}m^3-\frac{4}{9}m^2-(\frac{5}{6}\epsilon+\frac{1}{2}\epsilon^2)m-(\frac{5}{2}\epsilon^2+\epsilon^3)} \\
\geq \; & p^{\frac{2}{27}m^3-\frac{4}{9}m^2-\frac{4}{3}m-\frac{7}{2}}.
\end{aligned}
$$

Set $M = \frac{2}{27}m^3 - \frac{4}{9}m^2 - \frac{4}{3}m - \frac{7}{2}$. Then the maximum value of $f(r,i)$ is at least p^M. The maximum value of $f(r,i)$ occurs at some point when our upper bound for $f(r,i)$ is greater than p^M. Define

$$g(r,i) = \frac{1}{2}r(r-1)i - i(i-1) + r(m-r)$$

for $1 \leq r \leq m$ and $0 \leq i \leq m-r$. Then we have that $f(r,i) \leq p^{g(r,i)}$. To show that $r_0 = \frac{2}{3}m + \delta$ where $|\delta| \leq \sqrt{m}$, it is sufficient to show that $g(r,i) \leq M$ for $0 \leq i \leq m-r$ and either $1 \leq r \leq \frac{2}{3}m - \sqrt{m}$ or $\frac{2}{3}m + \sqrt{m} \leq r \leq m$. It is therefore enough to show:

1. $g(r,i)$ has no internal local maxima for $1 \leq r \leq m$, $0 \leq i \leq m-r$.

2. $g(r,0) \leq M$ for $1 \leq r \leq m$. Also $g(1,i) \leq M$ for $0 \leq i \leq m-1$.

3. $g(r,m-r) \leq M$ for $1 \leq r \leq \frac{2}{3}m - \sqrt{m}$ and for $\frac{2}{3}m + \sqrt{m} \leq r \leq m$.

4. $g(\frac{2}{3}m + c\sqrt{m}, i) \leq M$ where $1 \leq i \leq \frac{1}{3}m - c\sqrt{m}$ and where $c = \pm 1$.

We will proceed to do this, assuming that $m \geq 15$.

1. $g(r,i)$ has no internal local maxima.

   We have

   $$\frac{\partial g}{\partial i} = \frac{1}{2}r(r-1) - 2i + 1$$

   and

   $$\frac{\partial g}{\partial r} = (r - \frac{1}{2})i + m - 2r.$$

   Now $\frac{\partial g}{\partial i} = 0$ gives

   $$i = \frac{1}{4}r(r-1) + \frac{1}{2}.$$

Hence if $\frac{\partial g}{\partial i} = \frac{\partial g}{\partial r} = 0$ we have

$$(r - \frac{1}{2})(\frac{1}{4}r(r-1) + \frac{1}{2}) + m - 2r = 0.$$

Multiplying by 8 and rearranging we get

$$2r^3 - 3r^2 - 11r + 8m - 2 = 0.$$

Does this equation have any solutions? Differentiating with respect to r we find that the extrema of the cubic occur when

$$6r^2 - 6r - 11 = 0$$

so the cubic has a local maximum at $\frac{3-5\sqrt{3}}{6} \leq 0$ and a local minimum at $\frac{3+5\sqrt{3}}{6}$. Since we are assuming that $m \geq 15$, then the cubic is positive at $r = 0$ and at its minima, so has no solutions for $1 \leq r \leq m$. Hence $g(r,i)$ has no internal local maxima on $1 \leq r \leq m$ and $0 \leq i \leq m - r$.

2. $g(r,i) \leq M$ on $i = 0$ and $r = 1$.

   We have

   $$g(1,i) = -i(i-1) + m - 1.$$

   This is maximal at $i = \frac{1}{2}$. Since i must be an integer, we have that $i = 0$ or $i = 1$, so the maximum value that $g(1,i)$ attains is $m-1$ which is less than M for $m \geq 15$. Now consider

   $$g(r,0) = r(m-r).$$

   There is a local maximum when $r = \frac{1}{2}m$ where g has the value $\frac{1}{4}m^2$, again less than M.

3. $g(r, m-r) \leq M$ for $1 \leq r \leq \frac{2}{3}m - \sqrt{m}$ and for $\frac{2}{3}m + \sqrt{m} \leq r \leq m$.

If we define $h(r) = g(r, m-r)$ we have that

$$\begin{aligned} h(r) &= \frac{1}{2}r(r+1)(m-r) - (m-r)(m-r-1) \\ &= -\frac{1}{2}r^3 + (\frac{1}{2}m - \frac{3}{2})r^2 + (\frac{5}{2}m - 1)r - m(m-1). \end{aligned}$$

We find the extrema of h. We have

$$\frac{dh}{dr} = -\frac{3}{2}r^2 + (m-3)r + \frac{5}{2}m - 1$$

and so h has a local minimum at

$$r = \frac{m}{3} - 1 - \frac{\sqrt{m^2+9m+3}}{3} \leq 0$$

and, since $m < \sqrt{m^2+9m+3} < m+5$, h has a local maximum at

$$r = \frac{2}{3}m + \delta$$

where $0 \leq \delta \leq \frac{2}{3}$. Hence to show that $h(r) \leq M$ for the ranges of r required, it is sufficient to check that $h(\frac{2}{3}m + c\sqrt{m}) \leq M$ for $c = \pm 1$. We have

$$\begin{aligned} & h(r + c\sqrt{m}) - M \\ &\leq -\frac{1}{2}(\frac{8}{27}m^3 + \frac{4}{3}cm^2\sqrt{m} + 2c^2m^2 + c^2m\sqrt{m}) \\ &\quad +(\frac{1}{2}m - \frac{3}{2})(\frac{4}{9}m^2 + \frac{4}{3}cm\sqrt{m} + c^2m) \\ &\quad +(\frac{5}{2}m - 1)(\frac{2}{3}m + c\sqrt{m}) - m^2 + m - M \\ &= -\frac{17}{18}m^2 + \frac{1}{2}(c-1)m\sqrt{m} - \frac{15}{6}m - c\sqrt{m} - \frac{7}{2} \qquad (8.3) \end{aligned}$$

which is negative for $c = 1$ for any m and for $c = -1$ for the case $m \geq 15$ that we are considering.

4. $g(\frac{2}{3}m + c\sqrt{m}, i) \leq M$ where $0 \leq i \leq \frac{1}{3}m - c\sqrt{m}$.

Since we know from (8.3) that $g(r, m-r) \leq M$ when $r = \frac{2}{3}m + c\sqrt{m}$, it is sufficient to show that $\frac{\partial g}{\partial i} \geq 0$ when $r = \frac{2}{3}m + c\sqrt{m}$, $0 \leq i \leq m - r$ or equivalently that $\frac{\partial g}{\partial i} = 0$ when $r = \frac{2}{3}m + c\sqrt{m}$ only when $i > m - r$. When $r = \frac{2}{3}m + c\sqrt{m}$ and $\frac{\partial g}{\partial i} = 0$ it is easy to show that, since $m \geq 15$,

$$\begin{aligned} i &= \frac{1}{2}(\frac{1}{2}(\frac{2}{3}m + c\sqrt{m})(\frac{2}{3}m + c\sqrt{m} - 1) + 1) \\ &= \frac{1}{9}m^2 + \frac{1}{3}cm\sqrt{m} + \frac{1}{12}m - \frac{1}{4}c\sqrt{m} + \frac{1}{2} \\ &\geq \frac{1}{3}m - c\sqrt{m}. \end{aligned}$$

Hence we have shown 4.

We have proved 1 to 4, hence the result follows. □

Appendix A

Checking that $\hat{\alpha}$ is a Homomorphism

We show that $\hat{\alpha}$, defined in the proof of Lemma 4, is a homomorphism. We use induction, proving that $\hat{\alpha}$ is a homomorphism on an ascending series $H_0, \ldots, H_d$ of subgroups of P_1. Assume that $\hat{\alpha}$ is a homomorphism on

$$H_i = \langle x_{d-i+1}, \ldots, x_d \rangle \, Z(P_1)P_1'.$$

This is certainly true for $i = 0$. Set $k := d - i$. We prove that $\hat{\alpha}$ is a homomorphism on $H_{i+1} = \langle x_k, \ldots, x_d \rangle \, Z(P_1)P_1'$. Let $x, y \in \langle x_k, \ldots, x_d \rangle \, Z(P_1)P_1'$. Then

$$x = x_k^{\beta} h$$

and

$$y = x_k^{\beta'} h'$$

where $0 \leq \beta, \beta' < p^{e_k}$ and $h, h' \in \langle x_{k+1}, \ldots, x_d \rangle \, Z(P_1)P_1'$. We have that

$$\hat{\alpha}(x)\hat{\alpha}(y) \;=\; \hat{\alpha}(x_k^{\beta})\hat{\alpha}(h)\hat{\alpha}(x_k^{\beta'})\hat{\alpha}(h')$$

$$
\begin{aligned}
&= \hat{\alpha}(x_k^{\beta})\hat{\alpha}(x_k^{\beta'})\hat{\alpha}(h)[\hat{\alpha}(h), \hat{\alpha}(x_k^{\beta'})]\hat{\alpha}(h') \\
&= \hat{\alpha}(x_k^{\beta})\hat{\alpha}(x_k^{\beta'})\hat{\alpha}(h)\hat{\alpha}([h, x_k^{\beta'}])\hat{\alpha}(h')
\end{aligned}
$$

by (4.9). Suppose that $\beta + \beta' < p^{e_k}$. Then we have that

$$\hat{\alpha}(x)\hat{\alpha}(y) = \hat{\alpha}(x_k^{\beta+\beta'})\hat{\alpha}(h[h, x_k^{\beta'}]h')$$

by (4.7) and because

$$h,\ [h, x_k^{\beta'}] \text{ and } h' \in \langle x_{k+1}, \ldots, x_d \rangle\ Z(P_1)P_1'.$$

Hence, by (4.6),

$$
\begin{aligned}
\hat{\alpha}(x)\hat{\alpha}(y) &= \hat{\alpha}(x_k^{\beta+\beta'}h[h, x_k^{\beta'}]h') \\
&= \hat{\alpha}(x_k^{\beta}hx_k^{\beta'}h') \\
&= \hat{\alpha}(xy).
\end{aligned}
$$

Finally, suppose that $\beta + \beta' \geq p^{e_k}$. Then

$$
\begin{aligned}
\hat{\alpha}(x_k^{\beta})\hat{\alpha}(x_k^{\beta'}) &= y_k^{\beta+\beta'} \\
&= y_k^{\beta+\beta'-p^{e_k}} y_k^{p^{e_k}} \\
&= \hat{\alpha}(x_k^{\beta+\beta'-p^{e_k}})\hat{\alpha}(x_k)^{p^{e_k}} \\
&= \hat{\alpha}(x_k^{\beta+\beta'-p^{e_k}})\hat{\alpha}(x_k^{p^{e_k}})
\end{aligned}
$$

by (4.8). Hence

$$
\begin{aligned}
\hat{\alpha}(x)\hat{\alpha}(y) &= \hat{\alpha}(x_k^{\beta+\beta'-p^{e_k}})\hat{\alpha}(x_k^{p^{e_k}})\hat{\alpha}(h)\hat{\alpha}([h, x_k^{\beta'}])\hat{\alpha}(h') \\
&= \hat{\alpha}(x_k^{\beta+\beta'-p^{e_k}})\hat{\alpha}(x_k^{p^{e_k}}h[h, x_k^{\beta'}]h')
\end{aligned}
$$

since

$$x_k^{p^{\epsilon_k}},\ h,\ [h, x_k^{\beta'}] \text{ and } h' \in \langle x_{k+1}, \ldots, x_d \rangle\ Z(P_1)P_1'.$$

Therefore using (4.6) we can deduce that

$$\begin{aligned} \hat{\alpha}(x)\hat{\alpha}(y) &= \hat{\alpha}(x_k^{\beta+\beta'-p^{\epsilon_k}} x_k^{p^{\epsilon_k}} h[h, x_k^{\beta'}]h') \\ &= \hat{\alpha}(xy). \end{aligned}$$

Hence $\hat{\alpha}$ is a homomorphism on $\langle x_k, \ldots, x_d \rangle\ Z(P_1)P_1'$, so by induction we have that $\hat{\alpha}$ is a homomorphism from P_1 to P_2 as required. □

Appendix B

Construction of Groups with a Given Associated Lie Algebra

In this appendix, we verify that the binary operation defined in Section 5.2 is in fact a group operation. We first recall the definition of our binary operation.

Let P be a group of exponent p, nilpotency class at most 3 and order p^m. Let $L = L_1 \oplus L_2 \oplus L_3$ be the associated graded Lie algebra of P. Let $e_1, \ldots, e_m$ be a basis for L such that

$$\begin{aligned} L_1 &= \langle e_1, \ldots, e_r \rangle \\ L_2 &= \langle e_{r+1}, \ldots, e_{r+s} \rangle \\ L_3 &= \langle e_{r+s+1}, \ldots, e_{r+s+r} \rangle . \end{aligned}$$

Let $x_1, \ldots, x_m$ be fixed elements of P such that x_i maps to e_i under the natural maps

$$P/(\gamma_2(P)) \longrightarrow L_1 \text{ if } 1 \leq i \leq r$$

$$(\gamma_2(P))/(\gamma_3(P)) \longrightarrow L_2 \text{ if } r+1 \leq i \leq r+s$$
$$\gamma_3(P) \longrightarrow L_3 \text{ if } r+s+1 \leq i \leq m.$$

Every element of P can be uniquely expressed in the form

$$x_1^{\alpha_1} x_2^{\alpha_2} \dots x_m^{\alpha_m}$$

for some elements $\alpha_i \in \mathbb{F}_p$. Suppose that

$$\{\beta_{ijk} \in \mathbb{F}_p \mid 1 \leq j < i \leq r, 1 \leq k \leq t\}$$

is fixed. We define an object $P_{\{\beta_{ijk}\}}$ by defining a binary operation $*$ on the set of m-tuples in $\mathbb{F}_p$ as follows. If we have that

$$(x_1^{\alpha_1} x_2^{\alpha_2} \dots x_m^{\alpha_m})(x_1^{\alpha_1'} x_2^{\alpha_2'} \dots x_m^{\alpha_m'}) = x_1^{\gamma_1} x_2^{\gamma_2} \dots x_m^{\gamma_m}$$

in P, we define

$$(\alpha_1, \dots, \alpha_m) * (\alpha_1', \dots, \alpha_m') = (\gamma_1, \dots, \gamma_{r+s}, \delta_1, \dots, \delta_t)$$

in $P_{\{\beta_{ijk}\}}$ where

$$\delta_k = \gamma_k + \sum_{j=1}^{r} \sum_{i=j+1}^{r} \alpha_i \alpha_j' \beta_{ijk}.$$

For brevity, we will define

$$\sigma(\alpha, \alpha', k) := \sum_{j=1}^{r} \sum_{i=j+1}^{r} \alpha_i \alpha_j' \beta_{ijk}.$$

We also define a function $\psi : P_{\{\beta_{ijk}\}} \longrightarrow P$ by

$$\psi((\alpha_1, \dots, \alpha_m)) = x_1^{\alpha_1} \dots x_m^{\alpha_m}.$$

We check that $P_{\{\beta_{ijk}\}}$ is a group. Clearly we have an identity element, namely $(0, 0, \ldots, 0)$. Suppose that

$$w = (\alpha_1, \ldots, \alpha_m) \in P_{\{\beta_{ijk}\}}.$$

We find the inverse of w. If

$$x_1^{\alpha_1'} x_2^{\alpha_2'} \ldots x_m^{\alpha_m'}$$

is an inverse for $\psi(w)$ in P, consider the element

$$\overline{w} = (\alpha_1', \ldots, \alpha_{r+s}', \alpha_{r+s+1}' - \sigma(\alpha, \alpha', 1), \ldots, \alpha_{r+s+t}' - \sigma(\alpha, \alpha', t)) :$$

Then

$$\psi(\overline{w}) = \psi(w)^{-1} x_{r+s+1}^{-\sigma(\alpha,\alpha',1)} \ldots x_{r+s+t}^{-\sigma(\alpha,\alpha',t)}$$

since $x_{r+s+1}, \ldots, x_m \in Z(P)$. Hence

$$\psi(w)\psi(\overline{w}) = x_{r+s+1}^{-\sigma(\alpha,\alpha',1)} \ldots x_{r+s+t}^{-\sigma(\alpha,\alpha',t)}.$$

So

$$w * \overline{w} = (0, 0, \ldots, 0)$$

in $P_{\{\beta_{ijk}\}}$, as required.

Finally, we check that $*$ is associative. Let

$$\begin{aligned} w &= (\alpha_1, \ldots, \alpha_m) \\ w' &= (\alpha_1', \ldots, \alpha_m') \\ w'' &= (\alpha_1'', \ldots, \alpha_m'') \end{aligned}$$

be arbitrary elements of $P_{\{\beta_{ijk}\}}$. Suppose that

$$\begin{aligned}(x_1^{\alpha_1}\dots x_m^{\alpha_m})(x_1^{\alpha'_1}\dots x_m^{\alpha'_m}) &= x_1^{\gamma_1}\dots x_m^{\gamma_m}\\ (x_1^{\alpha'_1}\dots x_m^{\alpha'_m})(x_1^{\alpha''_1}\dots x_m^{\alpha''_m}) &= x_1^{\gamma'_1}\dots x_m^{\gamma'_m}\end{aligned}$$

in P. Note that

$$\gamma_i = \alpha_i + \alpha'_i \tag{B.1}$$

and

$$\gamma'_i = \alpha'_i + \alpha''_i \tag{B.2}$$

for $1 \le i \le r$. Finally, suppose that

$$(x_1^{\gamma_1}\dots x_m^{\gamma_m})(x_1^{\alpha''_1}\dots x_m^{\alpha''_m}) = (x_1^{\alpha_1}\dots x_m^{\alpha_m})(x_1^{\gamma'_1}\dots x_m^{\gamma'_m}) = x_1^{\delta_1}\dots x_m^{\delta_m}$$

in P. Then

$$\begin{aligned}&(w * w') * w''\\ &= (\gamma_1,\dots,\gamma_{r+s},\gamma_{r+s+1}+\sigma(\alpha,\alpha',1),\dots,\gamma_{r+s+t}+\sigma(\alpha,\alpha',t)) * w''\\ &= (\delta_1,\dots,\delta_{r+s},\delta_{r+s+t}+\sigma(\alpha,\alpha',1)+\sigma(\gamma,\alpha'',1),\dots,\\ &\quad \delta_{r+s+t}+\sigma(\alpha,\alpha',t)+\sigma(\gamma,\alpha'',t))\end{aligned}$$

since, because $x_{r+s+1},\dots,x_m$ are central in P, we have

$$\begin{aligned}\psi(w*w')\psi(w'') &= \psi(w)\psi(w')\psi(w'')x_{r+s+1}^{\sigma(\alpha,\alpha',1)}\dots x_{r+s+t}^{\sigma(\alpha,\alpha',t)}\\ &= x_1^{\delta_1}\dots x_{r+s}^{\delta_{r+s}}x_{r+s+1}^{\delta_{r+s+1}+\sigma(\alpha,\alpha',1)}\dots x_{r+s+t}^{\delta_{r+s+t}+\sigma(\alpha,\alpha',t)}\end{aligned}$$

in P. Now, by (B.1) and (B.2) we have

$$\alpha_i\alpha'_j\beta_{ijk}+\gamma_i\alpha''_j\beta_{ijk} = (\alpha_i\alpha'_j+\alpha_i\alpha''_j+\alpha'_i\alpha''_j)\beta_{ijk} = \alpha_i\gamma'_j\beta_{ijk}+\alpha'_i\alpha''_j\beta_{ijk}.$$

In other words

$$\sigma(\alpha, \alpha', k) + \sigma(\gamma, \alpha'', k) = \sigma(\alpha, \gamma', k) + \sigma(\alpha', \alpha'', k).$$

Hence we have that

$$\begin{aligned}
&(w * w') * w'' \\
&= (\delta_1, \ldots, \delta_{r+s}, \delta_{r+s+1} + \sigma(\alpha, \gamma', 1) + \sigma(\alpha', \alpha'', 1), \ldots, \\
&\quad \delta_{r+s+t} + \sigma(\alpha, \gamma', t) + \sigma(\alpha', \alpha'', t)) \\
&= w * (\gamma'_1, \ldots, \gamma'_{r+s}, \gamma_{r+s+1} + \sigma(\alpha', \alpha'', 1), \ldots, \gamma_{r+s+t} + \sigma(\alpha', \alpha'', t)) \\
&= w * (w' * w'').
\end{aligned}$$

Hence $P_{\{\beta_{ijk}\}}$ is a group as required.

We now check that $P_{\{\beta_{ijk}\}} \in \mathcal{B}_{p,3}$ and find a presentation. Set $y_i \in P_{\{\beta_{ijk}\}}$ to be

$$(0, 0, \ldots, 0, 1, 0, \ldots, 0, 0)$$

where the '1' is in the i th place. The set $\{y_1, \ldots, y_m\}$ generates $P_{\{\beta_{ijk}\}}$. It is clear, from the fact that

$$y_i^k = (0, 0, \ldots, 0, k, 0, \ldots, 0, 0)$$

that the elements $y_1, \ldots, y_m$ are of order p. We want to find $[y_i, y_j]$ where $1 \leq j < i \leq m$. Suppose that

$$[x_i, x_j] = x_1^{\gamma_{ij1}} \ldots x_m^{\gamma_{ijm}}$$

in P (where $\gamma_{ijk} = 0$ if $k \leq i$). Then if $i \geq r + 1$, we have that

$$y_i y_j = y_1^{\alpha_1} \ldots y_m^{\alpha_m}$$

where

$$\begin{aligned} x_i x_j &= x_1^{\alpha_1} \dots x_m^{\alpha_m} \\ &= x_j x_i [x_i, x_j] \\ &= x_j x_i x_{i+1}^{\gamma_{ij(i+1)}} \dots x_m^{\gamma_{ijm}}. \end{aligned} \tag{B.3}$$

Hence, if $i \geq r+1$, then

$$y_i y_j = y_j y_i y_{i+1}^{\gamma_{ij(i+1)}} \dots y_m^{\gamma_{ijm}},$$

so

$$[y_i, y_j] = y_1^{\gamma_{ij1}} \dots y_m^{\gamma_{ijm}}$$

in this case. Similarly, if $i \leq r$ we have that

$$y_i y_j = y_1^{\alpha_1} \dots y_{r+s}^{\alpha_{r+s}} y_{r+s+1}^{\alpha_{r+s+1}+\beta_{ij1}} \dots y_{r+s+t}^{\alpha_{r+s+t}+\beta_{ijt}}$$

where the elements α_i are defined as in (B.4). Hence

$$[y_i, y_j] = y_1^{\gamma_{ij1}} \dots y_{r+s}^{\gamma_{ij(r+s)}} y_{r+s+1}^{\gamma_{ij(r+s+1)}+\beta_{ij1}} \dots y_{r+s+t}^{\gamma_{ij(r+s+t)}+\beta_{ijt}}$$

when $i \leq r$. Hence $P_{\{\beta_{ijk}\}}$ has a presentation of the form (5.2) as required. Finally, we use this presentation to show that $P_{\{\beta_{ijk}\}} \in \mathcal{B}_{p,3}$. By examining the presentation, we see that

$$\begin{aligned} \gamma_2(P_{\{\beta_{ijk}\}}) &= \langle y_{r+1}, \dots, y_m \rangle \\ \gamma_3(P_{\{\beta_{ijk}\}}) &= \langle y_{r+s+1}, \dots, y_m \rangle \end{aligned}$$

and that

$$\gamma_4(P_{\{\beta_{ijk}\}}) = 1.$$

Hence our group is of nilpotency class at most 3. Since $P_{\{\beta_{ijk}\}}$ is generated by elements of order p, $P_{\{\beta_{ijk}\}}$ is of exponent p when $p > 3$. When $p = 3$, let

$$w = (\alpha_1, \ldots, \alpha_m) \in P_{\{\beta_{ijk}\}}.$$

We must show that $w^3 = 1$. As in the proof of the associativity of $*$, we can calculate, since $\psi(w)^3 = 1$ in P, that

$$w^3 = (0, 0, \ldots, 0, \sigma(\alpha, \alpha, 1) + \sigma(2\alpha, \alpha, 1), \ldots, \sigma(\alpha, \alpha, t) + \sigma(2\alpha, \alpha, t)).$$

But

$$\sigma(\alpha, \alpha, k) + \sigma(2\alpha, \alpha, k) = \sum_{j=1}^{r} \sum_{i=j+1}^{r} (\alpha_i \alpha_j + 2\alpha_i \alpha_j)\beta_{ijk} = 0$$

hence $w^3 = 1$. We therefore have that $P_{\{\beta_{ijk}\}} \in \mathcal{B}_{p,3}$ for any odd prime p and the result follows.

Bibliography

[1] G.E. Andrews *The Theory of Partitions* (Addison-Wesley, 1976)

[2] E.E.Balash 'Determination of the number of non-isomorphic groups of squarefree order' *Isv. Vyssh. Uchebn. Zaved. Mat.*, 3-8 1966(Russian)

[3] F. Rudolf Beyl and Jürgen Tappe *Group Extensions, Representations and the Schur Multiplicator LNM 958* (Springer, 1982)

[4] A.R. Camina, G.R. Everest and T.M. Gagen 'Enumerating nonsoluble groups — a conjecture of John G. Thompson' *Bull. London Math. Soc.* 18 (1986), 265-268

[5] Gabrielle A. Dickenson 'On the Enumeration of Certain Classes of Soluble Groups' *Quart. J. Math. Oxford* (2) 20 (1969), 383-394

[6] P. Erdős, M. Ram Murty and V. Kumar Murty 'On the Enumeration of Finite Groups' *J.Number Theory* 25 (1987), 360-378

[7] L. Fuchs *Abelian Groups* (Pergamon Press, 1960)

[8] Patrick X. Gallagher 'Counting Finite Groups of a Given Order' *Math. Z.* 102 (1967), 236-7

[9] Daniel Gorenstein *Finite Groups* (Harper and Row, 1968)

[10] Philip Hall 'The Classification of Prime Power Groups' *J. reine angew. Math.* 182(1940), 130-141

[11] Graham Higman 'Enumerating p-groups. I: Inequalities' *Proc. London Math. Soc.* (3) 10 (1960), 24-30

[12] Graham Higman 'Enumerating p-groups. II: Problems whose Solution is PORC' *Proc. London Math. Soc.* (3) 10 (1960), 566-582

[13] I. Kaplansky *Infinite Abelian Groups* (University of Michigan Press, 1954)

[14] Michael E. Mays 'Counting Abelian, Nilpotent, Solvable and Supersolvable groups' *Arch. Math. (Basel)* 31 (1978), 536-538

[15] Michael E. Mays 'Groups of Square-Free Order are Scarce' *Pacific J. Math.* 91 (1980), 373-375

[16] Annabelle McIver and Peter M. Neumann 'Enumerating Finite Groups' *Quart. J. Math. Oxford* (2) 38 (1987), 473-488

[17] M. Ram Murty and V. Kumar Murty 'On the Density of Various Classes of Groups' *J. Number Theory* 17 (1983) no. 1, 29-36

[18] M. Ram Murty and V. Kumar Murty 'On the Number of Groups of a Given Order' *J. Number Theory* 18 (1984), 178-191

[19] M. Ram Murty and V. Kumar Murty 'On Groups of Square-Free Order' *Math. Annalen* 267 (1984), 299-309

[20] Hanna Neumann *Varieties of Groups* (Springer, 1967)

[21] Peter M. Neumann 'An Enumeration Theorem for Finite Groups' *Quart. J. Math. Oxford* (2) 20 (1969), 395-401

[22] Carl Pomerance 'On the Average Number of Groups of Square-Free Order' *Proc. Amer. Math. Soc.* 99 (1987), 223-231

[23] L. Pyber 'Enumerating Finite Groups of Given Order', *Annals of Mathematics, to appear*

[24] Charles C. Sims 'Enumerating p-groups' *Proc. London Math. Soc.* (3) 15 (1965), 151-66

[25] William L. Voxman and Roy H. Goetschel, Jr *Advanced Calculus. An Introduction to Modern Analysis* (Dekker, 1981)