NILPOTENCY AND RELATED PROPERTIES OF GROUP EXTENSIONS

by

David Shield

A thesis presented to the
Australian National University
for the degree of
Master of Arts
in the Department of Pure Mathematics,
School of General Studies.

Canberra 1969

Preface

Professor Hanna Neumann, in the preface to [10], suggested that the theory of product varieties could be based on Šmel'kin's embedding theorem, and with this in mind suggested to me that the use of Šmel'kin's theorem in systematising the considerable but scattered set of known results about groups non-trivially of the form $F/\underline{\underline{V}}(R)$ would make an interesting research project. The very first such result considered, that F/R' can not be an Engel group except in trivial cases, proved so beguiling that it led to the development of all the results reported in this thesis. The properties of $F/\underline{\underline{V}}(R)$ remain scattered.

I wish to record my sincere thanks to Professor Hanna Neumann, my supervisor until August of this year, for her sympathetic encouragement as results appeared and disappeared; and to Dr M.F. Newman, who even before taking over as supervisor in August acted as an invaluable guide to facts and references, and since then has suggested generalisations and simplifications of some results, which have led to the organisation of Chapter 1 in its present form. Both supervisors have made many suggestions which greatly improved the presentation of this work. With these reservations the results shown, except where otherwise acknowledged, are my own.

While working on this thesis I have been employed as Tutor and Senior Tutor in the Department of Applied Mathematics of the School of General Studies, and wish to acknowledge the cooperation and consideration shown by Professor A. Brown, which has made this work possible.

Table of Contents

t/

Introduction

The main results reported in this thesis are bounds on the Engel length and nilpotency class of certain group extensions, G, in terms of parameters depending only on a normal subgroup H and the quotient group G/H. Closely related to these are results giving sufficient conditions on H and G/H for the group G to have certain properties, ranging from being an Engel group (the weakest) to being nilpotent (the strongest). There are also results in the converse direction, giving corresponding necessary conditions in some special cases of group extensions, one of which is the wreath product.

0.1 Notation

Lower case letters of the Roman alphabet are generally reserved for integers, though "S" and "F" occur for particular integer-valued functions. Upper case script ($\mathcal{H}, \mathcal{N}$, etc.) is used for sets of integers; in particular $\mathcal{N}$ is the set of all positive integers and $\mathcal{P}$ the set of all primes. Group elements (except the identity, which is everywhere "1") are denoted by lower case letters of the Greek alphabet. Upper case German script (here written $\underline{\underline{U}}$, $\underline{\underline{V}}$, etc.) is used for varieties; in particular $\underline{\underline{N}}_c$ is the variety of all nilpotent groups of class less than or equal to c, $\underline{\underline{B}}_v$ is the variety of all groups of exponent dividing v, $\underline{\underline{A}}(= \underline{\underline{N}}_1)$ is the variety of all abelian groups, and $\underline{\underline{A}}_v = \underline{\underline{A}} \cap \underline{\underline{B}}_v$.

For any group G and variety $\underline{\underline{V}}$, the corresponding verbal subgroup (the intersection of all normal subgroups H of G such that $G/H \in \underline{\underline{V}}$) is written $\underline{\underline{V}}(G)$; where $\underline{\underline{V}} = \underline{\underline{A}}$ it is usually written G' rather than $\underline{\underline{A}}(G)$.

The usual notation is used for conjugates $(\alpha^{\beta} = \beta^{-1}\alpha\beta,\ \alpha^{-\beta} = (\alpha^{-1})^{\beta})$, commutators $([\alpha,\beta] = \alpha^{-1}\beta^{-1}\alpha\beta = \alpha^{-1}\alpha^{\beta}$, inductively $[\alpha_1,\alpha_2, \ldots, \alpha_{n-1},\alpha_n] = [[\alpha_1,\alpha_2, \ldots, \alpha_{n-1}],\alpha_n])$, and Engel commutators $([\alpha,n\beta] = [\alpha,\underbrace{\beta, \ldots, \beta}_{n}]$, in particular $[\alpha,0\beta] = \alpha)$.

Square brackets are also used for references, and to denote the integer part of a real number ($[r/s]$ is the greatest integer n such that $n \leq r/s$); no confusion should arise.

If Π_1 and Π_2 are any two properties of groups, and the group G has a normal subgroup H such that H has property Π_1 and G/H has property Π_2 then G will be said to have the product $\Pi_1\Pi_2$ of these properties. If for some Π every group with property $\Pi\,\Pi$ also has property Π, then Π is said to be idempotent.

The restricted and unrestricted direct products of the indexed set of groups $\{A_\delta \mid \delta \in \Delta\}$ are denoted by $\prod^{(x)}_{\delta\in\Delta} A_\delta$, and $\prod^{x}_{\delta\in\Delta} A_\delta$ respectively, the free product (see 18.11 of [10] for definition) by $\prod^{*}_{\delta\in\Delta} A_\delta$, and the verbal product associated with the variety $\underline{\underline{V}}$ (defined in 18.31 of [10]) by $\prod^{\underline{\underline{V}}}_{\delta\in\Delta} A_\delta$.

The restricted and unrestricted wreath products, A wr B and A Wr B respectively, of the groups A and B are well-known constructions. When the base group, $K = \prod^{(x)}_{\beta\in B} A(\beta)$ or $\prod^{x}_{\beta\in B} A(\beta)$, is regarded as a set of functions from B to A with multiplication defined componentwise, the support of any element ϕ of the base group is defined to be $\{\beta \in B \mid \beta\phi \neq 1\}$. For any $\beta \in B$, the set of elements of K whose support is contained in $\{\beta\}$ is clearly a subgroup isomorphic with A. It is denoted $A(\beta)$ and called the coordinate subgroup of W corresponding to β; when $\beta = 1$, it will be called the first coordinate subgroup, $A(1)$. Under a fixed isomorphism from A to $A(\beta)$, the image of arbitrary element $\alpha \in A$ will be written $\alpha(\beta)$. Note that when B is identified with a complement of K in W, $\alpha(\beta) = \alpha(1)^{\beta}$ for all $\beta \in B$.

Similar notation will be employed for the verbal wreath product $A \text{ wr}_{\underline{\underline{V}}} B$, corresponding to the variety $\underline{\underline{V}}$, of the groups A and B which is defined in a similar way to the restricted standard wreath product, except that $\prod^{\underline{\underline{V}}}_{\beta\in B} A(\beta)$ replaces $\prod^{(x)}_{\beta\in B} A(\beta)$ as the base group. Elements of the base group can now no longer be regarded as functions; however, if an order, $\dot{\leq}$ say, is defined on the elements of B, then 18.35 of [10] shows that every element of the base group may be written uniquely in the form

$$\alpha_1(\beta_1)\ \alpha_2(\beta_2)\ \ldots\ \alpha_m(\beta_m)\ \gamma$$

where $\beta_1 \dot{<} \beta_2 \dot{<} \ldots \dot{<} \beta_m$, $\alpha_i \neq 1$ for $1 \leq i \leq m$, and γ belongs to the cartesian of the verbal product. Note that γ depends on the particular ordering, $\dot{\leq}$, chosen; but the α_i do not. Hence it is still possible to speak unambiguously of the support of an element of the base group, and of coordinate subgroups.

0.2 Background

The bounds on Engel length and nilpotency class presented in Chapters 3 and 4 do not involve the concept of varieties of groups, but they arose from an enquiry directed toward the properties of product varieties.

A group G is said to belong to the product variety $\underline{\underline{VW}}$ if and only if it contains a normal subgroup N such that $N \in \underline{\underline{V}}$ and $G/N \in \underline{\underline{W}}$. As Šmel'kin has pointed out (in [12]), the fact that every variety can be uniquely represented as a product of indecomposable varieties gives rise to an interest in knowing the properties of a product variety in terms of the properties of its factors. (A variety is said to have a property, applicable to groups, if every group in the variety has that property.)

Some such results are trivial. For example, a product variety clearly is soluble if and only if all its factors are soluble, and has finite exponent equal to the product of the exponents of its factors if and only if they all have finite exponent. Several non-trivial properties are proved by Šmel'kin in the same paper. A product $\underline{\underline{VW}}$ of two non-trivial varieties $\underline{\underline{V}}$ and $\underline{\underline{W}}$ possess a "root property" residually if and only if both $\underline{\underline{V}}$ and $\underline{\underline{W}}$ do (3.4);

it can never be nilpotent (4.2); its free groups of finite rank may be presented with a finite number of relators if and only if $\underline{\underline{V}}$ has the same property and $\underline{\underline{W}}$ is locally finite (5.4); and it is a Cross variety (i.e., is generated by a finite group) if and only if $\underline{\underline{V}}$ is nilpotent, $\underline{\underline{W}}$ is abelian, and $\underline{\underline{V}}$ and $\underline{\underline{W}}$ have finite coprime exponents (6.3).

To this list we add, in §1.6 of the present thesis, that if $\underline{\underline{V}}$ and $\underline{\underline{W}}$ are both non-trivial, then $\underline{\underline{VW}}$ is locally nilpotent if and only if $\underline{\underline{V}}$ and $\underline{\underline{W}}$ are both locally nilpotent, and both have exponents equal to powers of one prime, p; and that for $\underline{\underline{VW}}$ to be an Engel variety, it is necessary that $\underline{\underline{V}}$ and $\underline{\underline{W}}$ both have p-power exponent and both be Engel varieties, and is sufficient that both have p-power exponent, $\underline{\underline{V}}$ be locally nilpotent, and $\underline{\underline{W}}$ be Engel.

Šmel'kin's results about the free groups of product varieties were obtained as special cases of results about groups of the form $F/\underline{\underline{V}}(R)$, where F is an absolutely free group, $R \trianglelefteq F$, and $\underline{\underline{V}}$ is a non-trivial variety. In the special case $R = \underline{\underline{W}}(F)$, the group $F/\underline{\underline{V}}(\underline{\underline{W}}(F))$ is free with the same rank as F in the variety $\underline{\underline{VW}}$. A major tool used by Šmel'kin was his "embedding theorem", stated here in a form due to Kovács [8] :

<u>0.2.1</u> <u>Theorem</u> (ŠMEL'KIN, [12], Theorem 2.1)

Let F be an absolutely free group on the generators $\{\alpha_i \mid i \in \Lambda\}$, R a normal subgroup of F, and $\underline{\underline{V}}$ a variety. Then the factor group $F/\underline{\underline{V}}(R)$ may be embedded in $F/\underline{\underline{V}}(F) \text{ wr}_{\underline{\underline{V}}} F/R$ in such a way that $f_i \underline{\underline{V}}(R)$ is mapped onto $f_i N \, . \, f_i \underline{\underline{V}}(F)(1)$ where $f_i N$ is in the top group, and $f_i \underline{\underline{V}}(F)(1)$ is the corresponding generator in the first coordinate subgroup of the base group.

It was pointed out by Šmel'kin - see also Kovács [8] and Dunwoody [3] - that the "Magnus embedding" is the special case $\underline{\underline{V}} = \underline{\underline{A}}$ of Šmel'kin's embedding theorem. Bachmuth and Hughes [1] have used the Magnus embedding to give simple proofs of the following earlier results :

<u>0.2.2</u> <u>Theorem</u> (B.H. NEUMANN, K. GRUENBERG)

If F/R' is an Engel group, then $F = R$.

<u>0.2.3</u> <u>Theorem</u> (M. AUSLANDER and R.C. LYNDON)

The group F/R is finite if and only if F/R' has non-trivial centre.

<u>0.2.4</u> <u>Theorem</u> (K. GRUENBERG)

If $F/\underline{\underline{B}}_m(R).R'$ is an Engel group, then either $F = R$ or m is a power of a prime p, and F/R is a p-group.

Šmel'kin has generalised the "if" part of 0.2.3 :

<u>0.2.5</u> <u>Theorem</u> (A.L. ŠMEL'KIN, [12], 4.1)

If F is a non-cyclic (absolutely) free group, $\underline{\underline{V}}$ is a non-trivial variety, and F/R is infinite, then $F/\underline{\underline{V}}(R)$ has trivial centre.

The "only if" part of 0.2.3 can not be similarly generalised. Though it remains true if $\underline{\underline{V}} = \underline{\underline{N}}_c$ or even $\underline{\underline{V}} = (\underline{\underline{N}}_{c_1}\underline{\underline{N}}_{c_2}\ldots\underline{\underline{N}}_{c_r}) \cap \underline{\underline{N}}_c$ or if $\underline{\underline{V}} \subseteq \underline{\underline{A}}$, it is not hard to show that it is false if $\underline{\underline{V}}$ is a variety, such as $\underline{\underline{A}}_2\underline{\underline{A}}$, whose non-cyclic free groups have trivial centre. Theorem 1.2.1 of this thesis generalises both 0.2.2 and 0.2.4, and 1.4.1 provides a partial converse.

Baumslag in §3 of [2] has found a necessary and sufficient condition for a wreath product to be nilpotent; the sufficient condition actually applies to group extensions in general (Lemma 3.8). Liebeck [9] has found the exact nilpotency class of a nilpotent wreath product A wr B in the special case where A and B are both abelian. Scruton in [11] has obtained upper and lower bounds for the nilpotency class of nilpotent wreath products in general, but these bounds are of widely different magnitudes. In Chapter 4 of this thesis, an upper bound for the nilpotency class of any group extension satisfying Baumslag's sufficient condition is obtained. It coincides with that of Liebeck for A wr B when A and B are both abelian, and is in fact attained by the wreath product A wr B when A and B have arbitrary nilpotency class. However it suffers in depending on two rather complicated parameters of the group B, whereas Scruton's bounds use simply the order of this group.

0.3 Note on weight of a commutator

In Chapters 3 and 4, ideas closely connected with the weight of a commutator occur frequently. The weight of a particular given commutator expression may be defined quite simply; however some difficulty arises when it is not the expression as such but the group element represented by the expression that is under consideration.

In the introduction of [13], Ward gives a summary of the "conventional theory of basic commutators". If a group G is generated by the set of elements G_1, elements of G_1 are considered to be basic commutators of weight 1, and may be well-ordered in any way. When $c > 1$ and basic commutators of weight less than c have been defined and ordered, the basic commutators of weight c are expressions of the form $[\xi,\eta]$ where ξ and η are basic commutators of weights r and s respectively, $r+s = c$, ξ follows η in the ordering, and if $\xi = [\xi_1,\xi_2]$ then ξ_2 preceds η.

If the last two conditions (about ordering) are omitted, this same process gives the weight of any commutator expression, not necessarily basic.

One difficulty which arises in assigning a weight to a commutator as a group element is the possibility that two commutator expressions with different weights may be equal as group elements. For example, if $\alpha,\beta,\gamma,\delta,\mathcal{E} \in G_1$, and $[\alpha,\beta] = [\gamma,\delta,\mathcal{E}] = \xi$, shall we say that ξ as an element of G has weight two or three?

Another difficulty is the choice of generating set. Clearly it is possible for a group element to have widely differing weights when expressed as a commutator in terms of different generating sets.

Still another question is that of extending the idea of weight to arbitrary group elements, including those which cannot be expressed as commutators. What will happen to an element which can be expressed as a single commutator of weight two (but not higher weight) or as a product of other commutators all of weight four?

A full discussion of these problems becomes very involved. For the purposes of the present thesis, the second difficulty will be met by choosing $G_1 = G$, so that every element of every group is considered to be a commutator of weight one. Let G_i be the set of group elements which may be expressed as commutators of weight i in terms of G_1. For some applications, we will be concerned simply with the fact that an element belongs to G_i. One way (which will not concern us in this thesis) of defining uniquely the weight of an element ξ is to say that ξ has weight i when $\xi \in G_i$ and $\xi \notin G_j$ for $j > i$. The weight of an element belonging to an infinite number of the G_i (in particular, the identity) could be considered infinite.

Another possible approach, which can give a different answer to the third question above, is to say that ξ has weight i if

$$\xi \in \operatorname{sgp}\{G_j \mid i \leq j\} \quad \text{and} \quad \xi \notin \operatorname{sgp}\{G_j \mid i < j\}$$

The choice $G_1 = G$ means that $\operatorname{sgp}\{G_j \mid i \leq j\} = \underset{=}{N}_{i-1}(G)$. In some applications this idea of weight also will be used.

Chapter 1

Non-numerical results

Related to (i) being nilpotent, but progressively weaker, are the group properties: (ii) being locally nilpotent, (iii) having all k-generator subgroups nilpotent for some fixed $k \in \mathcal{N}$, and (iv) being an Engel group. The class of all groups having any one of these properties is not a variety.

However, corresponding to each, there is a bounded, varietal property. These are: (i)' being nilpotent of class at most c for fixed $c \in \mathcal{N}$, (ii)' having all k-generator subgroups nilpotent of class at most $c(k)$ for all $k \in \mathcal{N}$, where c is a function from $\mathcal{N}$ to $\mathcal{N}$; this we will call being boundedly locally nilpotent; (iii)' having all k-generator subgroups nilpotent of class at most c for fixed $k, c \in \mathcal{N}$, and (iv)' satisfying an Engel condition.

Every nilpotent group is, of course, nilpotent of finite class, so that each group having the property (i) also has (i)'. However a group G may have one of the properties (ii), (iii), or (iv) without having the corresponding bounded property. In this case there are groups in the variety generated by G - for example, the countably infinite Cartesian power of G - which do not have the property. In a variety in which every group has one of the properties (i) to (iv), every group has, in fact, the corresponding bounded property. In particular, every group of an Engel variety satisfies the ℓ th Engel condition for a fixed $\ell \in \mathcal{N}$ depending only on the variety, and every group of a locally nilpotent variety is boundedly locally nilpotent, the function $c : \mathcal{N} \to \mathcal{N}$ determined by the variety.

In order that an arbitrary group G with normal subgroup H should have any one of these properties, the only necessary condition on H and G/H is that both have the required property. This is shown by the example in which H is a direct factor of G and the given condition is sufficient. Besides being trivial, this necessary condition is much weaker than a sufficient condition in general cases, and for this reason necessary conditions are considered only for two special types of group extensions.

In both of these types, one of splitting and one of non-splitting extensions, all elements outside the normal subgroup H have a genuine effect on the normal subgroup, inducing non-trivial automorphisms. They are, in §1.2, groups non-trivially of the form $F/\underline{\underline{V}}(R)$, whose importance in the study of product varieties has already been discussed, and in §1.3 the restricted standard wreath product A wr B of non-trivial groups.

It may illuminate the proofs of 1.2.1 and 1.3.1 to point out, in very imprecise terms, some other common features of these two types of groups which are not shared by group extensions in general. It is possible to select an element of the normal subgroup (a free generator of R in $F/\underline{\underline{V}}(R)$; an element of one coordinate subgroup in the wreath product) whose conjugates by distinct powers, modulo the normal subgroup, of any element outside it satisfy two properties: firstly, independence, in that no power of any one of them can be expressed in terms of powers of the others, and secondly, the possibility of a certain amount of commutativity for themselves and their non-trivial powers. In the wreath product, they actually commute, since they have trivially-intersecting support; and since every variety contains an abelian subvariety with the same exponent, $R/\underline{\underline{V}}(R)$ has an abelian homomorphic image, $R/(\underline{\underline{V}} \cap \underline{\underline{A}})(R)$, in which the powers remain non-trivial.

These properties are not satisfied in general extensions; for example the "commutativity" can not be provided when the normal subgroup is perfect.

In this chapter, §1.1 provides some preliminary information about certain Engel commutators. In §1.4 sufficient conditions are found for group extensions in general to have most of the properties being discussed; these sufficient conditions are closely related to the necessary conditions found for certain types of extensions in §1.2 and §1.3. Examples given in §1.5 illuminate the distinction between the bounded and unbounded conditions. The results of §1.2 and §1.4 are applied in §1.6 to find conditions for a product variety to be Engel and locally nilpotent.

1.1.1 Lemma

If β and γ are elements of the abelian normal subgroup A of the group G, and σ and τ are commuting elements of G, then for all $n \in \mathcal{N}$,

$$[\sigma\beta,\, n(\tau\gamma)] = \beta^{(\tau-1)^n}\gamma^{(\tau-1)^{n-1}(1-\sigma)} .$$

Proof Proceed by induction on n. When $n = 1$,

$$\begin{aligned}[\sigma\beta,\, \tau\gamma] &= \beta^{-1}\sigma^{-1}\gamma^{-1}\tau^{-1}\sigma\beta\tau\gamma \\ &= \beta^{-1}\gamma^{-\sigma}\beta^{\tau}\gamma \\ &= \beta^{(\tau-1)}\gamma^{(1-\sigma)} .\end{aligned}$$

When $n > 1$,

$$\begin{aligned}[\sigma\beta,\, n(\tau\gamma)] &= [\beta^{(\tau-1)^{n-1}}\gamma^{(\tau-1)^{n-2}(1-\sigma)},\, \tau\gamma] \\ &= \gamma^{-(\tau-1)^{n-2}(1-\sigma)} . \beta^{-(\tau-1)^{n-1}}\gamma^{-1} . \beta^{(\tau-1)^{n-1}\tau} . \\ &\qquad \gamma^{(\tau-1)^{n-2}(1-\sigma)\tau} . \gamma \\ &= \beta^{(\tau-1)^n}\gamma^{(\tau-1)^{n-1}(1-\sigma)} ,\end{aligned}$$

and the lemma is proved.

For the most part, only the special case $\sigma = 1$ will be required, and without further loss of generality γ may also be chosen to be trivial:

1.1.2 Corollary

If β is an element of the abelian normal subgroup A of the group G, and $\tau \in G$, then for all $n \in \mathcal{N}$

$$[\beta,\, n\tau] = \beta^{(\tau-1)^n} .$$

1.2.1 Theorem

If $\underline{\underline{V}}$ is a non-trivial variety, R is a proper normal subgroup of the non-cyclic (absolutely) free group F, and $F/\underline{\underline{V}}(R)$ is an Engel group, then F/R is a p-group for some $p \in \mathcal{P}$, and $\underline{\underline{V}}$ is an Engel variety with exponent equal to a power of p.

Proof Clearly $\underline{\underline{V}}$ is an Engel variety, since the non-cyclic free group $R/\underline{\underline{V}}(R)$ is an Engel group.

Let $\eta \in F \setminus R$, and $L = \mathrm{sgp}\{R,\eta\}$. Now $R \trianglelefteq L$ (since $R \trianglelefteq F$), L/R is cyclic, and L and R are both free groups. By Lemma 43.42 of [10] we may, if η has finite order t modulo R, choose a set of generators $\{\alpha,\beta,\ldots\}$ of L such that $\{\beta^t,\alpha,\alpha^\beta,\ldots,\alpha^{\beta^{t-1}}\}$ is part of a set of generators of R. If η has infinite order modulo R, the same procedure gives $\{\alpha^{\beta^i} | i$ an integer$\}$ as part of a set of free generators of R. In each case, let R^* be the subgroup of R generated by the subset of generators shown, and let $L^* = \mathrm{sgp}\{R^*,\beta\}$. It follows from 12.62 of [10] that $\underline{\underline{V}}(R^*) = \underline{\underline{V}}(R)_\cap R^*$. Clearly L^* is a free group of rank two generated by α and β, and $R^* \trianglelefteq L^*$.

The next step is to show that the case in which η, and hence β, has infinite order modulo R^* can not occur. Since $F/\underline{\underline{V}}(R)$ is an Engel group, there must be some $\ell \in \mathcal{N}$ such that $[\alpha,\ell\beta] \in \underline{\underline{V}}(R)$, and since $\alpha \in R^* \trianglelefteq L^*$ and $\beta \in L^*$, this means that $[\alpha,\ell\beta] \in \underline{\underline{V}}(R)_\cap R^* = \underline{\underline{V}}(R^*)$. However, for arbitrary $\ell \in \mathcal{N}$, Corollary 1.1.2 shows that modulo $(\underline{\underline{V}}_\cap\underline{\underline{A}})R^*$,

$$[\alpha,\ell\beta] = \alpha^{(\beta-1)^{\ell}} = \prod_{0\leq i\leq \ell} \alpha^{(-1)^{\ell-i}\binom{\ell}{i}\beta^{i}} .$$

If β has infinite order modulo R^*, the conjugates of α whose powers occur in this product are distinct elements of a set of free generators of R^*, and one of the powers (corresponding to $i = 0$)
r α^{-1}/ is equal to α / and is therefore non-trivial modulo the verbal subgroup $(\underline{\underline{V}}\cap\underline{\underline{A}})(R^*)$. Hence the Engel commutator $[\alpha,\ell\beta]$ is also non-trivial modulo $(\underline{\underline{V}}\cap\underline{\underline{A}})(R^*)$, and a fortiori is not contained in $\underline{\underline{V}}(R^*)$.

This shows that F/R is periodic, and β has finite order, t say, modulo R and also modulo R^*. The theorem will be proved if we show that t and the exponent of $\underline{\underline{V}}$ are powers of the same prime.

If they are not, there exist distinct primes p and q such that $t = uq$ for some $u \in \mathcal{N}$, and $\underline{\underline{A}}_p \subseteq \underline{\underline{V}}$. Now $\underline{\underline{A}}_p(R^*) \supseteq \underline{\underline{V}}(R^*)$, and as before, for some $\ell \in \mathcal{N}$ the Engel commutator $[\alpha,\ell\beta]$ in the free generators of L^* is contained in $\underline{\underline{V}}(R)\cap R^*$ and so in $\underline{\underline{A}}_p(R^*)$. Hence $L^*/\underline{\underline{A}}_p(R^*)$ is an Engel group; but it is finite, of order $t\, p^{t+1}$, and so by the well-known result of Zorn and Zassenhaus (reported without proof in [14]) , is nilpotent. It can easily be checked that α and β^{up} are, modulo $\underline{\underline{A}}_p(R^*)$, elements of orders p and q respectively which do not commute (since α and $\alpha^{\beta^{up}}$ are distinct free generators of R^*). This contradicts the nilpotency of $L^*/\underline{\underline{A}}_p(R^*)$, and hence contradicts the hypothesis that the theorem is false.

1.2.2 Corollary

If $\underline{\underline{V}}$ is a non-trivial variety, R is a proper normal subgroup of the non-cyclic (absolutely) free group F, and $F/\underline{\underline{V}}(R)$ satisfies the ℓ th Engel condition for some $\ell \in \mathcal{N}$, then F/R satisfies the ℓ_oth Engel condition with $\ell_o \leq \ell$, and has finite p-power exponent for some $p \in \mathcal{P}$; and $\underline{\underline{V}}$ is an Engel variety with finite p-power exponent.

Proof It is clear that F/R must satisfy the ℓ_oth Engel condition with $\ell_o \leq \ell$; and from Theorem 1.2.1 it follows that for some $p \in \mathcal{P}$, F/R is a p-group and $\underline{\underline{V}}$ is an Engel variety of p-power exponent. We still need to show that there is an upper bound on the order of elements of F/R; and in fact ℓ is such a bound.

To see this, repeat the working of the proof of Theorem 1.2.1 to show that modulo $(\underline{\underline{V}}\cap\underline{\underline{A}})(R^*)$, for the given integer ℓ,

$$[\alpha, \ell\beta] = \alpha^{(\beta-1)^{\ell}} = \prod_{0\leq i\leq \ell} \alpha^{(-1)^{\ell-i}\binom{\ell}{i}\beta^{i}} .$$

If t is the order of β modulo R, the conjugates $\{\alpha^{\beta^{i}} \mid 0 \leq i \leq t-1\}$ are distinct modulo $(\underline{\underline{V}}\cap\underline{\underline{A}})(R^*)$; so for this final product to be trivial modulo $(\underline{\underline{V}}\cap\underline{\underline{A}})(R^*)$, it is necessary that $t-1 < \ell$, or $t \leq \ell$, as claimed.

1.2.3 Corollary

normal

If $\underline{\underline{V}}$ is a non-trivial variety, R is a proper subgroup of the non-cyclic (absolutely) free group F, and for some $k \in \mathcal{N}$,

$k \geq 2$, all k-generator subgroups of $F/\underline{\underline{V}}(R)$ are nilpotent (nilpotent of class at most c), then F/R is a p-group (a p-group of finite exponent $p^h \leq c$) for some $p \in \mathcal{P}$, whose k-generator subgroups are nilpotent; and $\underline{\underline{V}}$ is a variety of p-power exponent whose k'-generator groups are all nilpotent, where $k' = \max\{k, p^h + 1\}$, if F/R has exponent p^h; and $\underline{\underline{V}}$ is locally nilpotent if F/R does not have finite exponent.

Proof A group whose two-generator (and a fortiori, whose k-generator, where $k \geq 2$) subgroups are nilpotent is necessarily an Engel group, and if there is a bound on the class of two-generator subgroups, the group satisfies an Engel condition. Thus all conclusions except that concerning the k'-generator groups of $\underline{\underline{V}}$ follow from 1.2.1 and 1.2.2. Clearly k-generator groups of $\underline{\underline{V}}$ are nilpotent.

Let α be an element of F with order t modulo R, and let $L = \mathrm{sgp}\{R,\alpha\}$. As in 1.2.1, use 43.42 of [10] to choose a set of free generators of R of the form $\{\eta^t, \beta, \beta^\eta, \ldots, \beta^{\eta^{t-1}}, \ldots\}$ where $\{\beta, \eta, \ldots\}$ is a set of free generators of L, and let $L^* = \mathrm{sgp}\{\beta,\eta\}$ and $R^* = \mathrm{sgp}\{\eta^t, \beta, \beta^\eta, \ldots, \beta^{\eta^{t-1}}\}$. By hypothesis, $L^*.\underline{\underline{V}}(R)/\underline{\underline{V}}(R)$ $(\cong L^*/L^* \cap \underline{\underline{V}}(R))$, being a two-generator subgroup of $F/\underline{\underline{V}}(R)$, is nilpotent. Its subgroup $R^*.\underline{\underline{V}}(R)/\underline{\underline{V}}(R) \cong R^*/\underline{\underline{V}}(R) \cap R^*$ is therefore nilpotent; but from 12.62 of [10] it follows that $\underline{\underline{V}}(R) \cap R^* = \underline{\underline{V}}(R^*)$, so that the free group $R^*/\underline{\underline{V}}(R^*)$ of rank $t + 1$ in the variety $\underline{\underline{V}}$ is nilpotent. The required result now follows.

From Theorem 4.6 in Chapter 4, it will follow that if c is an upper bound for the class of two-generator subgroups of $F/\underline{\underline{V}}(R)$, and p^h is the exponent of F/R, then c/p^h is an upper bound for the class of $R^*/\underline{\underline{V}}(R^*)$, and so of all $p^h + 1$-generator groups of $\underline{\underline{V}}$.

Clearly we also have:

<u>1.2.4</u> <u>Corollary</u>

If $\underline{\underline{V}}$ is a non-trivial variety, R is a proper normal subgroup of the (absolutely) free group F of countably infinite rank, and $F/\underline{\underline{V}}(R)$ is locally nilpotent (boundedly locally nilpotent), then for some $p \in \mathcal{P}$, F/R is a locally nilpotent p-group (a boundedly locally nilpotent group of p-power exponent), and $\underline{\underline{V}}$ is a locally nilpotent variety of p-power exponent.

This result is of interest in that these necessary conditions for $F/\underline{\underline{V}}(R)$ to be locally nilpotent are also sufficient (see 1.4.3 and 1.4.4)

<u>1.2.5</u> <u>Corollary</u>

If $\underline{\underline{V}}$ is a non-trivial variety, R is a proper normal subgroup of the non-cyclic free group F, and $F/\underline{\underline{V}}(R)$ is nilpotent, then F/R is a finite p-group for some $p \in \mathcal{P}$, and $\underline{\underline{V}}$ has p-power exponent. (Clearly also $R/\underline{\underline{V}}(R)$ is nilpotent, so that if F and hence R has infinite rank, then $\underline{\underline{V}}$ is also nilpotent).

Proof Since a nilpotent group satisfies an Engel condition, all the required conclusions except the finiteness of F/R follow from Corollary 1.2.2. However, Šmel'kin has shown (Theorem 4.1 of [12], see 0.2.5 above) that under the given conditions if F/R is infinite then $F/\underline{\underline{V}}(R)$ has trivial centre, and so is not nilpotent. This completes the proof.

Again, the necessary conditions for nilpotency of $F/\underline{\underline{V}}(R)$ are also sufficient, as is shown in 1.4.5, due to Baumslag.

. . .

For the sake of completeness in making comparisons, the results applicable to wreath products corresponding to those of §1.2 for groups of the form $F/\underline{\underline{V}}(R)$ are also stated. Dr. J.Wiegold has informed me that those labelled 1.3.1, 1.3.2, and 1.3.4 have been proved by R.B.J.T. Allenby (M.Sc.Tech. thesis, University of Manchester, 1963); and 1.3.5 is part of a well-known result of Baumslag.

1.3.1 Theorem

If A and B are non-trivial groups and $W = A \text{ wr } B$ is an Engel group, then A and B and hence W are Engel p-groups for some $p \in \mathcal{P}$.

Proof A and B are clearly Engel groups. To show that both are p-groups choose arbitrary elements β from $A(1)$, the first coordinate subgroup of W, and τ from B, the top group, and apply a similar argument to that of 1.2.1 in the subgroup of W generated by these elements.

1.3.2 Corollary

If A and B are non-trivial and $W = A \text{ wr } B$ satisfies the ℓ th Engel condition, then A and B satisfy Engel conditions and have finite p-power exponents for some $p \in \mathcal{P}$.

Proof As before, that A and B satisfy Engel conditions is obvious; that both are p-groups follows from 1.3.1. If, given $\ell \in \mathcal{N}$, there exists an element $\beta(1)$ of $A(1)$ whose order exceeds 2^{ℓ}, then in the expression

$$[\beta(1), \ell\tau] = \prod_{0 \leq i \leq \ell} \beta^{(-1)^{\ell-i}\binom{\ell}{i}}(\tau^{i}) ,$$

it is clear that the power to which each of the conjugates of $\beta(1)$ is raised is non-trivial. Hence A has finite exponent. The proof that B has finite exponent is similar to the proof of the corresponding result for F/R in 1.2.2.

The bound given here for the exponent of A is of course far too high; a much better bound may be obtained as a corollary of Theorem 3.3.

1.3.3 Corollary

If A and B are non-trivial, and for some $k \in \mathcal{N}$, $k \geq 2$, all k-generator subgroups of $W = A \text{ wr } B$ are nilpotent (nilpotent of class at most c) then A and B are both p-groups (groups of p-power exponent) for some $p \in \mathcal{P}$, whose k-generator subgroups are nilpotent.

1.3.4 Corollary

If A and B are non-trivial and $W = A \text{ wr } B$ is locally nilpotent (boundedly locally nilpotent), then A and B are both locally nilpotent p-groups (boundedly locally nilpotent p-groups of finite exponent) for some $p \in \mathcal{P}$.

1.3.5 Corollary (BAUMSLAG)

If A and B are non-trivial, and $W = A \text{ wr } B$ is nilpotent, then for some $p \in \mathcal{P}$ A is a nilpotent group of finite p-power exponent and B is a finite p-group.

This was proved by Baumslag in §3 of [2]; alternatively, it follows from 1.3.2 above and Corollary 3.2 of [2].

Again the necessary conditions of 1.3.4 and 1.3.5 are shown to be sufficient in 1.4.3, 1.4.4 and 1.4.5.

1.4.1 Theorem

An extension of a locally nilpotent p-group, for some $p \in \mathcal{P}$, by an Engel p-group is an Engel (p-)group.

Proof Let H be a locally nilpotent p-group which is a normal subgroup of the group G, such that G/H is an Engel p-group. Let α, β be arbitrary elements of G. Since G/H is an Engel group, there is a positive integer ℓ_o such that $\gamma = [\alpha, {}_{\ell_o}\beta] \in H$.

Let $L = \mathrm{sgp}\{\gamma,\beta\}$ and let H^* be the normal closure of γ in L. Since $H_\cap L \trianglelefteq L$, it follows that $H^* \leq H_\cap L$, and so H^* is a locally nilpotent p-group. Since β has finite p-power order, q say, modulo H^*, and H^* is generated by the set $\{\gamma^{\beta^i} \mid 0 \leq i \leq q-1\} \cup \{\beta^q\}$ which is finite, H^* is nilpotent and therefore finite.

Now L, being an extension of H^* by a q-cycle is also a finite p-group, and therefore nilpotent. Hence $[\gamma, \ell_1\beta] = 1$ for some $\ell_1 \in \mathcal{N}$, and $[\alpha, \ell\beta] = 1$ where $\ell = \ell_o + \ell_1$. Thus G is an Engel group, as claimed.

<u>1.4.2</u> <u>Corollary</u>

A group satisfies an Engel condition if it is an extension of a boundedly locally nilpotent group of p-power exponent for some $p \in \mathcal{P}$ by a group also of p-power exponent satisfying an Engel condition.

<u>Proof</u> Let H be a boundedly locally nilpotent group of exponent p^k which is normal in the group G, such that G/H satisfies the ℓ_0th Engel condition and has exponent p^h. Let $\underline{V}$ be the variety generated by H and $\underline{W}$ the variety generated by G/H. Then $\underline{V}$ is a locally nilpotent variety of exponent p^k, and $\underline{W}$ is an Engel variety of exponent p^h. From 1.4.1, every group in the product variety $\underline{\underline{VW}}$ is an Engel group, and hence, by the remarks made in the introduction to this chapter, every group in $\underline{\underline{VW}}$, and in particular G, satisfies an Engel condition.

A bound on the Engel length of groups satisfying the conditions of this corollary is given in 3.3.2.

The next two results are conveniently stated in terms of the idea of product of properties of a group, described in §0.1.

<u>1.4.3</u> <u>Theorem</u>

The property of being a locally nilpotent p-group for fixed $p \in \mathcal{P}$ is idempotent.

<u>Proof</u> Let $H \trianglelefteq G$ be such that H and G/H are locally nilpotent p-groups. If G^* is a finitely generated subgroup of G, then $G^*/H \cap G^* \cong G^*H/H \leq G/H$ is nilpotent and finite. Then $H \cap G^*$ has finite index in the finitely-generated group G^*, so is also finitely generated, therefore nilpotent, and hence finite. This means that G^* is a finite p-group and is therefore nilpotent, and the result follows.

<u>1.4.4</u> <u>Corollary</u>

The property of being a boundedly locally nilpotent group of p-power exponent, for fixed $p \in \mathcal{P}$, is idempotent.

<u>Proof</u> This follows from 1.4.3 in the same way that 1.4.2 follows from 1.4.1.

<u>1.4.5</u> <u>Theorem</u> (BAUMSLAG, [2], Lemma 3.8)

An extension of a nilpotent group of p-power exponent, for some $p \in \mathcal{P}$, by a finite p-group is nilpotent.

This was proved by Baumslag. It also follows from Theorem 4.6 of the present thesis, where an upper bound on the class of such groups is obtained.

1.5 Examples

To illustrate the difference between the corresponding theorems relating to bounded and unbounded properties, consider the groups (i) $F/\underline{\underline{V}}(R)$ where $F/R \cong Z_{p^\infty}$ and $\underline{\underline{V}} = \underline{\underline{A}}_p$; and (ii) $C_p \text{ wr } Z_{p^\infty}$; for arbitrary $p \in \mathcal{P}$. Each is an extension of an abelian group of exponent p by an abelian p-group. Both groups are locally nilpotent, and hence Engel; but they do not satisfy any Engel condition, and so also there is no bound on the class of two-generator subgroups.

1.6.1 Theorem

The product $\underline{\underline{VW}}$ of the non-trivial varieties $\underline{\underline{V}}$ and $\underline{\underline{W}}$ is locally nilpotent if and only if both $\underline{\underline{V}}$ and $\underline{\underline{W}}$ are locally nilpotent varieties with finite exponents equal to powers of one prime, p.

Proof Since $F/\underline{\underline{V}}(\underline{\underline{W}}(F))$ is relatively free with the same rank as F in the variety $\underline{\underline{VW}}$ (e.g., by 21.12 of [10]), the "if" part follows from 1.4.3. The "only if" part of the theorem follows from 1.2.4, but is more easily proved directly by noting that if $\underline{\underline{V}}$ and $\underline{\underline{W}}$ do not both have p-power exponent, there exist distinct primes q and q' such that $C_q \in \underline{\underline{V}}$, $C_{q'} \in \underline{\underline{W}}$, and hence the non-nilpotent group $C_q \text{ wr } C_{q'} \in \underline{\underline{VW}}$.

1.6.2 Theorem

For the product $\underline{\underline{VW}}$ of the non-trivial varieties $\underline{\underline{V}}$ and $\underline{\underline{W}}$ to be an Engel variety, it is necessary that $\underline{\underline{V}}$ and $\underline{\underline{W}}$ be Engel varieties whose exponents are both powers of one prime, p; and it is sufficient that both have p-power exponent, $\underline{\underline{V}}$ be locally nilpotent, and $\underline{\underline{W}}$ be an Engel variety.

The proof parallels that of 1.6.1, following from 1.2.2 and 1.4.2.

The results of this chapter raise or leave unanswered several interesting questions. Firstly, is it true that every Engel variety of prime power exponent is locally nilpotent? This is a restriction of the well-known unsolved problem whether every Engel variety is locally nilpotent. A footnote in [4], and a similar independent result of M.F. Newman (unpublished) show the existence of finitely-generated infinite Engel p-groups. These, however, neither satisfy an Engel condition nor have finite exponent. If the answer to this first question is in the affirmative, then the necessary and sufficient conditions of Theorem 1.6.2 are equivalent; and 1.4.1 and 1.4.2 show that the necessary conditions of 1.2.1, 1.2.2, and 1.3.2 are also sufficient.

Secondly, if H is an Engel p-group and G/H is (to take the simplest case) a p-cycle, does it follow that G is an Engel group? Even more restricted forms of this question, where H is made to satisfy an Engel condition or to have prime-power exponent, appear very difficult; though an affirmative answer to the first question above would solve one case at least.

Thirdly, does there exist an Engel group of finite (prime-power) exponent which does not satisfy an Engel condition? This question is raised by the observation that every extension G, of a boundedly locally nilpotent p-group H by a boundedly Engel p-group G/H is boundedly Engel unless it fails to have finite exponent; and that among the examples of unboundedly Engel groups considered, not one has had finite exponent.

Chapter 2

Arithmetical preliminaries

The results of this section are included in order to obtain Theorem 2.8, which is a useful - in fact a basic - tool in obtaining the bounds of Chapters 3 and 4. Essentially, Theorem 2.8 combines 2.4, due to Liebeck, with 2.7, used by Bachmuth and Hughes. Apart from 2.8 the only result used later is Lemma 2.1, which is in any case well-known.

In this section, we write $p^a \| n$ if p^a is the highest power of p dividing n for some $p \in \mathcal{P}$, $n \in \mathcal{N}$.

2.1 Lemma

For arbitrary $p \in \mathcal{P}$ and $h \in \mathcal{N}$, and for r and s such that $0 < r \le p^h$ and $0 \le s \le h$,

$$p^s \| r \Rightarrow p^{h-s} \| \binom{p}{r}$$

Proof For any integer n,

$$p^a \| n! \quad \text{where} \quad a = \sum_{1 \le i < \infty} [n/p^i] ;$$

the sum actually contains only k terms where $p^k \le n < p^{k+1}$. Thus

$$p^b \| \binom{n}{r} \quad \text{where} \quad b = \sum_{1 \le i \le \infty} \{[n/p^i] - [r/p^i] - [(n-r)/p^i]\} .$$

In the present case, $n = p^h$, $r = p^s t$ with h.c.f. $\{t, p\} = 1$. Now a term of the form $\{[(k+\ell)/m] - [k/m] - [\ell/m]\}$ is zero whenever $m | k$ and $m | \ell$. Hence the first s terms are zero. If further terms occur, that is, if $h > s$, each of the $h-s$ remaining terms is of the form $\{[(k+\ell)/m] - [k/m] - [\ell/m]\}$ where $k+\ell$ is divisible by m, but k and ℓ are not; and each such term is equal to 1.

Thus $b = h-s$, as claimed.

2.2 Lemma

For any $p \in \mathcal{P}$ and integers h and r satisfying $h \geq 2$ and $0 \leq r \leq p$,

$$\binom{p^h}{rp^{h-1}} \equiv \binom{p^{h-1}}{rp^{h-2}} \quad \text{modulo } p^h.$$

Proof $$\binom{p^h}{rp^{h-1}} = \prod_{1\leq i\leq rp^{h-1}} (p^h-i+1) / \prod_{1\leq i\leq rp^{h-1}} (i)$$

$$= \binom{p^{h-1}}{rp^{h-2}} \,.\, a/b$$

where, if we set $\mathcal{H} = \{i \mid 0 \leq i \leq rp^{h-1},\ p \nmid i\}$, $a = \prod_{i\in\mathcal{H}}(p^h-i)$ and $b = \prod_{i\in\mathcal{H}} i$, and the remaining terms in the two products give the binomial coefficient $\binom{p^{h-1}}{rp^{h-2}}$.

Note that for each $i \in \mathcal{H}$

$$p^h - i \equiv -i \pmod{p^h}$$

and hence $a \equiv (-1)^{r(p-1)p^{h-2}} b \pmod{p^h}$

$$\equiv b \pmod{p^h},$$

except in the single case $p = 2, h = 2, r = 1$. In this case the lemma may easily be verified directly. In all other cases, we now have $b\binom{p^h}{rp^{h-1}} = a\binom{p^{h-1}}{rp^{h-2}}$, therefore

$b\binom{p^h}{rp^{h-1}} \equiv b\binom{p^{h-1}}{rp^{h-2}} \mod p^h$, and so $\binom{p^h}{rp^{h-1}} \equiv \binom{p^{h-1}}{rp^{h-2}} \mod p^h$,

since b is coprime with p^h.

. . .

2.3.1 Definition

For arbitrary $u, \ell \in \mathcal{N}$ and r such that $0 \leq r \leq u-1$,

$$S(u,\ell,r) = \sum_{0\leq i\leq[\ell/u]} (-1)^{ui+r} \binom{\ell}{ui+r} .$$

This definition we extend to all integers r by adopting the convention that the third argument is to be taken modulo the first; that is, if $r = au+b$, $0 \leq b \leq u-1$, then $S(u,\ell,r) = S(u,\ell,b)$.

2.3.2 Definition

For arbitrary $u,\ell \in \mathcal{N}$,

$$F(u,\ell) = \text{h.c.f. } \{S(u,\ell,r) \mid 0 \leq r \leq u-1\} .$$

2.3.3 Lemma

If $a \in \mathcal{N}$, then:

$$S(u,\ell+a,r) = \sum_{0\leq i\leq a} (-1)^i \binom{a}{i} S(u,\ell,r-i).$$

Proof

$$S(u,\ell+a,r) = \sum_{0\leq j\leq[(\ell+a)/u]} (-1)^{ju+r} \binom{\ell+a}{ju+r}$$

$$= \sum_{0\leq j\leq[(\ell+a)/u]} (-1)^{ju+r} \sum_{0\leq i\leq a} \binom{a}{i}\binom{\ell}{ju+r-i}$$

(where we set $\binom{\ell}{b} = 0$ if $b < 0$ or $b > \ell$)

$$= \sum_{0 \le i \le a} (-1)^i \binom{a}{i} \sum_{0 \le j \le [(\ell+a)/u]} (-1)^{ju+r-i} \binom{\ell}{ju+r-i}$$

$$= \sum_{0 \le i \le a} (-1)^i \binom{a}{i} S(u,\ell,r-i) .$$

2.4 Lemma (LIEBECK, [9], Theorem 4.3)

If $t = p^h + (s-1)(p^h - p^{h-1})$

then (i) $p^s \mid S(p^h,\ell,r)$ for $0 \le r \le p^h-1$, $\ell \ge t$

(ii) $p^s \nmid S(p^h,t-1,r)$ for $0 \le r \le p^h-1$.

The proof is rather involved, and is omitted. A fairly detailed discussion is given in [9].

2.5 Corollary

If $\ell \in \mathcal{N}$ satisfies

$$p^h + (s-1)(p^h - p^{h-1}) \le \ell < p^h + s(p^h - p^{h-1})$$

then $p^s \parallel F(p^h,\ell)$.

Proof The fact that $p^s \mid S(p^h,\ell,r)$ for all r, $0 \le r \le p^{h-1}$, and hence that $p^s \mid F(p^h,\ell)$ follows immediately from Lemma 2.4(i). If $p^{s+1} \mid F(p^h,\ell)$, it would follow by Lemma 2.3 that $p^{s+1} \mid S(p^h,p^h+s(p^h - p^{h-1}) - 1, r)$, which contradicts Lemma 2.4 (ii).

2.6 Lemma

If $u,v,\ell \in \mathcal{N}$, $u \mid v$, then $F(v,\ell) \mid F(u,\ell)$.

<u>Proof</u> Let $v = au$. From the definitions, $F(v,\ell) \mid S(v,\ell,r)$ for all r, $0 \leq r \leq v-1$. Hence $F(v,\ell) \mid \sum_{0\leq i\leq a-1} (-1)^{iu} S(v,\ell,r+iu)$ for all r, $0 \leq r \leq u-1$, that is, $F(v,\ell) \mid S(u,\ell,r)$ for all r, $0 \leq r \leq u-1$. But this means that $F(v,\ell) \mid F(u,\ell)$.

<u>2.7</u> <u>Lemma</u> (BACHMUTH and HUGHES, [1])

If $u = p^h$, $p,q \in \mathcal{P}$, and if there is $\ell \in \mathcal{N}$ such that $q \mid F(u,\ell)$, then $q = p$.

<u>Proof</u> Let ε be a p th root of unity; then

$(1-\varepsilon)^\ell = \sum_{0\leq r\leq p-1} S(p,\ell,r)\varepsilon^r$. Also on substituting $x = 1$ in the relation $\sum_{0\leq i\leq p-1} x^i = \prod_{1\leq i\leq p-1}(x-\varepsilon^i)$, we obtain $\prod_{1\leq i\leq p-1}(1-\varepsilon^i) = p$.

$$
\begin{aligned}
\text{Now } q \mid F(u,\ell) &\Rightarrow q \mid F(p,\ell) \quad \text{(Lemma 2.6)} \\
&\Rightarrow q \mid S(p,\ell,r) \quad \text{for all } r,\ 0 \leq r \leq p-1 \\
&\Rightarrow q \mid (1-\varepsilon)^\ell \\
&\Rightarrow q \mid p^\ell \\
&\Rightarrow q = p, \quad \text{as required.}
\end{aligned}
$$

<u>2.8</u> <u>Theorem</u>

$$
F(u,\ell) = \begin{cases} p^k \quad \text{where } k = [(\ell - p^{h-1})/(p^h - p^{h-1})] & \text{if } u = p^h \\ 1, \quad \text{if } u \text{ is divisible by two distinct primes.} \end{cases}
$$

<u>Proof</u> The first part, the case in which u is a prime power, follows immediately from Corollary 2.5 and Lemma 2.7. Now suppose

that p and q are distinct primes, both dividing u. By Lemma 2.6, $F(u,\ell) \mid F(p,\ell)$ and $F(u,\ell) \mid F(q,\ell)$. Lemma 2.7 shows that $F(p,\ell)$ and $F(q,\ell)$ are coprime, and so $F(u,\ell) = 1$, as required.

Chapter 3

Upper bounds on the Engel length of certain group extensions

The main result of this chapter is the bound presented in Theorem 3.3; the crux of the proof is in Lemma 3.2, for which the definitions and Lemmas of §3.1 provide useful tools. Following 3.3 some applications to slightly more general situations are made; and then in 3.4 the result is adapted to give a slightly improved bound for the special case of a cyclic extension. The results of §3.5 show that the results obtained are best possible for small nilpotency class.

Throughout section 3.1, p is a fixed but arbitrary prime.

3.1.1 Definition

For arbitrary $t \in \mathcal{N}$, an element α is a t-element of a group H if and only if there exists an element κ which can be expressed as a commutator of weight w in H such that $\alpha = \kappa^{p^s}$ and $w + s \geq t$.

The weight of the t-element expressed in this way is defined to be w, i.e., the weight of the corresponding commutator κ. Because of the possibility of a variety of expressions for a single element, "weight" of a t-element is not in general uniquely defined; what concerns us is whether a group element can be expressed as a t-element of a particular weight.

3.1.2 Lemma

If H is a normal subgroup of a group G, and α is a t-element of weight w in H, then every commutator in G which has α as an entry is a product of t-elements of weight w in H.

Proof For arbitrary $\gamma \in G$, $[\alpha,\gamma] = \alpha^{-1}.\alpha^{\gamma}$ and $[\gamma,\alpha] = \alpha^{-\gamma}.\alpha$. Clearly, by induction on the number of its entries, the given commutator in G may be expressed as a product of conjugates in G of α and α^{-1}, each of which is a t-element of weight w in H.

The following lemma is easily proved by induction on n; it is well-known in metabelian groups where each μ_j or ν_j is trivial.

3.1.3 Lemma

If ξ and η are arbitrary elements of a group H, then

$$[\xi^n,\eta] = \prod_{1\leq i\leq n} [\xi,\eta,(i-1)\xi]^{\binom{n}{i}} \cdot \prod_j \mu_j$$

$$[\xi,\eta^n] = \prod_{1\leq i\leq n} [\xi,i\eta]^{\binom{n}{i}} \cdot \prod_j \nu_j$$

where each μ_j may be expressed as a commutator with at least two entries, each of which is a commutator of the form $[\xi,\eta,(i-1)\xi]$ with $1 \leq i \leq n$; and each ν_j may be expressed as a commutator with at least two entries, each of the form $[\xi,i\eta]$ with $1 \leq i \leq n$.

In both cases, if ν_j or μ_j is non-trivial, it cannot have $i = 1$ for each of its entries; so each μ_j may be expressed (by re-writing, if necessary) as a commutator with $[\xi,\eta,\xi]$ as one entry, and each ν_j with $[\xi,\eta,\eta]$ as one entry.

3.1.4 Lemma

If α and β are respectively t- and u-elements of weights w and x in a group H which is nilpotent of class c for some $c \in \mathcal{N}$, then the commutator $[\alpha,\beta]$ is a product of $(t+u)$-elements of weights at least $w+x$ in H. The result is independent of c.

<u>Proof</u> By definition, $\alpha = \kappa^{p^r}$ and $\beta = \lambda^{p^s}$ where κ and λ are commutators of weights w and x respectively in H, $r,s \in \{0\} \cup \mathcal{N}$, $w, x \in \mathcal{N}$, $w+r \geq t$, and $x+s \geq u$. The proof will proceed by induction on $(r+s)$ within the general stage of a reverse induction on $(w+x)$ to show that $[\alpha,\beta]$ is a product of $(w+x+r+s)$-elements of H, each having weight at least $w+x$. The lemma will then follow.

If $w+x > c$, then, since $\alpha \in \underline{\underline{N}}_{w-1}(H)$ and $\beta \in \underline{\underline{N}}_{x-1}(H)$, it follows that $[\alpha,\beta] \in \underline{\underline{N}}_c(H) = \{1\}$, and the lemma is trivially true.

Suppose $w+x \leq c$, and the hypothesis proved for all pairs of powers of commutators such that the sum of the weights of the commutators is greater than $w+x$. When $r = s = 0$, the commutator $[\alpha,\beta] = [\kappa^{p^r},\lambda^{p^s}]$ is simply $[\kappa,\lambda]$ which is by definition a commutator of weight $w+x$, and hence a $(w+x)$-element of weight $w+x$ in H, as required. When $(r+s) > 0$, since the inverse of a t-element in H is also a t-element in H, with the same weight, suppose without loss of generality that $r > 0$. Let $\eta = \kappa^{p^{r-1}}$ so that $\alpha = \eta^p$. Then, by Lemma 3.1.3,

$$[\alpha,\beta] = [\eta^p,\beta]$$

$$= \prod_{1\leq i\leq p} [\eta,\beta(i-1)\eta]^{\binom{p}{i}} \cdot \prod_{k\in\Delta} \mu_k ,$$

where each μ_k, and also each commutator in the first product except that in the term corresponding to $i = 0$, may be expressed with $[\eta,\beta,\eta]$ as one of its entries.

Consider now the commutator $[\eta,\beta,\eta]$. The inductive hypothesis on $r+s$ shows that

$$[\eta,\beta] = [\kappa^{p^{r-1}}, \lambda^{p^{s}}] = \prod_{j\in\Gamma} \nu_j$$

where each ν_j is a $(w+x+r+s-1)$- element of weight at least $(w+x)$ in H. By repeated application of the Hall identities, $[\prod_{j\in\Gamma} \nu_j, \eta]$ is a product of commutators each containing an entry of the form $[\nu_j, \eta]$ for some $j \in \Gamma$. From the reverse-induction hypothesis on $w+x$, this entry is a product of $(2w+x+2r+s-2)$- elements of H, each of weight at least $2w+x$; and since $r \geq 1$ and $w \geq 1$, this is a fortiori a product of $(w+x+r+s)$- elements of H, each of weight at least $w+x$. By Lemma 3.1.2, each factor in the expansion of $[\prod_{j\in\Gamma} \nu_j, \eta]$ is a product of $(w+x+r+s)$- elements of H, each of weight at least $w+x$; and hence, again by 3.1.2, so is each commutator in the expression for $[\alpha,\eta]$ which has $[\eta,\beta,\eta]$ as an entry.

Only the term corresponding to $i = 1$, that is, $[\eta,\beta]^p$, in the expression for $[\alpha,\beta]$ remains to be considered. As before, $[\eta,\beta] = \prod_{j\in\Gamma} \nu_j$ where each ν_j is a $(w+x+r+s-1)$- element of weight at least $w+x$ in H. Now

$$[\eta,\beta]^p = (\prod_{j\in\Gamma} \nu_j)^p = \prod_{j\in\Gamma} \nu_j^{\,p} . \prod_{\ell\in\Delta} \rho_\ell \quad ,$$

where for each $\ell \in \Delta$, ρ_ℓ is a commutator with at least two entries, each from the set $\{\nu_j \mid j \in \Gamma\}$. By the hypothesis on $w+x$ and Lemma 3.1.2, each ρ_ℓ is a product of $2(w+x+r+s-1)$- elements of weights at least $2(w+x)$ in H, so a fortiori is of the required form. Clearly

$\nu_j^{\,p}$ is a $(w+x+r+s)$- element of weight $w+x$ in H, so also of the required form.

This establishes the truth of the inductive hypothesis, and hence that of the lemma.

Though they are not immediately required, the following corollaries will be useful in chapter 4 :

<u>3.1.5</u> <u>Corollary of the proof</u>

The p-th power of a product of t-elements of weight w in H is a product of $(t+1)$-elements of weight w in H.

This was proved in the last stage of the proof of 3.1.4, when $(\prod_{j\in\Gamma} \nu_j)^p$ was considered.

<u>3.1.6</u> <u>Corollary</u>

The commutator of a product of t-elements of weight at least w in H with a product of u-elements of weight at least x in H is a product of $(t+u)$-elements of weight at least $w+x$ in H.

<u>Proof</u> If α_i is a t-element of weight at least w in H for each $i \in \Gamma$, and β_j is a u-element of weight at least x in H for each $j \in \Delta$ (where Γ and Δ are both finite sets) then from the Hall identities

$$[\prod_{i\in\Gamma} \alpha_i, \prod_{j\in\Delta} \beta_j] = \prod_{k\in\Theta} \gamma_k$$

where each γ_k contains an entry of the form $[\alpha_i, \beta_j]$ with $i \in \Gamma$, $j \in \Delta$. The result now follows from 3.1.4 and 3.1.2.

<u>3.2</u> <u>Lemma</u>

If β is an element of a normal subgroup H of a group G, and if an element τ of G has order p^h modulo H for some $p \in \mathcal{P}$ and $h \in \mathcal{N}$ then

$$[\beta, \ell\tau] = \prod_{1 \leq i \leq y} \theta_i^{\,d(i)} . \eta$$

where $\eta \in \underline{\underline{N}}_{r_0}$ for arbitrary $r_o \in \mathcal{N}$, the element θ_i may be expressed as a commutator of weight w_i in H, $1 \leq w_i \leq r_o$, for $1 \leq i \leq y$, and $d(i) = p^{v(i)}$ where $v(i) \geq 0$ and $v_i \geq 1 + [(\ell - w_i p^h)/(p^h - p^{h-1})]$.

<u>Proof</u> For brevity, let $a = p^h$ and $b = p^h - p^{h-1}$. Since $p^s | S(a,\ell,i)$ for $0 \leq i \leq a-1$ if $s = \max\{0, 1 + [(\ell - a)/b]\}$, the lemma will follow when it is proved by induction on ℓ that, with the same hypotheses,

$$[\beta, \ell\tau] = \prod_r \Big(\prod_{0 \leq j \leq a-1} \mu_r^{\,v(r,\ell,j) q(r) \tau^j} \Big) . \eta$$

where $\eta \in \underline{\underline{N}}_{r_0}(H)$, μ_r is a commutator of weight w_r in H, $1 \leq w_r \leq r_o$, $q(r) = p^{u_r}$ for some $u_r \in \{0\} \cup \mathcal{N}$, and

$$v(r,\ell,j) = \begin{cases} (-1)^{\ell} S(a, \ell - (w_r - 1)a - u_r b, j) & \\ \qquad \text{if } \ell > (w_r - 1)a + u_r b & \text{(form (A))} \\ \left.\begin{array}{ll} 1 & \text{if } j = 0 \\ 0 & \text{if } j \neq 0 \end{array}\right\} \text{if } \ell \leq (w_r - 1)a + u_r b & \\ & \text{(form (B))}. \end{cases}$$

(Note that the third argument of v can be any integer and the value of v depends only on the residue modulo a of this third argument.)

When $\ell = 1$,

$$[\beta,\tau] = \beta^{-1}\beta^{\tau} = \beta^{-S(a,1,0)}.\beta^{-S(a,1,1)\tau},$$

which is of form (A) with $\mu_1 = \beta$, $w_1 = 1$, $u_1 = 0$ (since for arbitrary prime-power a, the definition of $S(a,1,j)$ with $2 \leq j \leq a-1$ gives simply $\binom{1}{j}$, which is interpreted as being zero).

When $\ell > 1$, suppose the result proved for $\ell-1$, expand $[\beta,\ell\tau] = [\beta,(\ell-1)\tau]^{-1}[\beta,(\ell-1)\tau]^{\tau}$ using the result for $[\beta,(\ell-1)\tau]$, and collect conjugates of each commutator μ_r. Resulting terms either

(i) are in collections of the form

$$\prod_{0\leq j\leq a-1} \mu_r^{q(r)(v(r,\ell-1,j-1) - v(r,\ell-1,j))\tau^j} . \mu_r^{-q(r)v(r,\ell-1,a-1)} .$$
$$\mu_r^{q(r)v(r,\ell-1,a-1)\tau^a}$$

$$= \prod_{0\leq j\leq a-1} \mu_r^{q(r)v(r,\ell,j)\tau^j} . [\mu_r^{q(r)v(r,\ell-1,a-1)},\tau^a]$$

with $\ell > (w_r-1)a + u_r b$ (These expressions follow from the definition 2.3.1 and the case $a = 1$ of Lemma 2.3.3. The case in which $\ell-1 = (w_r-1)a + u_r b$ is simple, but requires separate checking; μ_r may be either one of the commutators μ_r in the expression for $[\beta,(\ell-1)\tau]$ or the inverse of such a commutator.); or

(ii) are of the form $\mu_r^{q(r)}$ with $\ell \leq (w_r-1)a + u_r b$ (in this case μ_r is either the inverse or the τ-conjugate of one of the commutators μ_r in the expression for $[\beta,(\ell-1)\tau]$); or

(iii) are commutators, each of which has as an entry a commutator of the form

$$[\mu_r^{\,q(r)v(r,\ell-1,i)\tau^i}, \mu_s^{\,q(s)v(r,\ell-1,j)\tau^j}]$$

whose entries are from the expansion for $[\beta,(\ell-1)\tau]$.

At this stage, note that if $d_r = \max\{0, 1+[(\ell-1-w_r a)/b]\}$, then each term of the form $\mu_r^{q(r)v(r,\ell-1,j)}$ is a (d_r+w_r)-element of weight w_r in H. Note also that if α, say, is a (d_r+w_r+1)-element of weight at least w_r+1 in H, then α can be regarded as having the form (B) required by the hypothesis, since $\alpha = \kappa^{p^s}$ where κ is a commutator of weight $w \geq w_r+1$ in H and $w+s \geq d_r+w_r+1$; and hence

$$\begin{aligned}(w-1)a+sb &= w_r a + (w-w_r-1)(a-b) + (w-w_r+s-1)\\ &\geq w_r a + d_r b\\ &> \ell-1 \quad \text{(from the definition of } d_r).\end{aligned}$$

Hence $(w-1)a+sb \geq \ell$, as required.

Return now to the expansion of $[\beta,\ell\tau]$. For terms of type (i), the first part of the product is clearly of the form (A) required by the hypothesis. The remaining factor, $[\mu_r^{q(r)v(r,\ell-1,a-1)},\tau^a]$ is the commutator of a (d_r+w_r)- element of weight w_r with a 1-element of weight 1 in H, hence by Lemma 3.1.4 is a product of (d_r+w_r+1)-elements of weights at least w_r+1 in H, and hence by the preceding paragraph is a product of terms of the form (B) required by the hypothesis.

Terms of type (ii) are clearly of the form (B). Terms of type (iii) are, by Lemmas 3.1.4 and 3.1.2, products of $(d_r+d_s+w_r+w_s)$- elements of weights at least (w_r+w_s) in H and these, since $d_s \geq 0$ and $w_s \geq 1$, are (d_r+w_r+1)- elements of H of weights at least $w_r + 1$, and so are of form (B).

3.3 Theorem

If H is a normal subgroup of a group G such that G/H satisfies the ℓ_o th Engel condition and has exponent p^h for some $p \in \mathcal{P}$ and $h \in \mathcal{N}$, H is nilpotent of class r_o, and for $1 \leq r \leq r_o$ every element which can be expressed as a commutator of weight r in H has order dividing p^{k_r} for some $k_r \in \mathcal{N}$, then G satisfies the ℓ th Engel condition where

$$\ell = \ell_o + \max_{1\leq r\leq r_o} \{rp^h + (k_r-1)(p^h - p^{h-1})\}$$

Proof Let α and τ be arbitrary elements of G. Then $\beta = [\alpha, \ell_o\tau] \in H$, since G/H satisfies the ℓ_o th Engel condition.

Let $\ell_1 = \max_{1\leq r\leq r_o} \{rp^h + (k_r-1)(p^h - p^{h-1})\}$ so that

$$k_r \leq 1 + (\ell_1 - rp^h)/(p^h - p^{h-1}) \quad \text{for } 1 \leq r \leq r_o ,$$

and, since k_r is an integer,

$$k_r \leq 1 + [(\ell_1 - rp^h)/(p^h - p^{h-1})] = v_r , \quad \text{say.}$$

Since τ has order dividing p^h and $\ell_1 \geq r_op^h$, Lemma 3.2 shows that $[\beta, \ell_1\tau]$ is a product of commutators each raised to a power which is a multiple of its order. Thus $[\alpha, (\ell_o + \ell_1)\tau] = [\beta, \ell_1\tau] = 1$, and so G satisfies the ℓ th Engel condition where $\ell = \ell_o + \ell_1$, as required.

A simpler, though slightly cruder, bound may be obtained as an immediate consequence of 3.3.

3.3.1 Corollary

If H is a normal subgroup of the group G, with exponent p^k and nilpotency class c, and G/H satisfies the ℓ_o th Engel condition and has exponent p^h, then G satisfies the ℓ th Engel condition where $\ell = \ell_o + cp^h + (k-1)(p^h - p^{h-1})$.

Corollary 3.3.1 may be applied in the more general situation of 1.4.2:

3.3.2 Corollary

If H is a normal subgroup of G with exponent p^k, such that for all $d \in \mathcal{N}$, every d-generator subgroup of H is nilpotent of class $c(d)$ for some function $c : \mathcal{N} \to \mathcal{N}$, and if G/H satisfies the ℓ_o th Engel condition and has exponent p^h, then G satisfies the ℓ th Engel condition where $\ell = \ell_o + c(p^h + 1).p^h + (k-1)(p^h - p^{h-1})$.

Proof The proof proceeds as for Theorem 1.4.1. Since H^* has index dividing p^h in the two-generator group L, it follows that H^* is $p^h + 1$-generator, and hence nilpotent of class at most $c(p^h + 1)$. The result follows on applying 3.2 to the group L.

In the special case where F/R is cyclic, the preceding results may be improved:

3.4 Corollary of the proofs of 3.2 and 3.3.

If G/H is cyclic of order p^h for some $p \in \mathcal{P}$ and $h \in \mathcal{N}$, and H is nilpotent of class r_o and such that for $1 \leq r \leq r_o$ every element which can be expressed as a commutator of weight r in H has order dividing p^{k_r} for some $k_r \in \mathcal{N}$, then G satisfies the m th Engel condition, where

$$m = \max_{1 \leq r \leq r_o} \{rp^h + (k_r - 1)(p^h - p^{h-1})\} .$$

Proof Let ξ and τ be arbitrary elements of G. If the order of τ modulo H is less than p^h, then 3.2 and the proof of 3.3 already show that there is an integer $n < m$ such that $[\xi, n\tau] = 1$. Otherwise, τH generates the cyclic group G/H, and so $\xi = \tau^z \beta$ with $0 \leq z \leq p^h - 1$ and $\beta \in H$. Now

$$[\xi, \tau] = [\tau^z \beta, \tau] = [\tau^z, \tau]^\beta [\beta, \tau] = [\beta, \tau] .$$

Hence for all $n \in \mathcal{N}$, $[\xi, n\tau] = [\beta, n\tau]$, and the required result follows from 3.2 and the proof of 3.3.

Alternatively, this result may be obtained as an immediate consequence of 3.3 and 4.6. In fact this is analogous to the way in which Liebeck ([9], Theorem 6.2) obtains the corresponding result for the Engel length of $A \text{ wr } B$ when A is abelian and B is cyclic. The preceding proof has been included because it is independent of the involved arguments early in Chapter 4.

A group G satisfying the conditions of Theorem 3.3 or Corollary 3.4 may of course satisfy an Engel condition for a much smaller integer than that given by the corresponding result. The simplest and most extreme example is the case in which H is a direct factor of G. Nevertheless, the results even of Corollary 3.3.1 are best possible when H has small nilpotency class, in the sense that for arbitrary $p \in \mathcal{P}$ and $h, k \in \mathcal{N}$, and r_o such that $1 \leq r_o \leq p-1$, there is a group satisfying the conditions of 3.3 (3.4) with $k_r = k$ for $1 \leq r \leq r_o$, but not satisfying the $\ell-1$ th ($m-1$ th) Engel condition, respectively. Example 3.5.1 following is for $\ell_o = 1$ in Theorem 3.3; the same method should serve to construct examples for arbitrary $\ell_o \in \mathcal{N}$.

The proofs of 3.5.1 and 3.5.2 follow Lemma 3.5.3, on which they depend.

<u>3.5.1</u> <u>Example</u>

Given $p \in \mathcal{P}$ and $h,k \in \mathcal{N}$, and an integer c such that $1 \leq c \leq p-1$, let F be the absolutely free group of rank two generated by α and β, and R the normal subgroup of F generated by α^{p^h}, β^{p^h}, and $[\alpha,\beta]$, so that $F/R \cong C_{p^h} \times C_{p^h}$. Let $\underline{\underline{V}} = \underline{\underline{N}}_c \cap \underline{\underline{B}}_{p^k}$. Now the group $F/\underline{\underline{V}}(R)$ satisfies the conditions of 3.3 and 3.3.1, and contains a non-trivial Engel commutator $[\alpha,(\ell-1)\beta].\underline{\underline{V}}(R)$ of length

$$(\ell-1) = cp^h + (k-1)(p^h - p^{h-1}).$$

3.5.2 Example

Given $p \in \mathcal{P}$ and $h,k \in \mathcal{N}$, and an integer c such that $1 \leq c \leq p-1$, let F be the absolutely free group of rank two generated by α and β, and R the normal subgroup of F generated by α and β^{p^h}, so that F/R is a p^h-cycle. Now with $\underline{\underline{V}} = \underline{\underline{N}}_c \cap \underline{\underline{B}}_{p^k}$, the group $F/\underline{\underline{V}}(R)$ contains a non-trivial Engel commutator $[\alpha, (m-1)\beta].\underline{\underline{V}}(R)$ of length $m-1 = cp^h + (k-1)(p^h - p^{h-1}) -1$.

The proof of these examples depends on the following result about free groups in the variety $\underline{\underline{V}} = \underline{\underline{N}}_c \cap \underline{\underline{B}}_{p^s}$:

3.5.3 Lemma

If ξ and η are distinct elements of a set of free generators of a relatively free group in the variety $\underline{\underline{N}}_c \cap \underline{\underline{B}}_{p^s}$, where $1 \leq c \leq p-1$, then $[\xi, (c-1)\eta]^{p^{s-1}} \neq 1$.

Proof It is sufficient to construct a two-generator group of exponent p^s and class c with an Engel commutator of length c-1 whose order is p^s, since this group must be a homomorphic image of the free group described.

Let A and B be cyclic groups of order p^s generated by σ and τ respectively, $W = A \text{ wr } B$, and K the base group of W. By induction on r, it is easily shown that the subset $\{\sigma(\tau^i) \mid 0 \leq i \leq r\}$ of elements of the natural basis of K is equivalent to the set $\{[\sigma, i\tau] \mid 0 \leq i \leq r\}$ and hence that $\{[\sigma, i\tau] \mid 0 \leq i \leq p^s-1\}$ is a basis for K. It is also easy to see that for $c \in \mathcal{N}$, $\underline{\underline{N}}_c(W)$ is generated by $\{[\sigma, i\tau] \mid c \leq i < \infty\}$.

Now $X = W/\underline{\underline{N}}_c(W)$ is the required group. Clearly it has class c. Every element of W may be expressed in the form $\tau^v\beta$ with $\beta \in K$ and $0 \leq v \leq p^s-1$. If $v = 0$, this is clearly of order dividing p^s, and if $v \neq 0$, then

$$(\tau^v\beta)^{p^s} \equiv \tau^{vp^s}\beta^{p^s} \cdot \prod_{1 \leq i \leq c-1} [\beta, i\tau]^{\binom{p^s}{i+1}} \quad \text{modulo } \underline{\underline{N}}_c(W).$$

However for $1 \leq i+1 \leq c \leq p-1$, the exponent $\binom{p^s}{i+1}$ is divisible by p^s, so this expression represents the identity element, and X has exponent p^s. The Engel commutator $[\sigma, (c-1)\tau]$ is clearly displayed as one of the basis elements outside $\underline{\underline{N}}_c(W)$, with order p^s.

<u>Proof</u> of 3.5.1 For this example let $p^h = q$. First obtain a set of free generators of R by the Schreier-Reidemeister procedure, using $\{\alpha^a\beta^b \mid 0 \leq a < q, \ 0 \leq b < q\}$ as a Schreier transversal for R in F. The generators are:

α^q, $\alpha^a\beta^b\alpha\,\beta^{-b}\alpha^{-(a+1)}$ $(0 \le a \le q-2,\ \ 1 \le b \le q-1)$,

$\alpha^{q-1}\beta^b\alpha\,\beta^{-b}$ $(1 \le b \le q-1)$, and $\alpha^a\beta^q\alpha^{-a}$ $(0 \le a \le q-1)$.

Only $q+2$ of these q^2+1 free generators of R will be needed, namely :

$$\psi_o = \alpha^{q-1}\beta^q\alpha^{-(q-1)},\ \psi_i = \alpha^{q-1}\beta^{q-i}\alpha\,\beta^{-(q-i)}\ \ (1 \le i \le q-1)$$

$$\psi_q = \alpha^q\ ,\ \text{ and }\ \psi_{q+1} = \beta^q$$

These, however, are now replaced by an equivalent set obtained as follows:

Let
$$\phi_o = \psi_{q+1} = \beta^q$$
$$\phi_1 = \psi_q^{-1}\psi_o^{-1}\psi_1\,\psi_{q+1} = [\alpha,\beta]$$
$$\phi_i = \psi_{q+1}^{-1}\psi_{i-1}^{-1}\psi_i\,\psi_{q+1} = [\alpha,\beta]^{\beta^{i-1}},\ 2 \le i \le q$$
$$\phi_{q+1} = \psi_q = \alpha^q$$

Since the ψ's can be expressed also in terms of the ϕ's, the two sets are equivalent, and $\{\phi_i \mid 0 \le i \le q+1\}$ is part of a set of free generators for R.

From now on, work modulo $\underline{\underline{V}}(R)$. From above, $[\alpha,\beta] = \phi_1$, and for $1 \le i \le q-1$, $\phi_i^{\ \beta} = \phi_{i+1}$. Hence an induction similar to that in Lemma 1.1.1 shows that for $1 \le \ell \le q$,

$$[\alpha,\ell\beta] = \prod_{1\le i\le \ell} \phi_i^{\,(-1)^{\ell-i}\binom{\ell-1}{i-1}} \cdot \prod_j \kappa_{j,\ell}$$

where the $\kappa_{j,\ell}$ are the commutators of weights from 2 to c whose entries are from $\{\phi_i \mid 1 \le i \le q\}$. In particular, this is true when $\ell = q$, and so, when $\ell = q+1$:

$$[\alpha,(q-1)\beta] = \prod_{1\le i\le q} \phi_i^{(-1)^{q-i+1}\binom{q}{i-1}} \cdot \phi_1^{\beta^q} \cdot \sigma$$

$$= \prod_{1\le i\le q} \phi_i^{S(q,q,i-1)} \cdot \phi_1^{-1}\, \phi_1^{\beta^q} \cdot \prod_j \kappa_{j,q+1}$$

$$= \prod_{1\le i\le q} \phi_i^{S(q,q,i-1)} \cdot [\phi_1,\phi_o] \cdot \prod_j \kappa_{j,q+1} ,$$

since $\beta^q = \phi_o$. Here σ is a product of commutators. The product on the second line, $\prod_j \kappa_{j,q+1}$, is equal to σ multiplied by further commutators which are the result of moving ϕ_1^{-1} to its new position. Entries of a commutator $\kappa_{j,\ell}$ when $\ell > q$ may come from the larger subset, $\{\phi_i \mid 0 \le i \le q\}$, of the free generators of R, but note that of those κ's which have weight two, none has an entry equal to ϕ_o; and as the process of commutation by β is repeated, the only commutators of weight two with ϕ_o as an entry are those arising from the factor $[\phi_1,\phi_o]$ in the expression for $[\alpha,(q+1)\beta]$.

Now assume inductively that for some r, $1 \le r \le c-2$, the commutator $[\alpha,(rq+1)\beta]$ may be expressed as a product in which one of the factors is $[\phi_1,r\phi_o]$, and that no other commutator factor of weight $r+1$ has r of its entries equal to ϕ_o; and a similar procedure shows that the same is true for the integer $r+1$. Hence it is true for all $r \le c-1$; and in particular $[\alpha,((c-1)q+1)\beta]$ may be expressed as a product in which one of the terms is $\gamma = [\phi_1, (c-1)\phi_o]$, and no other term has $c-1$ entries equal to ϕ_o.

Now Lemma 3.5.3 shows, since ϕ_1 and ϕ_o belong to a set of free that generators of R, ~~and~~ $[\phi_1, (c-1)\phi_o]$ has order p^k modulo $(\underline{\underline{N}}_c \cap \underline{\underline{B}}_{p^k})(R) = \underline{\underline{V}}(R)$.

In addition, $\gamma \circ \underline{\underline{V}}(R) \in Z(R/\underline{\underline{V}}(R))$ so Corollary 1.1.2 shows that modulo $\underline{\underline{V}}(R)$, for $j \in \mathcal{N}$,

$$[\gamma, j\beta] = \gamma^{(\beta-1)^j} = \prod_{0 \leq i \leq j} \gamma^{(-1)^{j-i}\binom{j}{i}\beta^i} .$$

Since $\beta^q \in R$, and all conjugates of γ are in $Z(R)$ modulo $\underline{\underline{V}}(R)$,

$$\gamma^{\beta^{(aq+i)}} = \gamma^{\beta^{aq} \cdot \beta^i} \equiv \gamma^{\beta^i} \quad \text{modulo } \underline{\underline{V}}(R).$$

It follows that

$$[\gamma, j\beta] = \prod_{0 \leq i \leq q-1} \gamma^{S(q,j,i)\beta^i} \quad \text{modulo } \underline{\underline{V}}(R)$$

The elements γ^{β^r} and γ^{β^s} with $0 < r-s < q$, can not be equal, for then

$$\gamma = \gamma^{\beta^{r-s}} \Rightarrow [\phi_1, (c-1)\phi_o] \equiv [\phi_{r-s+1}, (c-1)\phi_o] \text{ modulo } \underline{\underline{V}}(R)$$

$$\Rightarrow [\phi_1^{-1}\phi_{r-s+1}, (c-1)\phi_o] \in \underline{\underline{V}}(R) ,$$

and Lemma 3.5.3 shows this to be impossible.

Thus the conjugates of γ in the product $\prod_{0 \leq i \leq q-1} \gamma^{S(q,j,i)\beta^i}$ are all distinct; and some of their powers remain non-trivial as long as p^k does not divide $F(q,j)$. But, by Theorem 2.8, the smallest value of j for which $p^k \mid F(q,j)$ is

$$j = p^h + (k-1)(p^h - p^{h-1}) .$$

Hence $[\gamma, \{p^h + (k-1)(p^h - p^{h-1})-1\}\beta] \notin \underline{\underline{V}}(R)$;

hence $[\alpha, \{cp^h + (k-1)(p^h - p^{h-1})\}\beta] \notin \underline{\underline{V}}(R)$;

that is, $[\alpha, (\ell-1)\beta] \notin \underline{\underline{V}}(R)$, as required.

. . .

Proof of 3.5.2 By Lemma 43.42 of [10], $\{\phi_i \mid 0 \leq i \leq q\}$ is a set of free generators for R, where $\phi_o = \beta^q$ and

$\phi_i = \alpha^{\beta^{i-1}}$, $1 \leq i \leq q$. Now $[\alpha,\beta] = \alpha^{-1}\alpha^{\beta} = \phi_1^{-1} . \phi_2$; and the proof that $[\alpha, (m-1)\beta] \notin \underline{\underline{V}}(R)$ exactly parallels the corresponding proof in the previous example, with the length of the Engel commutator in α and β reduced by 1 throughout.

. . . . .

When $c \geq p \geq 3$, the results of this chapter are no longer best possible, and may be improved by combining two results described here in brief outline only. The proof that groups of exponent p satisfy the $p-1$ th Engel congruence given in [6], Kapitel III, Satz 5.9, is very easily adapted to show that in a group H of exponent p^k,

$$[\alpha, (p-1)\beta]^{p^{k-1}} \in \underline{\underline{N}}_p(H) \quad \text{for all } \alpha,\beta \in H.$$

When $c \geq 3$, Lemma 3.2 may be refined to show that as the length of an Engel commutator in G is increased, the last commutator of weight c in H to remain raised to the p^{k-1} th and not the p^k th power is in fact an Engel commutator in H.

When $p = 2$, the arguments described in the previous paragraph show that in a group H of exponent 2^k, every commutator of weight $w \geq 2$ has in fact order dividing 2^{k-1} modulo $\underline{\underline{N}}_w(H)$. By this method, then, 3.3.1 but not 3.3 may be improved.

Chapter 4

An upper bound on the nilpotency class of certain group extensions

The main result of this chapter is the bound given in Theorem 4.6 for the class of those group extensions shown to be nilpotent by Baumslag in Lemma 3.8 of [2], stated as 1.4.5 earlier in this thesis. Lemmas 4.3 and 4.5 play parts in the proof of 4.6 similar to those of 3.1 and 3.2 respectively in the proof of 3.3. The results of §4.2 and 4.4 on rearrangement of commutators are needed mainly to overcome difficulties caused by the fact that the quotient group G/H is not abelian. Most of the calculations are carried out in terms of the ordered basis for a finite p-group defined in §4.1.

In §4.7 it is shown that the wreath product always attains the bound given by 4.6, and therefore that this result gives the exact class of every nilpotent wreath product. This result is closely related to the lower bound on the class of a wreath product found by Scruton in Theorem 3.5 of [11]; the improvement is made possible by the use of the ordered basis defined in §4.1, in place of the generating set described in Lemma 3.1 of [11].

4.1.1 Definition and Notation

Suppose that G/H is a finite p-group with nilpotency class c, and that for $1 \leq i \leq c$ $\underline{\underline{N}}_{i-1}(G/H) \,/\, \underline{\underline{N}}_i(G/H)$ is a direct product of $z(i)$ cyclic groups of orders $p^{h_{ij}}$, $1 \leq j \leq z(i)$, where $h_{i1} \geq h_{ij}$ for $1 \leq j \leq z(i)$. For $1 \leq i \leq c$, let

$T_i = \{\tau_{ij} \mid 1 \leq j \leq z(i)\}$ be a set of elements of $\underline{\underline{N}}_{i-1}(G)$ which form a basis for $\underline{\underline{N}}_{i-1}(G/H)$ modulo $\underline{\underline{N}}_i(G/H)$, ordered in such a way that τ_{ij} has order $p^{h_{ij}}$ modulo $\underline{\underline{N}}_i(G).H$. Let $T = \bigcup_{1\leq i\leq c} T_i$, and extend the orderings defined on each of the T_i separately to one, which we denote "$\overset{\circ}{\leq}$", on the whole of T, by adding the condition that

$$1 \leq i < i' \leq c \Rightarrow \tau_{ij} \overset{\circ}{<} \tau_{i'j'}$$

The ordered set T will be called an ordered basis for G modulo H.

The use of the term "basis" may be justified by the following result, which is stated without proof :

4.1.2 Lemma

If $H \trianglelefteq G$, and $T = \{\tau_{ij} \mid 1 \leq i \leq c, 1 \leq j \leq z(i)\}$ is an ordered basis for G modulo H, as described in 4.1.1, then every element of G may be expressed uniquely in the form

$$\alpha = \tau_{11}^{e_{11}} \tau_{12}^{e_{12}} \cdots \tau_{c\,z(c)}^{e_{c\,z(c)}}.\eta$$

where $0 \leq e_{ij} \leq p^{h_{ij}}-1$ for $1 \leq i \leq c$, $1 \leq j \leq z(i)$, and $\eta \in H$.

4.2 Lemma

If β is an element in the centre of the normal subgroup H of G, where G/H is a finite p-group and T is an ordered basis for G modulo H, and if $\alpha_i \in \underline{\underline{N}}_{w_i-1}(G) \setminus \underline{\underline{N}}_{w_i}(G)$ for

$1 \leq i \leq m$, then the commutator $[\beta, \alpha_1, \ldots, \alpha_m]$ may be expressed as a product of commutators of the form $[\beta, \theta_1, \ldots, \theta_n]$ where

a) $\theta_i \in T_{v_i}$ $1 \leq i \leq n$, $1 \leq v_i \leq c$;

b) $\sum_{1 \leq i \leq n} v_i \leq \sum_{1 \leq i \leq m} w_i$; and

c) if $1 \leq i < i' \leq n$, then $\theta_i \mathrel{\dot{\leq}} \theta_{i'}$, where "$\dot{\leq}$" is the ordering on T.

The proof depends on the following auxiliary lemma :

<u>4.2.1</u> <u>Lemma</u>

If β^* is an element in the centre of the normal subgroup H of G, where G/H is a finite p-group and T is an ordered basis for G modulo H (see 4.1.1), if for all $i \in \mathcal{L} = \{j \in \mathcal{N} \mid 1 \leq j \leq \ell\}$ the element $\tau_i \in T_{u_i}$, and k is the least integer in $\mathcal{L}$ such that $\tau_k \mathrel{\dot{\leq}} \tau_i$ for all $i \in \mathcal{L}$, and if there are precisely x integers $f \in \mathcal{L}$ such that $u_f = u_k$, then

$$[\beta^*, \tau_1, \ldots, \tau_\ell] = \prod_{a \in \Gamma} \eta_a ,$$

where either (first form) $\eta_a = [\beta^*, \tau_k, \theta_1, \ldots, \theta_{m_a}]$ or (second form) $\eta_a = [\beta^*, \theta_1, \ldots, \theta_{m_a}]$; in either case, $\theta_i \in T_{v_i}$ where $v_i \geq u_k$ for all $i \in \mathcal{M}_a = \{j \in \mathcal{N} \mid 1 \leq j \leq m_a\}$ and there are at most x-1 integers $f \in \mathcal{M}_a$ such that $v_f = u_k$; also if η_a has the first form, then $u_k + \sum_{i \in \mathcal{M}_a} v_i \geq \sum_{i \in \mathcal{L}} u_i$, while if η_a has the second form, then $\sum_{i \in \mathcal{M}_a} v_i \geq \sum_{i \in \mathcal{L}} u_i$.

Proof If $k = 1$, the given commutator already satisfies all conditions on η, and the result is obvious. Suppose inductively that the result is proved if $k < r$ for some integer $r > 1$, and consider a commutator $[\beta^*, \tau_1, \ldots, \tau_\ell]$ such that $\tau_r \dot{\leq} \tau_i$ for all $i \in \mathcal{L}$, and $d < r \Rightarrow \tau_r \dot{<} \tau_d$. Let $\xi_* = [\beta^*, \tau_1, \ldots, \tau_{r-2}]$ and $\xi = [\xi_*, \tau_{r-1}, \tau_r]$. Now

$$\xi = \xi_*^{-\tau_{r-1}} \xi_*^{-\tau_r} \xi_*^{\tau_{r-1}\tau_r} \xi_*$$

$$= \xi_*^{-\tau_r} \xi_*^{-\tau_{r-1}} \xi_*^{\tau_r\tau_{r-1}} \xi_*^{-\tau_r\tau_{r-1}} \xi_*^{\tau_r\tau_{r-1}[\tau_{r-1},\tau_r]}$$

$$= [\xi_*, \tau_r, \tau_{r-1}]\,[\xi_*^{\tau_r\tau_{r-1}}, [\tau_{r-1}, \tau_r]]$$

and eventually, after more computation of the same sort,

$$\xi = [\xi_*, \tau_r, \tau_{r-1}].[\xi_*, \tau_r, [\tau_{r-1}, \tau_r]].[\xi_*, \tau_{r-1}, [\tau_{r-1}, \tau_r]].$$
$$[\xi_*, \tau_r, \tau_{r-1}, [\tau_{r-1}, \tau_r]].[\xi_*, [\tau_{r-1}, \tau_r]] \ .$$

From the fact that $[\tau_{r-1}, \tau_r] = x_1 x_2 \ldots x_d$ where for $1 \leq i \leq d$, $x_i \in T_{(u_{r-1} + u_r)}$, and the Hall identities

$$[\alpha\beta,\gamma] = [\alpha,\gamma][\alpha,\gamma,\beta][\beta,\gamma]$$

and $$[\alpha,\beta\gamma] = [\alpha,\gamma][\alpha,\beta][\alpha,\beta,\gamma] \ ,$$

it follows that

$$\xi = \prod_{b\in\Delta} \zeta_b$$

where for each $b \in \Delta$, ζ_b either is equal to

(i) $[\xi_*,\tau_r,\tau_{r-1}] \qquad = [\beta^*,\tau_1,\ldots,\tau_{r-2},\tau_r,\tau_{r-1}]$

or is of one of the forms :

(ii) $[\xi_*,\tau_r,x_{i_1},\ldots,x_{i_y}] \qquad = [\beta^*,\tau_1,\ldots,\tau_{r-2},\tau_r,x_{i_1},\ldots,x_{i_y}]$

(iii) $[\xi_*,\tau_r,\tau_{r-1},x_{i_1},\ldots,x_{i_y}] \quad = [\beta^*,\tau_1,\ldots,\tau_{r-2},\tau_r,\tau_{r-1},x_{i_1},\ldots,x_{i_y}]$

(iv) $[\xi_*,\tau_{r-1},x_{i_1},\ldots,x_{i_y}] \qquad = [\beta^*,\tau_1,\ldots,\tau_{r-2},\tau_{r-1},x_{i_1},\ldots,x_{i_y}]$

or (v) $[\xi_*,x_{i_1},\ldots,x_{i_y}] \qquad = [\beta^*,\tau_1,\ldots,\tau_{r-2},x_{i_1},\ldots,x_{i_y}]$

with $i_y \geq 1$ in each case. The commutator first given now takes the form

$$[\beta^*,\tau_1,\ldots,\tau_\ell] = [\xi,\tau_{r+1},\ldots,\tau_\ell] = \prod_{b\in\Delta}[\zeta_b,\tau_{r+1},\ldots,\tau_\ell]$$

since $\zeta_b \in Z(H)$ for all $b \in \Delta$. It is easily checked that when each commutator of the last product above is written out in full as a left-normed commutator with β^* as its first entry and the i th of the remaining (n, say) entries from T_{w_i} for $1 \leq i \leq n$, then $\sum_{1\leq i\leq n} w_i \geq \sum_{i\in\mathcal{L}} u_i$.

For each $b \in \Delta$ such that ζ_b has form (i), (ii) or (iii), the inductive hypothesis shows that the corresponding commutator in the product may itself be expressed as a product of commutators of the required form. For the other $b \in \Delta$, ζ_b has form (iv) or (v), and the corresponding expanded commutator already satisfies the required conditions, taking the second form for η_a and having at most $x-1$ entries which are elements of T_{u_r} .

<u>Proof of 4.2</u> Consider the given commutator $[\beta,\alpha_1, \ldots, \alpha_m]$. Since $\alpha_k \in \underline{\underline{N}}_{w_k-1}(G) \setminus \underline{\underline{N}}_{w_k}(G)$ for $1 \leq i \leq m$, the expansion for α_k given by 4.1.2 has $e_{ij} = 0$ when $i < w_k$. By repeated applications of the Hall commutator identities (quoted in the proof of 4.2.1 above) and the expansions for α_k, the given commutator may, since $\beta \in Z(H)$, be expressed as a product of commutators of the form $[\beta, \tau_1, \ldots, \tau_\ell]$ where $\tau_i \in T_{u_i}$ for $1 \leq i \leq \ell$, and where at least one of the later entries τ_i in each commutator comes from the expansion of each of the α_k, $1 \leq k \leq m$, so that $\sum_{1\leq i\leq \ell} u_i \geq \sum_{1\leq k\leq m} w_k$.

As in 4.2.1, let $\mathcal{L} = \{j \in \mathcal{N} \mid 1 \leq j \leq \ell\}$ and let k be the least integer in $\mathcal{L}$ such that $\tau_k \dot{\leq} \tau_i$ for all $i \in \mathcal{L}$. The result will now be proved by reverse induction on u_k (remember that $\tau_k \in T_{u_k}$).

If $u_k \geq [c/2] + 1$, so that $u_i \geq [c/2] + 1$ for all $i \in \mathcal{N}$, and hence $[\tau_i,\tau_j] \in H$ for all $i,j \in \mathcal{N}$, then for arbitrary $\xi \in Z(H)$, it follows that

$$[\xi,\tau_i,\tau_j] = \xi^{-\tau_i}\, \xi\, \xi^{-\tau_j}\, \xi^{\tau_i\tau_j} = [\xi,\tau_j,\tau_i] .$$

Hence, by interchange of adjacent elements, if π is a permutation on $\mathcal{L}$, then

$$[\beta,\tau_1, \ldots, \tau_\ell] = [\beta,\tau_{1\pi}, \ldots, \tau_{\ell\pi}] .$$

In particular, if π is such a permutation that

$1 \leq i \leq i' \leq \ell \Rightarrow \tau_{i\pi} \dot{\leq} \tau_{i'\pi}$, then the lemma is proved for $u_k \geq [c/2] + 1$.

Now suppose the lemma proved when $u_k > s$ for some fixed s, $1 \leq s \leq [c/2]$, and let $\kappa = [\beta, \tau_1, \ldots, \tau_\ell]$ be a commutator satisfying the same conditions as before, in which $u_k = s$ and there are precisely x integers $f \in \mathcal{L}$ such that $u_f = u_k = s$. By x repeated applications of Lemma 4.2.1, κ may be expressed as a product of commutators of the form

$$[\beta, \tau_1', \ldots, \tau_y', \theta_1, \ldots, \theta_m]$$

in which $0 \leq y \leq x$, the entries τ_i' satisfy $\tau_i' \in T_s$ for $1 \leq i \leq y$ and $\tau_i' \dot{\leq} \tau_{i'}'$ wherever $1 \leq i < i' \leq y$, and the entries θ_i satisfy $\theta_i \in T_{v_i}$ where $s+1 \leq v_i \leq c$ for $1 \leq i \leq m$, such that :

$$sy + \sum_{1 \leq i \leq m} v_i \geq \sum_{i \in \mathcal{L}} u_i$$

Now let $\beta^* = [\beta, \tau_1', \ldots, \tau_y']$; and from the inductive hypothesis applied to each commutator of the form $[\beta^*, \theta_1, \ldots, \theta_m]$, this commutator may be expressed as a product of other commutators, each with β^* as its first entry, which when expanded to show β as their first entry satisfy all the conditions required in the statement of the lemma.

<u>4.3</u> <u>Lemma</u>

If β is an element in the centre of the normal subgroup H of G, such that G/H is a finite p-group of class c, and for $1 \leq i \leq c$ $\underline{\underline{N}}_{i-1}(G/H) \,/\, \underline{\underline{N}}_i(G/H)$ is a direct product of $z(i)$ cyclic groups of orders $p^{h_{ij}}$, $1 \leq j \leq z(i)$, where $h_{i1} \geq h_{ij}$ for $1 \leq j \leq z(i)$; if G has ordered basis T modulo H, if

$a = 1 + \sum_{1 \leq i \leq c} (i \sum_{1 \leq j \leq z(i)} (p^{h_{ij}} - 1))$ and

$b = \max_{1 \leq i \leq c} \{i\,(p^{h_{i1}} - p^{h_{i1}-1})\}$, if for $1 \leq i \leq m$,

$\alpha_i \in \underline{\underline{N}}_{w_i-1}(G) \setminus \underline{\underline{N}}_{w_i}(G)$, and if s is a positive or zero integer such that

$$\sum_{1 \leq i \leq m} w_i = w \geq a + (s-1)b,$$

then the commutator $[\beta, \alpha_1, \alpha_2, \ldots, \alpha_m]$ may be expressed as a product of p^s th powers of conjugates of β in G.

<u>Proof</u> Lemma 4.2 shows that the given commutator $[\beta, \alpha_1, \ldots, \alpha_m]$ may be expressed as a product of commutators, each of the form $[\beta, u_{11}\tau_{11}, u_{12}\tau_{12}, \ldots, u_{cz(c)}\tau_{cz(c)}]$ where $\sum_{1 \leq i \leq c} (i \sum_{1 \leq j \leq z(i)} u_{ij}) \geq \sum_{1 \leq i \leq m} w_i = w$. For $1 \leq i \leq c$, $1 \leq j \leq z(i)$, let s_{ij} be the least non-negative integer such that

$$\text{(i)} \quad u_{ij} \leq p^{h_{ij}} + s_{ij}(p^{h_{ij}} - p^{h_{ij}-1}) - 1;$$

and hence either $p^{h_{ij}} + (s_{ij} - 1)(p^{h_{ij}} - p^{h_{ij}-1}) \leq u_{ij}$ or $s_{ij} = 0$. In either case, (from Lemma 3.1 in the first case) the commutator $[\beta, u_{11}\tau_{11}]$ is expressible as a product of $p^{s_{11}}$ th powers of conjugates of β, and if t_{ij} is defined by

$$t_{ij} = \sum_{1\le i'\le i-1} \left(\sum_{1\le j'\le z(i)} s_{i'j'}\right) + \sum_{1\le j'\le j} s_{ij'}$$

(where of course an empty sum is taken to be zero) then by induction following the ordering on T, it follows that $[\beta, u_{11}\tau_{11}, \ldots, u_{ij}\tau_{ij}]$ is a product of $p^{t_{ij}}$ th powers of conjugates of β.

The lemma will be proved when it is shown that $t_{cz(c)} \ge s$. Multiply each of the inequalities labelled (i) above for $1 \le i \le c$, $1 \le j \le z(i)$ by the appropriate i, and add the resulting inequalities, to obtain :

$$\sum_{1\le i\le c} \left(i \sum_{1\le j\le z(i)} u_{ij}\right) \le \sum_{1\le i\le c} \left(i \sum_{1\le j\le z(i)} (p^{h_{ij}} - 1)\right)$$

$$+ \sum_{1\le i\le c} \left(i \sum_{1\le j\le z(i)} s_{ij}(p^{h_{ij}} - p^{h_{ij}-1})\right)$$

From earlier, $\sum_{1\le i\le c} \left(i \sum_{1\le j\le z(i)} u_{ij}\right) \ge \sum_{1\le i\le m} w_i \ge a+(s-1)b$, and so this reduces to :

$$a + (s-1)b \le (a-1) + \sum_{1\le i\le c} \left(i \sum_{1\le j\le z(i)} s_{ij}(p^{h_{ij}} - p^{h_{ij}-1})\right)$$

whence

$$1 + (s-1)b \le \sum_{1\le i\le c} \left(\sum_{1\le j\le z(i)} s_{ij}.i.\,(p^{h_{i1}} - p^{h_{i1}-1})\right)$$

$$\le \left(\sum_{1\le i\le c} \left(\sum_{1\le j\le z(i)} s_{ij}\right)\right).b$$

Thus $(s-1)b < t_{cz(c)}.b$, and so $s-1 < t_{cz(c)}$. Since both sides of the last inequality are integers, it follows that $s \le t_{cz(c)}$, as required.

4.4 Lemma

If the group G splits over its normal subgroup H, the quotient G/H is nilpotent of class c, and for an integer w satisfying $w \geq c$, and each i, $0 \leq i \leq w$, $\alpha_i \in G$, then the commutator $[\alpha_o, \alpha_1, \ldots, \alpha_w]$ may be expressed as a product of commutators of the form $[\beta, \theta_1, \ldots, \theta_\ell]$ where $\beta \in H$, $\theta_i \in \underline{N}_{v_i - 1}(G)$ for $1 \leq i \leq \ell$, and $\sum_{1\leq i\leq \ell} v_i \geq w$.

Proof Let J be a complement of H in G, so that $J \cong G/H$ is nilpotent of class c, and every element of G may be expressed uniquely in the form $\alpha = \beta\tau$ where $\beta \in H$, $\tau \in J$. In particular, let $\alpha_i = \beta_i\tau_i$ for $0 \leq i \leq w$. The proof proceeds by induction on w to show that for $w \geq 1$, every left-normed commutator of the given form is a product of a left-normed commutator of weight $1+w$ in J with commutators of the required form. Since J has class c, the truth of the lemma will follow for $w \geq c$.

When $w = 1$, a routine expansion shows that

$$[\beta_o\tau_o, \beta_1\tau_1] = [\tau_o,\tau_1].[\beta_1,\tau_o^{-1}].[\beta_1,\tau_o^{-1},\tau_o\tau_1].[\beta_o,\beta_1\tau_1].[\beta_o,\beta_1\tau_1,\tau_o^{\beta_1\tau_1}],$$

confirming the inductive hypothesis for this case.

Suppose that for $w \geq 2$,

$$[\beta_o\tau_o, \beta_1\tau_1, \ldots, \beta_{w-1}\tau_{w-1}] = [\tau_o, \tau_1, \ldots, \tau_{w-1}] . \prod_{a\in\Delta} \gamma_a$$

where each γ_a is of the required form with $w-1$ replacing w.

Further application of the Hall identities now shows that $[\beta_o\tau_o, \beta_1\tau_1, \ldots, \beta_w\tau_w]$ can be expressed as a product of commutators of the forms

(i) $[\gamma_a, \beta_w\tau_w]$, (ii) $[\gamma_a, \beta_w\tau_w, \ldots]$,

(iii) $[\tau_o, \ldots, \tau_{w-1}, \beta_w\tau_w]$, and (iv) $[\tau_o, \ldots, \tau_{w-1}, \beta_w\tau_w, \gamma_a, \ldots]$.

The first two of these are clearly of the required form. There is only one commutator of form (iii), and on expansion, it is equal to

$$[\tau_o, \tau_1, \ldots, \tau_w].[\beta_w, [\tau_o, \ldots, \tau_{w-1}]^{-1}] \,.$$
$$[\beta_w, [\tau_o, \ldots, \tau_{w-1}]^{-1}, [\tau_o, \ldots, \tau_{w-1}]\tau_w]$$

in which the first factor is the particular commutator of weight w in J required by the inductive hypothesis, and the second and third are of the required form. Commutators of the form (iv) may be expressed as a product of commutators of the required form using the expression already obtained for form (iii); the only term requiring special checking is

$$\begin{aligned}[\tau_o, \tau_1, \ldots, \tau_w, \gamma_i] &= [\gamma_i, [\tau_o, \ldots, \tau_w]]^{-1} \\ &= [\gamma_i, [\tau_o, \ldots, \tau_w], [\tau_o, \ldots, \tau_w]^{-1}] \,. \\ &\qquad [\gamma_i, [\tau_o, \ldots, \tau_w]^{-1}] \,,\end{aligned}$$

and the last expression is clearly of the required form. The inductive hypothesis is thus confirmed, and the truth of the lemma follows.

<u>4.5</u> <u>Lemma</u>

If the group G splits over its normal subgroup H, if J, a complement of H in G, is a finite p-group of class c such that for $1 \le i \le c$, $\underset{=}{N}_{i-1}(J) / \underset{=}{N}_i(J)$ is a direct product of $z(i)$ cyclic groups of orders $p^{h_{ij}}$, $1 \le j \le z(i)$, where $h_{i1} \ge h_{ij}$ for $1 \le j \le z(i)$, if

$$a = 1 + \sum_{1 \le i \le c} \left(i \sum_{1 \le j \le z(i)} (p^{h_{ij}} - 1)\right)$$

and $$b = \max_{1 \le i \le c} \{i\,(p^{h_{i1}} - p^{h_{i1}-1})\},$$

if $w \ge ra$ for some $r \in \mathcal{N}$, and if $\alpha_i \in G$, $1 \le i \le w$, then

$$[\alpha_o, \alpha_1, \ldots, \alpha_w] = \prod_{1 \le k \le y} \theta_k^{q_k} \circ \eta$$

where $\eta \in \underset{=}{N}_r(H)$ and for $1 \le k \le y$, θ_k may be expressed as a commutator of weight w_k in H, $1 \le w_k \le r$, and $q_k = p^{v_k}$ where $v_k = 1 + [(w - w_k a)/b]$.

<u>Proof</u> The proof exactly parallels* that of Lemma 3.2, proceeding

---

* This statement referred to an earlier lacunary proof of Lemma 3.2, which has now been replaced. The proof of 4.5 now no longer parallels that of 3.2. A new proof (using different preliminary lemmas in place of §§4.2 and 4.3 preceding) has been constructed, and will appear in the published version.

In the case $r = 1$, Lemma 4.4 shows that the initial segment $[\alpha_o, \alpha_1, \ldots, \alpha_{a+(s-1)b}]$ of the given commutator may be expressed as a product of commutators of the form $[\beta, \alpha'_1, \ldots, \alpha'_\ell]$ where $\beta \in H$, $\alpha'_i \in \underline{\underline{N}}_{w_i - 1}(G)$ for $1 \leq i \leq \ell$, and $\sum_{1 \leq i \leq \ell} w_i \geq a+(s-1)b$. Since, modulo $\underline{\underline{N}}_1(H)$, $Z(H) = H$, the induction hypothesis simply restates Lemma 4.3.

For $r \geq 2$, let κ be the commutator $[\alpha_o, \alpha_1, \ldots, \alpha_{ra+(s-1)b}]$, and κ' the left-normed commutator whose entries are the first

1/ $1+(r-1)a$ entries of κ, so that κ may be written $\kappa = [\kappa', \alpha_1'', \ldots, \alpha''_{a+(s-1)b}]$. The proof follows as in Lemma 3.2, with κ and κ' replacing γ and γ' and other commutators altered accordingly, using Lemma 4.3 wherever the proof of 3.2 uses 3.1.

4.6 Theorem

If H is a normal subgroup of the group G such that G/H is a finite p-group of class c and for $1 \leq i \leq c$, $\underline{\underline{N}}_{i-1}(G/H) \,/\, \underline{\underline{N}}_i(G/H)$ is a direct product of $z(i)$ cyclic groups of orders $p^{h_{ij}}$, $1 \leq j \leq z(i)$, where $h_{i1} \geq h_{ij}$ for $1 \leq j \leq z(i)$, if $a = 1 + \sum_{1 \leq i \leq c} (i \sum_{1 \leq j \leq z(i)} (p^{h_{ij}} - 1))$ and

$$b = \max_{1 \leq i \leq c} \{i\,(p^{h_{i1}} - p^{h_{i1}-1})\},$$

and if H is nilpotent of class r_o, such that for $1 \leq r \leq r_o$ every element which can be expressed as a commutator of weight r in H has order dividing p^{s_r}, then G is nilpotent of class at most

$$\max_{1 \leq r \leq r_o} \{ra + (s_r - 1)b\}$$

<u>Proof</u> By the embedding theorem of Krasner and Kaloujnine (see, e.g., 22.21 of [10], G may be embedded in the wreath product $W = H \text{ Wr } G/H$ $(= H \text{ wr } G/H$, since G/H is finite). The base group K of this wreath product is a direct power of H, so satisfies the conditions on H in this theorem. Since W is a splitting extension of K, Lemma 4.5 shows that every left-normed commutator of weight $1+w = \max_{1 \leq r \leq r_o} \{1 + ra + (s_r - 1)b\}$ may, since $w \geq r_o a$, be expressed in the form $\prod_{1 \leq i \leq y} \theta_i^{q_i}$ where for $1 \leq i \leq y$, θ_i is a commutator of weight w_i in H and $q_i = p^{v_i}$ where $v_i = 1 + [(w - w_i a)/b]$. Since $w \geq w_i a + (s_{w_i} - 1)b$ for $1 \leq i \leq y$, it follows that $v_i \geq s_{w_i}$ for $1 \leq i \leq y$, and hence that the given commutator is trivial, and W is nilpotent of class at most w. However G is isomorphic to a subgroup of W; and the theorem is proved.

<u>4.6.1</u> <u>Corollary</u>

If G/H satisfies the same conditions as in Theorem 4.6, and H has exponent p^k and is nilpotent of class r_o, then G is nilpotent of class at most $r_o a + (k-1)b$.

Liebeck, in Theorem 5.1 of [9], found the exact nilpotency class of $A \text{ wr } B$ when A is an abelian group of prime-power exponent and B is a finite abelian p-group for the same prime, p. His result gives an upper bound for the class of any abelian-by-finite-abelian group of p-power exponent, as the embedding theorem of Krasner and Kaloujnine shows. This bound coincides with the special case $c = r_o = 1$ of the bound found in Theorem 4.6 above.

Thus the result of Theorem 4.6 is best possible, and gives the exact class of the wreath product, in the special case $c = r_o = 1$. Example 4.7 shows that in fact the result of Theorem 4.6 is best possible for arbitrary $c, r_o \in \mathcal{N}$, and that it gives the exact nilpotency class of every nilpotent wreath product, since every nilpotent wreath product must (by 1.3.5 above) satisfy the conditions of 4.6.

4.7 Example

If A is a nilpotent group of class r_o, such that for $1 \leq r \leq r_o$ every element which can be expressed as a commutator of weight r in A has order dividing p^{s_r} (and at least one has order exactly p^{s_r}) for some fixed $p \in \mathcal{P}$, and B is a finite p-group of class c such that for $1 \leq i \leq c$, $\underline{\underline{N}}_{i-1}(B)/\underline{\underline{N}}_i(B)$ is a direct product of $z(i)$ cyclic groups of orders $p^{h_{ij}}$ for $1 \leq j \leq z(i)$, where $h_{i1} \geq h_{ij}$ for $1 \leq j \leq z(i)$, with

$$a = 1 + \sum_{1\le i\le c} (i \sum_{1\le j\le z(i)} (p^{h_{ij}} - 1))$$

and $$b = \max_{1\le i\le c} \{i\,(p^{h_{i1}} - p^{h_{i1}-1})\},$$

then $W = A \text{ wr } B$ is nilpotent of class exactly

$$n = \max_{1\le r\le r_0} \{ra + (s_r - 1)b\}$$

Notation Let x be an integer, $1 \le x \le r_o$, such that $xa + (s_x - 1)b = n = \max_{1\le r\le r_0} \{ra + (s_r - 1)b\}$, and let $[\alpha_1, \alpha_2, \ldots, \alpha_x]$ be a commutator of weight x in A whose order is p^{s_x}. Let y be an integer, $1 \le y \le c$, such that

$$y(p^{h_{y1}} - p^{h_{y1}-1}) = b = \max_{1\le i\le c} \{i\,(p^{h_{i1}} - p^{h_{i1}-1})\}.$$

Let $u_{ij} = p^{h_{ij}} - 1$ for $1 \le i \le c$ and $1 \le j \le z(i)$, and denote by χ the sequence of elements of the ordered basis T of B in which the first u_{11} entries are all τ_{11}, the next u_{12} are τ_{12}, and so on through the ordering on T. Denote by χ_* the same sequence with the u_{y1} entries equal to τ_{y1} deleted from their place in the order, and by χ^* the sequence χ_* followed by $u_{y1} + (s_x - 1)(p^{h_{y1}} - p^{h_{y1}-1})$ entries equal to τ_{y1} inserted at the end.

Theorem 4.6 shows that W is nilpotent of class at most n. The example will be proved by showing that the commutator $\kappa = [\alpha_1(1), \chi, \alpha_2(1), \chi, \ldots, \chi, \alpha_x(1), \chi^*]$ may be expressed as a product of commutators of weight n in W, and is non-trivial.

Hence at least one commutator of weight n in W is non-trivial, and so the exact class of W is determined.

The first part of this programme is quite easily carried out. For $1 \leq i \leq c$, $1 \leq j \leq z(i)$, the entry τ_{ij} in the commutator κ may be expressed as a product of commutators in B of weight i and more; and on expansion using the Hall identities and the fact that commutators of weight greater than n in W are trivial, κ is expressed as a product of commutators of weight n.

For the second part, to show that κ is non-trivial, let $\lambda_v = [\alpha_1(1), \alpha_2(1), \ldots, \alpha_v(1)]$ and $\kappa_v = [\alpha_1(1), x, \alpha_2(1), x, \ldots, x, \alpha_v(1)]$ for $1 \leq v \leq x$. Clearly $\lambda_1 = \kappa_1 = \alpha_1(1)$. Assume inductively that for some v, $2 \leq v \leq x$, either $\lambda_{v-1} \equiv \kappa_{v-1}$ or $\lambda_{v-1}^{-1} \equiv \kappa_{v-1}$ modulo $\underline{\underline{N}}_{v-1}(K)$. With the

t/ former case (adaptation necessary for the latter is obvious) Lemma 1.1.2 gives :

$$[\kappa_{v-1}, u_{11}\tau_{11}] \equiv \prod_{0\leq k\leq u_{11}} \lambda_{v-1}^{(-1)^{u_{11}-k}\binom{p^{h_{11}}}{k}\,\tau_{11}^{k}} \quad \text{modulo } \underline{\underline{N}}_{v-1}(K),$$

since λ_{v-1}, and hence κ_{v-1}, is in the centre of K modulo $\underline{\underline{N}}_{v-1}(K)$. Clearly the element of K on the right-hand side of this congruence has support $\{\tau_{11}^{k} \mid 0 \leq k \leq u_{11}\}$, and since the order of τ_{11} is $u_{11} + 1$, the component in the first coordinate subgroup $A(1)$ of this element is $\lambda_{v-1}^{(-1)^{u_{11}}}$. Similarly, by a finite induction following the ordering of T, the commutator $[\kappa_{v-1}, u_{11}\tau_{11}, \ldots, u_{ij}\tau_{ij}]$ is equal modulo $\underline{\underline{N}}_{v-1}(K)$ to an element of K with support consisting of the elements of B which can be expressed in the form $\tau_{11}^{e_{11}}\,\tau_{12}^{e_{12}} \cdots \tau_{ij}^{e_{ij}}$ with $0 \leq e_{ij} \leq u_{ij}$ for $1 \leq i \leq c$, $1 \leq j \leq z(i)$, which has component in $A(1)$ equal to either λ_{v-1} or λ_{v-1}^{-1}. In particular, the same is true of $[\kappa_{v-1}, \chi]$; and so

$$\begin{aligned}\kappa_v &= [\kappa_{v-1}, \chi, \alpha_v(1)]\\ &\equiv [\lambda_{v-1}^{\pm 1}, \alpha_v(1)] \quad \text{modulo } \underline{\underline{N}}_v(K)\\ &= \lambda_v^{\pm 1}\end{aligned}$$

By induction then, modulo $\underline{\underline{N}}_x(K)$, $\kappa_x \equiv \lambda_x^{\pm 1}$.

The same argument shows that $[\kappa_x, \chi_*]$ is equal, modulo $\underline{\underline{N}}_x(K)$, to an element of K whose component in $A(1)$ is either λ_x or λ_x^{-1}, and whose support is the set of all elements of B which, when expressed in their standard form given by Lemma 4.1.2, have $e_{y1} = 0$. Such elements of B, except the identity, when multiplied on the right by any power of τ_{y1} remain outside the (cyclic) subgroup of B generated by τ_{y1}. Thus, modulo $\underline{\underline{N}}_x(K)$, the component in $A(\tau_{y1}^{t})$ for $0 \leq t \leq u_{y1}$ of

$$[\kappa_x, \chi^*] = [\kappa_x, \chi_*, (u_{y1} + (s_x - 1)b)\,\tau_{y1}]$$

is congruent with that of

$$[\lambda_x^{\pm 1}, (p^{h_{y1}} + (s_x - 1)(p^{h_{y1}} - p^{h_{y1}-1}) - 1)\,\tau_{y1}]$$

which, as the proof of Lemma 3.1 shows, is for some t a non-trivial power of λ_x (since λ_x has order p^{s_x}). The given commutator is therefore non-trivial modulo $\underline{\underline{N}}_x(K)$ and so non-trivial; and the example is verified.

The tools used in this thesis have some interesting applications to the more detailed study of some group extensions which are p-groups. Two simple applications are described briefly.

The iterated wreath product of p-cycles is defined by

$G_o = \{1\}$ and for $n \geq 1$, $G_n = G_{n-1} \text{ wr } C_p$.

An induction using Lemma 3.1 shows quite easily that the maximum order of a commutator of weight w in G_n, where $p^{i-1} < w \leq p^i$, is p^{n-i} for $0 \leq i \leq n-1$ (or even $i = n$), and hence that G_n has nilpotency class p^{n-1}. This confirms the result of Kapitel I Satz 15.3(e) of [6]. The same method may be applied to an iterated wreath product of p^h-cycles, though the detailed results are much more complicated.

The basis for the base group of the wreath product $C_{p^s} \text{ wr } C_{p^s}$ used in the proof of Lemma 3.5.3 is readily adapted to a detailed investigation of the lower central series of $W = C_{p^k} \text{ wr } C_{p^h}$ for arbitrary $h,k \in \mathcal{N}$, which reveals a rather surprising increase in the order of factor groups $\underline{\underline{N}}_{i-1}(W)/\underline{\underline{N}}_i(W)$ in this series from p when $i = p^h + s(p^h - p^{h-1})$, $0 \leq s \leq k-2$, to p^{k-s-1} when $i = p^h + s(p^h - p^{h-1}) + 1$.

References

[1] Bachmuth, S. and Hughes, I. : Applications of a Theorem of Magnus. Arch.Math. 17, 380-382 (1966).

[2] Baumslag, G. : Wreath products and p-groups. Proc. Cambridge Philos. Soc. 55, 224-231 (1959).

[3] Dunwoody, M.J. : The Magnus embedding. J. London Math. Soc. 44, 115-117 (1969).

[4] Golod, E.S. : Nil-algebras and residually finite p-groups. Izvestiya Akad. Nauk S.S.S.R., Ser. Mat. 28, 261-272 (1964).

[5] Hall, P. : Some sufficient conditions for a group to be nilpotent. Illinois J. Math. 2, 787-801 (1958).

[6] Huppert, B. : Endliche Gruppen I. Springer-Verlag, Berlin, etc. 1967.

[7] Kostrikin, A.I. : On the connection between periodic groups and Lie rings. Izv. Akad. Nauk S.S.S.R., Ser. Mat. 21 289-310 (1957), and Amer. Math. Soc. Translations Ser. 2, 45, 165-189 (1965).

[8] Kovács, L.G. : Three embedding theorems. Duplicated notes of a seminar given at A.N.U., October 1968.

[9] Liebeck, H. : Concerning nilpotent wreath products. Proc. Cambridge Philos. Soc. 58, 443-451 (1962).

[10] Neumann, Hanna : Varieties of Groups. Springer-Verlag, Berlin etc., 1967.

[11] Scruton, T.: Bounds on the class of nilpotent wreath products. Proc. Cambridge Philos. Soc. 62, 165-169 (1966).

[12] Šmel'kin, A.L. : Wreath products and varieties of groups. Izvestiya Akad. Nauk S.S.S.R., Ser. Mat. 29, 149-170 (1965).

[13] Ward, M.A. : Basic Commutators. Philos. Trans. Royal Soc. London Ser. A. 264, 343-412 (1969).

[14] Zorn, M. : Nilpotency of finite groups. Bull Amer. Math. Soc. 42, 485 (1936).

Appendix

Since most of this thesis was typed, Dr. L.G. Kovács has brought to my attention a preprint of a paper entitled "Bounds for the class of nilpotent wreath products" by L.J. Morley. In the present thesis, the exact class of a nilpotent wreath product is given in §4.7 in the form

$$\max_{1 \leq r \leq r_0} \{ra + (s_r - 1)b\},$$

where a and b are parameters depending on the top group, and commutators of weight r in the bottom group have maximum order p^{s_r}.

The lower bounds of Scruton [11], Morley, and the present thesis are obtained by essentially the same principle, using a standard form for elements of the top group in terms of generators of the factor groups in a central series of the top group. Instead of the extremely fine central series (with every factor of order p) used by Scruton, Morley uses an arbitrary central series, and so improves Scruton's lower bound to one of the form $\max_{1 \leq r \leq r_0} \{ra' + (s_r - 1)b'\}$. The specific use of the lower central series in the present thesis makes it possible, roughly speaking, to multiply each term connected with the i th step of the series in the sums forming a' and b' by i, and so to obtain the sums forming a and b.

When the bottom group is abelian, Morley's upper bound takes the form $a'' + (s_1 - 1)b''$, where a'' and b'' differ from a' and b' in having each summand connected with the i th step of the series multiplied by the product of the exponents of the $i-1$ higher steps (instead of simply by i). The adaptation of this result to a nilpotent base group in general is of the form $r_o a'' + \sum_{1 \le r \le r_o} (s_r - 1)b''$, instead of $\max_{1 \le r \le r_o} \{ra + (s_r - 1)b\}$.