1

MicroD

National Library
of Canada

Bibliothèque nationale
du Canada

Canadian Theses Service

Service des thèses canadiennes

Ottawa, Canada
K1A 0N4

NOTICE

The quality of this microform is heavily dependent upon the quality of the original thesis submitted for microfilming. Every effort has been made to ensure the highest quality of reproduction possible.

If pages are missing, contact the university which granted the degree.

Some pages may have indistinct print especially if the original pages were typed with a poor typewriter ribbon or if the university sent us an inferior photocopy.

Reproduction in full or in part of this microform is governed by the Canadian Copyright Act, R.S.C. 1970, c. C-30, and subsequent amendments.

AVIS

La qualité de cette microforme dépend grandement de la qualité de la thèse soumise au microfilmage. Nous avons tout fait pour assurer une qualité supérieure de reproduction.

S'il manque des pages, veuillez communiquer avec l'université qui a conféré le grade.

La qualité d'impression de certaines pages peut laisser à désirer, surtout si les pages originales ont été dactylographiées à l'aide d'un ruban usé ou si l'université nous a fait parvenir une photocopie de qualité inférieure.

La reproduction, même partielle, de cette microforme est soumise à la Loi canadienne sur le droit d'auteur, SRC 1970, c. C-30, et ses amendements subséquents.

The minimal number of generators
of a group

by

Kieh Wong

A thesis submitted to
the Faculty of Graduate Studies and Research
in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

Department of Mathematics and Statistics

Carleton University

Ottawa, Canada

February, 1989

© copyright

1989, Kieh Wong

National Library
of Canada

Bibliothèque nationale
du Canada

Canadian Theses Service Service des thèses canadiennes

Ottawa, Canada
K1A 0N4

The author has granted an irrevocable non-exclusive licence allowing the National Library of Canada to reproduce, loan, distribute or sell copies of his/her thesis by any means and in any form or format, making this thesis available to interested persons.

The author retains ownership of the copyright in his/her thesis. Neither the thesis nor substantial extracts from it may be printed or otherwise reproduced without his/her permission.

L'auteur a accordé une licence irrévocable et non exclusive permettant à la Bibliothèque nationale du Canada de reproduire, prêter, distribuer ou vendre des copies de sa thèse de quelque manière et sous quelque forme que ce soit pour mettre des exemplaires de cette thèse à la disposition des personnes intéressées.

L'auteur conserve la propriété du droit d'auteur qui protège sa thèse. Ni la thèse ni des extraits substantiels de celle-ci ne doivent être imprimés ou autrement reproduits sans son autorisation.

ISBN 0-315-51154-0

The undersigned hereby recommend to
the Faculty of Graduate Studies and Research
acceptance of the thesis,

"The minimal number of generators of a group"

submitted by

Kieh Wong

in partial fulfilment of the requirements
for the degree of Doctor of Philosophy

Chairman, Department of
Mathematics and Statistics

Thesis Supervisor

External Examiner

Carleton University

Abstract

The crux of this thesis is the determination of the minimal numbers of generators of the wreath product and direct product of certain finite groups. These constructions are used to answer the following question positively for some families of groups:

Given two finite groups G and H , does there exist a finite group T containing G and H so that $T = \langle G, H \rangle$ and $d(T) = d(G) + d(H)$?

In the profinite setting, these constructions can be used to show that the profinite analogue of Grushko-Neumann's Theorem holds for certain families of groups.

If C_n is the cyclic group of order n and D_m is the dihedral group of order $2m$, then $d(C_n \sim D_m) = 3$ if $(m, n) \neq 1$. If G is a finitely generated group such that $d(G/G') = d(G)$, then $d(G \sim C_m) = d(G) + 1$ for all $m \geq 1$. If G is a finite nilpotent group, then $d(G \sim C_m) = d(G) + 1$. If G is a finitely generated imperfect group, then there exists some k such that $d(G^r \sim C_m) = d(G^r) + 1$ for $m \geq 1$ and $r \geq k$.

Let $\bar{G}$ and $\bar{H}$ be finitely generated periodic groups. Then, there exist infinitely many pairs of finitely generated group G and H such that $d(G) = d(\bar{G})$, $d(H) = d(\bar{H})$, there exists an epimorphism from G onto $\bar{G}$, there exists an epimorphism from H onto $\bar{H}$ and $d(G \times H) = d(G) + d(H)$.

Let K and H be nontrivial finite groups so that $d(K_q) = \max_{p \mid |K|} \{d(K_p)\}$ and q is coprime to the order of H , where K_p denotes a p -sylow subgroup of K . If $G = K \wr H$ is the wreath product of K by H , then

$$d(G) = \begin{cases} \max_{p \mid |G|} \{d(G_p)\} & \text{if } |H| > 2, \\ \max_{p \mid |G|} \{d(G_p)\} + 1 & \text{if } |H| = 2. \end{cases}$$

Acknowledgements

I would like to convey my deeply felt gratitude to Professor Luis Ribes, who helped me embark on the adventurous journey of mathematical research. His insightful suggestions, tenacious encouragement and contagious enthusiasm have played a vital role in the creation of this thesis. My thanks also go to Mrs. Gill Murray for the excellent preparation of this typescript.

TABLE OF CONTENTS

Abstract	i
Acknowledgements	iii
Table of contents	iv
Introduction	1
Preliminaries	6
Chapter 1: The Wreath product	12
Chapter 2: A group with a minimal generating set consisting of elements of finite and mutually coprime orders	18
Chapter 3: The minimal numbers of generators of some finite groups	27
Chapter 4: The minimal numbers of generators of some finitely generated groups	51
Chapter 5: Bounds for the numbers of generators of some groups	75
Chapter 6: Grushko-Neumann's Theorem for the free profinite product of some groups	85
References	99

Introduction

In 1982, Aschbacher and Guralnick [1] proved that the minimal number of generators of a finite simple group is two by using the monumental classification theorem for finite simple groups. This completed the work started in 1900 by G.A. Miller [13, p.92] who showed that the minimal number of generators for certain finite simple groups is two. The minimal numbers of generators of some other classes of groups have also been studied. However, the recondite problem of the determination of the minimal number of generators of an arbitrary finite group remains unresolved.

The focal point of this thesis is the determination of the minimal numbers of generators of the wreath product and direct product of certain classes of groups. These constructions are used to answer the following question positively for certain groups:

- (A) Given two finite groups G and H , does there exist a finite group T containing G and H so that $T = \langle G, H \rangle$ and $d(T) = d(G) + d(H)$?

The finite problem (A) is equivalent to the following problem:

- (B) If G and H are finite groups, does there exist a finite quotient group T of $G * H$ so that $d(T) = d(G) + d(H)$?

The motivation for posing (B) is Grushko-Neumann's Theorem. The question, whether Grushko-Neumann's Theorem holds for the free profinite product of finitely generated profinite groups, can be reduced to (B). A positive solution to (B) or (A) would imply that the profinite analogue of Grushko-Neumann's Theorem is valid.

In Chapter 3, we use the wreath product and the direct product to answer (A) positively for some classes of finite groups. For example, we show that $C_n \wr D_m$ needs 3 generators when n and m are not coprime. Similarly, $C_n \wr Q_m$ needs 3 generators if n and $m/2$ are not coprime. In order to establish corollaries of these results, we invoke some lemmas concerning wreath products. These lemmas are proved in Chapter 1.

In Chapter 2, some special properties of a finitely generated group G , with a minimal generating set consisting of elements of finite and mutually coprime orders, are discussed. Groups of this type are used, as examples, to elucidate certain results in the subsequent chapters. The dihedral group D_n of order $2n$, where n is odd, is an example of such a group. Any finite nilpotent group is not a group of this type. One property of G is that $d(G^r)$ is equal to $d(G)$ for every r which is at most $d(G)$. However, $d(G^r)$ is equal to r if r exceeds $d(G)$. Moreover, for any finite group H , $d(G \wr H)$ is at most $d(H)+1$ whenever $d(G)$ is at most the order of H .

We generalize the finite problem (A) to a problem, concerning finitely generated groups, as follows:

- (C) Given two finitely generated groups G and H , construct a group T containing G and H such that $T = \langle G, H \rangle$ and $d(T) = d(G) + d(H)$. The construction should form a group T which is finite whenever G and H are both finite.

In Chapter 4, explicit constructions will be employed to give a positive solution to (C) for certain classes of finitely generated groups. Since the constructions used are the wreath product and the

direct product, the constructed groups are finite whenever the given groups are finite. Consequently, this increases the number of pairs of groups for which (A) has a positive solution as well. We will state some of the major results in Chapter 4. For two finitely generated abelian groups G and H , we give a criterion for when $d(G \times H)$ is equal to $d(G) + d(H)$. This happens when G and H have canonical decompositions which are related as follows:

$$G = C_{m_1} \times C_{m_2} \times \dots \times C_{m_s} \times \mathbb{Z}^\alpha, \quad m_i | m_{i+1}, \quad 1 \leq i \leq s-1;$$

$$H = C_{n_1} \times C_{n_2} \times \dots \times C_{n_t} \times \mathbb{Z}^\beta, \quad n_j | n_{j+1}, \quad 1 \leq j \leq t-1,$$

and $(m_1, n_1) \neq 1$.

Following the definition in 3.15, G and H are said to be not coprime. The result can be generalized to finitely generated groups G and H with abelianized groups which are not coprime, $d(G/G') = d(G)$ and $d(H/H') = d(H)$. For every finitely generated group G such that $d(G/G')$ is equal to $d(G)$, we show that $G \circ C_m$ needs $d(G) + 1$ generators for every m greater than 1. In particular, $d(G/G')$ is equal to $d(G)$ if G is a finite nilpotent group. Another interesting corollary makes use of a result of Wiegold and Wilson [19] on the growth sequences of finitely generated groups. If G is a finitely generated imperfect group, then there exists a positive integer k so that $G^r \circ C_m$ needs $d(G^r) + 1$ generators for every $r \geq k$ and $m \geq 2$. Finally, given any two finitely generated periodic groups $\bar{G}$ and $\bar{H}$, we construct infinitely many pairs of finitely generated groups G and H so that $G \times H$ needs $d(G) + d(H)$ generators. G and H are chosen so that $d(G) = d(\bar{G})$,

$d(H) = d(\bar{H})$, $\bar{G}$ is an epimorphic image of G and $\bar{H}$ is an epimorphic image of H .

While the preceding chapters are concerned with the determination of the precise minimal numbers of generators of some groups, Chapter 5 gives only bounds for the minimal numbers of generators of certain families of groups. We show that for any finite group G and $D = G^r$, the minimal number of generators of D is bounded by $\max_{p \mid |G|} \{d(D_p)\} + 1$ for all sufficiently large r . This observation is heavily based on results of Wiegold [18] and Roggenkamp [17]. Let K and H be non-trivial finite groups where $d(K_q) = \max_{p \mid |K|} \{d(K_p)\}$ and q does not divide the order of H . If $G = K \vee H$, then $d(G)$ is at most $\max_{p \mid |G|} \{d(G_p)\}$ when H has more than 2 elements. If H has precisely 2 elements, $d(G)$ is bounded by $\max_{p \mid |G|} \{d(G_p)\} + 1$. We appeal to a recent result by Longobardi and Maj [12] to establish these bounds. We give similar bounds for the propitious cases of direct products of groups as well.

The connection between the results, obtained in Chapter 3 and 4, and the profinite analogue of Grushko-Neumann's Theorem are discussed in detail in Chapter 6. We show that (A) and (B) are equivalent. Moreover, (B) holds for "large enough" groups. In the penultimate section of this thesis, we give a summary of the results from Chapter 3 and Chapter 4 to give a partial solution to (B). Finally we pose some problems of immediate interest. We state three of the problems here. Does (B) have a positive solution if G and H are two

finite abelian groups which are coprime? Does (B) have a positive solution if G and H are two finite groups such that $d(G/G') = d(G)$ and $d(H/H') < d(H)$? Moreover, does (B) have a positive solution if G and H are finite groups such that $d(G/G') < d(G)$ and $d(H/H') < d(H)$? Positive solutions to these three problems would establish the profinite analogue of Grushko-Neumann's Theorem.

PRELIMINARIES

0.1 Notation

$\cong$	Isomorphism
$\rightarrow$	mapping
$\rightarrow\sim$	epimorphism
$\mapsto$	value of a mapping on an element
$\hookrightarrow$	monomorphism
$\subseteq$	is a subset of (equality is included)
$\leq$	is a subgroup of; is less than or equal to
$\trianglelefteq$	is a normal subgroup of
$\{x_i : i \in I\}$	set consisting of the elements x_i , indexed by I
$\langle x_i : i \in I \rangle$	subgroup generated by the elements x_i
G/H	quotient group with elements the (left) cosets of H
(m,n)	greatest common divisor of m and n
$[x,y]$	commutator $x^{-1}y^{-1}xy$
x^y	conjugate $y^{-1}xy$
$\langle X R \rangle$	group on generators X and relators R
$\sim$	is congruent to
$ $	is a divisor of
$\cap$	intersection
$\text{Aut}(G)$	automorphism group of G
$B(n,r)$	free Burnside group of exponent n and rank r
C_n	cyclic group of order n ; $\langle x x^n = 1 \rangle$
D_n	dihedral group of order $2n$; $\langle x, y x^2 = y^2 = (xy)^2 = 1 \rangle$

$d(G)$	minimal number of generators of G
G^*	Frattni subgroup of G
G'	derived group of G ; $[G, G]$
G_p	a p -Sylow subgroup of G
$ G $	order of G
$\text{gap}(G)$	generation gap of G ; $d(G) - d_{\mathbb{Z}G}(G)$
$\mathcal{I}$	augmentation ideal of G
$\mathbb{N}$	the natural numbers
$\text{pr}(G)$	presentation rank of G ; equal to $\text{gap}(G)$
Q_n	dicyclic group of order $2n$; n even; $\langle x, y \mid y^n = 1, y^{n/2} = x^2, x^{-1}yx = y^{-1} \rangle$
S_n	symmetric group of degree n
$\mathbb{Z}$	cyclic group of infinite order; the integers
$\mathbb{Z}G$	group ring of G over $\mathbb{Z}$
$A \times B$	direct product
$\prod_{i=1}^n A_i$	direct product
$A * B$	free product
$\ast_{i \in I} A_i$	free product
$A \rtimes B$	semidirect product
$A \wr B$	wreath product
$A \coprod B$	free profinite product
$A \circ B$	the wreath or direct product
A^r	the direct product of r copies of A
A^{or}	the o-product of r copies of A

All the essential group theoretic terminology will be introduced here. In addition to the definitions, some pertinent theorems will be stated.

0.2 Definition. If p is a prime number, a group G is a p -group if every element of G has order equal to some power of p .

0.3 Definition. A finite group is an *elementary abelian p -group* if it is a direct product of cyclic groups of order p .

0.4 Definition. A group is *simple* if it is nontrivial and contains no proper normal subgroup.

0.5 Definition. A group G is *solvable* if there exists a chain of subgroups $G = G_0 > G_1 > \dots > G_n = \{1\}$ so that each G_i is normal in G_{i+1} and G_i/G_{i+1} is abelian.

0.6 Definition. For a group G , define a chain of subgroups $\gamma_i(G)$ inductively: $\gamma_1(G) = G$, $\gamma_{i+1}(G) = [\gamma_i(G), G]$. Then $\gamma_i(G) \triangleleft G$, and G is *nilpotent* if there exists some integer n so that $\gamma_{n+1}(G) = \{1\}$. The least possible integer n is called the *class* of G .

0.7 Definition. The *Frattini subgroup* of G , denoted by G^* , is the intersection of all the maximal subgroups of G . $G^* \triangleleft G$. If G has no maximal subgroup, then $G^* = G$.

0.8 Definition. A group G is *perfect* if $G' = G$. A group G is *imperfect* if it is not perfect.

0.9 The *canonical decomposition* of a finitely generated abelian group is $A \cong C_{n_1} \times C_{n_2} \times \dots \times C_{n_s} \times \mathbb{Z} \times \dots \times \mathbb{Z}$, where $n_i \mid n_{i+1}$ for

every i . This representation is unique.

We state two theorems by Burnside which are proved in [13, p.163] and [3, p.321] respectively.

0.10 Theorem (Burnside). If all the p -Sylow subgroups of a finite group G are cyclic, then G is solvable.

0.11 Burnside's pq -theorem (1904). If p and q are prime numbers, then a group of order $p^m q^n$ is solvable.

0.12 Definition. A group F is *free* on a subset X if, for every group G and every mapping $f : X \rightarrow G$, there is a unique homomorphism $\tilde{f} : F \rightarrow G$ extending f ; i.e. $\tilde{f}(x) = f(x)$ for every $x \in X$. X is called a *basis* for F and the cardinality of X is the *rank* of F .

Assume that

X is a set,

F is the free group on X ,

R is a subset of F ,

$N = \overline{R}$ is the normal closure of R in F , and

$G \cong F/N$.

0.13 Definition. $G = \langle X | R \rangle$ is a *presentation* of G . The elements of X are called the *generators* of G , and those of R *relations*.

X is called a *generating set* for G . G is *finitely generated* if it can be generated by a finite set. If X is of finite order, it is called a *minimal generating set* of G if it generates G and for every set Y which generates G , the cardinality of X is less than or equal to that of Y . In this case, the cardinality of X is the *minimal number of generators* of G and is denoted by $d(G)$.

0.14 In certain contexts, it is convenient to regard a subset of a group G as a well ordered set. Given a subset X of G , we can think of X as a tuple $X = (x_1, x_2, \dots)$ regardless of its cardinality. However, this will not prevent us from using the same symbol X for the corresponding set which has not been ordered.

Consider the following types of transformations on a tuple $X = (x_1, x_2, \dots)$:

- (T1) replace x_i by x_i^{-1} ;
- (T2) replace some x_i by $x_i x_j$ where $j \neq i$;
- (T3) delete some x_i where $x_i = 1$.

It is assumed implicitly that all the x_k where $k \neq i$ remain fixed. A transformation of the type T1, T2 or T3 is called an *elementary Nielsen transformation*. A product of elementary Nielsen transformations is called a *Nielsen transformation*.

We state a result which can be found in Lyndon & Schupp's book on combinatorial group theory [13, p.6].

0.15 Proposition. If X is carried to Y by a Nielsen transforma-

tion, then $\langle X \rangle = \langle Y \rangle$.

0.16 Definition. If $G_1 = \langle X | R \rangle$ and $G_2 = \langle Y | S \rangle$, the group $\langle X, Y | R, S \rangle$ is called the *free product* of G_1 and G_2 denoted by $G_1 * G_2$. Alternatively, the free product is a group P having the following universal mapping property:

- (i) For each i , there is a monomorphism $\alpha_i : G_i \rightarrow P$;
- (ii) For every group H and a pair of homomorphisms, $\beta_i : G_i \rightarrow H$, there is a unique homomorphism $\psi : P \rightarrow H$ which extends $\{\beta_i\}$, i.e. $\psi\alpha_i = \beta_i$.

0.17 Let $G_1, G_2, \dots, G_n$ be groups. The *direct product* of the groups G_i is the set $G = G_1 \times G_2 \times \dots \times G_n$ of n -tuples $(g_1, \dots, g_n)$, $g_i \in G_i$ with componentwise multiplication $(g_1, \dots, g_n)(h_1, \dots, h_n) = (g_1 h_1, \dots, g_n h_n)$. The groups G_i are called the *direct factors* of G .

We can generalize this construction to the case when there is an arbitrary number of factors G_k , $k \in I$. Let G be the set of functions $f : I \rightarrow \bigcup_{k \in I} G_k$ which satisfy the condition $f(k) \in G_k$ for every $k \in I$. The set G with multiplication defined by $(fg)(k) = f(k)g(k)$ is a group called the *direct product* of the groups G_k , denoted by $\prod_{k \in I} G_k$. $f(k)$ is called the *projection* of the function f on the factor G_k .

Chapter 1

THE WREATH PRODUCT

In some instances, the wreath product will be useful in the formation of groups which have certain numbers of generators. Since we will be constructing the wreath products of groups frequently during the course of this thesis, it is appropriate to start with the definition of this product and some relevant lemmas. These lemmas will be invoked repeatedly in subsequent chapters.

1.1 A group G acts on a set X if there is a function $G \times X \rightarrow X$ denoted by $(g, x) \mapsto gx$ so that

- (i) $1x = x$;
- (ii) $g(hx) = (gh)x$ for every $x \in X$, and every $g, h \in G$.

1.2 Definition. A group G is a *semidirect product* of K by H , denoted by $K \rtimes H$, if G contains K and H so that:

- (i) $K \triangleleft G$;
- (ii) $KH = G$;
- (iii) $K \cap H = \{1\}$.

Unlike the direct product, the semidirect product is not uniquely determined by K and H . In fact, a semidirect product depends on the action of H on K . There is a homomorphism $\theta : H \rightarrow \text{Aut}(K)$ defined by $\theta_x(k) = x^{-1}kx$ for every $k \in K$ and $x \in H$.

Given K, H and $\theta : H \rightarrow \text{Aut}(K)$, $K \rtimes_{\theta} H$ consists of the set of ordered pairs $(k, x) \in K \times H$ under the binary operation

$$(k, x)(\ell, y) = (k\theta_{x^{-1}}(\ell), xy) = (k\ell^{x^{-1}}, xy).$$

A construction based on that of the semidirect product, which is of special interest to us, is the wreath product. Let K and H be groups. Let $K^{|H|}$ be the direct product of isomorphic copies of K indexed by elements of H . So, $K^{|H|}$ is the group of all functions $H \rightarrow K$ with the usual multiplication. If f and g are functions from H to K , then

$$(fg)(x) = f(x)g(x), \quad x \in H.$$

For every $f \in K^{|H|}$ and $y \in H$, we define f^y by

$$f^y(x) = f(xy), \quad x \in H.$$

The map $\hat{y} : K^{|H|} \rightarrow K^{|H|}$ defined by $\hat{y}(f) = f^y$ is an automorphism of $K^{|H|}$. The map $\theta : H \rightarrow \text{Aut}(K^{|H|})$ sending each y to the automorphism $\hat{y}$ is a monomorphism.

If H is finite of order n , then f can be regarded as an n -tuple (k_x) with its x^{th} coordinate $k_x = f(x)$. f^y is obtained from f by permuting its coordinates by translating the indices by y . Let $f = (g_{h_1}, \dots, g_{h_n}) \in K^{|H|}$. Then, $f^y = (g_{h_1 y}, \dots, g_{h_n y})$.

1.3 Definition. Let K and H be groups. The *wreath product* of K and H , denoted by $K \wr H$, is the semidirect product

$$K \wr H = K^{|H|} \rtimes_{\theta} H$$

where $\theta : H \rightarrow \text{Aut}(K^{|H|})$ is defined by $\theta_y(f) = f^y$ and $f^y(x) = f(xy)$, $x \in H$. $K \wr H$ is the set $K^{|H|} \times H$ with the multiplication given by

$$(f, y)(g, z) = (fg^{y^{-1}}, yz).$$

1.4 Notation $G \circ H$ denotes either the wreath product or direct product of G by H . For the sake of brevity, the parentheses of $((G_1 \circ G_2) \circ G_3 \circ \dots) \circ G_n$ will be omitted and we will simply write $G_1 \circ G_2 \circ \dots \circ G_n$.

1.5 Lemma. If G and H are groups, then any epimorphism $\gamma : G \twoheadrightarrow K$ induces an epimorphism $G \sim H \twoheadrightarrow K \sim H$.

Proof. Let $\gamma : G \rightarrow K$ be an epimorphism. Denote an element of $G \sim H$ by fy where $y \in H$ and $f : H \rightarrow G$. Define the mapping $\phi : G \sim H \rightarrow K \sim H$ by $\phi(fy) = \bar{f}y$ where $\bar{f}(x) = \gamma(f(x))$ for every $x \in H$. Then, $\phi[(fy)(gz)] = \phi(fg^{y^{-1}}yz) = \overline{fg^{y^{-1}}}yz$. On the other hand,

$$\phi(fy)\phi(gz) = (\bar{f}y)(\bar{g}z) = \bar{f}\bar{g}^{y^{-1}}yz.$$

$$\begin{aligned} \text{Now, } \overline{fg^{y^{-1}}}(x) &= \gamma(fg^{y^{-1}}(x)) = \gamma(f(x)g^{y^{-1}}(x)) \\ &= \gamma(f(x))\gamma(g^{y^{-1}}(x)) = \gamma(f(x))\gamma(g(xy^{-1})). \end{aligned}$$

$$\begin{aligned} \text{Moreover, } \bar{f}\bar{g}^{y^{-1}}(x) &= \bar{f}(x)\bar{g}^{y^{-1}}(x) \\ &= \gamma(f(x))\bar{g}(xy^{-1}) \\ &= \gamma(f(x))\gamma(g(xy^{-1})). \end{aligned}$$

Consequently, $\overline{fg^{y^{-1}}} = \bar{f}\bar{g}^{y^{-1}}$ and ϕ is a homomorphism and obviously an epimorphism. $\square$

1.6 Lemma. If G is a group and H is a finite group, there exists an epimorphism $G \circ H \twoheadrightarrow G/G' \times H/H'$, where G' and H' are the derived groups of G and H respectively.

Proof. Firstly, the mapping $G \times H \rightarrow G/G' \times H/H'$ which sends (g, h) onto (gG', hH') is an epimorphism.

Define the mapping $\phi : G \sim H \rightarrow G/G' \times H/H'$ so that $(g_{h_1}, \dots, g_{h_n})h \mapsto (g_{h_1} \dots g_{h_n} G', hH')$ where $n = |H|$. We will show that ϕ is a homomorphism.

Let $(g_{h_1}, \dots, g_{h_n})h, (c_{h_1}, \dots, c_{h_n})d \in G \sim H$.

$$\begin{aligned} \text{Then, } \phi[(g_{h_1}, \dots, g_{h_n})h(c_{h_1}, \dots, c_{h_n})d] \\ &= \phi[(g_{h_1}, \dots, g_{h_n})(c_{h_1}, \dots, c_{h_n})^{h^{-1}}hd] \\ &= \phi[(g_{h_1}, \dots, g_{h_n})(c_{h_1 h^{-1}}, \dots, c_{h_n h^{-1}})hd] \\ &= \phi[(g_{h_1 c_{h_1 h^{-1}}}, \dots, g_{h_n c_{h_n h^{-1}}})hd] \\ &= \left(\left(\prod_{i=1}^n g_{h_i c_{h_i h^{-1}}} \right) G', hdH' \right). \end{aligned}$$

On the other hand,

$$\begin{aligned} \phi[(g_{h_1}, \dots, g_{h_n})h] \phi[(c_{h_1}, \dots, c_{h_n})d] \\ &= \left(\prod_{i=1}^n g_{h_i} G', hH' \right) \left(\prod_{i=1}^n c_{h_i} G', dH' \right) \\ &= \left(\prod_{i=1}^n g_{h_i} \prod_{i=1}^n c_{h_i} G', hdH' \right) \\ &= \left(\prod_{i=1}^n g_{h_i c_{h_i}} G', hdH' \right). \end{aligned}$$

Since $\left(\prod_{i=1}^n g_{h_i c_{h_i h^{-1}}} \right) G' = \left(\prod_{i=1}^n g_{h_i c_{h_i}} \right) G'$, the mapping ϕ is a

homomorphism and hence an epimorphism. $\square$

1.17 Lemma. Let A be an abelian group and G be any group with a finite normal subgroup H . Then there is a "natural" epimorphism $\phi : A \sim G \twoheadrightarrow A \sim G/H$.

Proof. Denote an element of $A \sim G$ by αg where $g \in G$ and $\alpha : G \rightarrow A$. Define $\phi(\alpha g) = \overline{\alpha} \overline{g}$ where $\overline{g} = gH$ and $\overline{\alpha}(xH) = \prod_{h \in H} \alpha(xh)$. Note that $\overline{\alpha}$ is well-defined since H is finite and A is abelian. It is clear that ϕ is onto and we will show that it is a homomorphism as well.

$$\phi[(\alpha g)(\beta g')] = \phi[\alpha \beta^{g^{-1}} g g'] = \overline{\alpha \beta^{g^{-1}}} \overline{g g'}.$$

$$\phi(\alpha g) \phi(\beta g') = \overline{\alpha} \overline{g} \overline{\beta} \overline{g'} = \overline{\alpha} \overline{\beta} \overline{g}^{-1} \overline{g} \overline{g'} = \overline{\alpha} \overline{\beta} \overline{g}^{-1} \overline{g g'}.$$

Moreover,

$$\begin{aligned} \overline{\alpha \beta^{g^{-1}}}(xH) &= \prod_{h \in H} (\alpha \beta^{g^{-1}})(xh) \\ &= \prod_{h \in H} \alpha(xh) \beta(xhg^{-1}) \\ &= \left(\prod_{h \in H} \alpha(xh) \right) \left(\prod_{h' \in H} \beta(xg^{-1}h') \right). \end{aligned}$$

On the other hand,

$$\begin{aligned} (\overline{\alpha} \overline{\beta} \overline{g}^{-1})(xH) &= \overline{\alpha}(xH) \overline{\beta} \overline{g}^{-1}(xH) \\ &= \overline{\alpha}(xH) \overline{\beta}(xHg^{-1}) \end{aligned}$$

$$\begin{aligned}
&= \bar{\alpha}(xH) \bar{\beta}(xg^{-1}H) \\
&= \left(\prod_{h \in H} \alpha(xh) \right) \left(\prod_{h \in H} \beta(xg^{-1}h) \right).
\end{aligned}$$

Consequently, $\overline{\alpha\beta g^{-1}} = \bar{\alpha} \bar{\beta} \bar{g}^{-1}$ and ϕ is a homomorphism.

The map ϕ is natural in the sense that if $A \rightsquigarrow A'$, then the following diagram

$$\begin{array}{ccc}
A \rightsquigarrow G & \longrightarrow & A \rightsquigarrow G/H \\
\downarrow & & \downarrow \\
A' \rightsquigarrow G & \longrightarrow & A' \rightsquigarrow G/H
\end{array}
\quad \text{commutes.} \quad \square$$

Chapter 2

A GROUP WITH A MINIMAL GENERATING SET CONSISTING OF ELEMENTS
OF FINITE AND MUTUALLY COPRIME ORDERS

We will explore some of the properties of a finitely generated imperfect group, which has a minimal generating set consisting of elements of finite and mutually coprime orders. An example of a group of this type is the dihedral group of order $2n$, where n is odd. Groups of this sort are endowed with special properties which make them convenient examples of some results in the following chapters. Moreover, some properties are of independent interest.

Recall that a group G is imperfect if $G' < G$.

2.1 Proposition. Let G be a finitely generated imperfect group. If G has a generating set consisting of elements of finite and mutually coprime orders, then G/G' is nontrivial and cyclic.

Proof. Assume that G is a finitely generated imperfect group. Let $\{x_1, \dots, x_n\}$ be a generating set for G , where x_i has order s_i for every i and $(s_i, s_j) = 1$ for every $i \neq j$. If $s = \prod_{k=1}^n s_k$, it follows that $(\prod_{k=1}^n x_k)^s G' = x_i^s G'$. Since $(s, s_i) = 1$, $x_i G' = \prod_{k=1}^n x_k G'$ for every i . Consequently, G/G' is isomorphic to C_r where r is a divisor of $\prod_{k=1}^n s_k$. Moreover, r is not equal to 1 since G is imperfect. $\square$

2.2 Example. If n is odd, D_n and S_n are groups which satisfy the conditions of this proposition.

Now, we will determine precisely the minimal number of generators of the direct product of r copies of this group, denoted by G^r . As long as r is less than or equal to $d(G)$, $d(G^r)$ will not grow but stays the same as $d(G)$. However, if r exceeds $d(G)$ then $d(G^r)$ is precisely r . We have to start with a lemma, showing that the abelianized group of G^r can be generated by r elements.

2.3 Lemma. If G is a finitely generated imperfect group with a generating set consisting of elements of finite and mutually coprime orders, then $d(G^r/(G^r)') = r$ for every $r \geq 1$.

Proof. Let $\{s_i \mid 1 \leq i \leq d(G)\}$ be the orders of the elements of a generating set of G , where $(s_i, s_j) = 1$ for all $i \neq j$. Firstly, $G^r/(G^r)' \cong (G/G')^r$. By proposition 2.1, $G^r/(G^r)' \cong C_n^r$ where n divides $\prod_{i=1}^{d(G)} s_i$. Therefore, $d(G^r/(G^r)') = r$. $\parallel$

2.4 Proposition. Let G be a finitely generated group which has a minimal generating set consisting of elements of finite and mutually coprime orders. If $r \leq d(G)$, then $d(G^r) = d(G)$. If $r > d(G)$ and G is imperfect, then $d(G^r) = r$.

Proof. Let $d(G) = n$ and $\{g_i \mid 1 \leq i \leq n\}$ be a minimal generating set for G , where each g_i has order s_i and $(s_i, s_j) = 1$ if $i \neq j$. Consider G^r which denotes $G \times G \times \dots \times G$, the direct product of r copies of G . Then, denote the corresponding generating set of the j^{th} copy of G by $\{x_{i,j} = (1, 1, \dots, 1, g_i, 1, \dots, 1) \mid 1 \leq i \leq n\}$. The element $x_{i,j}$ represents the r -tuple with g_i in the j^{th} entry and 1's in all other entries. Then $x_{i,j}$ has order s_i and the orders

of $x_{i,j}$ and $x_{k,j}$ are coprime if $i \neq k$.

Firstly, let $r < n$. Consider the element $x_{1,1}x_{2,2}\dots x_{k,k}\dots x_{r,r}$ of G^r . The elements $x_{1,1}, x_{2,2}, \dots, x_{k,k}, \dots, x_{r,r}$ have orders $s_1, s_2, \dots, s_k, \dots, s_r$ respectively, which are mutually coprime.

a) $n = d(G) \cdot r$

$$G \times G \times G \times \dots \times G$$

x_{11}	x_{12}	x_{13}	$\dots$	x_{1r}
x_{21}	x_{22}	x_{23}	$\dots$	x_{2r}
x_{31}	x_{32}	x_{33}	$\dots$	x_{3r}
$\vdots$				$\vdots$
x_{r1}	x_{r2}	x_{r3}	$\dots$	x_{rr}
x_{n1}	x_{n2}	x_{n3}	$\dots$	x_{nr}

b) $n = d(G) \cdot r$ and G is imperfect

$$G \times G \times G \times \dots \times G$$

x_{11}	x_{12}	x_{13}	$\dots$		x_{1r}
x_{21}	x_{22}	x_{23}	$\dots$		x_{2r}
x_{31}	x_{32}	x_{33}	$\dots$		x_{3r}
$\vdots$					$\vdots$
x_{n1}	x_{n2}	x_{n3}	$\dots$	x_{nn}	$x_{n,n+1} \dots x_{nr}$

If $\varepsilon = \prod_{\ell \neq k}^b s_\ell$, then $(x_{1,1} x_{2,2} \dots x_{k,k} \dots x_{r,r})^\varepsilon = x_{k,k}^\varepsilon$. Since $(\varepsilon, s_k) = 1$, there exist integers r_k and t_k such that $r_k \varepsilon = 1 + t_k s_k$. Hence, $(x_{k,k}^\varepsilon)^{r_k} = x_{k,k}$, whereby $x_{k,k} \in \langle x_{1,1} x_{2,2} \dots x_{k,k} \dots x_{r,r} \rangle$ for each k , $1 \leq k \leq r$.

If $2 \leq i \leq n$, consider the element of G^r , $x_{1,1} x_{i+1,2} x_{i+2,3} \dots x_{j+i-1,j} \dots x_{i+r-1,r}$, where $x_{j+i-1,j}$ denotes the $(j+i-1)$ -th generator of the j th copy of G . The indices are modulo n . The difference between the indices of every element $x_{j+i-1,j}$ is $i-1 \pmod{n}$. The elements $x_{i,1}, x_{i+1,2}, x_{i+2,3}, \dots, x_{j+i-1,j}, \dots, x_{i+r-1,r}$ have orders $s_i, s_{i+1}, s_{i+2}, \dots, s_{j+i-1}, \dots, s_{i+r-1}$ respectively. As in the case when $i = 1$, let $\varepsilon = \prod_{\substack{\ell=i \\ \ell \neq k}} s_\ell$.

Then, $(x_{i,1} x_{i+1,2} \dots x_{i+r-1,r})^\varepsilon = x_{k,k-i+1}^\varepsilon$. Since $(\varepsilon, s_k) = 1$, there exist integers r_k and t_k such that $r_k \varepsilon = 1 + t_k s_k$. Hence, $(x_{k,k-i+1}^\varepsilon)^{r_k} = x_{k,k-i+1}$ whereby $x_{k,k-i+1}$ is contained in the subgroup generated by $x_{i,1} x_{i+1,2} \dots x_{i+r-1,r}$, for every k , $1 \leq k \leq r$. Hence, the subgroup generated by the n elements $x_{1,1} x_{2,2} \dots x_{r,r}$, $x_{2,1} x_{3,2} \dots x_{r+1,r}, \dots, x_{i,1} x_{i+1,2} \dots x_{i+r-1,r}, \dots, x_{n,1} x_{1,2} \dots x_{r-1,r}$ is the whole group G^r . Therefore, $d(G^r) = d(G)$. On the other hand, the homomorphism $G^r \twoheadrightarrow G$ guarantees that $d(G^r) \geq d(G)$. Hence $d(G^r) = d(G)$.

Now, consider the case when $r > n$ and G is imperfect. By Lemma 2.3, the epimorphism $G^r \twoheadrightarrow G^r / (G^r)'$ implies that $d(G^r) = d(G^r / (G^r)') = r$. A similar argument as in the previous case shows that only r elements are needed to generate G^r . Namely, the

element $x_{1,1} x_{2,2} \dots x_{k,k} \dots x_{n,n}$ generates all the elements $x_{1,1}, x_{2,2}, \dots, x_{k,k}, \dots, x_{n,n}$ since these elements have mutually coprime orders. Similarly, $x_{1,2} x_{2,3} \dots x_{k,k+1} \dots x_{n,n+1}$ generates the elements $x_{1,2}, x_{2,3}, \dots, x_{k,k+1}, \dots, x_{n,n+1}$. When $3 \leq i \leq r$, the element $x_{1,i} x_{2,i+1} \dots x_{k,k+i-1} \dots x_{n,n+i-1}$ generates $x_{1,i}, x_{2,i+1}, \dots, x_{k,k+i-1}, \dots, x_{n,n+i-1}$. All indices are modulo r . Hence the subgroup generated by the r elements $x_{1,1} x_{2,2} \dots x_{n,n}, x_{1,2} x_{2,3} \dots x_{n,n+1}, \dots, x_{1,i} x_{2,i+1} \dots x_{n,n+i-1}, \dots, x_{1,r} x_{2,1} \dots x_{k,k+r-1} \dots x_{n,n+r-1}$ is the entire group G^r . Therefore $d(G^r) \leq r$, whereby $d(G^r) = r$. $\square$

2.5 Proposition. Let G be a finitely generated group with a minimal generating set consisting of elements of finite and mutually coprime orders. Let H be a finite group. If $d(G) \leq |H|$, then $d(G \sim H) \leq d(H) + 1$.

Proof. Let $\{x_1, x_2, \dots, x_n\}$ be a minimal generating set consisting of elements of finite and mutually coprime orders for G . Let the order of x_i be s_i for every i , where $1 \leq i \leq n$. Let $\{u_1, u_2, \dots, u_t\}$ be a minimal generating set of H and $H = \{\alpha_1, \alpha_2, \dots, \alpha_r\}$. Then, $G \sim H = G^r \rtimes H$. The generators of the α th copy of G^r are denoted by $\{x_{1\alpha}, x_{2\alpha}, \dots, x_{n\alpha}\}$ for $\alpha \in H$.

$$G \sim H = \left\langle \begin{array}{l} x_{1\alpha}, \dots, x_{n\alpha}; \alpha \in H \\ u_1, \dots, u_t \end{array} \left| \begin{array}{l} u_i^{-1} x_{j\alpha} u_i = x_{j, \alpha u_i} \quad \forall i \leq n, j \leq t \\ [x_{i\alpha}, x_{j\beta}] = 1 \quad \forall \alpha \neq \beta; \alpha, \beta \in H; R \end{array} \right. \right\rangle$$

where R represents the remaining relators of the group. Note that $n \sim r$. Consider $x_{1\alpha_1} x_{2\alpha_2} \dots x_{n\alpha_n}$ where the orders of $x_{i\alpha_i}$ and $x_{j\alpha_j}$ are s_i and s_j . For every $i \neq j$, s_i and s_j are coprime.

Let $s = \prod_{k \neq i}^n s_k$. Then, $\left(\prod_{k=1}^n x_{k\alpha_k} \right)^s = x_{i\alpha_i}^s$ for every $i \leq n$. Since $(s_i, s) = 1$, there exists an integer ϵ so that $(x_{i\alpha_i}^s)^\epsilon = x_{i\alpha_i}$, whereby $x_{i\alpha_i} \in \left\langle \prod_{k=1}^n x_{k\alpha_k} \right\rangle$. Since for each j , where $1 \leq j \leq n$, there exists some $h_j \in H$ such that $x_{i\alpha_i}^{h_j} = x_{i\alpha_j}$, it follows that $\left\langle \prod_{k=1}^n x_{k\alpha_k}, u_1, \dots, u_t \right\rangle = G \sim H$. Consequently, $d(G \sim H) \leq d(H) + 1$. $\square$

2.6 Remark. In Proposition 2.5, if the condition for G is weakened so that only at least 2 generators have finite coprime orders, then $d(G \sim H) \leq d(G) + d(H) - 1$.

2.7 Remark. In Proposition 2.5, if $d(G) > |H|$ then $d(G \sim H) = d(H) + \alpha$, where α is equal to the smallest integer greater than or equal to $d(G)/|H|$.

2.8 Corollary. Let G be a finitely generated imperfect group with a minimal generating set of mutually coprime finite orders. Let $G/G' \cong C_r$. If $t \geq 2$, $tm \geq d(G)$ and $(r, m) \neq 1$, then $d(G \sim C_m^t) = t+1$ where C_m^t is the direct product of t copies of C_m . If $t = 1$, then $d(G \sim C_m) = 2$ for every integer $m \geq 2$.

Proof. By Proposition 2.5, $d(G \sim C_m^t) \leq t+1$. On the other hand, Lemma 1.6 gives the epimorphism $G \sim C_m^t \twoheadrightarrow C_r \times C_m^t$ and hence the reverse inequality $d(G \sim C_m^t) \geq t+1$. In the case when $t = 1$, $d(G \sim C_m) = 2$ for every m since it is clearly nonabelian. $\square$

2.9 Proposition. Let G be a finitely generated imperfect group

which has a minimal generating set consisting of elements of finite and mutually coprime orders and $G/G' = C_n$. Let H be a finite group so that $d(G) < |H|$. If $d(C_n \sim H) = d(H) + 1$, then $d(G \sim H) = d(H) + 1$.

Proof. Lemma 1.5 gives the epimorphism $G \sim H \twoheadrightarrow C_n \sim H$. This implies that $d(G \sim H) \geq d(C_n \sim H) = d(H) + 1$. On the other hand, it follows from Proposition 2.5 that $d(G \sim H) \leq d(H) + 1$. Hence, $d(G \sim H) = d(H) + 1$. $\square$

We will now consider the direct product of 2 finitely generated groups. If the two groups are related in a special way, it is easy to obtain a bound for the minimal number of generators of the direct product. The bound depends on how many generators of one group has finite orders which are coprime to the generators of finite orders of the other group.

2.10 Proposition. Let G and H be finitely generated groups, such that r generators of G have finite orders which are coprime to the orders of r corresponding generators of H of finite orders. Then $d(G \times H) \leq d(G) + d(H) - r$.

Proof. Let $G = \langle x_1, \dots, x_n | S \rangle$, where each x_i is of order s_i for $1 \leq i \leq r$ and S is the set of relators for G . Let $H = \langle y_1, \dots, y_m | T \rangle$, where each y_i is of order t_i such that $(s_i, t_i) = 1$ for $1 \leq i \leq r$ and T is the set of relators for G . Then, the presentation of the direct product of G and H is

$$G \times H = \langle x_1, \dots, x_n; y_1, \dots, y_m \mid S, T, [x_i, y_j] = 1, 1 \leq i \leq n, 1 \leq j \leq m \rangle.$$

Then, $\langle x_1 y_1, x_2 y_2, \dots, x_r y_r; x_{r+1}, \dots, x_n; y_{r+1}, \dots, y_m \rangle$ is the group $G \times H$, since each $x_i y_i$ generates both x_i and y_i . Hence,
 $d(G) \leq d(G) + d(H) - r. \quad \square$

2.11 Remark. Let G, H and r be as in Proposition 2.10, and suppose that $d(G) \geq d(H)$ and $r = d(H)$. Then, $d(G \times H) = d(G)$. Proposition 2.10 provides us with a method for enlarging a group without increasing the minimal number of generators.

2.12 Remark. Even if G and H do not have any pair of generators of coprime finite orders, it does not necessarily mean that $d(G \times H) = d(G) + d(H)$. For example, $d(C_6 \times S_3) = 2$. Consider the presentation $C_6 \times S_3 = \langle x, u, v \mid x^6 = u^2 = v^3 = 1, uvu = v^2, xu = ux, xv = vx \rangle$. Then $\langle xu, xv \rangle$ generates the whole group since $(xv)^3(xu)^2 = x^5$ and $(x^5)^5 = x$.

For finitely generated groups, we give a criterion for when the abelianized group does not retain the same number of generators as the original group.

2.13 Proposition. Let G be a finitely generated nonabelian imperfect group. If $d(G/G') = d(G)$, then the elements of every minimal generating set of G are not of coprime finite orders.

Proof. Assume that $d(G/G') = d(G)$. Suppose that there exists a minimal generating set of G with at least 2 generators of coprime

finite orders, say x and y . Then, xG' and yG' can be generated by xyG' . Hence $d(G/G') < d(G)$ and this contradicts the assumption. Therefore, the elements of every minimal generating set of G are not of coprime finite orders. $\square$

2.14 Remark. The class of finite nilpotent groups satisfy the condition $d(G/G') = d(G)$. This will be proved in Chapter 4.

Chapter 3

THE MINIMAL NUMBERS OF GENERATORS OF SOME FINITE GROUPS

The focus of this chapter is the following finite group theoretic problem:

- (I) Given two finite groups G and H , does there exist a finite group T containing G and H so that $T = \langle G, H \rangle$ and $d(T) = d(G) + d(H)$?

Although what will be done here is far from a perlustration of the above problem, concrete constructions will be used to answer the question affirmatively for certain classes of finite groups. Not the entire collection of such groups will be presented here. In fact, some will be included in the next chapter in a more generalized setting. Depending on the situation, the construction used will usually be the direct product or wreath product. However, we will also show how the semidirect product can be used in one case.

If p and q are prime numbers such that q divides $p-1$, we will show how a semidirect product can be employed to construct an appropriate group for $C_p \times \dots \times C_p$ and C_q . This naturally raises the hope of replacing the cyclic group by an elementary abelian q -group. After a few attempts, one would start realizing that any such endeavour is futile. The futility is not surprising in light of Kovács' bound for the number of generators of finite solvable groups. In 1967 [11], Kovács proved that if each p -Sylow subgroup of a finite

solvable group can be generated by d elements, the group itself can be generated by $d+1$ elements. Let $G = C_p^s \rtimes C_q^t$. Then, G is solvable by Burnside's Theorem 0.11. By the epimorphism $G \twoheadrightarrow C_q^t$, $d(G) \leq t$. By Kovács's theorem, $d(G) \leq \max(s, t) + 1$. In particular, if $t \leq s$ then $d(G) = t$ or $t+1$. If $\min(s, t) \geq 2$, then $d(G) < s+t$. Hence, the only way for $d(G)$ to be $s+t$ is if one of the groups C_p^s or C_q^t is cyclic, i.e. $\min(s, t) = 1$. We will now show that $d(C_p^n \rtimes C_q) = n+1$ for a particular semidirect product.

3.1 Let $B = C_p^n$ and $A = C_q$ where q divides $p-1$. Consider $G = B \rtimes A$ which is given by the following presentation.

$$G = \left\langle x_1, x_2, \dots, x_n, u \mid \begin{array}{l} x_i^p = u^q = 1, x_i x_j = x_j x_i, u x_i u^{-1} = x_i^r \\ r \not\equiv 1 \pmod{p}, r^q \equiv 1 \pmod{p} \end{array} \right\rangle$$

Note that elements of the form $\prod_{i=1}^n x_i^{\alpha_i} \not\equiv 1$ have order p .

3.2 Lemma. Let p, q, r be as in 3.1. For every integer

$$\delta \in \{1, 2, \dots, q-1\}, \quad \sum_{k=0}^{q-1} r^{k\delta} \equiv 0 \pmod{p}.$$

Proof. By the assumptions $r^q \equiv 1 \pmod{p}$ and $r \not\equiv 1 \pmod{p}$, it follows that $r^\delta \not\equiv 1 \pmod{p}$ if $1 \leq \delta \leq q-1$ since q is a prime number. Then, $r^{q\delta} \equiv 1 \pmod{p}$. Therefore, $0 \equiv r^{q\delta} - 1 = (r^\delta - 1)(1 + r^\delta + \dots + r^{(q-1)\delta})$. Since $r^\delta \not\equiv 1 \pmod{p}$, $1 + r^\delta + \dots + r^{(q-1)\delta} = \sum_{k=0}^{q-1} r^{k\delta} \equiv 0 \pmod{p}$. $\square$

3.3 Corollary. Let $x_1, \dots, x_n$ and u be as in 3.1. For every integer $\delta \in \{1, \dots, q-1\}$, $\left(\prod_{i=1}^n x_i^{\alpha_i} \right) u^\delta$ has order q .

Proof. The q th power of $\left(\prod_{i=1}^n x_i^{\alpha_i}\right)u^\delta$ is $\left(\left(\prod_{i=1}^n x_i^{\alpha_i}\right)u^\delta\right)^q = \left(\prod_{i=1}^n x_i^{\alpha_i}\right)^{\sum_{k=0}^{q-1} r^{k\delta}} u^{\sum_{k=0}^{q-1} r^{k\delta} \delta}$. By Lemma 3.2, $\sum_{k=0}^{q-1} r^{k\delta} \equiv 0 \pmod{p}$, whereby $\left(\prod_{i=1}^n x_i^{\alpha_i}\right)u^\delta$ has order q . $\square$

3.4 Proposition. If G is the group described in 3.1, then

$$d(G) = n+1.$$

Proof. Clearly, $d(G) \leq n+1$. Let B be a set of n elements of G . If B consists of only elements of order p , then by Corollary 3.3, $\langle B \rangle \leq B$ and hence $\langle B \rangle \neq G$. Suppose that B consists of r elements of order p and $n-r$ elements of order q , where r is less than n . Let $g_1, g_2, \dots, g_r$ be the elements of order p and $g_{r+1}, g_{r+2}, \dots, g_n$ be the elements of order q . The element g_n is of the form $\prod_{i=1}^n x_i^{\beta_i} u^\delta$, where $\delta \in \{1, 2, \dots, q-1\}$. Since u^δ is a generator for C_q , we may assume that $\delta = 1$. Then, $g_n = \prod_{i=1}^n x_i^{\beta_i} u$. For every m such that $r+1 \leq m \leq n-1$, $g_m = \left(\prod_{i=1}^n x_i^{\gamma_i^{(m)}}\right)u^{\epsilon_m}$ where

$\epsilon_m \in \{1, 2, \dots, q-1\}$. Transform the set B into the set B' , replacing

g_m by g'_m for every m which exceeds r . Let $g'_n = g_n^{-1}$ and

$$g'_m (g_n^{-1})^{\epsilon_m} = \prod_{i=1}^n x_i^{\alpha_i^{(m)}}. \text{ Then, } B' = \{g_1, g_2, \dots, g_r, g'_{r+1}, g'_{r+2}, \dots, g'_n\}.$$

The transformation from B to B' is a Nielsen transformation and

$\langle B' \rangle = \langle B \rangle$ by Proposition 0.15.

Relabel B' by letting $a_1 = g_1, a_2 = g_2, \dots, a_r = g_r, a_{r+1} = g'_{r+1}, a_{r+2} = g'_{r+2}, \dots, a_{n-1} = g'_{n-1}, b = g'_n$. Then, $B' = \{a_1, a_2, \dots,$

$a_{n-1}, b\}$ where $a_1, \dots, a_{n-1}$ are elements of order p and b is an element of order q . Then,

$$\begin{aligned}
 ba_m b^{-1} &= ba_m b^{q-1} \\
 &= \left(\prod_{i=1}^n x_i^{\beta_i} \right) u \left(\prod_{i=1}^n x_i^{\alpha_i^{(m)}} \right) \left(\left(\prod_{i=1}^n x_i^{\beta_i} \right) u \right)^{q-1} \\
 &= \left(\prod_{i=1}^n x_i^{\beta_i} \right) \left(\prod_{i=1}^n x_i^{\alpha_i^{(m)} r} \right) u \left(\prod_{i=1}^n x_i^{\beta_i \left(\sum_{k=0}^{q-2} r^k \right)} \right) u^{q-1} \\
 &= \left(\prod_{i=1}^n x_i^{\beta_i} \right) \left(\prod_{i=1}^n x_i^{\alpha_i^{(m)} r} \right) \prod_{i=1}^n x_i^{\beta_i r \left(\sum_{k=0}^{q-2} r^k \right)} \\
 &= \left(\prod_{i=1}^n x_i^{\alpha_i^{(m)} r} \right) \prod_{i=1}^n x_i^{\beta_i + \beta_i r \left(\sum_{k=0}^{q-2} r^k \right)} \\
 &= \left(\prod_{i=1}^n x_i^{\alpha_i^{(m)} r} \right) \prod_{i=1}^n x_i^{\beta_i \left(1 + \sum_{k=1}^{q-1} r^k \right)} \\
 &= \left(\prod_{i=1}^n x_i^{\alpha_i^{(m)} r} \right) \prod_{i=1}^n x_i^{\beta_i \left(\sum_{k=0}^{q-1} r^k \right)}
 \end{aligned}$$

which is equal to $\prod_{i=1}^n x_i^{\alpha_i^{(m)} r}$ by Lemma 3.2. Since $\prod_{i=1}^n x_i^{\alpha_i^{(m)} r} = a_m^r$,

$$ba_m b^{-1} = a_m^r.$$

Since $a_m^p = 1$, $b^q = 1$, $a_m a_\ell = a_\ell a_m$ and $ba_m b^{-i} = a_m^r$ for every m and ℓ , $1 \leq m \leq n-1$, $1 \leq \ell \leq n-1$, $\langle \beta^i \rangle = \langle \beta \rangle$ is a homomorphic image of the group $\bar{G} = \langle a_1, \dots, a_{n-1}, b \mid a_m^p = b^q = 1, a_m a_\ell = a_\ell a_m, ba_m b^{-1} = a_m^r \rangle$.

$\bar{G}$ is isomorphic to $C_p^{n-1} \rtimes C_q$ and $\bar{G}$ has $p^{n-1}q$ elements. Hence, $|\langle \beta \rangle| \leq p^{n-1}q < |G| = p^n q$. Consequently, $\langle \beta \rangle$ is a proper subgroup of G . $\square$

3.5 Proposition. Consider the dihedral group of order $2m$,

$$D_m = \langle u, v \mid u^2 = v^m = (uv)^2 = 1 \rangle. \text{ Then,}$$

$$d(\mathbb{Z} \times D_m) = \begin{cases} 2 & \text{if } m \text{ is odd,} \\ 3 & \text{if } m \text{ is even,} \end{cases}$$

$$\text{and } d(C_n \times D_m) = \begin{cases} 2 & \text{if } m \text{ is odd,} \\ 2 & \text{if } m \text{ is even and } n \text{ is odd,} \\ 3 & \text{if } m \text{ is even and } n \text{ is even.} \end{cases}$$

Proof. Firstly, $\mathbb{Z} \times D_m = \langle x, u, v \mid u^2 = v^m = (uv)^2 = [u, x] = [v, x] = 1 \rangle$.

Consider the two elements xv and $x^{-2}u$ of $\mathbb{Z} \times D_m$. Then, $(xv)(x^{-2}u)(xv) = vuv = u$, $(x^{-2}u)u = x^{-2}$ and $x^{-2}(xv)^2 = v^2$. Now, v^2 generates v if m is odd. Therefore, $\langle xv, x^{-2}u \rangle = \mathbb{Z} \times D_m$ if m is odd. So, $d(\mathbb{Z} \times D_m) = 2$ if m is odd. Moreover the epimorphism from $\mathbb{Z} \times D_m$ onto $C_n \times D_m$ induced by the epimorphism from $\mathbb{Z}$ onto C_n implies that $d(\mathbb{Z} \times D_m) \geq d(C_n \times D_m)$. Since $d(C_n \times D_m) \geq 2$, we have $d(C_n \times D_m) = 2$ if m is odd as well.

Now, let m and n be even positive integers. Since m is even, $D_m / (D_m)' \cong C_2 \times C_2$, whereby there exists an epimorphism from D_m onto $C_2 \times C_2$ which induces an epimorphism from $C_n \times D_m$ onto $C_n \times C_2 \times C_2$. Then, $d(C_n \times D_m) \geq d(C_n \times C_2 \times C_2)$ and $d(C_n \times C_2 \times C_2) = 3$ since n is even. Since it is clear that $d(C_n \times C_m) < 3$, we

have $d(C_n \times D_m) = 3$ if m and n are both even. The epimorphism from $\mathbb{Z} \times D_m$ onto $C_n \times D_m$ implies that $d(\mathbb{Z} \times D_m) \geq d(C_n \times D_m)$ and $d(\mathbb{Z} \times D_m) = 3$ if m is even.

Finally, let m be an even integer and n be an odd integer. Then, consider $C_n \times D_m = \langle y, u, v \mid y^n = u^2 = v^m = (uv)^2 = [u, y] = [v, y] = 1 \rangle$. Since n is odd, y and u have coprime orders and $\langle y, u \rangle = C_n \times D_m$. Hence, $d(C_n \times D_m) \leq 2$. Since there is an epimorphism from $C_n \times D_m$ onto D_m , it is clear that $d(C_n \times D_m) \geq 2$. Therefore, $d(C_n \times D_m) = 2$. $\square$

3.6 Theorem. Let $C_n = \langle x \mid x^n = 1 \rangle$ and $D_m = \langle u, v \mid u^2 = v^m = (uv)^2 = 1 \rangle$. If $G = C_n \sim D_m$, then $d(G) = 3$ if $(m, n) \neq 1$.

Proof. If $G = C_n \sim D_m$, then $G \cong K \times D_m$ where $K = C_n^{2m}$. If we denote the generator of the copy of C_n corresponding to r by x_r , $r \in D_m$, we have the following presentation for G :

$$G = \left\langle \begin{array}{l} x_r, u, v \\ (r \in D_m) \end{array} \mid \begin{array}{l} x_r^n = u^2 = v^m = (uv)^2 = [x_r, x_t] = 1, ux_r u = x_{ru}, \\ v^{-1} x_r v = x_{rv}; r, t \in D_m \end{array} \right\rangle$$

There is a natural epimorphism $C_n \sim D_m \twoheadrightarrow C_p \sim D_m$, induced by the epimorphism $C_n \twoheadrightarrow C_p$, according to Lemma 1.5. Hence, we may assume that n is prime. Let $n = p$ and $G = C_p \sim D_m$. Then, $K = C_p^{2m}$ is a vector space of dimension $2m$ over $\mathbb{F}_p$. Clearly, $d(G) = 3$. For example, $G = \langle x_1, u, v \rangle$. Consider two elements a and b in G .

Let H be the subgroup generated by a and b . We will demonstrate that H is not all of G , if p divides m , by showing that

$H \cap K \neq K$ or $\dim_{\mathbb{P}}(H \cap K) \leq 2m-1$. It suffices to consider the case when $a = yv$ and $b = xu$, where $x, y \in K$. All other possible cases can be reduced to this case by a Nielsen transformation, as we are going to show.

Case 1: $a = yv$, $b = xu$.

Case 2: $a = yv^i$, $b = xu$; $i \neq 1$ and $(i, m) = 1$.

This case is equivalent to Case 1.

Case 3: $a = yv^i$, $b = xu$; $i \neq 1$ and $(i, m) \neq 1$.

If $(j, m) = 1$, then $v^j \notin H$. Hence, H is not all of G .

Case 4: $a = yuv^i$, $b = xu$.

By Proposition 0.15, $\langle a, b \rangle = \langle ba, b \rangle$ and $\langle ba, b \rangle = \langle zv^i, xu \rangle$, where $z \in K$. This case is equivalent to Case 1, 2 or 3.

Case 5: $a = yv^j$, $b = xuv^i$.

If there exists an integer s so that $i+sj \equiv 0 \pmod{m}$, then $\langle a, b \rangle = \langle a, ba^s \rangle = \langle yv^j, zu \rangle$ for some $z \in K$ by Proposition 0.15. Thus, this is equivalent to Case 1, 2 or 3. If there is no integer s satisfying the condition $i+sj \equiv 0 \pmod{m}$, we will show that H is not all of G .

Since uv^i has order 2, any word in $\langle a, b \rangle$ can be expressed in the form $zw = zv^{jk_t}(uv^i) \dots v^{jk_4}(uv^i) v^{jk_3}(uv^i) v^{jk_2}(uv^i) v^{jk_1}$, where $z \in K$. Let r be the number of uv^i 's in w . If r is even, u does not appear in w , implying that it is impossible to generate u .

Now, consider the case when r is odd. Let w_r denote w when uv^i occurs r times. Let $r = 1$. If $t = r$, then $w_1 = uv^i v^{jk_1} =$

uv^{i+jk_1} . If $t = r+1$, then $w_1 = v^{jk_2} uv^{i+jk_1} = uv^{i+j(k_1-k_2)}$. We will prove the following formula by induction.

$$w_r = \begin{cases} uv^{i+j(k_1+k_3+\dots+k_t)-j(k_2+k_4+\dots+k_{t-1})}, & \text{if } t = r, \\ uv^{i+j(k_1+k_3+\dots+k_{t-1})-j(k_2+k_4+\dots+k_t)}, & \text{if } t = r+1. \end{cases} \quad (*)$$

Assume that (*) holds for w_{r-2} . If $t = r$, then

$$\begin{aligned} w_r &= (uv^i) v^{jk_r} (uv^i) v^{jk_{r-1}} w_{r-2} \\ &= v^{-i-jk_r+i+jk_{r-1}} w_{r-2} \\ &= v^{jk_{r-1}-jk_r} w_{r-2} \\ &= v^{jk_{r-1}-jk_r} uv^{i+j(k_1+k_3+\dots+k_{r-2})-j(k_2+k_4+\dots+k_{r-3})} \\ &= uv^{-jk_{r-1}+jk_r} uv^{i+j(k_1+k_3+\dots+k_{r-2})-j(k_2+k_4+\dots+k_{r-3})} \\ &= uv^{i+j(k_1+k_3+\dots+k_r)-j(k_2+k_4+\dots+k_{r-1})}. \end{aligned}$$

If $t = r+1$, then

$$\begin{aligned} w_r &= v^{jk_{r+1}} uv^{i+j(k_1+k_3+\dots+k_r)-j(k_2+k_4+\dots+k_{r-1})} \\ &= uv^{i+j(k_1+k_3+\dots+k_r)-j(k_2+k_4+\dots+k_{r+1})}. \end{aligned}$$

Consequently, (*) holds for every r . From (*) and the assumption that there is no s so that $i+sj \equiv 0 \pmod{m}$, it is impossible to generate u .

Case 6: $a = yuv^i$, $b = xuv^j$.

By Proposition 0.15, $\langle a, b \rangle = \langle b, ba \rangle$. But $\langle b, ba \rangle = \langle xuv^j, cv^{i-j} \rangle$ where c is an element of K . This case is then equivalent to Case 5.

Hence, from now on we may assume that we are in Case 1. Let $a = yv$ and $b = xu$ where $x, y \in K$. Any element in H can be expressed in the form $a^{\gamma_1} b^{\delta_1} \dots a^{\gamma_i} b^{\delta_i}$ where $\gamma_j, \delta_j \in \mathbb{Z}$. Then, $ba = xuyv = xy^u uv = y^u xuv = y^u xv^{-1}u = (y^u v^{-1})(xv^{-1}u) = a^u(xv^{-1}u)$.

Note that

$$(a^u)^i = (y^u v^{-1})^i = y^u y^{uv} \dots y^{uv^{i-1}} v^{-i} = (a^i)^u.$$

$$\text{Then, } ba^i = xu(yv^{v^{-1}} y^{v^{-2}} \dots y^{v^{-i+1}} v^i)$$

$$\begin{aligned} &= xy^u y^{uv} \dots y^{uv^{i-1}} v^i \\ &= y^u y^{uv} \dots y^{uv^{i-1}} v^{-i} x v^i u \\ &= (a^u)^i (x v^{-i} u), \end{aligned}$$

$$\text{and } b(a^u)^i = xu(y^u y^{uv} \dots y^{uv^{i-1}} v^{-i})$$

$$\begin{aligned} &= yy^{v^{-1}} \dots y^{v^{-i+1}} xv^i u \\ &= yy^{v^{-1}} \dots y^{v^{-i+1}} v^i x v^i u \\ &= a^i (x v^i u). \end{aligned}$$

Thus we have

$$ba^i = (a^u)^i (x v^{-i} u) \quad (3.3.1)$$

$$\text{and} \quad b(a^u)^i = a^i(x^{v^i}u). \quad (3.3.2)$$

Define $b_0 = b$, $b_1 = x^v u, \dots, b_k = x^{v^k} u, \dots, b_{m-1} = x^{v^{m-1}} u$, where $0 \leq k \leq m-1$. We will explain how an arbitrary element in H , $a^{\gamma_1 \delta_1} b^{\gamma_2 \delta_2} \dots a^{\gamma_m \delta_m} b^{\gamma_{m+1} \delta_{m+1}}$, can be expressed in the form gh where $g \in \langle a, a^u \rangle = A$ and $h \in \langle b_0, b_1, \dots, b_{m-1} \rangle = H_1$. This can be achieved by using the formulas 3.3.1 and 3.3.2 recursively, starting from the right hand side of the word. We will show the first few steps.

$w = a^{\gamma_1 \delta_1} b^{\gamma_2 \delta_2} \dots a^{\gamma_m \delta_m} b^{\gamma_{m+1} \delta_{m+1}}$ is equal to $a^{\gamma_1 \delta_1} b^{\gamma_2 \delta_2} \dots a^{\gamma_m \delta_m} (b^{\gamma_{m+1} \delta_{m+1}} a^{\gamma_m \delta_m}) b^{\gamma_{m-1} \delta_{m-1}}$ where $g_1 \in A$ and $h_2 \in H_1$. $b^{\gamma_{m+1} \delta_{m+1}} a^{\gamma_m \delta_m} = g_1 h_2$ is obtained by applying 3.3.1 and 3.3.2 recursively to $b^{\gamma_{m+1} \delta_{m+1}} a^{\gamma_m \delta_m}$. Next, apply 3.3.1 and 3.3.2 recursively to $b^{\gamma_{m+1} \delta_{m+1}} a^{\gamma_m \delta_m} g_1$ until it is of the form $g_2 h_3$ where $g_2 \in A$ and $h_3 \in H_1$. Then, $w = a^{\gamma_1 \delta_1} b^{\gamma_2 \delta_2} \dots a^{\gamma_m \delta_m} (g_2 h_3) h_2 b^{\gamma_{m-1} \delta_{m-1}}$. Continue this process until all the elements in A have been collected to the left and all the elements in H_1 have been collected to the right.

Apply a Nielsen transformation to the generating set of H_1 , $\{b_0, b_1, \dots, b_{m-1}\}$ as follows: For every i such that $1 \leq i \leq m-1$, replace $x^{v^i} u$ by $(xu)(x^{v^i} u)$. The subgroup generated by the resulting set is $\langle xu, xx^{uv^{m-1}}, xx^{uv^{m-2}}, \dots, xx^{uv} \rangle = H_1$ by Proposition 0.15. Let $d_1 = xx^{uv^{m-1}}$, $d_2 = xx^{uv^{m-2}}$, $\dots$, and $d_{m-1} = xx^{uv}$. An element in H_1 can be written as a word of the form

$$(d_1^{\delta_{1,1}} d_2^{\delta_{2,1}} \dots d_{m-1}^{\delta_{m-1,1}} b^{\beta_1}) \dots (d_1^{\delta_{1,i}} d_2^{\delta_{2,i}} \dots d_{m-1}^{\delta_{m-1,i}} b^{\beta_i}) = db^{\beta},$$

where $\langle b \rangle \cap K = \langle xx^u \rangle$ and d is contained in

$$\langle xx^{uv^{m-1}}, xx^{uv^{m-2}}, \dots, xx^{uv}; x^u x^v, x^u x^{v^2}, \dots, x^u x^{v^{m-1}} \rangle. \text{ Hence,}$$

$$H_1 \cap K = \langle xx^u, xx^r, x^u x^t \mid r \in \{uv^i \mid i=1, \dots, m-1\}, t \in \{v^i \mid i=1, \dots, m-1\} \rangle$$

On the other hand, $A = \langle a, a^u \rangle = \langle yv, y^u v^{m-1} \rangle = \langle yv, (yv)(y^u v^{m-1}) \rangle$
 $= \langle yv, yy^{uv^{m-1}} \rangle$ by Proposition 0.15. Let $c = yy^{uv^{m-1}}$. An element
of A can be written as a word of the form $c^{\gamma_1 \delta_1} \dots c^{\gamma_i \delta_i} = fa^q$,
where $f \in \langle c^{v^j} \mid j=0, 1, \dots, m-1 \rangle = \langle yy^{uv^{m-1}}, y^v y^u, \dots, y^{v^{m-1}} y^{uv^{m-2}} \rangle$.

Note that $\langle a \rangle \cap K = \langle yy^v y^{v^2} \dots y^{v^{m-1}} \rangle$.

If $g \in A$ and $h \in H_1$, gh is in K iff g and h are both
in K . Hence, $H \cap K$ is contained in the set

$$S = \left\langle xx^r, x^u x^t, y^{vk} y^{uk}, yy^v \dots y^{v^{m-1}} \mid \begin{array}{l} r \in \{uv^i \mid i=0, \dots, m-1\} \\ t \in \{v^i \mid i=1, \dots, m-1\} \\ k \in \{v^i \mid i=0, \dots, m-1\} \end{array} \right\rangle.$$

We will prove that $H \cap K$ spans a subspace of K of dimension at
most $2m-1$ if p divides m . It suffices to show that the subspace
of K , spanned by the $3m$ elements in S , has dimension at most $2m-1$
if p divides m .

Suppose that x and y are as follows:

$$x = \begin{matrix} \alpha_1 & \alpha_v & & \alpha_{v^{m-1}} & \alpha_u & \alpha_{uv} & & \alpha_{uv^{m-1}} \\ x_1 & x_v & \dots & x_{v^{m-1}} & x_u & x_{uv} & \dots & x_{uv^{m-1}} \end{matrix}$$

and

$$y = \begin{matrix} \beta_1 & \beta_v & & \beta_{v^{m-1}} & \beta_u & \beta_{uv} & & \beta_{uv^{m-1}} \\ x_1 & x_v & \dots & x_{v^{m-1}} & x_u & x_{uv} & \dots & x_{uv^{m-1}} \end{matrix}.$$

Now, consider the $3m \times 2m$ matrix consisting of $2m$ columns

representing the exponents of $x_1, x_v, \dots, x_{v^{m-1}}, x_u, x_{uv}, \dots, x_{uv^{m-1}}$ and $3m$ rows corresponding to the elements in the set S .

$x_1 x_v \dots x_{v^{m-1}}$	$x_u x_{uv} \dots x_{uv^{m-1}}$	
		m rows represent xx^r
		where $r \in \{uv^i \mid i=0, \dots, m-1\}$
		m-1 rows represent $x^u x^t$
		where $t \in \{v^i \mid i=1, \dots, m-1\}$
		m rows represent $y^{vk} y^{uk}$
		where $k \in \{v^i \mid i=0, \dots, m-1\}$
		1 row represents $yy^v y^{v^2} \dots y^{v^{m-1}}$

Let $s = \sum_{r \in D_m} \alpha_r$ and $t = \sum_{r \in D_m} \beta_r$. If $r \in \{uv^i \mid i=0, \dots, m-1\}$,

then $\{v^i(r) \mid i=0, \dots, m-1\} = \{uv^i \mid i=0, \dots, m-1\}$ and $\{uv^i(r) \mid i=0, \dots, m-1\} = \{v^i \mid i=0, \dots, m-1\}$. So, the sum of the first m columns and the sum of the last m columns of xx^r are both s .

If $t \in \{v^i \mid i=1, \dots, m-1\}$, then $\{v^i(t) \mid i=0, \dots, m-1\} = \{v^i \mid i=0, \dots, m-1\}$ and $\{uv^i(t) \mid i=0, \dots, m-1\} = \{uv^i \mid i=0, \dots, m-1\}$, $\{v^i(u) \mid i=0, \dots, m-1\} = \{uv^i \mid i=0, \dots, m-1\}$ and $\{uv^i(u) \mid i=0, \dots, m-1\} = \{v^i \mid i=0, \dots, m-1\}$. It follows that the sum of the first m columns and the sum of the last m columns of $x^u x^t$ are both s .

If $vk \in \{v^i \mid i=0, \dots, m-1\}$ and $uk \in \{uv^i \mid i=0, \dots, m-1\}$, then $\{v^i(vk) \mid i=0, \dots, m-1\} = \{v^i \mid i=0, \dots, m-1\}$, $\{uv^i(vk) \mid i=0, \dots, m-1\} = \{uv^i \mid i=0, \dots, m-1\}$, $\{v^i(uk) \mid i=0, \dots, m-1\} = \{uv^i \mid i=0, \dots, m-1\}$, and

$\{uv^i(uk) \mid i=0, \dots, m-1\} = \{v^i \mid i=0, \dots, m-1\}$. Hence, the sum of the first m columns and the sum of the last m columns of $y^{vk} y^{uk}$ are both equal to t .

Finally, the sum of the first m columns and the sum of the last m columns of $yy^v \dots y^{v^{m-1}}$ are $m(\beta_1 + \beta_v + \dots + \beta_{v^{m-1}})$ and $m(\beta_u + \beta_{uv} + \dots + \beta_{uv^{m-1}})$, respectively. Therefore, the sum of the first m columns and the sum of the last m columns of the matrix are

$$\underbrace{(s, \dots, s; \quad t, \dots, t; \quad m(\beta_1 + \dots + \beta_{v^{m-1}}))}_{2m-1 \text{ copies} \quad m \text{ copies}}^T \text{ and}$$

$$\underbrace{(s, \dots, s; \quad t, \dots, t; \quad m(\beta_u + \dots + \beta_{uv^{m-1}}))}_{2m-1 \text{ copies} \quad m \text{ copies}}^T, \text{ respectively.}$$

In particular, if p divides m , these two vectors are equal and so $\dim_{\mathbb{F}_p}(H \cap K) \leq 2m-1$. Hence H is not all of G and $d(G) = 3$. $\square$

The following result, which follows from Theorem 5.17 and Theorem 5.20 of Gruenberg, is a consequence of Theorem 3.6 as well.

3.7 Corollary. $d(\mathbb{Z} \wr D_m) = 3$.

Proof. Let n be a positive integer such that $(n, m) \neq 1$. The epimorphism from $\mathbb{Z} \wr D_m$ onto $C_n \wr D_m$, induced by the epimorphism from $\mathbb{Z}$ onto C_n , implies that $d(\mathbb{Z} \wr D_m) \geq d(C_n \wr D_m)$. By Theorem 3.6, $d(\mathbb{Z} \wr D_m) \leq 3$. Since it is clear that $d(\mathbb{Z} \wr D_m) \geq 3$, it follows that $d(\mathbb{Z} \wr D_m) = 3$. $\square$

3.8 Corollary. $d(D_m \sim D_n) = \begin{cases} 4 & \text{if } m \text{ is even and } n \text{ is even,} \\ 3 & \text{if } m \text{ is odd and } n \text{ is even.} \end{cases}$

Proof. Clearly, $d(D_m \sim D_n) \leq 4$. If m and n are both even, then $D_m/(D_m)' \cong C_2 \times C_2$ and $D_n/(D_n)' \cong C_2 \times C_2$. By Lemma 1.6, there exists an epimorphism from $D_m \sim D_n$ onto $D_m/(D_m)' \times D_n/(D_n)'$. Hence, $d(D_m \sim D_n) \geq d(D_m/(D_m)' \times D_n/(D_n)') = d(C_2^4) = 4$. Therefore, $d(D_m \sim D_n) = 4$ if m is even and n is even.

Now, consider the case when m is odd and n is even. By Proposition 2.5, $d(D_m \sim D_n) \leq 3$. Moreover, Lemma 1.5 gives the epimorphism $D_m \sim D_n \twoheadrightarrow C_2 \sim D_n$ induced by the epimorphism $D_m \twoheadrightarrow C_2$. Hence, $d(D_m \sim D_n) \geq d(C_2 \sim D_n) = 3$ by Theorem 3.6. Therefore $d(D_m \sim D_n) = 3$, if m is odd and n is even. $\square$

3.9 Corollary. Let G be a finitely generated imperfect group which has a minimal generating set consisting of elements of finite and mutually coprime orders and $G/G' \cong C_n$. If $(m, n) \neq 1$ and $d(G) \leq 2m$, then $d(G \sim D_m) = 3$.

Proof. By Proposition 1.5, the epimorphism $G \sim D_m \twoheadrightarrow C_n \sim D_m$ is induced by the epimorphism $G \twoheadrightarrow C_n$. Hence, $d(G \sim D_m) \geq d(C_n \sim D_m)$. Moreover, $d(C_n \sim D_m) = 3$ if $(m, n) \neq 1$ by Theorem 3.6. So, $d(G \sim D_m) \geq 3$. It follows from Proposition 2.5 that $d(G \sim D_m) \leq 3$. Consequently, $d(G \sim D_m) = 3$ if $(m, n) \neq 1$. $\square$

3.10 Corollary. Consider a finite group H which can be generated by x_1 and x_2 with orders e_1 and e_2 , respectively. If one of the following conditions hold:

$$(i) \quad (e_1, 2) = 1 \quad \text{and} \quad (e_2, m) = 1;$$

$$(ii) \quad (e_1, m) = 1 \quad \text{and} \quad (e_2, 2) = 1;$$

then $d(C_n \sim (D_m \times H)) = d(D_m \times H) + 1 = 3$ if $(n, m) \neq 1$.

Proof. Either condition (i) or (ii) would guarantee that $d(D_m \times H) = 2$ by Proposition 2.10. Clearly, $d(C_n \sim (D_m \times H)) \leq 3$. By Lemma 1.7, the epimorphism $D_m \times H \twoheadrightarrow D_m$ induces the epimorphism $C_n \sim (D_m \times H) \twoheadrightarrow C_n \sim D_m$. Hence, $d(C_n \sim (D_m \times H)) \geq d(C_n \sim D_m)$. If $(n, m) \neq 1$, then $d(C_n \sim D_m) = 3$ by Theorem 3.6. It follows that $d(C_n \sim (D_m \times H)) = 3$ if $(m, n) \neq 1$. $\square$

3.11 Corollary. If m is an even positive integer, consider the dicyclic group of order $2m$, $Q_m = \langle u, x \mid x^m = 1, x^{m/2} = u^2, u^{-1}xu = x^{-1} \rangle$. Then, $d(C_n \sim Q_m) = 3$ if $(n, m/2) \neq 1$.

Proof. If $m/2$ is even, then $Q_m/(Q_m)' \cong C_2 \times C_2$. Hence, the epimorphism $Q_m \twoheadrightarrow C_2 \times C_2$ induces the epimorphism $C_n \sim Q_m \twoheadrightarrow C_n \times C_2 \times C_2$ by Lemma 1.6. Hence, $d(C_n \sim Q_m) \geq d(C_n \times C_2 \times C_2) = 3$ when n is even. Since it is clear that $d(C_n \sim Q_m) \leq 3$, it follows that $d(C_n \sim Q_m) = 3$ if both n and $m/2$ are even.

Now consider the case when $m/2$ is odd. Clearly, $d(C_n \sim Q_m) = 3$. $Q_m \cong C_{m/2} \times C_4 = \langle u, v \mid v^{m/2} = u^4 = 1, u^{-1}vu = v^{-1} \rangle$. By adding the relation $u^2 = 1$ to this presentation, the dihedral group of order m , $D_{m/2}$ can be realized as a homomorphic image of Q_m . This homomorphism induces the epimorphism $C_n \sim Q_m \twoheadrightarrow C_n \sim D_{m/2}$ by Lemma 1.7. Since $d(C_n \sim D_{m/2}) = 3$ if $(n, m/2) \neq 1$ by Theorem 3.6 and $d(C_n \sim Q_m) =$

$d(C_n \sim D_{m/2})$, it follows that $d(C_n \sim Q_m) \geq 3$. Consequently,

$$d(C_n \sim Q_m) = 3 \text{ if } (n, m/2) \neq 1. \quad \square$$

$$3.12 \text{ Corollary. } d(Q_m \sim Q_n) = \begin{cases} 4 & \text{if } m/2 \text{ and } n/2 \text{ are both even,} \\ 3 & \text{if } m/2 \text{ is odd and } n/2 \text{ is even.} \end{cases}$$

Proof. It is clear that $d(Q_m \sim Q_n) \leq 4$ for all positive even integers m and n . If $m/2$ and $n/2$ are both even, then

$Q_m/(Q_m)' \cong C_2 \times C_2$ and $Q_n/(Q_n)' \cong C_2 \times C_2$. By Lemma 1.6, there exists an epimorphism $Q_m \sim Q_n \twoheadrightarrow Q_m/(Q_m)' \times Q_n/(Q_n)'$, whereby $d(Q_m \sim Q_n) \geq d(C_2^4) = 4$. Hence, $d(Q_m \sim Q_n) = 4$ if $m/2$ and $n/2$ are both even.

Now, consider the case when $m/2$ is odd and $n/2$ is even. Then, $Q_m \cong C_{m/2} \times C_4 = \langle u, v \mid v^{m/2} = u^4 = 1, u^{-1}vu = v^{-1} \rangle$. This means that there is a minimal generating set of Q_m which has generators of coprime orders. By Proposition 2.5, $d(Q_m \sim Q_n) \leq 3$. Moreover, the epimorphism $Q_m \twoheadrightarrow C_4$ induces the epimorphism $Q_m \sim Q_n \twoheadrightarrow C_4 \sim Q_n$ by Lemma 1.5. Hence, $d(Q_m \sim Q_n) \geq d(C_4 \sim Q_n) = 3$ if $(m/2, n/2) \neq 1$ by Theorem 3.6. Hence, $d(Q_m \sim Q_n) = 3$ if $m/2$ is odd and $n/2$ is even. $\square$

3.13 Corollary. Consider a finite group H which can be generated by x_1 and x_2 with orders e_1 and e_2 , respectively. If one of the following conditions hold:

$$(i) \quad (e_1, 4) = 1 \text{ and } (e_2, m) = 1;$$

$$(ii) \quad (e_1, m) = 1 \text{ and } (e_2, 4) = 1;$$

then $d(C_n \sim (Q_m \times H)) = 3$ if $(n, m/2) \neq 1$.

Proof. By Proposition 2.10, either condition (i) of (ii) would imply that $d(Q_m \times H) = 2$. Clearly, $d(C_n \sim (Q_m \times H)) \sim 3$. By Lemma 1.7, the epimorphism $Q_m \times H \twoheadrightarrow Q_m$ induces the epimorphism $C_n \sim (Q_m \times H) \twoheadrightarrow C_n \sim Q_m$. Hence, $d(C_n \sim (Q_m \times H)) \geq d(C_n \sim Q_m)$. If $(n, m/2) \neq 1$, it follows from Corollary 3.11 that $d(C_n \sim Q_m) = 3$. Thus, $d(C_n \sim (Q_m \times H)) \geq 3$ and consequently $d(C_n \sim (Q_m \times H)) = 3$. ||

The following result, which follows from Theorem 5.17 and Theorem 5.20 of Gruenberg, is a consequence of Corollary 3.11 as well.

3.14 Corollary $d(\mathbb{Z} \sim Q_m) = 3$.

Proof. Let n be a positive integer such that $(n, m/2) \neq 1$. The epimorphism from $\mathbb{Z} \sim Q_m$ onto $C_n \sim Q_m$, induced by the epimorphism $\mathbb{Z} \twoheadrightarrow C_n$, implies that $d(\mathbb{Z} \sim Q_m) \geq d(C_n \sim Q_m)$. By Corollary 3.11, $d(\mathbb{Z} \sim Q_m) \geq 3$. Since it is obvious that $d(\mathbb{Z} \sim Q_m) \leq 3$, $d(\mathbb{Z} \sim Q_m) = 3$. ||

3.15 Definition. Two finitely generated abelian groups A and B are *coprime* if their canonical decompositions are related as follows:

$$A \cong C_{m_1} \times C_{m_2} \times \dots \times C_{m_s} \times \mathbb{Z}^\alpha, \quad m_i \mid m_{i+1} \text{ for every } i, 1 \leq i \leq s-1;$$

$$B \cong C_{n_1} \times C_{n_2} \times \dots \times C_{n_t} \times \mathbb{Z}^\beta, \quad n_i \mid n_{j+1} \text{ for every } j, 1 \leq j \leq t-1;$$

$$\text{and } (m_1, n_1) = 1.$$

3.16 Lemma. If $G_1, G_2, \dots, G_n$ are finite groups, then there exists an epimorphism from $G_1 \circ G_2 \circ \dots \circ G_n$ onto $\prod_{i=1}^n G_i / (G_i)'$. (Recall that $A \circ B$ denotes the wreath or direct product of A and B and was defined in 1.4.)

Proof. By Lemma 1.6, there exists an epimorphism $G_1 \sim G_2 \twoheadrightarrow$

$G_1/(G_1)' \times G_2/(G_2)'$. Then, by Lemma 1.5, there exists an epimorphism from $G_1 \circ G_2 \circ G_3$ onto $(G_1/(G_1)' \times G_2/(G_2)') \circ G_3$. By Lemma 1.6, there is an epimorphism from $(G_1/(G_1)' \times G_2/(G_2)') \circ G_3$ onto $\prod_{i=1}^3 G_i/(G_i)'$. Assume that there exists an epimorphism $G_1 \circ G_2 \circ \dots \circ G_{n-1} \twoheadrightarrow \prod_{i=1}^{n-1} G_i/(G_i)'$. By Lemma 1.5 and the assumption, there exists an epimorphism from $G_1 \circ G_2 \circ \dots \circ G_n$ onto $\left(\prod_{i=1}^{n-1} G_i/(G_i)' \right) \circ G_n$. By Lemma 1.6, there exists an epimorphism from $\left(\prod_{i=1}^{n-1} G_i/(G_i)' \right) \circ G_n$ onto $\prod_{i=1}^n G_i/(G_i)'$. Consequently, there exists an epimorphism from $G_1 \circ G_2 \circ \dots \circ G_n$ onto $\prod_{i=1}^n G_i/(G_i)'$. $\square$

3.17 Theorem. Consider a finite group $G = G_1 \circ G_2 \circ \dots \circ G_n$

satisfying the following conditions:

- (i) $d(G_1 \circ G_2 \circ \dots \circ G_{n-1}) = d\left(\prod_{i=1}^{n-1} G_i/(G_i)'\right)$;
- (ii) $\prod_{i=1}^{n-1} G_i/(G_i)'$ and $G_n/(G_n)'$ are not coprime;
- (iii) $d(G_n/(G_n)') = d(G_n)$.

Then, $d(G) = d(G_1 \circ G_2 \circ \dots \circ G_{n-1}) + d(G_n)$.

Proof. Lemma 3.16 provides the epimorphism $G \twoheadrightarrow \prod_{i=1}^n G_i/(G_i)'$. Hence, $d(G) = d\left(\prod_{i=1}^n G_i/(G_i)'\right) = d\left(\prod_{i=1}^{n-1} G_i/(G_i)'\right) + d(G_n/(G_n)')$ by (ii) and Proposition 4.11. By condition (iii), $d\left(\prod_{i=1}^{n-1} G_i/(G_i)'\right) + d(G_n/(G_n)') = d\left(\prod_{i=1}^{n-1} G_i/(G_i)'\right) + d(G_n)$. On the other hand,

$$\begin{aligned} d(G) &= d(G_1 \circ G_2 \circ \dots \circ G_n) \\ &= d(G_1 \circ G_2 \circ \dots \circ G_{n-1}) + d(G_n) \end{aligned}$$

$$= d\left(\prod_{i=1}^{n-1} G_i / (G_i)'\right) + d(G_n), \text{ by condition (ii).}$$

Hence, $d(G) = d(G_1 \circ G_2 \circ \dots \circ G_{n-1}) + d(G_n)$. $\square$

3.18 Remark. We will use several examples to elucidate the point of the theorem. Note that most of the examples are particularly interesting since they are not nilpotent. A simple way to see that they are not nilpotent is to notice that there are elements of coprime orders which do not commute.

3.19 Example. Let $G = C_2 \wr S_3$. We will show that $d(G) = 2$. Let $C_2 = \langle x \mid x^2 = 1 \rangle$ and $S_3 = \langle u, v \mid u^2 = v^3 = (uv)^2 = 1 \rangle$. If x_r denotes the generator of the r -th copy of C_2 in G , where $r \in S_3$, then the following is a presentation for G :

$$G = \left\langle \begin{array}{l} x_r, u, v \\ (r \in S_3) \end{array} \middle| \begin{array}{l} x_r^2 = u^2 = v^3 = (uv)^2 = 1, x_r x_t = x_t x_r, \\ ux_r u = x_{ru}, v^{-1} x_r v = x_{rv}; r, t \in S_3 \end{array} \right\rangle.$$

Let $B = \{a, b\}$ be the subset of G given by $a = x_1 v$ and $b = x_{uv} u$.

Then, $a^3 = x_1 x_v x_{v^2}$, $b^2 = x_{uv} x_{v^2}$, $(ab)^2 = x_1 x_u x_{uv^2} x_{v^2}$,

$(ba)^2 = x_{uv} x_u x_1 x_v$, and $(a^3 (ba)^3)^2 = x_{v^2} x_{uv^2}$ are all contained in

$\langle B \rangle$. Hence, their product $a^3 b^2 (ab)^2 (ba)^2 (a^3 (ba)^3)^2 = x_1$ is also in

$\langle B \rangle$. Thus, $v = x_1 a$ is in $\langle B \rangle$. Moreover, $u = b(x_1)^{v^2} \in \langle B \rangle$.

Since x_1, u and v are all in $\langle B \rangle$, $\langle B \rangle = G$. Since G is clearly nonabelian and G can be generated by 2 elements, $d(G) = 2$.

Let $G_1 = C_2$ and $G_2 = S_3$. Then, $d(G_1 \wr G_2) = d((C_2 \wr (S_3)) / (S_3)')$
 $= d(C_2 \times C_2) = 2$. Then, $G_1 \wr G_2$ satisfies condition (i) of

Theorem 3.17. Let G_3 be any finite abelian group which is not coprime to C_2 . Then, By Theorem 3.17, $d((C_2 \sim S_3) \circ G_3)$ is equal to $d(C_2 \sim S_3) + d(G_3)$. Similarly, we can consider finite abelian groups $G_4, G_5, \dots, G_n$ which are all not coprime to C_2 . Moreover, $d(C_2 \times S_3) = 2$. Then, $d(((C_2 \circ S_3) \circ G_3 \circ \dots \circ G_{n-1}) \circ G_n)$ is equal to $d((C_2 \circ S_3) \circ G_3 \circ \dots \circ G_{n-1}) + d(G_n)$ by Theorem 3.17.

3.20 Example. Let G_1 be a finite imperfect group with a minimal generating set of finite and mutually coprime orders, such that $G_1/(G_1)' \cong C_n$. Let $G_2 = C_m^t$ where $t \geq 1$, $(n, m) \neq 1$ and $tm : d(G_1)$. Then $d(G_1 \sim G_2) = t+1$ by Corollary 2.8.

Since $d(G_1/(G_1)') \times G_2/(G_2)' = d(C_n \times C_m^t) = t+1$ coincides with $d(G_1 \sim G_2)$, condition (i) of Theorem 3.17 is satisfied. If we let G_3 be any finite abelian group which is not coprime to n and m , it follows from Theorem 3.17 that $d(C_n \sim C_m^t \circ G_3) = d(C_n \sim C_m^t) + d(G_3)$.

3.21 Example. Let $G_1 = C_2$ and $G_2 = C_3^t$ where $t \geq 2$. We will show that $d(C_1 \sim G_2) = t$. Let $G_1 = \langle x \mid x^2 = 1 \rangle$ and $G_2 = \langle u_1, \dots, u_t \mid u_i^3 = [u_i, u_j] = 1, 1 \leq i, j \leq t \rangle$. Then, $G_1 \sim G_2 \cong C_2^{3t} \sim C_3^t$. Denote the generator of the α -th copy of G_1 by x_α where $\alpha \in C_3^t$. Then,

$$C_2 \sim C_3^t = \left\langle \begin{array}{l} x_\alpha, u_1, \dots, u_t \\ (\alpha \in C_3^t) \end{array} \mid \begin{array}{l} x_\alpha^2 = u_i^3 = [x_\alpha, x_\beta] = [u_i, u_j] = 1 \\ u_i x_\alpha u_i^{-1} = x_{\alpha u_i} \quad \alpha, \beta \in C_3^t, 1 \leq i, j \leq t \end{array} \right\rangle.$$

Let $S = \{a, b, u_3, \dots, u_t\}$ where $a = x_1 u_1$ and $b = x_{u_1} u_2$. Then,

$$a^3 = x_1 x_{u_1} x_{u_1}^2, \quad (a^2 b)^3 = x_{u_1}^2 x_{u_2} x_{u_1}^2 x_{u_2}^2, \quad (ab)^3 =$$

$$x_1 x_{u_1}^2 x_{u_2} x_{u_1} x_{u_2} x_{u_1}^2 x_{u_2}^2 x_{u_1} x_{u_2}^2 \quad \text{and} \quad b^3 = x_{u_1} x_{u_1} x_{u_2} x_{u_1} x_{u_2}^2. \quad \text{Thus,}$$

$$a^3 (a^2 b)^3 (ab)^3 b^3 = x_{u_1}. \quad \text{Moreover, } x_{u_1} a^4 x_{u_1} = u_1, \quad \text{whereby } x_{u_1},$$

u_1 and u_2 are in $\langle \beta \rangle$. Hence, $\langle \beta \rangle$ is all of G . This implies that $d(G) \leq t$. On the other hand, the epimorphism from G onto C_3^t implies that $d(G) \geq t$.

3.22 Example. Let $G_1 = C_n$ and $G_2 = C_2^t$, where n is odd and $t \geq 2$. We will prove that $d(G_1 \vee G_2) = t$. Let the presentations of G_1 and G_2 be as follows:

$$C_n = \langle x \mid x^n = 1 \rangle \quad \text{and}$$

$$G_2 = \langle u_1, u_2, \dots, u_t \mid u_i^2 = [u_i, u_j] = 1, \quad 1 \leq i \leq t, \quad 1 \leq j < i \leq t \rangle.$$

Then, $G_1 \vee G_2 \cong C_n^{2t} \times C_2^t$. Let the generator, of the r th copy of the direct product C_n^{2t} , be denoted by x_r , where $r \in G_2$. Then,

$$C_n \vee C_2^t = \left\langle x_r, u_1, \dots, u_t \mid \begin{array}{l} x_r^n = u_i^2 = [x_r, x_s] = [u_i, u_j] = 1, \\ (r \in C_2^t) \quad u_i x_r u_i = x_{ru_i}; \quad r, s \in C_2^t, \quad 1 \leq i \leq t \end{array} \right\rangle.$$

Consider the subset, $B = \{a, b, u_3, u_4, \dots, u_t\}$, of G , where $a = x_1 u_1$ and $b = x_{u_1} u_2$. Then,

$$\begin{aligned} (ab)^2 (a^2)^2 (b^2)^{n-2} &= (x_1^2 x_{u_1}^2 u_2^2) (x_1^2 x_{u_1}^2) (x_{u_1}^{n-2} x_{u_1}^{n-2}) \\ &= x_1^4. \end{aligned}$$

Since $(4, n) = 1$, some power of x_1^4 generates x_1 , whereby $x_1 \in \langle B \rangle$.

Now $x_1^{n-1}a = u_1$ implies that $u_1 \in \langle B \rangle$. Moreover, $(u_1 x_1 u_1)^{n-1}b = x_{u_1}^{n-1}b = u_2$, whereby $u_2 \in \langle B \rangle$. Hence C_2^t is contained in $\langle B \rangle$. Since $rx_1r = x_r$ for every $r \in C_2^t$, every x_2 is in $\langle B \rangle$. Hence, $\langle B \rangle = G$ and $d(G) \leq t$. Moreover, the epimorphism from G onto C_2^t implies that $d(G) > t$.

3.23 Proposition. If $G = (C_n \times C_n) \sim C_m \sim C_m \sim C_m$ then

$$d(G) = \begin{cases} 3 & \text{if } (m,n) = 1, \\ 5 & \text{if } (m,n) \neq 1. \end{cases}$$

Proof. Let $G_1 = C_n \times C_n = \langle x, y \mid x^n = y^n = [x, y] \rangle$, $G_2 = C_m = \langle u \mid u^m = 1 \rangle$, $G_3 = C_m = \langle v \mid v^m = 1 \rangle$ and $G_4 = C_m = \langle w \mid w^m = 1 \rangle$. Then,

$$\begin{aligned} G &= G_1 \sim G_2 \sim G_3 \sim G_4 \\ &\cong (((C_n \times C_n)^m \times C_m)^m \times C_m)^m \times C_m. \end{aligned}$$

Denote the generators of the j th copy of G_3 by v_j where $1 \leq j \leq m$.

Denote the generators of the (i, j) -th copy of G_2 by $u_{i,j}$ where

$1 \leq i \leq m$, and $1 \leq j \leq m$. The generators of the (r, i, j) -th copy of

G_1 are denoted by $x_{r,i,j}$ and $y_{r,i,j}$ where $1 \leq r \leq m$, $1 \leq i \leq m$,

$1 \leq j \leq m$. Then, $\{x_{r,i,j}, y_{r,i,j}, u_{i,j}, v_j, w\}$ forms a generating set

for G . The relations of G are as follows:

$$[x_{r,i,j}, y_{\alpha,\beta,\gamma}] = 1 \text{ for every } r, i, j, \alpha, \beta, \gamma;$$

$$[x_{r,i,j}, v_k] = [y_{r,i,j}, v_k] = [u_{i,j}, v_k] = 1 \text{ if } j \neq k;$$

$$[x_{r,i,j}, u_{\ell,k}] = [y_{r,i,j}, u_{\ell,k}] = 1 \text{ if } i \neq \ell;$$

$$[u_{i,j}, u_{\ell,k}] = [v_i, v_\ell] = 1 \text{ if } i \neq \ell;$$

$$u_{i,j}^{-1} x_{r,i,j} u_{i,j} = x_{r+1,i,j}; u_{i,j}^{-1} y_{r,i,j} u_{i,j} = y_{r+1,i,j};$$

$$v_j^{-1} x_{r,i,j} v_j = x_{r,i+1,j}; w^{-1} x_{r,i,j} w = x_{r,i,j+1};$$

$$w^{-1} y_{r,i,j} w = y_{r,i,j+1}; w^{-1} u_{i,j} w = u_{i,j+1};$$

$$w^{-1} v_j w = v_{j+1}; v_j^{-1} y_{r,i,j} v_j = y_{r,i+1,j}; v_j^{-1} u_{i,j} v_j = u_{i+1,j};$$

$$1 \leq i \leq m, 1 \leq j \leq m, 1 \leq r \leq m, 1 \leq \alpha \leq m, 1 \leq \beta \leq m, 1 \leq \gamma \leq m, 1 \leq k \leq m, 1 \leq \ell \leq m.$$

Firstly, assume that $(n,m) = 1$. Consider the elements

$$a = x_{r,i,j} u_{\ell,k}, b = y_{r,i,j} v_k, c = w \text{ where } k \neq j \text{ and } \ell \neq i.$$

Since $x_{r,i,j}$ and $u_{\ell,k}$ commute and have orders m and n , respectively, there exist integers s, t such that $sn = tm + 1$. Thus,

$$a^{sn} = (x_{r,i,j} u_{\ell,k})^{2n} = u_{\ell,k}^{sn} = u_{\ell,k}.$$

Hence, $u_{\ell,k} \in \langle a, b, c \rangle$ and hence $x_{r,i,j} \in \langle a, b, c \rangle$. Similarly $y_{r,i,j}$ and v_k commute since $k \neq j$ and have orders m and n respectively. Hence, b generates both $y_{r,i,j}$ and v_k , whereby $y_{r,i,j}$ and v_k are contained in $\langle a, b, c \rangle$.

Moreover, for every α, β, γ where $1 \leq \alpha \leq m$, $1 \leq \beta \leq m$ and $1 \leq \gamma \leq m$, we have the following:

$$w^{-\beta+k} v_k w^{\beta-k} = v_\beta; w^{-\beta+k} u_{\ell,k} w^{\beta-k} = u_{\ell,\beta};$$

$$w^{-\beta+j} x_{r,i,j} w^{\beta-j} = x_{r,i,\beta}; w^{-\beta+j} y_{r,i,j} w^{\beta-j} = y_{r,i,\beta};$$

$$v_k^{-\alpha+\ell} u_{\ell,k} v_k^{\alpha-\ell} = u_{\alpha,k}; v_k^{-\alpha+i} x_{r,i,j} v_k^{\alpha-i} = x_{r,\alpha,j};$$

$$v_k^{-\alpha+i} y_{r,i,j} v_k^{\alpha-i} = y_{r,i,j}; u_{\ell,k}^{-\gamma+r} x_{r,i,j} u_{\ell,k}^{\gamma-r} = x_{\gamma,i,j};$$

$$\text{and } u_{\ell,k}^{-\gamma+r} y_{r,i,j} u_{\ell,k}^{\gamma-r} = y_{\gamma,i,j}.$$

This implies that the entire generating set of G is contained in $\langle a, b, c \rangle$ whereby $d(G) \leq 3$.

On the other hand, there exists an epimorphism from G onto $C_n \times C_n \times C_m \times C_m \times C_m$, which is isomorphic to $C_{nm} \times C_{nm} \times C_m$, by Lemma 3.16. Hence, $d(G) \geq d(C_{nm} \times C_{nm} \times C_m) = 3$ by Proposition 4.6.

Now, consider the case when $(m, n) \neq 1$. Then there exists an epimorphism from G onto $C_n \times C_n \times C_m \times C_m \times C_m$ by Lemma 3.16. By Proposition 4.6, $d(G) \geq d(C_n^2 \times C_m^3) = 5$. Clearly, G can be generated by 5 elements.

Remark. Proposition 3.23 gives another example to Theorem 3.17. Let $r = 4$. Then, $G = G_1 \sim G_2 \sim G_3 \sim G_4 = (C_n \times C_n) \sim C_m \sim C_m \sim C_m$. Proposition 3.23 shows that this group satisfies condition (i) of Theorem 3.17. If we take G_5 to be any finite abelian group which is not coprime to C_m , then consider $G \circ G_5$. $d(G \circ G_5) = d(G) + d(G_5)$ by Theorem 3.17.

Chapter 4

THE MINIMAL NUMBERS OF GENERATORS OF SOME FINITELY GENERATED GROUPS

The analogue of the finite problem, stated in the introduction of Chapter 3, for finitely generated groups is:

Given two finitely generated groups G and H , construct a group T containing G and H such that $T = \langle G, H \rangle$ and $d(T) = d(G) + d(H)$. The construction should form a group T which is finite whenever G and H are both finite.

For certain classes of finitely generated groups, explicit constructions will be used to show the existence of such groups. In the cases when the direct product and wreath product are used, the constructed groups are finite if the given groups are finite. Hence, this enlarges the collection of groups for which the finite problem has a positive solution as well.

The following summary on Burnside groups is based on an expository paper on the subject by Gupta [8].

4.1 Burnside groups. Consider the free r -generator Burnside group of exponent n ,

$$B(n, r) = \langle x_1, \dots, x_r \mid w^n = 1 \text{ for all words in } x_1, \dots, x_r \rangle.$$

In 1902, Burnside posed the problem: Is $B(n, r)$ finite, and if so what is its order? The first half of this problem is called the Burnside problem and the other half is called the order problem.

It is clear that $B(1,r)$ is the trivial group and $B(n,1)$ is the cyclic group of order n . $B(2,r)$ is finite since it is abelian, finitely generated and torsion. Clearly, $B(2,r)$ is an elementary abelian group of order 2^r .

Burnside proved that the order of $B(3,2)$ is 27 and the order of $B(4,2)$ is at most 2^{12} . Moreover, he showed that $B(3,r)$ is finite. In 1933, Levi and van der Waerden resolved the order problem for $B(3,r)$. They reduced every element of $B(3,r)$ into a unique normal form $\prod_i x_i^{\alpha_i} \prod_{i < j} [x_i, x_j]^{\alpha_{i,j}} \prod_{i < j < k} [x_i, x_j, x_k]^{\alpha_{i,j,k}}$, where $[x_i, x_j] = x_i^{-1} x_j^{-1} x_i x_j$ and $[x_i, x_j, x_k] = [[x_i, x_j], x_k]^{\alpha_i, \alpha_{i,j}}$, $\alpha_{i,j,k} \in \{0, 1, 2\}$. Hence, the order of $B(3,r)$ is precisely

$$2^{\binom{r}{1} + \binom{r}{2} + \binom{r}{3}}.$$

In 1940, Sanov proved that $B(4,r)$ is finite. However, the order problem for $B(4,r)$ remains open. In 1956, P. Hall and G. Higman proved that if $B(6,r)$ were finite, its order would be $2^{a_3 \binom{b}{1} + \binom{b}{2} + \binom{b}{3}}$ where $a = 1 + (r-1)3^{\binom{r}{1} + \binom{r}{2} + \binom{r}{3}}$ and $b = 1 + (r-1)2^r$. $B(6,r)$ was shown to be finite by M. Hall Jr., in 1958.

P.S. Novikov and Adian proved that $B(n,r)$ is infinite if $n \geq 665$ for odd n . Adian indicated the possibility of lowering the bound to $n \geq 33$. However, the problem remains unresolved for $n \leq 33$ except for $n = 2, 3, 4$ and 6 . In particular, the Burnside problem for $B(5,2)$ remains open.

4.2 Proposition. $B(n, r+s)$ is a $(r+s)$ -generator group containing isomorphic copies of $B(n, r)$ and $B(n, s)$.

Proof. Let $B(n, r+s) = \langle X, Y \mid T \rangle$ where $X = \{x_1, \dots, x_r\}$,
 $Y = \{y_1, \dots, y_s\}$ and $T = \{w^n \mid w \text{ is a word involving elements of } X \text{ and } Y\}$.

Clearly, $d(B(n, r+s)) \leq r+s$. Consider H , a homomorphic image of $B(n, r+s)$, given by the presentation

$$H = \langle X, Y \mid T, [x_i, x_j] = [y_i, y_j] = [x_i, y_j] = 1, 1 \leq i < r+s, 1 \leq j \leq r+s \rangle$$

$$\cong \langle X, Y \mid x_i^n = 1, y_j^n = 1, [x_i, x_j] = [y_i, y_j] = [x_i, y_j] = 1, 1 \leq i < r+s, 1 \leq j \leq r+s \rangle.$$

Since H is isomorphic to C_n^{r+s} , there is an epimorphism from $B(n, r+s)$ onto C_n^{r+s} . So, $d(B(n, r+s)) \leq d(C_n^{r+s}) = r+s$. Hence, $d(B(n, r+s)) = r+s$.

Let $B(n, t)$ be the Burnside group of exponent n on t generators $\{b_1, \dots, b_t\}$. $B(n, t)$ has the following universal property: Whenever G has exponent n and $g_1, \dots, g_t \in G$, there exists a unique homomorphism $f : B(n, t) \rightarrow G$ such that $f(b_i) = g_i$.

Let $B(n, r) = \langle Z \mid R \rangle$ where $Z = \{z_1, \dots, z_r\}$ and $R = \{w^n \mid w \text{ is a word involving elements of } Z\}$. Define a map $\phi : B(n, r+s) \rightarrow B(n, r)$ by $\phi(x_i) = z_i$ and $\phi(y_i) = 1$ for $1 \leq i \leq r$. Define a map $\psi : B(n, r) \rightarrow B(n, r+s)$ by $\psi(z_i) = x_i$ for $1 \leq i \leq r$. The restriction of the map $\psi\phi$ to $B(n, r)$ is the identity map. Therefore, ψ is injective and $\langle x_1, \dots, x_r \rangle$ is isomorphic to $B(n, r)$. Hence, $B(n, r+s)$ contains an isomorphic copy of $B(n, r)$. Similarly, $B(n, r+s)$ contains an isomorphic copy of $B(n, s)$.

4.3 Remark. When $n = 6$, $B(n, r+s)$ is a finite group generated by subgroups isomorphic to $B(6, r)$ and $B(6, s)$ according to Proposition 4.2. Moreover, $d(B(6, r+s)) = d(B(6, r)) + d(B(6, s)) = r+s$.

4.4 Remark. If $n = 3$, $B(3, r+s)$ is a finite 3-group. Proposition 4.2 shows that $B(3, r+s)$ is a finite group generated by subgroups isomorphic to $B(3, r)$ and $B(3, s)$, where $d(3, r+s) = r+s$. However, the group $B(3, r) \circ B(3, s)$ (with notation as in 1.4) needs at least $r+s$ generators as well, by Proposition 4.2. Similarly, when $n = 4$, $B(4, r+s)$ is a finite 2-group. By Proposition 4.2, $d(B(4, r+s)) = r+s$ and $B(4, r+s)$ contains isomorphic copies of $B(4, r)$ and $B(4, s)$. By Proposition 4.2, $B(4, r) \circ B(4, s)$ is another group which needs at least $r+s$ generators and contains isomorphic copies of $B(4, r)$ and $B(4, s)$.

4.5 Proposition. If G is a finite nilpotent group, then $d(G/G') = d(G)$.

Proof. Since G is finite and nilpotent, G' is contained in G^* . Since G' is normal in G , G' is normal in G^* as well. Hence, the mapping $G/G' \rightarrow G/G^*$ sending gG' to gG^* is a homomorphism. Therefore, $d(G/G') \leq d(G/G^*) = d(G)$. The epimorphism $G \twoheadrightarrow G/G'$ gives the reverse inequality $d(G) \geq d(G/G')$. Hence, $d(G/G') = d(G)$.

We will give some examples of groups for which $d(G/G') = d(G)$ but are not nilpotent.

4.6 Example. Let G be a finitely generated imperfect group with a minimal generating set consisting of elements of finite and mutually coprime orders. If $d(G) = 2$, then $d(G \times G) = 2$ by Proposition 2.10. Moreover, $(G \times G)/(G \times G)' = (G \times G)/(G' \times G') = G/G' \times G/G'$. By Proposition 2.1, $G/G' \times G/G' \cong C_n \times C_n$. Hence, $d((G \times G)/(G \times G)') = d(C_n \times C_n) = 2$ and $d((G \times G)/(G \times G)') = d(G \times G)$. $\square$

4.7 Example. Let $G = S_3 \times C_4$, with the presentation $S_3 \times C_4 = C_{12} \times C_2 = \langle x, y \mid x^{12} = y^2 = 1, y^{-1}xy = x^5 \rangle$. Then $G/G' \cong (S_3 \times C_4)/(S_3 \times C_4)' = C_2 \times C_4$. Thus, $d(G/G') = d(C_2 \times C_4) = 2$. $\square$

We state a result by Wiegold, concerning the growth sequences of finite imperfect groups.

4.8 Theorem. (Wiegold, 1973, [18]) Let G be a finite imperfect group.

- (i) If $d(G/G') \geq 2$, then $d(G^r) = rd(G/G')$ for $r \geq (d(G)-1)/(d(G/G')-1)$;
- (ii) If $d(G/G') = 1$, then $d(G^r) = r$ for $r \geq 2d(G) + 1$.

Growth sequences of finitely generated imperfect groups were explored further by Wiegold and Wilson who proved the following result.

4.9 Theorem. (Wiegold & Wilson, 1977, [19]) If G is a finitely generated imperfect group, then $d(G^r) = rd(G/G')$ for all $r \geq 2(2 + d(G)/d(G/G'))^2$.

For two finitely generated abelian groups A and B , we give a characterization of when their direct product cannot be generated by less than $d(A) + d(B)$ elements. In fact, $d(A \times B)$ is equal to

$d(A) + d(B)$ when A and B are not coprime. As defined in 3.15, two finitely generated abelian groups A and B are coprime if their canonical decompositions are related as follows:

$$A = C_{m_1} \times C_{m_2} \times \dots \times C_{m_s} \times \mathbb{Z}^\alpha, \quad m_i | m_{i+1} \text{ for every } i, 1 \leq i \leq s-1;$$

$$B = C_{n_1} \times C_{n_2} \times \dots \times C_{n_t} \times \mathbb{Z}^\beta, \quad n_j | n_{j+1} \text{ for every } j, 1 \leq j \leq t-1;$$

$$\text{and } (m_1, n_1) = 1.$$

4.10 Proposition. If A is a finitely generated abelian group, then $d(A)$ is equal to the number of direct factors of the canonical decomposition of A .

Proof. Consider $A = C_{m_1} \times C_{m_2} \times \dots \times C_{m_s} \times \underbrace{\mathbb{Z} \times \dots \times \mathbb{Z}}_{r \text{ copies}}$, where

$m_i | m_{i+1}$ for every i where $1 \leq i \leq s-1$. Clearly, $d(A) \leq r+s$. On the other hand, let p be a prime number dividing m_1 . For every i where $1 \leq i \leq s$, m_1 divides m_i and hence p divides m_i . Then, there is an epimorphism from C_{m_i} onto C_p for every i where $1 \leq i \leq s$. Clearly, there is an epimorphism from $\mathbb{Z}$ onto C_p as well. Therefore, there is an epimorphism from A onto the direct product of $r+s$ copies of C_p . Hence $d(A) \geq r+s$, whereby $d(A)$ is precisely the number of direct factors of the canonical decomposition of A .

4.11 Proposition. If A and B are finitely generated abelian groups, then $d(A \times B) = d(A) + d(B)$ iff A and B are not coprime.

Proof. By Proposition 4.10, A and B have canonical decompositions

as follows:

$$A = C_{m_1} \times C_{m_2} \times \dots \times C_{m_s} \times \underbrace{\mathbb{Z} \times \dots \times \mathbb{Z}}_{d(A)-s \text{ copies}}, m_i | m_{i+1}, 1 \leq i \leq s-1;$$

$$B = C_{n_1} \times C_{n_2} \times \dots \times C_{n_t} \times \underbrace{\mathbb{Z} \times \dots \times \mathbb{Z}}_{d(B)-t \text{ copies}}, n_j | n_{j+1}, 1 \leq j \leq t-1.$$

If A and B are not coprime, there exists a prime p dividing both m_1 and n_1 . Since m_1 divides every m_i for every i , $2 \leq i \leq s$, p divides every m_i . Similarly, p divides every n_j where $1 \leq j \leq t$. Hence, there is an epimorphism from C_{m_i} onto C_p for every i . Similarly, there is an epimorphism from C_{n_j} onto C_p for every j . Obviously, there is an epimorphism from $\mathbb{Z}$ onto C_p as well. Hence, we have an epimorphism from $A \times B$ onto C_p^r where $r = d(A) + d(B)$. Thus, $d(A \times B) \geq d(C_p^r) = d(A) + d(B)$. It is clear that the reverse inequality, $d(A \times B) \leq d(A) + d(B)$, holds too. Consequently, $d(A \times B) = d(A) + d(B)$ if A and B are not coprime.

In contrast, if A and B are coprime then m_1 and n_1 are coprime. Hence, $C_{m_1} \times C_{n_1} \cong C_{m_1 n_1}$. This implies that $A \times B \cong C_{m_1 n_1} \times C_{m_2} \times \dots \times C_{m_s} \times C_{n_2} \times \dots \times C_{n_t} \times \underbrace{\mathbb{Z} \times \dots \times \mathbb{Z}}_{d(A)+d(B)-s-t \text{ copies}}$

and $d(A \times B) < d(A) + d(B)$. Hence, the converse holds as well.

We enlarge our scope from finitely generated abelian groups to finitely generated groups, with abelianized quotient groups which are not coprime, and yield a similar result.

4.12 Theorem. Let G and H be finitely generated groups so that $d(G/G') = d(G)$ and $d(H/H') = d(H)$. If G/G' and H/H' are not coprime, then $d(G \times H) = d(G) + d(H)$. Moreover, if H is finite then $d(G \circ H) = d(G) + d(H)$.

Proof. Firstly, it is clear that $d(G \times H) \leq d(G) + d(H)$. The epimorphisms from G onto G/G' and from H onto H/H' induce an epimorphism from $G \times H$ onto $G/G' \times H/H'$. Hence, $d(G \times H) \geq d(G/G' \times H/H') = d(G/G') + d(H/H')$ by Proposition 4.11. But, by the hypothesis we have $d(G/G') + d(H/H') = d(G) + d(H)$. Therefore, $d(G \times H) = d(G) + d(H)$.

If H is finite, Lemma 1.6 gives the epimorphism $G \circ H \twoheadrightarrow G/G' \times H/H'$. The rest of the proof is the same as above. $\square$

4.13 Corollary. If G and H are finitely generated imperfect groups such that G/G' and H/H' are not coprime, there exist k and ℓ so that $d(G^r \times H^s) = d(G^r) + d(H^s)$ for all $r \geq k$ and $s \geq \ell$. In addition, if H is finite then $d(G^r \circ H^s) = d(G^r) + d(H^s)$.

Proof. Firstly, $d(G^r) = rd(G/G')$ for all $r \geq k$ where $k = 2(2 + d(G)/d(G/G'))^2$ by Theorem 4.9. Similarly, $d(H^s) = sd(H/H')$ for all $s \geq \ell$ where $\ell = 2(2 + d(H)/d(H/H'))^2$ by Theorem 4.9. Clearly, $d(G^r \times H^s) \leq d(G^r) + d(H^s)$. Now, assume that $r \geq k$ and $s \geq \ell$. There is an epimorphism from $G^r \times H^s$ onto $G^r/(G^r)' \times H^s/(H^s)'$. Then, $d(G^r \times H^s) \geq d(G^r/(G^r)' \times H^s/(H^s)')$. By Theorem 4.12, $d(G^r/(G^r)' \times H^s/(H^s)') = d(G^r/(G^r)') + d(H^s/(H^s)') = d(G/G')^r + d(H/H')^s$. Applying 4.12 again, we have $d(G/G')^r + d(H/H')^s = rd(G/G') + sd(H/H')$. But since $r \geq k$ and $s \geq \ell$,

$rd(G/G') + sd(H/H') = d(G^r) + d(H^s)$. Hence $d(G^r \times H^s) \geq d(G^r) + d(H^s)$ and consequently $d(G^r \times H^s) = d(G^r) + d(H^s)$ for all $r \geq k$ and $s \geq \ell$.

If H is finite, Lemma 1.6 provides the epimorphism from $G^r \circ H^s$ onto $G^r/(G^r)' \times H^s/(H^s)'$. The rest of the proof for $d(G^r \circ H^s) = d(G^r) + d(H^s)$, for $r \geq k$ and $s \geq \ell$, is identical to the one above. $\square$

4.14 Corollary. If G and H are finite nilpotent groups so that G/G' and H/H' are not coprime, then $d(G \circ H) = d(G) + d(H)$.

Proof. Firstly, it is obvious that $d(G \circ H) \geq d(G) + d(H)$. We will prove the reverse inequality. By Proposition 4.5, $d(G/G') = d(G)$ and $d(H/H') = d(H)$. By Lemma 1.6, we have an epimorphism from $G \circ H$ onto $G/G' \times H/H'$. Hence, $d(G \circ H) \leq d(G/G' \times H/H') = d(G) + d(H)$. Thus, $d(G \circ H) \geq d(G) + d(H)$ and we have the equality $d(G \circ H) = d(G) + d(H)$. $\square$

4.15 Remark. An obvious example when G and H satisfy the condition in Corollary 4.14 is when G and H are both p -groups.

4.16 Example. Let G be a finitely generated imperfect group with a minimal generating set of finite mutually coprime orders. Let $d(G) = 2$. Then, by Example 4.6, $d(G \times G/(G \times G)') = d(G \times G)$. Let $G/G' \cong C_n$ and A be any finitely generated abelian group such that A and C_n are not coprime. Then, if we let $H = G \times A$, $d(H \times A) = d(A) + 2$ by Theorem 4.12. $\square$

The direct product of two nontrivial cyclic groups cannot be generated by less than two elements iff the two groups are not coprime. However, regardless of the relationship between the two cyclic groups, their wreath product cannot be generated by less than two elements. In fact, the wreath product of C_n^s by C_m cannot be generated by less than $s+1$ elements.

4.17 Let n be a positive integer which is at least 2. Let p be a prime number and s be any positive integer. Consider a group G defined by

$$G = C_n^s \wr C_p = \langle x_{1,r}, x_{2,r}, \dots, x_{s,r}, u \mid \begin{array}{l} x_{1,r}^n = x_{2,r}^n = \dots = x_{s,r}^n = u^p = [x_{i,j}, x_{\alpha,\beta}] = 1, \\ u^{-1} x_{1,r} u = x_{1,r+1} \pmod{p}, \dots, \\ u^{-1} x_{s,r} u = x_{s,r+1} \pmod{p}; \quad 1 \leq r \leq p-1, \\ 1 \leq i \leq s, \quad 1 \leq \alpha \leq s, \quad 0 \leq j \leq p-1, \quad 0 \leq \beta \leq p-1. \end{array} \rangle$$

Define an element of type 1 to be an element of the form

$$\prod_{r=0}^{p-1} x_{1,r}^{i_{1,r}} x_{2,r}^{i_{2,r}} \dots x_{s,r}^{i_{s,r}}, \text{ where } 0 \leq i_{t,r} \leq n-1, \quad 1 \leq t \leq s.$$

Define an element of type 2 to be an element of the form

$$\left(\prod_{r=0}^{p-1} x_{1,r}^{i_{1,r}} x_{2,r}^{i_{2,r}} \dots x_{s,r}^{i_{s,r}} \right) u^k, \text{ where } 1 \leq k \leq p-1, \quad 0 \leq i_{t,r} \leq n-1,$$

$1 \leq t \leq s$. Note that an element of type 1 has order d , where d is a divisor of n . An element of type 2 has order pd where d is a divisor of n .

4.18 Lemma. Let the notation be as in 4.17. If a and b are elements of type 2, then there exists an integer ϵ such that $1 \leq \epsilon \leq p-1$ and ab^ϵ is of type 1.

Proof. Let $a = \left(\prod_{r=0}^{p-1} x_{1,r}^{i_{1,r}} \dots x_{s,r}^{i_{s,r}} \right) u^k$ and $b = \left(\prod_{r=0}^{p-1} x_{1,r}^{\alpha_{1,r}} \dots x_{s,r}^{\alpha_{s,r}} \right) u^\ell$

where $1 \leq k \leq p-1$, $1 \leq \ell \leq p-1$, $0 \leq i_{t,r} \leq n-1$, $0 \leq \alpha_{t,r} \leq n-1$ and $1 \leq t \leq s$.

There exists an integer c such that $1 \leq c \leq p-1$ and $\ell c \equiv -k \pmod{p}$.

Then $k + \ell c \equiv 0 \pmod{p}$ and ab^c is of type 1. $\square$

4.19. Proposition. Let the notation be as in 4.17. If m is a positive integer which is at least 2, then $d(C_n^S \sim C_m) = s+1$.

Proof. Obviously, $d(C_n^S \sim C_m) \leq s+1$. We will prove the reverse inequality. Let p be any prime number dividing m . By Lemma 1.7, the epimorphism from C_m onto C_p induces an epimorphism from $C_n^S \sim C_m$ onto $C_n^S \sim C_p = G$. Then $d(C_n^S \sim C_m) \geq d(G)$. We will show that G cannot be generated by s elements, in order to conclude that $C_n^S \sim C_m$ cannot be generated by s elements.

Let B be a subset of s nontrivial elements of G . If all the elements of B are of type 1, they can only generate elements of type 1. If B has at least one element of type 2, Lemma 4.18 shows that B can be transformed (if necessary) into a set consisting of $s-1$ elements of type 1 and one element of type 2. Let $a_1, \dots, a_{s-1}$ be the $s-1$ elements of type 1 and b be the element of type 2.

Then, an element in $\langle B \rangle$ can be expressed as a word in the form

$$\left(b^{\gamma_1} a_1^{\epsilon_{1,1}} a_2^{\epsilon_{2,1}} \dots a_{s-1}^{\epsilon_{s-1,1}} \right) \dots \left(b^{\gamma_{h-1}} a_1^{\epsilon_{1,h-1}} a_2^{\epsilon_{2,h-1}} \dots a_{s-1}^{\epsilon_{s-1,h-1}} \right) b^{\gamma_h} g b^k$$

where $0 \leq \gamma_t \leq pn-1$, $0 \leq k \leq pn-1$, $0 \leq \epsilon_{t,r} \leq n-1$, $0 \leq r \leq p-1$ and

$g \in \langle a_i, a_i^u, a_i^{u^2}, \dots, a_i^{u^{p-1}} \rangle$; $1 \leq i \leq s-1$. So, there are at most $n^{(s-1)p}$

possibilities for g . Note that b has order pd . Then $g b^k$ is

of type 1 only if $b^k \in \langle b^p \rangle$. Since $|\langle b^p \rangle| = d$, there are at most

$dn^{(s-1)p}$ elements of type 1 in $\langle \delta \rangle$. Since $d \leq n$, we have $|\langle \delta \rangle| \leq n^{sp}$. Now, $|G| = pn^{sp}$ implies that $\langle \delta \rangle \neq G$. So, $d(G) \geq s+1$ whereby $d(C_n^s \sim C_m) \leq s+1$. Consequently, $d(C_n^s \sim C_m) = s+1$. $\square$

The result we have just proved can be generalized to the wreath product of a finitely generated abelian group and a finite cyclic group. In fact, the group which is being acted on can be further generalized to a finitely generated group G such that $d(G/G') = d(G)$. Moreover, Theorem 4.9 of Wiegold and Wilson can be employed again to deduce an interesting corollary.

4.20 Proposition. If A is a finitely generated abelian group, then $d(A \sim C_m) = d(A) + 1$ for every integer m which is at least 2.

Proof. Obviously, $d(A \sim C_m) \leq d(A) + 1$. To show the reverse inequality, consider the canonical decomposition of $A = C_{n_1} \times C_{n_2} \times \dots \times C_{n_t} \times \underbrace{\mathbb{Z} \times \dots \times \mathbb{Z}}_{d(A)-t}$ where $n_i | n_{i+1}$ and $1 \leq i \leq t-1$. For any prime divisor p of n_1 , there is an epimorphism from C_{n_i} onto C_p for every i , $1 \leq i \leq t$. Clearly, there is also an epimorphism from $\mathbb{Z}$ onto C_p . Hence, there is an epimorphism from A onto $C_p^{d(A)}$. By Lemma 1.5 this epimorphism induces an epimorphism from $A \sim C_m$ onto $C_p^{d(A)} \sim C_m$. Hence, $d(A \sim C_m) \geq d(C_p^{d(A)} \sim C_m)$. By Proposition 4.17, $d(C_p^{d(A)} \sim C_m) = d(A) + 1$. Since $d(A) = d(C_p^{d(A)})$, we have $d(A \sim C_m) = d(A) + 1$. Consequently, $d(A \sim C_m) = d(A) + 1$. $\square$

4.21 Theorem. If G is a finitely generated group so that $d(G/G') = d(G)$, then $d(G \sim C_m) = d(G) + 1$ for every integer $m \geq 2$.

Proof. Clearly, $d(G \wr C_m) = d(G) + 1$. The epimorphism from G onto G/G' induces the epimorphism from $G \wr C_m$ onto $G/G' \wr C_m$ by Lemma 1.5. Thus, $d(G \wr C_m) \geq d(G/G' \wr C_m)$. By Proposition 4.20, $d(G/G' \wr C_m) = d(G/G') + 1$. Since $d(G/G') = d(G)$, $d(G/G') + 1 = d(G) + 1$. Therefore $d(G \wr C_m) = d(G) + 1$ and consequently $d(G \wr C_m) = d(G) + 1$. $\square$

4.22 Corollary. If G is a finitely generated imperfect group, then there exists a positive integer k so that $d(G^r \wr C_m) = d(G^r) + 1$ for all $r \geq k$ and $m \geq 1$.

Proof. Firstly, $d(G^r) = \text{rd}(G/G')$ for all $r \geq k$ where $r \geq 2(2 + d(G)/d(G/G'))^2$ by Theorem 4.9. Clearly, $d(G^r \wr C_m) = d(G^r) + 1$. Now, assume that $r \geq k$. Now, $d(G^r/(G^r)') = d((G/G')^r)$. By Proposition 4.11, $d((G/G')^r) = \text{rd}(G/G')$. Since $r \geq k$, $\text{rd}(G/G') = d(G^r)$. Therefore, $d(G^r/(G^r)') = d(G^r)$. By Theorem 4.21, $d(G^r \wr C_m) = d(G^r) + 1$ for all $r \geq k$ and $m \geq 2$. $\square$

4.23 Corollary. If G is a finite nilpotent group, then $d(G \wr C_m) = d(G) + 1$ for every integer $m \geq 2$.

Proof. If G is a finite nilpotent group, then $d(G/G') = d(G)$ by Proposition 4.5. Therefore, the result follows from Theorem 4.21.

4.24 Example. If G is a finitely generated imperfect group with a minimal generating set of finite mutually coprime orders, then $d(G^r) = \text{rd}(G/G') = r$ for all $r > d(G)$ by Proposition 2.1 and Proposition 2.4. Since $\text{rd}(G/G') = d(G^r/(G^r)')$, we have $d(G^r) = d(G^r/(G^r)')$. It follows from Theorem 4.21 that $d(G^r \wr C_m) = d(G^r) + 1 = r + 1$, for every $r > d(G)$. $\square$

4.25 Example. Let m be an even integer and D_m be the dihedral group of order $2m$. Then, $D_m/(D_m)' \cong C_2 \times C_2$. So, the epimorphism from D_m onto $C_2 \times C_2$ induces the epimorphism from $D_m \wr C_n$ onto $(C_2 \times C_2) \wr C_n$ by Lemma 1.5. Thus, $d(D_m \wr C_n) = d((C_2 \times C_2) \wr C_n)$. But, $d((C_2 \times C_2) \wr C_n) = 3$ by Proposition 4.21 and $d(D_m \wr C_n) \leq 3$. Since it is clear that $d(D_m \wr C_n) \neq 3$, we have $d(D_m \wr C_n) = 2$. In contrast, $d(D_m \wr C_n) = 2$ by Proposition 2.5 if m is odd. Since $D_m \wr C_n$ is clearly nonabelian, $d(D_m \wr C_n) = 2$ when m is odd. $\square$

4.26 Notation. Let G be a finite group and r be a positive integer. Then, $G \circ G$ denotes the direct product or wreath product of G by G , as defined in 1.4. Now, let G^{or} denote either $\underbrace{G \times G \times \dots \times G}_{r \text{ copies}}$ or $\underbrace{G \wr G \wr \dots \wr G}_{r \text{ copies}}$.

4.27 Proposition. If G is a finite imperfect group, then
 $d(G^{\text{or}},) \geq \text{rd}(G/G')$ and $\lim_{r \rightarrow \infty} d(G^{\text{or}}) = \infty$.

Proof. By Lemma 3.16, we have an epimorphism from G^{or} onto $(G/G')^r$. Hence, $d(G^{\text{or}}) \geq d(G/G')^r$. By Proposition 4.11, $d(G/G')^r = \text{rd}(G/G')$. Thus, $d(G^{\text{or}}) \geq \text{rd}(G/G')$ and $\lim_{r \rightarrow \infty} d(G^{\text{or}}) = \infty$. $\square$

The following results are in fact corollaries of Theorem 4.12 and Theorem 4.21. A result of Gruenberg (cf. [7, Lemma 3.2]) will be needed to establish the results.

4.28 Lemma. (Gruenberg, 1973) If G is a finitely generated group, where $G = P \times S$, P is perfect and S is solvable, then $d(G) = \max \{d(P), d(S)\}$.

4.29 Proposition. Let G_1 and G_2 be finitely generated solvable groups so that G_1/G_1' and G_2/G_2' are not coprime. In addition, $d(G_i) = d(G_i/G_i')$ for $i = 1, 2$. If P_1 and P_2 are finitely generated perfect groups so that $d(G_i) \leq d(P_i)$ for $i = 1, 2$, then

- (i) $d((G_1 \times P_1) \wr C_n) = d(G_1 \times P_1) + 1$; and
- (ii) $d((G_1 \times P_1) \times (G_2 \times P_2)) = d(G_1 \times P_1) + d(G_2 \times P_2)$.

Moreover, if G_2 and P_2 are finite then $d((G_1 \times P_1) \wr (G_2 \times P_2)) = d(G_1 \times P_1) + d(G_2 \times P_2)$.

Proof. (i) We will show that this result is a consequence of Theorem 4.21 by showing that $d((G_1 \times P_1)/(G_1 \times P_1)') = d(G_1 \times P_1)$.

Now, $d((G_1 \times P_1)/(G_1 \times P_1)') = d(G_1/G_1' \times P_1/P_1')$. Since P_1 is a perfect group, P_1/P_1' is the trivial group and $d(G_1/G_1' \times P_1/P_1') = d(G_1/G_1')$. By the hypothesis, $d(G_1/G_1') = d(G_1)$. But since $d(G_1) = d(P_1)$, $d(G_1) = d(G_1 \times P_1)$ by Lemma 4.28. Hence, $d((G_1 \times P_1)/(G_1 \times P_1)') = d(G_1 \times P_1)$ and $d((G_1 \times P_1) \sim C_n) = d(G_1 \times P_1) + 1$.

Alternatively, consider the epimorphism from $(G_1 \times P_1) \sim C_n$ onto $G_1 \sim C_n$ induced by the epimorphism from $G_1 \times P_1$ onto G_1 by Lemma 1.5. It follows that $d((G_1 \times P_1) \sim C_n) \geq d(G_1 \sim C_n)$. But, by Theorem 4.21 we have $d(G_1 \sim C_n) = d(G_1) + 1$. Now, by Lemma 4.28, $d(G_1) + 1 = d(G_1 \times P_1) + 1$. Hence, $d((G_1 \times P_1) \sim C_n) \geq d(G_1 \times P_1) + 1$. Since it is clear that $d((G_1 \times P_1) \sim C_n) \leq d(G_1 \times P_1) + 1$, it follows that $d((G_1 \times P_1) \sim C_n) = d(G_1 \times P_1) + 1$.

(ii) Clearly, $d(G_1 \times G_2) = d(G_1) + d(G_2)$. On the other hand, it follows from Lemma 1.6 that there is an epimorphism from $G_1 \times G_2$ onto $G_1/G_1' \times G_2/G_2'$. Hence, $d(G_1 \times G_2) \geq d(G_1/G_1' \times G_2/G_2')$. Hence, by the hypothesis and Theorem 4.12, $d(G_1/G_1' \times G_2/G_2') = d(G_1/G_1') + d(G_2/G_2') = d(G_1) + d(G_2)$. So, $d(G_1 \times G_2) = d(G_1) + d(G_2)$. Since $d(G_i) = d(P_i)$, for $i = 1$ and 2 , $d(G_1 \times G_2) \geq d(P_1 \times P_2)$. Therefore, $d((G_1 \times P_1) \sim (G_2 \times P_2)) = d((G_1 \times G_2) \sim (P_1 \times P_2))$. By Gruenberg's Lemma 4.28, $d((G_1 \times G_2) \sim (P_1 \times P_2)) = d(G_1 \times G_2) = d(G_1) + d(G_2) = d(G_1 \times P_1) + d(G_2 \times P_2)$.

Now, assume that G_2 and P_2 are finite. As in (i), $d((G_1 \times P_1)/(G_1 \times P_1)') = d(G_1 \times P_1)$ and $(G_1 \times P_1)/(G_1 \times P_1)' \cong G_1/G_1'$. Hence we have the epimorphism from $(G_1 \times P_1) \sim (G_2 \times P_2)$

onto $G_1/G_1' \times G_2/G_2'$ by Lemma 1.6. Hence, we have the inequality $d((G_1 \times P_1) \sim (G_2 \times P_2)) \geq d(G_1/G_1' \times G_2/G_2')$. By Theorem 4.12, $d(G_1/G_1' \times G_2/G_2') = d(G_1/G_1') + d(G_2/G_2')$. By the hypothesis and Lemma 4.28, we have $d(G_1/G_1') + d(G_2/G_2') = d(G_1) + d(G_2) = d(G_1 \times P_1) + d(G_2 \times P_2)$. Thus, $d((G_1 \times P_1) \sim (G_2 \times P_2)) = d(G_1 \times P_1) + d(G_2 \times P_2)$. Since the reverse inequality is obvious, we can conclude that $d((G_1 \times P_1) \sim (G_2 \times P_2)) = d(G_1 \times P_1) + d(G_2 \times P_2)$.

4.30 Remark. The same results as the ones in Proposition 4.29 hold if G_i and P_i are finitely generated groups which are related as follows:

- (i) $d(G_i \times P_i) = \max \{d(G_i), d(P_i)\} = m_i$;
- (ii) $d(G_i/G_i') = d(G_i)$ if $m_i = d(G_i)$;
- (iii) $d(P_i/P_i') = d(P_i)$ if $m_i = d(P_i)$.

An example of two groups, which are related in this way, can be described in terms of the relationship between the orders of their generators.

Let G_1 and G_2 be two finitely generated groups so that $d(G_1) \mid d(G_2)$. If the orders of the generators of finite orders of G_2 are coprime to the orders of $d(G_2)$ corresponding generators of finite orders of G_1 , then $d(G_1 \times G_2) = d(G_1)$ by Proposition 2.19. If $d(G_i/G_i') = d(G_i)$ for $i = 1$ and 2 , then the results in Proposition 4.29 follow.

4.31 Corollary. If G_1 is a noncyclic finite nilpotent group and P_1 is a finite nonabelian simple group, then $d((G_1 \times P_1) \sim C_n) = d(G_1 \times P_1) + 1$.

Proof. Since $d(P_1) = 2$ by [1], $d(G_1) \neq d(P_1)$. Now, by Proposition 4.29 (i), it follows that $d((G_1 \times P_1) \circ C_n) = d(G_1 \times P_1) + 1$. $\square$

4.32 Corollary. If G is a finitely generated imperfect solvable group, then there exists k so that $d((G^r \times P) \circ C_n) = d(G^r \times P) + 1$ for every $r \geq k$ and for every finitely generated perfect group P so that $d(G^r) = d(P)$.

Proof. By Theorem 4.9, $d(G^r) = \text{rd}(G/G')$ for all $r \geq k$ where $k = 2(2 + d(G)/d(G/G'))^2$. We will show that $d((G^r \times P)/(G^r \times P)') = d(G^r \times P)$ for every $r \geq k$. Firstly, $d((G^r \times P)/(G^r \times P)') = d(G^r/(G^r)' \times P/P') = d(G^r/(G^r)')$ because P is a perfect group. Moreover, $d(G^r/(G^r)') = d(G/G')^r = \text{rd}(G/G')$ by Theorem 4.12. But, $\text{rd}(G/G') = d(G^r)$ since $r \geq k$ and $d(G^r) = d(G^r \times P)$ by Lemma 4.28. Since $d((G^r \times P)/(G^r \times P)') = d(G^r \times P)$, the result follows from Proposition 4.29 (i). $\square$

4.33 Corollary. If G_1 and G_2 are noncyclic finite nilpotent groups so that G_1/G_1' and G_2/G_2' are not coprime, P_1 and P_2 are finite nonabelian simple groups, then $d((G_1 \times P_1) \circ (G_2 \times P_2)) = d(G_1 \times P_1) + d(G_2 \times P_2)$.

Proof. Since G_i is a finite nilpotent group, it follows from Proposition 4.5 that $d(G_i/G_i') = d(G_i)$, for $i = 1$ or 2 . Since G_1 and G_2 are noncyclic, P_1 and P_2 are finite nonabelian simple groups, $d(G_i) = d(P_i)$ for every i , by [1]. Now, the conditions of Proposition 4.29 are satisfied and $d((G_1 \times P_1) \circ (G_2 \times P_2)) = d(G_1 \times P_1) + d(G_2 \times P_2)$. $\square$

4.34 Corollary. Let G_1 and G_2 be finitely generated imperfect solvable groups, such that G_1/G_1' and G_2/G_2' are not coprime. Then there exist k and ℓ so that $d((G_1^r \times P_1) \times (G_2^s \times P_2)) = d(G_1^r \times P_1) + d(G_2^s \times P_2)$ for all $r \geq k$, $s \geq \ell$ and for every P_1 and P_2 such that $d(G_i^r) \leq d(P_i)$ where P_i is a finitely generated perfect group. Moreover, if G_2 and P_2 are finite then $d((G_1^r \times P_1) \sim (G_2^s \times P_2)) = d(G_1^r \times P_1) + d(G_2^s \times P_2)$.

Proof. By Theorem 4.9, $d(G_1^r) = rd(G_1/G_1')$ for every $r \geq k$ where $k = 2(2 + d(G_1)/d(G_1/G_1'))^2$, and $d(G_2^s) = sd(G_2/G_2')$ for every $s \geq \ell$ where $\ell = 2(2 + d(G_2)/d(G_2/G_2'))^2$. As shown in Corollary 4.32, $d((G_1^r \times P_1)/(G_1^r \times P_1)') = d(G_1^r \times P_1)$ for every $r \geq k$ and $d((G_2^s \times P_2)/(G_2^s \times P_2)') = d(G_2^s \times P_2)$. Hence, $d((G_1^r \times P_1) \times (G_2^s \times P_2)) = d(G_1^r \times P_1) + d(G_2^s \times P_2)$ by Proposition 4.29 (ii). Similarly, it follows that $d((G_1^r \times P_1) \sim (G_2^s \times P_2)) = d(G_1^r \times P_1) + d(G_2^s \times P_2)$ if G_2 and P_2 are finite. $\square$

4.35 For any finite group G , define $\tilde{G} = G/J$ where J is the intersection of all maximal normal subgroups of G . Let J_a be the intersection of the maximal normal subgroups containing G' . Let J_p be the intersection of the maximal normal subgroups, which do not contain G' . Gruenberg observed the following facts in [6, 6.5]:

- (i) $J = J_a \cap J_p$;
- (ii) $G/J_a = A$, a direct product of elementary abelian groups;
- (iii) $G/J_p = P$, a direct product of nonabelian simple groups;
- (iv) $\tilde{G} \cong A \times P$.

4.36 Proposition. Let G_1 and G_2 be finite groups, so that $d(G_1) = d(\tilde{G}_1)$. $\tilde{G}_i \cong A_i \times P_i$ where A_i and P_i are nontrivial abelian and perfect groups, respectively. If $d(A_i) \geq d(P_i)$ for $i = 1$ and 2 , A_1 and A_2 are not coprime, then the following statements hold:

- (i) $d(G_1 \sim C_m) = d(G_1) + 1$;
- (ii) $d(G \times G_2) = d(G) + d(G_2)$ if G is a finitely generated group so that $d(G/G') = d(G)$, A_2 and G/G' are not coprime;
- (iii) $d(G_1 \times G_2) = d(G_1) + d(G_2)$.

Proof. (i) Obviously, $d(G_1 \sim C_m) \leq d(G_1) + 1$. The epimorphism from G_1 onto $\tilde{G}_1$ induces an epimorphism from $G_1 \sim C_m$ onto $\tilde{G}_1 \sim C_m$ by Lemma 1.5. Hence, $d(G_1 \sim C_m) \geq d(\tilde{G}_1 \sim C_m)$. By Proposition 4.29, $d(G_1 \sim C_m) = d(\tilde{G}_1) + 1$. But, $d(\tilde{G}_1) + 1 = d(G_1) + 1$ by the hypothesis. Therefore, $d(G_1 \sim C_m) = d(G_1) + 1$ and consequently $d(G_1 \sim C_m) = d(G_1) + 1$.

(ii) Firstly, it is clear that $d(G \times G_2) \leq d(G) + d(G_2)$. Since there exists an epimorphism from $G \times G_2$ onto $G/G' \times \tilde{G}_2 \cong G/G' \times A_2 \times P_2$, we have $d(G \times G_2) \geq d(G/G' \times A_2 \times P_2)$. Moreover, $d(G/G' \times A_2 \times P_2) = d(G/G') + d(A_2 \times P_2)$ by the hypothesis and Proposition 4.29. Finally, $d(G/G') + d(A_2 \times P_2) = d(G) + d(G_2)$ by the hypothesis. Hence, $d(G \times G_2) \geq d(G) + d(G_2)$ and $d(G \times G_2) = d(G) + d(G_2)$.

(iii) Clearly, $d(G_1 \times G_2) \leq d(G_1) + d(G_2)$. Since there exists an epimorphism from $G_1 \times G_2$ onto $\tilde{G}_1 \times \tilde{G}_2$, $d(G_1 \times G_2) \geq d(\tilde{G}_1 \times \tilde{G}_2)$.

By Proposition 4.29, $d(\tilde{G}_1 \times \tilde{G}_2) = d(\tilde{G}_1) + d(\tilde{G}_2)$. Since $d(\tilde{G}_1) + d(\tilde{G}_2) = d(\tilde{G}_1) + d(\tilde{G}_2)$, by the hypothesis, $d(G_1 \times G_2) = d(G_1) + d(G_2)$. Therefore, $d(G_1 \times G_2) = d(G_1) + d(G_2)$. $\square$

4.37 Remark. For $\tilde{G}_1$ to have a nontrivial abelian component, G_1 has to be imperfect.

4.38 Example. Let D_n be the dihedral group of order $2n$ with n even. Let Q_m be the dicyclic group of order $2m$ such that $m/2$ is even. Let P_1 and P_2 be finite nonabelian simple groups. Then, $d(D_n/(D_n)') = d(C_2 \times C_2) = d(D_n)$ and $d(Q_m/(Q_m)') = d(C_2 \times C_2) = d(Q_m)$. Moreover, $d(D_n) = d(P_1)$ and $d(Q_m) = d(P_2)$ since according to [1], $d(P_1) = d(P_2) = 2$. By Proposition 4.29 (ii), $d((D_n \times P_1) \times (Q_m \times P_2)) = d(D_n \times P_1) + d(Q_m \times P_2)$ and $d((D_n \times P_1) \times (Q_m \times P_2)) = d(D_n \times P_1) + d(Q_m \times P_2)$. $\square$

4.39 Proposition. Let A be a finitely generated abelian group and S be a finite solvable group. If P is a finite perfect group such that $d(S) \geq d(P)$ and $d(A \times S) = d(A) + d(S)$, then $d(A \times (S \times P)) = d(A) + d(S \times P)$.

Proof. Clearly, $d(A \times (S \times P)) = d(A) + d(S \times P)$. By Lemma 1.7, there exists an epimorphism $A \times (S \times P) \twoheadrightarrow A \times S$. Thus, $d(A \times (S \times P)) \geq d(A \times S)$. But, by Lemma 4.28, $d(A \times S) = d(A) + d(S) = d(A) + d(S \times P)$. Therefore, $d(A \times (S \times P)) = d(A) + d(S \times P)$. $\square$

4.40 Corollary. Let P be a finite perfect group so that $d(P) = 2$. Then, $d(C_n \times (D_m \times P)) = d(D_m \times P) + 1$ if $(n, m) \neq 1$.

Proof. By Theorem 3.6, $d(C_n \sim D_m) = d(D_m) + 1 = 3$ if $(n, m) \neq 1$.

Hence, it follows from Proposition 4.39 that $d(C_n \sim (D_m \times P)) = d(D_m \times P) + 1 = 3$ if $(n, m) \neq 1$. $\square$

4.41 Corollary. Let P be a finite perfect group so that $d(P) = 2$.

Then, $d(C_n \sim (Q_m \times P)) = d(Q_m \times P) + 1$ if $(n, m/2) \neq 1$.

Proof. By Corollary 3.11, $d(C_n \sim Q_m) = d(Q_m) + 1 = 3$ if $(n, m/2) \neq 1$.

It follows from Proposition 4.38 that $d(C_n \sim (D_m \times P)) = d(Q_m \times P) + 1 = 3$. $\square$

4.42 Proposition. Let H be a finitely generated imperfect group, with a minimal generating set of mutually coprime orders so that

$H/H' \cong C_n$. Let G be a finite solvable group and P be a finite

perfect group such that $d(G) = d(P)$. If $d(C_n \sim G) = d(G) + 1$,

then $d(H \sim (G \times P)) = d(G \times P) + 1$.

Proof. Lemma 1.5 gives an epimorphism from $H \sim (G \times P)$ onto

$C_n \sim (G \times P)$ induced by the epimorphism from H onto C_n . Also,

the epimorphism from $G \times P$ onto G induces an epimorphism from

$C_n \sim (G \times P)$ onto $C_n \sim G$. It follows that $d(H \sim (G \times P)) \geq$

$d(C_n \sim G)$. By Proposition 2.5, $d(H \sim (G \times P)) \leq d(G \times P) + 1$. But,

$d(G \times P) + 1 = d(G) + 1$ by Lemma 4.28. Therefore, $d(H \sim (G \times P)) =$

$d(G \times P) + 1$. $\square$

4.43 Corollary. Let H be a finitely generated imperfect group with a minimal generating set of mutually coprime orders so that $H/H' \cong C_n$

and P is a finite perfect group so that $d(P) = 2$. Then,

$d(H \sim (D_m \times P)) = d(D_m \times P) + 1$ for every m such that $(n, m) \neq 1$.

Proof. If $(n,m) \neq 1$, then $d(C_n \vee D_m) = d(D_m) + 1$ by Theorem 3.6.

Then, $d(H \vee (D_m \times P)) = d(D_m \times P) + 1$ by Proposition 4.42. $\square$

4.44 Corollary. Let H be a finitely generated imperfect group with a minimal generating set of finite mutually coprime orders so that

$H/H' \cong C_n$ and P is a finite perfect group so that $d(P) = 2$.

Then, $d(H \vee (Q_m \times P)) = d(Q_m \times P) + 1$ for all m where $(n,m/2) \neq 1$.

Proof. By Corollary 3.11, $d(C_n \vee Q_m) = d(Q_m) + 1$ for every m so

that $(n,m/2) \neq 1$. Then, $d(H \vee (Q_m \times P)) = d(Q_m \times P) + 1$ by

Proposition 4.42. $\square$

4.45 Remark. The same results as those in Proposition 4.39 and Proposition 4.42 hold if G and P are any finite groups such that $d(G \times P) = \max \{d(G), d(P)\}$.

4.46 Proposition. Let G be a finitely generated group and H be a finite group. If $d(G \vee H) = d(G) + d(H)$, then for any epimorphism from H onto $\bar{H}$, $d(G \vee H) = d(G \vee \bar{H})$.

Proof. Clearly, $d(G \vee \bar{H}) \leq d(G) + d(\bar{H}) \leq d(G) + d(H)$ but

$d(G) + d(H) = d(G \vee H)$ by the hypothesis.

4.47 Theorem. Let $\bar{G}$ and $\bar{H}$ be finitely generated periodic groups. Then, there exist infinitely many pairs of finitely generated groups G and H such that there exist epimorphisms from G onto $\bar{G}$ and from H onto $\bar{H}$, $d(G) = d(\bar{G})$, $d(H) = d(\bar{H})$ and $d(G \vee H) = d(G) + d(H)$.

Proof. Let $\{g_1, \dots, g_s\}$ be a minimal generating set of $\bar{G}$ and

$\{h_1, \dots, h_t\}$ be a minimal generating set of $\bar{H}$. Let the order of g_i be m_i for every i where $1 \leq i \leq s$. Let the order of h_j be n_j for every j where $1 \leq j \leq t$. Consider the groups $G = \bar{G} \times C_k^s$ and $H = \bar{H} \times C_k^t$ where $(k, m_i) = 1$ and $(k, n_j) = 1$ for every i and j such that $1 \leq i \leq s$ and $1 \leq j \leq t$. By Proposition 2.10, $d(G) = d(\bar{G})$ and $d(H) = d(\bar{H})$. The epimorphism from $G \times H$ onto C_k^{s+t} implies that $d(G \times H) \leq d(C_k^{s+t}) = s+t$. On the other hand, $d(G \times H) \geq d(G) + d(H) = d(\bar{G}) + d(\bar{H})$. Consequently, $d(G \times H) = d(G) + d(H)$. $\square$

4.48 Remarks. It is possible to build more groups G_1 and H_1 such that $d(G_1 \times H_1) = d(G_1) + d(H_1)$. Starting with the groups G and H , in the proof of Theorem 4.47, we can build larger groups by attaching suitable finitely generated groups to them. Let A be a group such that $d(A) < d(G)$ and $d(G \times A) = d(G)$. Similarly, choose any group B such that $d(B) < d(H)$ and $d(H \times B) = d(H)$. Consider $G_1 = G \times A$ and $H_1 = H \times B$. Then, $d(G_1 \times H_1) \leq d(G_1) + d(H_1) = d(G) + d(H)$. Moreover, the epimorphism from $G_1 \times H_1$ onto $G \times H$ gives the reverse inequality $d(G_1 \times H_1) \geq d(G \times H) = d(G) + d(H)$. Consequently, $d(G_1 \times H_1) = d(G_1) + d(H_1)$.

One way of choosing a periodic group A so that $d(G \times A) = d(G)$ is by ensuring that the orders of its minimal generating set are coprime to the orders of a minimal generating set of G . This provides us with a method of constructing infinitely many groups with the desired minimal numbers of generators.

Chapter 5

BOUNDS FOR THE NUMBERS OF GENERATORS OF SOME GROUPS

Although the task of pinpointing the exact minimal number of generators of a finite group can prove to be an intractable one, the attempts to bound the number of generators have yielded some interesting results. For a finite nilpotent group G , we know that if $d = \max\{d(G_p) \mid p \mid |G|\}$ then the minimal number of generators of the group G is precisely d . In 1967, Kovács [11] enlarged the scope to finite solvable groups and showed that if each p -Sylow subgroup can be generated by d elements, the group itself can be generated by $d+1$ elements. In 1986, Longobardi and Maj [12] obtained a bound for arbitrary finite groups. For finite groups with zero generation gaps, the bound given by Roggenkamp [17] for finite groups in 1973 is lower. In fact, Roggenkamp's result includes Kovács' bound as a special case. In light of these results, the natural question that arises is whether these bounds can be improved in some situations.

5.1 Theorem (Kovács, 1967, [11]) If every p -Sylow subgroup of a finite solvable group can be generated by d elements, then the group itself can be generated by $d+1$ elements.

5.2 Theorem (Longobardi & Maj, 1986, [12]) If every p -Sylow subgroup of a finite group can be generated by d elements, then the group itself can be generated by $2d$ elements.

Roggenkamp's bound, for the number of generators of a finite group,

exceeds the one for a solvable group by exactly $\text{gap}(G)$. We will show that the lower one, corresponding to the one for solvable groups, would suffice for at least some groups with nonzero gap. An example of such a group with nonzero gap is the direct product of sufficiently many copies of a perfect group. It turns out that this lower bound would work for the direct product of sufficiently many copies of any finite group. This observation is heavily based on a combination of results of Wiegold [18] and Roggenkamp [17]. Before proceeding with the statement of the relevant results, it is essential to introduce the terminology that will be used.

5.3 Definition. Let G be a finite group. Consider the ring homomorphism, $\mathbb{Z}G \rightarrow \mathbb{Z}$ given by $\sum m_g g \mapsto \sum m_g$. The kernel of this homomorphism, which is called the augmentation of $\mathbb{Z}G$, is called the *augmentation ideal* of G and is denoted by $\mathcal{G}$.

5.4 Definition. Let G be a finite group and $\mathcal{G}$ be its augmentation ideal. Let $d_{\mathbb{Z}G}(\mathcal{G})$ be the minimal number of generators of $\mathcal{G}$ as a left $\mathbb{Z}G$ -module. The *generation gap* of G is $d(G) - d_{\mathbb{Z}G}(\mathcal{G})$ and is denoted by $\text{gap}(G)$.

$\text{Gap}(G)$ is always nonnegative since for every system of generators for G , $\{g_i \mid 1 \leq i \leq n\}$, there is a canonical system of generators for $\mathcal{G}$ as a left $\mathbb{Z}G$ -module, $\{g_i - 1 \mid 1 \leq i \leq n\}$. Roggenkamp showed in [17] that $\text{gap}(G)$ coincides with the presentation rank of G and attained a bound for $d(G)$ in terms of it.

5.5 Theorem. (Roggenkamp, 1973, [17]) If G is a finite group, then $d(G) \leq \max_{p \mid |G|} \{d(G_p)\} + \text{gap}(G) + 1$.

5.6 Theorem. (Roggenkamp, 1973, [17]) If G is a finite group, then $d(G) - d(G/G') \geq \text{gap}(G)$.

5.7 Theorem. (Wiegold, 1975, [18]) If G is a nontrivial finite perfect group, s is the size of the smallest simple image of G and c is any real number greater than 1, then $d(G^r) \leq c \log_s r$ for all sufficiently large r .

5.8 Proposition. If G is a finite group and $D = G^r$, then $d(D) \leq \max_{p \mid |G|} \{d(D_p)\} + 1$ for all sufficiently large r .

Proof. Firstly, consider the case when G is an imperfect finite group. Then $d(G^r/(G^r)') = d(G/G')^r = \text{rd}(G/G')$ by Proposition 4.11. Moreover, $\text{rd}(G/G') = d(G^r)$ for all sufficiently large r by Theorem 4.8 of Wiegold. It follows from Theorem 5.6 of Roggenkamp that $\text{gap}(G^r) = 0$, for all sufficiently large r . Consider $D = G^r$. Then $d(D) \leq \max_{p \mid |G|} \{d(D_p)\} + 1$, for all sufficiently large r , by Roggenkamp's bound in Theorem 5.5.

Now, consider the case when G is a perfect finite group. Wiegold's bound in Theorem 5.7 is $d(D) \leq c \log_s r$ where s is the size of the smallest simple image of G , c is any real number greater than 1 and r is sufficiently large. We will show that $c \log_s r$ is less than the desired bound. Let $P = G_{P_1}$ where $d(P) = \max_{p \mid |G|} \{d(G_p)\}$. By the linearity of the growth of the number of

generators of the direct product of p -groups, $d(P^x) = \max_{P \mid |D|} \{d(D_P)\}$, where P^x is the p -Sylow subgroup of D with the maximal number of generators. By Theorem 0.10, since G is not solvable, G possesses a noncyclic p -Sylow subgroup, implying that P is noncyclic. Thus, $d(P) = m \geq 2$ and $d(P^x) = mr$ clearly exceeds the bound given by Wiegold in Theorem 5.7. Hence, $d(D) \leq \max \{d(D_P)\}$. $\square$

5.9 Remark. Since Theorem 4.9 holds for finitely generated groups, the same bound holds for $D = G^x$ if G is finitely generated and imperfect.

It is interesting to observe that the number of generators of the wreath products of many finite groups can be bounded by the maximum of the number of generators of its p -Sylow subgroups. However, it is not surprising if we consider the structure of the wreath product of two groups.

Let K and H be nontrivial finite groups and consider $K \wr H$. Intuitively, as long as H is large enough, we can produce a p -Sylow subgroup of K which has a "large" number of generators. This is ensured by the linear nature of the growth of the number of generators of the direct product of p -groups. If a particular p is coprime to the order of H , then this p -Sylow subgroup is also the p -Sylow subgroup of the wreath product itself.

5.10 Lemma. If H is a finite group with at least 3 elements, then $d(H) \leq |H| - 2$.

Proof. Let H be a finite group with at least 3 elements. Since it is obvious that $d(H)$ cannot exceed the order of H , it suffices to

show that it cannot be equal to the order of H or one less than the order of H .

Firstly, consider the case when $d(H)$ coincides with the order of H . Then H is a minimal generating for itself, implying that the identity element is a generator. This is possible only when H is the trivial group.

On the other hand, if $d(H)$ is one less than the order of H , H is nontrivial. This guarantees the exclusion of the identity element from any minimal generating set of H . Let $r = d(H)$ and $\{h_1, h_2, \dots, h_r\}$ be a minimal generating set for H . Then $H = \langle h_1, h_2, \dots, h_r, 1 \rangle$ where each h_i is nontrivial. If the order of some h_i exceeds 2, then h_i^2 coincides with h_k for some k other than i , thus contradicting the minimality of $\{h_1, \dots, h_r\}$. This eliminates all possibilities except when each h_i has order 2. Any group, with all nontrivial elements of order 2 on r generators, is isomorphic to the elementary abelian 2-group of rank r . Finally, the hypothesis $r = |H| - 1$ forces H to be C_2 . Consequently, $d(H) = |H| - 2$. $\square$

5.11 Theorem. Let K and H be nontrivial finite groups so that $d(K_q) = \max_{p \mid |K|} \{d(K_p)\}$ and q is coprime to the order of H . If $G = K \wr H$ is the wreath product of K by H , then

$$d(G) \leq \begin{cases} \max_{p \mid |G|} \{d(G_p)\} & \text{if } |H| > 2, \\ \max_{p \mid |G|} \{d(G_p)\} + 1 & \text{if } |H| = 2. \end{cases}$$

Proof. Let K and H be finite nontrivial groups and G be the wreath product of K by H . Then, $G \cong K^{|H|} \times H$. Let $k = d(K_q)$. Let us consider the case when H has more than 2 elements. Then, $d(G) = d(K) + d(H) = 2k + d(H)$ because of Theorem 5.2. By Lemma 5.10, $2k + d(H) = k|H|$. Moreover, $k|H| = d(K_q^{|H|})$ by Theorem 4.12. Since q is coprime to $|H|$, $d(K_q^{|H|}) = d(G_q)$. It is obvious that $d(G_q) = \max_{p \mid |G|} \{d(G_p)\}$. Consequently, $d(G) \leq \max_{p \mid |G|} \{d(G_p)\}$ if H has more than 2 elements.

Now, consider the case when H has exactly 2 elements. Then, $d(G) = d(K) + d(H)$ and $d(K) + d(H) = 2k + 1$ by Theorem 5.2. But $2k + 1 = k|H| + 1 = d(K_q^{|H|}) + 1$ by Theorem 4.7. Since q is coprime to $|H|$, $d(K_q^{|H|}) + 1 = d(G_q) + 1$. Obviously, we have $d(G_q) + 1 \leq \max_{p \mid |G|} \{d(G_p)\} + 1$. Hence, $d(G) \leq \max_{p \mid |G|} \{d(G_p)\} + 1$ if H has order 2.

5.12 Corollary. If G is the wreath product of K by H , where K and H are nontrivial finite groups of coprime orders and H has more than 2 elements, then $d(G) = \max_{p \mid |G|} \{d(G_p)\}$.

Proof. Since K and H have coprime orders, they satisfy the condition specified in Theorem 5.11. $\square$

Although the case when p_i and $|H|$ are coprime seems to be simple enough, the corresponding problem when they are not coprime is more complex. However, the case when both groups are finite p -groups is trivial since the resulting wreath product is a finite p -group.

Now, consider the direct product of two finitely generated groups.

Under certain conditions, it is possible to bound the number of generators of the direct product of two such groups.

5.13 Proposition. Let H and K be finitely generated groups such that $d(H) \geq d(K)$, $d(H) = \max_{p \mid |H \times K|} \{d(H_p)\} + 1$, and $d(H \times K) = \max\{d(H), d(K)\}$. Then, $d(H \times K) = \max_{p \mid |H \times K|} \{d(H \times K)_p\} + 1$.

Proof. By the hypothesis, we have $d(H \times K) = d(H) = \max_{p \mid |H \times K|} \{d(H_p)\} + 1$.

Clearly, $\max_{p \mid |H \times K|} \{d(H_p)\} + 1 = d(H_q) + 1$ for some q dividing $|H|$.

Obviously, $d(H_q) + 1 \leq d(H_q) + d(K_q) + 1$. By Theorem 4.12, $d(H_q) + d(K_q) + 1 = d(H \times K)_q + 1$ and clearly $d(H \times K)_q + 1 \leq \max_{p \mid |H \times K|} \{d(H \times K)_p\} + 1$.

Consequently, $d(H \times K) \leq \max_{p \mid |H \times K|} \{d(H \times K)_p\} + 1$. $\square$

5.14 Corollary. Let H and K be finitely generated solvable and perfect groups respectively, such that $d(H) = d(K)$. Then

$$d(H \times K) = \max_{p \mid |H \times K|} \{d(H \times K)_p\} + 1.$$

Proof. By Lemma 4.28 of Gruenberg, $d(H \times K) = d(H)$. By Theorem 5.1 of Kovács, $d(H) = \max_{p \mid |H|} \{d(H_p)\} + 1$. The desired result follows directly from Proposition 5.13. $\square$

5.15 Corollary. Let H be a finite simple nonabelian group and let K be a cyclic group. If $G = H \times K$, then $d(G) = \max_{p \mid |G|} \{d(G_p)\} + 1$.

Proof. According to Aschbacher & Guralnick [1], $d(H) = 2$ since H is a finite simple group. Hence, $d(H) = d(K)$. By Lemma 4.28, $d(H \times K) = d(H)$. By Theorem 0.10 of Burnside, H has a non-cyclic p -Sylow subgroup since it is not solvable. So, $d(H) = \max_{p \mid |H|} \{d(H_p)\}$.

The result follows directly from Proposition 5.13. $\square$

5.16 Corollary. Let H and K be finite groups satisfying the following conditions:

$$(i) \quad d(H) = d(K);$$

$$(ii) \quad d(H) = \max_{p \mid |H|} \{d(H)_p\} + 1;$$

(iii) There exists a minimal generating set of K , $\{k_1, k_2, \dots, k_n\}$ such that $n = d(K)$ and there exists a minimal generating set of H , $\{h_1, h_2, \dots, h_m\}$ where $m = d(H)$ and the order of k_i is coprime to the order of h_i for every i , $1 \leq i \leq n$. Then $d(H \times K) = \max_{p \mid |H \times K|} \{d(H \times K)_p\} + 1$.

Proof. It follows from condition (iii) and Proposition 2.10 that $d(H \times K) = d(H)$. The result follows from Proposition 5.13.

5.17 Theorem. (Gruenberg, 1973, [7]) If G is a finite group, then $d(\mathbf{Z} \rtimes G) = d(G) + 1$ iff $\text{gap}(G) = 0$.

This theorem by Gruenberg can be used to prove Proposition 5.13 if H and K are finite and $\text{gap}(H) = 0$. We do so by showing that $\text{gap}(H \times K)$ is also zero. By Theorem 5.17, $d(\mathbf{Z} \rtimes H) = d(H) + 1$ since $\text{gap}(H) = 0$. Moreover, we have the epimorphism $\mathbf{Z} \rtimes (H \times K) \twoheadrightarrow \mathbf{Z} \rtimes H$, by Lemma 1.7, which is induced by the natural epimorphism $H \times K \twoheadrightarrow H$. Thus, $d(\mathbf{Z} \rtimes (H \times K)) \geq d(\mathbf{Z} \rtimes H) = d(H) + 1$. On the other hand, $d(\mathbf{Z} \rtimes (H \times K)) \leq d(H \times K) + 1 = d(H) + 1$. Therefore, $d(\mathbf{Z} \rtimes (H \times K)) = d(H \times K) + 1$. By Theorem 5.17, $\text{gap}(H \times K)$ is zero. Now, it follows from Theorem 5.5 that $H \times K$ has the desired bound.

The following results of Gruenberg yields an interesting consequence in our context.

5.18 Theorem. (Gruenberg, 1973, [7]) Let G be a finite group.
 $d(\mathbb{Z} \wr G) = d(G)$ iff $d(C_p \wr G) = d(G)$ for every p dividing $|G|$,
 where p is a prime number.

5.19 Example. By Theorem 3.6 and Example 3.19, we have

$$d(C_p \wr S_3) = \begin{cases} 2 & \text{if } p = 2, \\ 3 & \text{if } p = 3. \end{cases}$$

5.20 Theorem. (Gruenberg, 1974, [5, p.37]) If G is a finite solvable group, then $\text{gap}(G) = 0$.

5.21 Remark. By Theorem 5.20, $\text{gap}(S_3) = 0$. Hence, $d(\mathbb{Z} \wr S_3) = d(S_3) + 1 = 3$ by Theorem 5.17. By Example 3.19, $d(C_2 \wr S_3) = 2$. By Theorem 5.18, $d(\mathbb{Z} \wr S_3) = 3$ implies that there exists a prime p dividing $|S_3|$ such that $d(C_p \wr S_3) = 3$. Since 3 is the only prime, other than 2, dividing S_3 , $d(C_3 \wr S_3) = 3$.

5.22 Proposition. Let G be a finite solvable group and let P be a finite perfect group such that $d(G) < d(P)$. Then there exists a prime number p dividing $|G|$ so that for every n which is a multiple of p , $d(C_n \wr (G \times P)) = d(G \times P) + 1$.

Proof. Clearly, $d(C_n \wr (G \times P)) \geq d(G \times P) + 1$. We will prove the reverse inequality. Since G is finite and solvable, $\text{gap}(G) = 0$ by Theorem 5.20. Also, $d(\mathbb{Z} \wr G) = d(G) + 1$ by Theorem 5.17. Moreover, Theorem 5.18 ensures that there is a prime number p dividing $|G|$ such that $d(C_p \wr G) = d(G) + 1$. By Lemma 1.5, for every n which is a multiple of p , there is an epimorphism $C_n \wr G \twoheadrightarrow C_p \wr G$ induced by the epimorphism from C_n to C_p . Thus, $d(C_n \wr G) = d(G) + 1$.

By Lemma 4.28, $d(G \times P) = d(G)$. Hence, we have the epimorphism

$C_n \sim (G \times P) \twoheadrightarrow C_n \sim G$ induced by the epimorphism $G \times P \twoheadrightarrow G$,

by Lemma 1.7. Therefore, $d(C_n \sim (G \times P)) \geq d(C_n \sim G) = d(G) + 1$.

Moreover, $d(G) + 1 = d(G \times P) + 1$. Consequently, $d(C_n \sim (G \times P))$

$= d(G \times P) + 1$ and $d(C_n \sim (G \times P)) = d(G \times P) + 1$. $\square$

5.23 Remark. The same result holds if G and P are finite groups such that $d(G) = d(P)$, $\text{gap}(G) = 0$ and $d(G \times P) = \max\{d(G), d(P)\}$.

Chapter 6

GRUSHKO-NEUMANN'S THEOREM FOR THE FREE PROFINITE PRODUCT OF SOME GROUPS

The theorem of Grushko (1940) and Neumann (1943) is undoubtedly a pinnacle in the theory concerning the free product of abstract groups. Since the theory of profinite groups thrives on parallelism to the existing theory of finite groups, it is natural for profinite group theorists to ponder about the adaptability of this theorem to the profinite setting. In contrast to the success in the creation of a profinite analogue of the Kurosh Subgroup Theorem for free products, little progress has been made towards the proof or disproof of the profinite analogue of Grushko-Neumann's Theorem. The original version of Grushko-Neumann's Theorem states that $d(G * H) = d(G) + d(H)$ if G and H are discrete finitely generated groups [13, p.91]. The main motivation of this thesis is the question whether the profinite analogue of Grushko-Neumann's Theorem holds. Before discussing the problem in detail, we will first review some basic notions in topology and profinite group theory.

The following basic topological terminology is based on Munkres [15].

6.1 Definition. A topology on a set X is a family $\mathcal{T}$ of subsets of X having the following properties:

- (i) $\emptyset$ and X are in $\mathcal{T}$;
- (ii) The union of any subfamily of $\mathcal{T}$ is in $\mathcal{T}$;
- (iii) The intersection of elements of any finite subfamily of $\mathcal{T}$ is in $\mathcal{T}$.

A set X with a topology $\mathcal{T}$ is called a *topological space*.

6.2 Definition. If X is a topological space of a topology $\mathcal{T}$, a subset U of X is an *open set* of X if U belongs to $\mathcal{T}$. A subset U is *closed* if $X \setminus U$ is open.

6.3 Definition. If X is any set, the family of all subsets of X is a topology on X called the *discrete topology*.

6.4 Definition. A topological space X is *Hausdorff* if for each pair x, y of distinct points of X , there exist disjoint neighbourhoods U, V of x, y respectively.

6.5 Definition. A family $\mathcal{Y}$ of subsets of X is a *covering* of X if the union of the elements of $\mathcal{Y}$ is equal to X . It is an *open covering* of X if the elements are open subsets of X .

6.6 Definition. A topological space X is *compact* if every open covering $\mathcal{Y}$ of X contains a finite subfamily which covers X .

6.7 Definition. A topological space is *totally-disconnected* if its only connected subsets are one-point sets.

Next, we will introduce the notion of an inverse limit of an inverse system. For more details, consult Eilenberg & Steenrod [4].

6.8 Definition. A set I is *quasi-ordered* if it has a relation $i \leq j$ which is reflexive and transitive.

6.9 Definition. A set I is *directed* if it is quasi-ordered and for every pair $i, j \in I$, there exists $k \in I$ so that $i \leq k$ and $j \leq k$.

6.10 Definition. Let I be a directed set. Let $\mathcal{C}$ be a category and $\{G_i\}$ be a family of objects in $\mathcal{C}$. For each $i \in I$, there is an object G_i . If $i \leq j$, assume that there is a morphism $\psi_{ji} : G_j \rightarrow G_i$ such that if $i \leq j \leq k$ then $\psi_{ji} \circ \psi_{kj} = \psi_{ki}$ and $\psi_{ii} = \text{id}$ for every $i \in I$. In other words, the following diagram commutes:

The system $\{G_i \mid \psi_{ji}\}$ is called an *inverse system* in $\mathcal{C}$, over the directed set I .

6.11 Definition. Let $\{G_i \mid \psi_{ji}\}$ be an inverse system, in a category $\mathcal{C}$ over a directed set I , where each morphism $\psi_{ji} : G_j \rightarrow G_i$ is an epimorphism. The *inverse limit* of $\{G_i \mid \psi_{ji}\}$, denoted by $G = \varprojlim G_i$, is an object in $\mathcal{C}$ with a family of morphisms, $\phi_i : G \rightarrow G_i$ such that $\phi_i = \psi_{ji} \phi_j$ and whenever $i \leq j$, the following diagram commutes

For example, if we consider the category of groups, note that each

morphism ϕ_i is onto, since each ψ_{ji} is onto. In addition, G is the subset of the product $\prod_{i \in I} G_i$, consisting of the functions $x = (x_i)$ such that for each relation $i \leq j$ in I , $\psi_{ji}(x_j) = x_i$.

We will state some basic concepts of profinite group theory.

This exposition follows the introduction of the subject by Ribes [16].

6.12 Definition. A *profinite group* is the inverse limit of an inverse system, over a directed set, of finite groups. We think of such a group as a topological group in a natural way. Specifically, if $\{G_i, \psi_{ji}\}$ is an inverse system over I where each G_i is a finite group with the discrete topology, then $\varprojlim G_i$ is the closed subgroup of $\prod_{i \in I} G_i$ consisting of (x_i) such that $\psi_{ji}(x_j) = x_i$ for every $i \leq j$. (The topology of $\prod_{i \in I} G_i$ is the product topology.)

6.13 Proposition. If $G = \varprojlim G_i$ is a profinite group, where $\{G_i \mid i \in I\}$ is an inverse system of discrete finite groups, then $\underline{S} = \{\text{Ker}(G \rightarrow G_i) \mid i \in I\}$ is a basis of open neighbourhoods of 1 in G .

6.14 We follow the convention that all subgroups are closed and that all maps between two profinite groups are continuous. If G is a profinite group, then the *open subgroups* of G are the closed subgroups of finite index in G . In fact, every open neighbourhood of 1 contains an open normal subgroup.

6.15 Definition. Let $\underline{C}$ be a class of finite groups, closed under the formation of subgroups, quotient groups and group extensions. A profinite group G is a *pro- $\underline{C}$ group* if $G/U \in \underline{C}$ for every open normal subgroup U of G .

6.16 Definition. Let A be a set and G a $\text{pro-}\underline{C}$ group. A map $x: A \rightarrow G$ is convergent to 1 if every open normal subgroup of G contains almost every (all but a finite number) of the images x_α , $\alpha \in A$.

6.17 Definition. A free $\text{pro-}\underline{C}$ group on a set A is a $\text{pro-}\underline{C}$ group F with a map $x: A \rightarrow F$ convergent to 1, satisfying the following universal property: If $y: A \rightarrow G$ is any map convergent to 1 of A into a $\text{pro-}\underline{C}$ group, then there exists a unique continuous homomorphism $h: F \rightarrow G$ such that the diagram

$$\begin{array}{ccc} A & \xrightarrow{x} & F \\ & \searrow y & \swarrow h \\ & G & \end{array}$$

commutes. The x_α 's generate a dense subgroup of F and form a (topological) system of generators of F .

We give the definition of the free $\text{pro-}\underline{C}$ product according to Binz, Neukirch and Wenzel [2].

6.18 Definition. The free $\text{pro-}\underline{C}$ product of $\text{pro-}\underline{C}$ groups G_1 and G_2 is a $\text{pro-}\underline{C}$ group, $G_1 \amalg G_2$, with the homomorphisms $\{G_i \rightarrow G_1 \amalg G_2 \mid i=1,2\}$ satisfying the following universal property: If $\{\phi_i: G_i \rightarrow H \mid i=1,2\}$ is any pair of homomorphisms into a $\text{pro-}\underline{C}$ group H , then there exists a unique homomorphism $\gamma: G_1 \amalg G_2 \rightarrow H$ so that the following diagrams commute:

$$\begin{array}{ccc} G_i & \longrightarrow & G_1 \amalg G_2 \\ & \searrow \phi_i & \swarrow \gamma \\ & H & \end{array}$$

The free $\text{pro-}\underline{C}$ product can be constructed explicitly as follows:

2 of/de 2

MicroD

Consider the discrete free product $G_1 * G_2$ and F the family of all normal subgroups N of $G_1 * G_2$ such that:

$$(i) \quad (G_1 * G_2)/N \in \underline{C};$$

(ii) $N \cap G_i$ is an open subgroup of G_i , where $i = 1$ or 2 . F is a basis of open neighbourhoods of 1 of $G_1 * G_2$, hence defining a topology on $G_1 * G_2$. The completion of $G_1 * G_2$ with respect to this topology, determined by F , is $G_1 \coprod G_2 = \varprojlim (G_1 * G_2)/N$.

Recall the finite problem (I) stated in the introduction of Chapter 3.

- (I) Given two finite groups G and H , does there exist a finite group T containing G and H so that $T = \langle G, H \rangle$ and $d(T) = d(G) + d(H)$?

A profinite group is finitely generated if it contains a dense subgroup which is finitely generated as an abstract group. (A subset Y of a topological space X is dense if $\overline{Y} = X$. $\overline{Y}$ is the intersection of closed sets containing Y and is called the closure of Y .) If G is a profinite group, then $d(G)$ is the smallest cardinality of a set of topological generators of G .

The focus of this chapter is the question whether the profinite analogue of Grushko-Neumann's Theorem holds. The problem can be stated as follows:

- (II) Let G and H be finitely generated profinite groups. If $G \coprod H$ is their free profinite product, is $d(G \coprod H) = d(G) + d(H)$?

Naturally, we can formulate an analogous problem for the free pro- $\underline{C}$ product of finitely generated pro- $\underline{C}$ groups as follows:

(III) Let G and H be finitely-generated pro- $\underline{C}$ groups. If

$G \coprod H$ is their free pro- $\underline{C}$ product, is $d(G \coprod H) = d(G) + d(H)$?

Lubotzky [14, prop. 2.9] has given a positive answer to (III) in the case when G and H are finitely generated pro- p groups, in 1982. We will relate (II) to (I). Before explaining the relation between these two problems, it is necessary to prove the following lemma and proposition.

6.19 Lemma. Let G be a profinite group such that $d(G) \leq n$. If $X = \{(x_1, \dots, x_n) \in G^n \mid \langle x_1, \dots, x_n \rangle = G\}$, then X is a nonempty compact subspace of G^n .

Proof. Let G be a profinite group with $d(G) \leq n$. By [15, Theorem 2.2], G can be expressed as $\varprojlim G/U$ where U is in the family of open normal subgroups of G . $\{G/U \mid \phi_{UV}\}$ is the inverse system of finite groups with $\phi_{UV} : G/U \rightarrow G/V$ for every $U \subseteq V$. Note that every G/U is finite and $d(G/U) \leq n$. Consider the subset of $(G/U)^n$, $X_U = \{(x_1^U, \dots, x_n^U) \in (G/U)^n \mid \langle x_1^U, \dots, x_n^U \rangle = G/U\}$. Then, X_U is nonempty and compact. Define the map $\bar{\phi}_{UV} : X_U \rightarrow X_V$ by $\bar{\phi}_{UV}(x_1^U, \dots, x_n^U) = (\phi_{UV}(x_1^U), \dots, \phi_{UV}(x_n^U))$. Then, $\bar{\phi}_{UV}(X_U) \subseteq X_V$ whenever $U \subseteq V$. Hence, $\{X_U, \bar{\phi}_{UV}\}$ forms an inverse system and $X = \varprojlim X_U$. Since X is the inverse limit of nonempty compact sets, X is nonempty and compact by [4, p.217]. $\square$

6.20 Proposition. Let $\{G_i \mid \phi_{ij}\}$ be an inverse system of profinite groups, with each ϕ_{ij} an onto map. If $G = \varprojlim G_i$, then $d(G) = \max \{d(G_i)\}$.

Proof. For every $i \geq j$, there exists an epimorphism ϕ_{ij} from G_i onto G_j . Also, there is an epimorphism ϕ_i from G onto G_i for every i . Hence, $d(G) \geq d(G_i)$. If $d(G_i)$ is unbounded, $d(G)$ would be infinite. So, we will assume that $d(G_i)$ is bounded for i in I . Let $\max\{d(G_i)\} = n$. Let X_i be the set of n -tuples as follows:

$$X_i = \{(x_1^i, \dots, x_n^i) \in G_i^n \mid \langle x_1^i, \dots, x_n^i \rangle = G_i\}.$$

Then, X_i is nonempty for every i . If $i \geq j$, define the map $\bar{\phi}_{ij} : X_i \rightarrow X_j$ by $\bar{\phi}_{ij}(x_1^i, \dots, x_n^i) = (\phi_{ij}x_1^i, \dots, \phi_{ij}x_n^i)$. Clearly, $\bar{\phi}_{ij}(X_i) \subseteq X_j$ for all i and j such that $i \geq j$. Hence, $\{X_i, \bar{\phi}_{ij}\}$ forms an inverse system. Since each X_i is nonempty and compact by Lemma 6.19, $X = \varprojlim X_i$ is nonempty and compact by [4, p.217]. Note that $(x_1, \dots, x_n) \in X$ implies that $x_r \in G = \varprojlim G_i$, for every r , $r = 1, \dots, n$. Then $\phi_i \langle x_1, \dots, x_n \rangle = \langle \phi_i x_1, \dots, \phi_i x_n \rangle = G_i$, whereby $\langle x_1, \dots, x_n \rangle = G$ by [16, p.19]. Therefore, $d(G) = \max \{d(G_i)\}$. $\square$

Given two finitely generated profinite groups, G and H , Proposition 6.20 shows that there exist finite quotients of G and H , $\bar{G}$ and $\bar{H}$ respectively such that $d(\bar{G}) = d(G)$ and $d(\bar{H}) = d(H)$. Since there exists an epimorphism from $G \amalg H$ onto $\bar{G} \amalg \bar{H}$, (II) can be reduced to the following problem:

(IV) Let G and H be finite groups. If $G \amalg H$ is their free profinite product, is $d(G \amalg H) = d(G) + d(H)$?

Consider $G * H$, the abstract free product of two finite groups G and H . Let F denote the family of finite quotients of $G * H$.

Then, $G \amalg H = \varprojlim F_i$ where $F_i \in F$. It follows from Proposition 6.20 that $d(G \amalg H) = \max \{d(F_i) \mid F_i \in F\}$. It is clear that $d(G \amalg H)$ is at most $d(G) + d(H)$ since each F_i is a quotient of $G * H$ and $d(F_i) \leq d(G * H) \leq d(G) + d(H)$.

Proposition 6.20 implies that (IV) is equivalent to the following problem:

(V) If G and H are finite groups, does there exist a finite quotient group T of $G * H$ so that $d(T) = d(G) + d(H)$?

It is clear that a positive solution to (I) would imply a positive solution to (V), (IV) and hence (II). In fact, we will show that (V) and (I) are equivalent.

6.21 Proposition. Let A and B be finite groups. Then $d(A \amalg B) = d(A) + d(B)$ if and only if there exists a finite group G containing A and B such that $G = \langle A, B \rangle$ and $d(G) = d(A) + d(B)$.

Proof. Suppose that there exists a finite group G containing A and B such that $G = \langle A, B \rangle$ and $d(G) = d(A) + d(B)$. Then, the natural homomorphism $\phi : A \amalg B \rightarrow G$ that sends A to A identically and B to B identically, is an epimorphism. Therefore, $d(A \amalg B) \geq d(G) = d(A) + d(B)$. But, obviously, $d(A \amalg B) \leq d(A) + d(B)$. Therefore, $d(A \amalg B) = d(A) + d(B)$.

Conversely, suppose that $d(A \amalg B) = d(A) + d(B)$. By Proposition 6.20, there exists an open normal subgroup N of $A \amalg B$ such that $d(A \amalg B) = d((A \amalg B)/N)$. Note that if $M \leq N$ and $M \triangleleft A \amalg B$, we also have $d(A \amalg B) = d((A \amalg B)/M)$ since $(A \amalg B)/N$ is a homomorphic image of $(A \amalg B)/M$. Choose such an M so that, in addition, $M \cap A = M \cap B = \{1\}$. Then, $(A \amalg B)/M \cong AM/M \cong A/M \cap A \cong A$ and $(A \amalg B)/M \cong BM/M \cong B/M \cap B \cong B$. Clearly, $(A \amalg B)/M = \langle AM/M, BM/M \rangle$. $\square$

The following lemma is a special case of a lemma by Herfort & Ribes [9].

6.22 Lemma. (Herfort & Ribes, 1985) Let G and H be pro- $\mathbb{C}$ groups.

If $G \amalg H$ is their free pro- $\mathbb{C}$ product, then $G \amalg H =$

$\varprojlim_{\substack{U \in F \\ V \in S}} (G/U \amalg H/V)$, where F and S denote the families of open normal subgroups of G and H , respectively.

6.23 Theorem. Let G and H be finitely generated free profinite groups. Then, there exist open normal subgroups $\bar{U}$ and $\bar{V}$ in G and H respectively such that for every open normal subgroup $U \leq \bar{U}$ of G , for every open normal subgroup $V \leq \bar{V}$ of H , $d(G/U \amalg H/V) = d(G/U) + d(H/V)$ for the free profinite product $G/U \amalg H/V$. Moreover, $d(G/U) = d(G)$ and $d(H/V) = d(H)$.

Proof. Let F and S be the families of open normal families of G and H , respectively. Let $G \amalg H$ be the free profinite product of G and H . Since G and H are free profinite groups, $G \amalg H$ is

a free profinite group. Thus, the generators of G and H form a basis for $G \coprod H$ and $d(G \coprod H) = d(G) + d(H)$. By Lemma 6.22,

$$d(G \coprod H) = d(\varprojlim_{\substack{U \in F \\ V \in S}} G/U \coprod H/V). \text{ Moreover, } d(\varprojlim_{\substack{U \in F \\ V \in S}} G/U \coprod H/V) =$$

$\max\{d(G/U \coprod H/V)\}$ by Proposition 6.20. But, $\max\{d(G/U \coprod H/V)\} =$

$d(G/\bar{U} \coprod H/\bar{V})$ for some $\bar{U} \in F$ and $\bar{V} \in S$. Clearly, $d(G/\bar{U} \coprod H/\bar{V})$

$\leq d(G/\bar{U}) + d(H/\bar{V}) \leq d(G) + d(H)$. However, these two inequalities

must be equalities as $d(G/\bar{U} \coprod H/\bar{V}) = d(G) + d(H)$. Hence,

$d(G/\bar{U}) + d(H/\bar{V}) = d(G) + d(H)$ and it follows that $d(G/\bar{U}) = d(G)$ and

$d(H/\bar{V}) = d(H)$. Thus, for all $U \leq \bar{U}$ and $V \leq \bar{V}$, we have

$d(G/U \coprod H/V) = d(G/U) + d(H/V) = d(G) + d(H)$. This is because there

is an epimorphism from $G/U \coprod H/V$ onto $G/\bar{U} \coprod H/\bar{V}$ induced by the

epimorphisms from G/U onto $G/\bar{U}$ and from H/V onto $H/\bar{V}$. $\square$

We will summarize the results obtained in Chapter 3 and Chapter 4 to give a partial solution to (V) and hence to (IV). If G and H are two finite groups, let $G \coprod H$ be their free profinite product. Then, $d(G \coprod H) = d(G) + d(H)$ if G and H satisfy the following conditions:

G	H	Conditions
C_n	D_m	$(m, n) \neq 1$
D_n	D_m	n and m even
C_n	Q_m	$(m/2, n) \neq 1$
Q_n	Q_m	$n/2$ and $m/2$ even
C_n	$D_m \times H$	$(m, n) \neq 1$, $d(H) \leq 2$ where the orders of a minimal generating set of H are coprime to those of D_m

G	H	Conditions
$G_1 \circ \dots \circ G_r$	G_{r+1}	<p>(i) $d(G_1 \circ \dots \circ G_r) = d(\prod_{i=1}^r G_i / (G_i)')$;</p> <p>(ii) $\prod_{i=1}^r G_i / (G_i)'$ and $G_{r+1} / (G_{r+1})'$ are not coprime;</p> <p>(iii) $d(G_i / (G_i)') = d(G_i)$.</p>
$B(n, r)$	$B(n, s)$	$B(n, r+s)$ is finite.
G_1	G_2	<p>$d(G_i / (G_i)') = d(G_i)$;</p> <p>$G_1 / (G_1)'$ and $G_2 / (G_2)'$ are not coprime.</p>
G^r	H^s	<p>G and H imperfect;</p> <p>G/G' and H/H' not coprime;</p> <p>$r \geq k$ for some k, $s \geq l$ for some l.</p>
G	C_m	$m \geq 2$; $d(G/G') = d(G)$.
G^r	C_m	<p>$m \geq 2$; G imperfect;</p> <p>$r \geq k$ for some k.</p>
$G \times P$	C_m	<p>$m \geq 2$; G solvable; P perfect;</p> <p>$d(G) \geq d(P)$; $d(G/G') = d(G)$.</p>
$G_1 \times P_1$	$G_2 \times P_2$	<p>G_i solvable, P_i perfect; $i = 1, 2$;</p> <p>$G_1 / (G_1)'$ and $G_2 / (G_2)'$ are not coprime;</p> <p>$d(G_i) \geq d(P_i)$; $d(G_i) = d(G_i / (G_i)')$.</p>
$G^r \times P$	C_m	<p>$m \geq 2$; G imperfect solvable;</p> <p>P perfect; $d(G^r) \leq d(P)$;</p> <p>$r \geq k$ for some k.</p>

G	H	Conditions
$G_1^r \times P_1$	$G_2^s \times P_2$	G_i imperfect solvable; P_i perfect; $d(G_i) \geq d(P_i)$ for $i = 1, 2$; $G_1/(G_1)'$ and $G_2/(G_2)'$ are not coprime.
G_1	C_m	$d(\tilde{G}_1) = d(G_1)$; $\tilde{G}_1 \cong A_1 \times P_1$; A_1 abelian; P_1 perfect;
G_1	G_2	$d(A_1) \geq d(P_1)$; A_1 and A_2 are not coprime.
G	C_n	$\text{gap}(G) = 0$; there exists $p \mid G $ such that for every n where $p \mid n$, this is true.
$G \times P$	C_n	The same conditions as above in addition to: G solvable; P perfect; $d(G) \geq d(P)$.
G	H	$\bar{G}$ and $\bar{H}$ finite groups; $G = \bar{G} \times C_k^s$, $H = \bar{H} \times C_k^t$ where $(k, m_i) = 1$, $(k, n_j) = 1$, for every i and j .
G	H	$\bar{G}$ and $\bar{H}$ are any of the above groups; $G \twoheadrightarrow \bar{G}$; $H \twoheadrightarrow \bar{H}$; $d(G) = d(\bar{G})$; $d(H) = d(\bar{H})$.

In the final section of this thesis, we will pose some open problems of immediate interest.

Problem 1: Consider two finite abelian groups A and B which are coprime. Does there exist a finite quotient group T of $A * B$ such that $d(T) = d(A) + d(B)$ and $T = \langle A, B \rangle$?

Problem 2: Consider a finite group G such that $d(G/G') < d(G)$.

Let n be a positive integer greater than 1. Does there exist a finite quotient group T of $G * C_n$ such that $d(T) = d(G) + 1$ and $T = \langle G, C_n \rangle$?

Problem 3: Consider finite groups G and H such that $d(G/G') = d(G)$ and $d(H/H') < d(H)$. Does there exist a finite quotient group T of $G * H$ such that $d(T) = d(G) + d(H)$ and $T = \langle G, H \rangle$?

Problem 4: Consider finite groups G and H such that $d(G/G') < d(G)$ and $d(H/H') < d(H)$. Does there exist a finite quotient group T of $G * H$ such that $d(T) = d(G) + d(H)$ and $T = \langle G, H \rangle$?

References

- [1] Aschbacher, M. & Guralnick, R., "Some applications of the first cohomology group", J. of Algebra 90, 446-460, 1984.
- [2] Binz, E., Neukirch, J. & Wenzel, G.H., "A subgroup theorem for free products of profinite groups", J. of Algebra 19, 104-109, 1971.
- [3] Burnside, W., "The theory of groups of finite order", 2nd ed., 1911.
- [4] Eilenberg, S. & Steenrod, N., "Foundations of algebraic topology", Princeton Univ. Press, 1952.
- [5] Gaschütz, W., "Die Eulersche Funktion endlicher auflösbaren Gruppen", Illinois J. Math. 3, 469-479, 1959.
- [6] Gruenberg, K.W., "Relation modules of finite groups", Conference board of the mathematical sciences, Regional conference series in mathematics, No.25, 1974.
- [7] Gruenberg, K.W., "Groups of nonzero presentation rank", Symposia Math. 17, 215-224, 1975.
- [8] Gupta, N., "On groups in which every element has finite order", Amer. Math. Monthly, to appear.
- [9] Herfort, W. & Ribes, L., "Subgroups of free pro-p products", Math. Proc. Camb. Phil. Soc. 101, 197-206, 1987.
- [10] Johnson, D.L., "Presentation of groups", Cambridge Univ. Press, 1976.
- [11] Kovács, L.G., "On finite solvable groups", Math. Z. 103, 37-39, 1968.

- [12] Longobardi, P. & Maj, M., "On the number of generators of a finite group", Arch. Math. 50, 110-112, 1988.
- [13] Lyndon, R.C. & Schupp, P.E., "Combinatorial group theory", Springer-Verlag, 1977.
- [14] Lubotzky, A., "Combinatorial group theory for pro-p groups", J. of Pure & Applied Algebra 25, 311-325, 1982.
- [15] Munkres, J., "Topology, a first course", Prentice-Hall Inc., 1985.
- [16] Ribes, L., "Introduction of profinite groups and Galois cohomology", Queen's papers in pure and applied mathematics, No.24, 1970.
- [17] Roggenkamp, K.W., "Relation modules of finite groups and related topics", Algebra i Logika 12, 351-359, 1973.
- [18] Wiegold, J., "Growth sequences of finite groups II", J. Aust. Math. Soc. Ser. A. 20, 224-229, 1975.
- [19] Wiegold, J. & Wilson, J.S., "Growth sequences of finitely generated groups", Arch. Math. 30, 337-343, 1978.

END

17/02.90

FIN