INFORMATION TO USERS

This manuscript has been reproduced from the microfilm master. UMI films the text directly from the original or copy submitted. Thus, some thesis and dissertation copies are in typewriter face, while others may be from any type of computer printer.

The quality of this reproduction is dependent upon the quality of the copy submitted. Broken or indistinct print, colored or poor quality illustrations and photographs, print bleedthrough, substandard margins, and improper alignment can adversely affect reproduction.

In the unlikely event that the author did not send UMI a complete manuscript and there are missing pages, these will be noted. Also, if unauthorized copyright material had to be removed, a note will indicate the deletion.

Oversize materials (e.g., maps, drawings, charts) are reproduced by sectioning the original, beginning at the upper left-hand corner and continuing from left to right in equal sections with small overlaps.

Photographs included in the original manuscript have been reproduced xerographically in this copy. Higher quality 6" x 9" black and white photographic prints are available for any photographs or illustrations appearing in this copy for an additional charge. Contact UMI directly to order.

**Bell & Howell Information and Learning
300 North Zeeb Road, Ann Arbor, MI 48106-1346 USA
800-521-0600**

UMI[®]

RESIDUAL PROPERTIES OF GROUPS

by

Kumudu Mallawa Arachchi, B.Sc.

A thesis submitted to
the Faculty of Graduate Studies
in partial fulfillment of
the requirement for the degree of

Master of Science

Carleton University

Ottawa, Ontario

November 15, 1999

copyright © by

1999, Kumudu Mallawa Arachchi

National Library
of Canada

Acquisitions and
Bibliographic Services

395 Wellington Street
Ottawa ON K1A 0N4
Canada

Bibliothèque nationale
du Canada

Acquisitions et
services bibliographiques

395, rue Wellington
Ottawa ON K1A 0N4
Canada

Your file *Votre référence*

Our file *Notre référence*

The author has granted a non-exclusive licence allowing the National Library of Canada to reproduce, loan, distribute or sell copies of this thesis in microform, paper or electronic formats.

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

L'auteur a accordé une licence non exclusive permettant à la Bibliothèque nationale du Canada de reproduire, prêter, distribuer ou vendre des copies de cette thèse sous la forme de microfiche/film, de reproduction sur papier ou sur format électronique.

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

0-612-48502-1

The undersigned recommended to
the Faculty of Graduate Studies and Research
acceptance of the thesis

Residual Properties of Groups

submitted by Don Kumudu Mallowa Arachchi
in partial fulfillment of the requirements for
the degree of Master of Science

A handwritten signature in black ink, appearing to read "Steve Kib", is written over a horizontal line.

Thesis Supervisor

A handwritten signature in black ink, reading "Kenneth S. Williams", is written over a horizontal line.

Director, School of Mathematics and Statistics

Carleton University

1999

Dedication

**To My Loving Parents
Who
Wish My Success Whole Heartedly**

Acknowledgment

First of all, I should express my gratitude to my academic supervisor Dr. Luis Ribes, who made arrangements to make this work a success, for his invaluable support and patient cooperation towards the completion of this exposition. Also, I should thank to the graduate advisor of the School of Mathematics and Statistics Dr. Cyril Garner and the staff for their kind support. I should also specially thank to Dr. Kenneth S. Williams who made me prepared in group theory by teaching a basic course in groups, about two years ago. Finally, I should say that it would have been impossible to complete this work without my wife who supported me all the time in all the ways, so one of the biggest thanks goes to her.

Abstract

This whole work is based on the article *Residually Finite Groups* by W. Magnus published in 1969. It contains a survey of residual properties of groups concentrating mainly on residual finiteness. A self-contained and thoroughly explained expansion of Magnus' article in which all the results are proven is the purpose of my exposition.

The preparation required for chapter 2 is made in the first chapter. Starting with some not-so-common results of group theory, a somewhat-deep discussion on free groups, free products, amalgamated free products and HNN extensions is given. While most of the results are proven, some long proofs have been avoided just because proving such results is beyond the scope of the thesis.

In the second chapter, the survey of residual properties starts. The main residual properties dealt with are “residual finiteness” and being “residually a finite p -group”, where p is a prime. The first section consists of some equivalent definitions of residual properties and examples having those properties. In the second section, some consequences of the definitions are explained. Residual properties of free groups are discussed in the third section. Some non-trivial results on residually finite groups are given in the fourth section. In sections 5-8, residual properties of finitely generated linear groups, polycyclic groups, free products and amalgamated free products are discussed. In sections 5, 6 and 8, only residual finiteness is considered while in the section 7, groups that are residually P , where P is a root property, are studied.

Contents

1 Preliminaries	8
1.1 On Indices of Subgroups	8
1.2 Normal Closure and Core	10
1.3 Characteristic Subgroups	12
1.4 Free Groups	13
1.5 Presentations of Groups	22
1.6 Free Products	23
1.7 Amalgamated Free Products	29
1.8 Extension of Groups and Subnormal Series	40
1.9 HNN extensions	40

2	Residual Properties of Groups	43
2.1	Definitions and Examples	43
2.2	Fundamental Properties	48
2.3	Residual Properties of Free Groups	50
2.4	Further Properties	56
2.5	Subgroups of General Linear Groups	64
2.6	Polycyclic Groups	68
2.7	Residual Properties of Free Products	75
2.8	Residual Finiteness of Amalgamated Free Products	82

Chapter 1

Preliminaries

Assuming the basics of groups, we start this chapter with some non standard results of elementary groups and then stretch out to rather advanced notions of group theory. Almost all the results we discuss here are basically from two very interesting books on introductory group theory, namely, “A Course in the Theory of Groups” by Derek J.S. Robinson and “Introduction to the Theory of Groups” by Joseph J. Rotman.

1.1 On Indices of Subgroups

Let us begin our journey with a theorem on index of a subgroup.

Theorem 1.1.1: Let $H_1, H_2, \dots, H_n$ be a finite collection of subgroups of a

group G . Then,

$$[G : \bigcap_{i=1}^n H_i] \leq \prod_{i=1}^n [G : H_i]$$

and the equality occurs if the indices $[G : H_1], [G : H_2], \dots, [G : H_n]$ are finite and the greatest common divisor of these n indices is 1.

Proof: We use induction on n . The result is trivially true for $n = 1$. Consider the case $n = 2$. Let

$$\begin{aligned} U &= \text{set of all right cosets of } H_1 \cap H_2 \text{ in } G \\ V &= \text{set of all right cosets of } H_1 \text{ in } G \\ W &= \text{set of all right cosets of } H_2 \text{ in } G. \end{aligned}$$

Define a map $\mu: U \rightarrow V \times W$ by $\mu((H_1 \cap H_2)x) = (H_1x, H_2x)$. This map is well defined and injective since

$$\begin{aligned} (H_1 \cap H_2)x = (H_1 \cap H_2)y &\iff xy^{-1} \in H_1 \cap H_2 \\ &\iff xy^{-1} \in H_1, xy^{-1} \in H_2 \\ &\iff H_1x = H_1y, H_2x = H_2y \\ &\iff (H_1x, H_2x) = (H_1y, H_2y) \\ &\iff \mu((H_1 \cap H_2)x) = \mu((H_1 \cap H_2)y). \end{aligned}$$

Hence, we conclude that the cardinality of U is less than or equal to that of $V \times W$, i.e.,

$$[G : H_1 \cap H_2] \leq [G : H_1][G : H_2].$$

Next inductive step is clear from the identity

$$\bigcap_{i=1}^m H_i = \left(\bigcap_{i=1}^{m-1} H_i \right) \cap H_m$$

and the case $n = 2$, and thus the first part of the theorem is proved.

If the greatest common divisor (GCD) of all these indices is 1 then, since each $[G : H_i]$ divides $[G : \bigcap_{i=1}^n H_i]$, we conclude that $\prod_{i=1}^n [G : H_i]$ divides $[G : \bigcap_{i=1}^n H_i]$ and thus the equality holds. ■

An immediate corollary to this is a result due to Poincaré.

Corollary 1.1.1 (Poincaré): The intersection of a finite set of subgroups each of which has finite index is itself of finite index.

1.2 Normal Closure and Core

Definition: Let X be a subset of a group G . The *normal closure* of X in G , denoted by X^G , is defined to be the smallest normal subgroup of G containing X . The *core* (or *normal interior*) of X in G , denoted by X_G , is defined to be the largest normal subgroup of G contained in X , with the convention that $X_G = \{1\}$ if there is no such subgroup.

Theorem 1.2.1: For a group G , a subset X and a subgroup H of G ,

$$(a) X^G = \langle g^{-1}Xg \mid g \in G \rangle = \langle g^{-1}xg \mid g \in G, x \in X \rangle$$

$$(b) H_G = \bigcap_{g \in G} g^{-1}Hg$$

Proof: (a) Write $K = \langle g^{-1}xg \mid g \in G, x \in X \rangle$. First we show that $K \triangleleft G$. Here we use the fact that any element $y \in \langle g^{-1}xg \mid g \in G, x \in X \rangle$ can be written in the form $\prod_{i=1}^n y_i^{\epsilon_i}$ where each $y_i \in \{g^{-1}xg \mid g \in G, x \in X\}$ and each ϵ_i is ± 1 . Thus, if we write $y_i = g_i^{-1}x_i g_i$ where $g_i \in G$ and $x_i \in X$ then,

for any $g \in G$ we have

$$\begin{aligned}
g^{-1}yg &= g^{-1} \left(\prod_{i=1}^n y_i^{\epsilon_i} \right) g \\
&= g^{-1} \left(\prod_{i=1}^n (g_i^{-1} x_i g_i)^{\epsilon_i} \right) g \\
&= g^{-1} \left(\prod_{i=1}^n g_i^{-1} x_i^{\epsilon_i} g_i \right) g \\
&= \prod_{i=1}^n g^{-1} (g_i^{-1} x_i^{\epsilon_i} g_i) g \\
&= \prod_{i=1}^n (g_i g)^{-1} x_i^{\epsilon_i} (g_i g) \\
&= \prod_{i=1}^n ((g_i g)^{-1} x_i (g_i g))^{\epsilon_i} \\
&\in \langle g^{-1} x g \mid g \in G, x \in X \rangle = K.
\end{aligned}$$

Thus $K \triangleleft G$. That K is the least normal subgroup is clear since any element $y = \prod_{i=1}^n (g_i^{-1} x_i g_i)^{\epsilon_i}$ in K is clearly in X^G , and hence part (a) is proved.

(b) Write $K = \bigcap_{g \in G} g^{-1} H g$. Clearly $K \leq H$. To prove that K is normal in G , take any $a \in G$. Consider the inner automorphism $\phi: G \rightarrow G$ defined by

$\phi(x) = a^{-1}xa$. Then we have

$$\begin{aligned}
a^{-1}Ka &= \phi(K) \\
&= \phi\left(\bigcap_{g \in G} g^{-1}Hg\right) \\
&= \bigcap_{g \in G} \phi(g^{-1}Hg) \text{ (as } \phi \text{ is a bijection)} \\
&= \bigcap_{g \in G} a^{-1}(g^{-1}Hg)a \\
&= \bigcap_{g \in G} (ga)^{-1}H(ga) \\
&= \bigcap_{g \in G} g^{-1}Hg \\
&= K,
\end{aligned}$$

and thus $K \triangleleft G$. To show that K is the largest normal subgroup of G in H , suppose there exists a subgroup L of G such that $K \leq L \leq H$ and $L \triangleleft G$. Then,

$$K = \bigcap_{g \in G} g^{-1}Hg \geq \bigcap_{g \in G} g^{-1}Lg = L \geq K$$

so that $K = L$ and thus (b) follows. ■

1.3 Characteristic Subgroups

Definition: A subgroup H of a group G is said to be *characteristic* in G if $\phi(H) = H$ for any $\phi \in \text{Aut}(G)$.

The following theorem states that being characteristic is a stronger condition than being normal (see Example 1.3.1 also).

Theorem 1.3.1: If H is characteristic in G then $H \triangleleft G$. Further, if H is characteristic in K and $K \triangleleft G$ then $H \triangleleft G$.

Proof: Let $g \in G$. Consider the inner automorphism ϕ of G defined by $\phi(x) = g^{-1}xg$. Then, $\phi(H) = H$ and hence $g^{-1}Hg = H$ so that $H \triangleleft G$. To show the other part, note that the map $\phi: K \rightarrow K$ defined by $\phi(x) = g^{-1}xg$ where $g \in G$, is an automorphism of K . Then, $\phi(H) = H$. Hence $g^{-1}Hg = H$ and thus, since g is arbitrary, $H \triangleleft G$.

Example 1.3.1: Consider the Four-group

$$K_4 = \langle a, b \mid a^2 = b^2 = (ab)^2 = 1 \rangle \cong C_2 \times C_2$$

and the automorphism ϕ of G defined by $\phi(a) = b$ and $\phi(b) = a$ (it is easy to check that this is an automorphism). The subgroup $H = \{1, a\}$ of G is mapped under ϕ to the subgroup $\{1, b\}$ so that H is not characteristic in G but $H \triangleleft G$ as G is abelian. ■

1.4 Free Groups

Now we pay our attention to one of the most important classes of groups, namely free groups.

Definition: Let X be a subset of a group F . Then F is said to be a *free group* with *basis* X if, for every group G and every function $f: X \rightarrow G$, there exists a unique homomorphism $\tilde{f}: F \rightarrow G$ extending f , i.e., diagrammatically, if the following diagram commutes:

Further, the cardinality of X is named the rank of the free group F .

This condition of extension is called the *extension property*.

Next we show that free groups actually exist. Let X be any nonempty set and let X^{-1} be another set, disjoint from X , for which there is a bijection $X \rightarrow X^{-1}$. Denote the image of $x \in X$ under this bijection by x^{-1} . Here, X^{-1} and x^{-1} are merely symbols we select for reasons that will be clear in the ongoing discussion.

Definition: A *word* on X is a sequence $w = (a_1, a_2, \dots)$ where $a_i \in X \cup X^{-1}$ for $i = 1, 2, \dots, n$ and $a_i = 1$ for all $i > n$ for some integer $n \geq 0$ (we consider 1 to be an element not in $X \cup X^{-1}$). In particular, when $n = 0$, the sequence $(1, 1, 1, \dots)$ is called the *empty word*.

We adopt the notations x^1 for x and x^0 for 1. Further, for the sake of simplicity, we denote the above word $(a_1, a_2, \dots, a_n)$ by $a_1 a_2 \dots a_n$ when w is nonempty and by 1 when w is empty. We may also denote, in a more suggestive way, a nonempty word w as

$$x_1^{\epsilon_1} x_2^{\epsilon_2} \dots x_n^{\epsilon_n}$$

where $x_i \in X$ and $\epsilon_i = \pm 1$. Call $x_i^{\epsilon_i}$ a syllable of the word w . Two sequences (a_i) and (b_i) are said to be equal if $a_i = b_i$ for each i , hence the syllables of the word $x_1^{\epsilon_1} x_2^{\epsilon_2} \cdots x_n^{\epsilon_n}$ are unique.

Definition: The *length* of a word w is said to be 0 if w is empty, and n if $w = x_1^{\epsilon_1} x_2^{\epsilon_2} \cdots x_n^{\epsilon_n}$. The *inverse* of the word $w = x_1^{\epsilon_1} x_2^{\epsilon_2} \cdots x_n^{\epsilon_n}$ is defined to be the word

$$x_n^{-\epsilon_n} \cdots x_2^{-\epsilon_2} x_1^{-\epsilon_1}$$

and is denoted by w^{-1} . A word w is said to be *reduced* if either w is empty or if $w = x_1^{\epsilon_1} x_2^{\epsilon_2} \cdots x_n^{\epsilon_n}$ where $x_i \in X$, $\epsilon_i = \pm 1$, and also if two syllables of the form x and x^{-1} are never adjacent. The word w is said to be *cyclically reduced* if $x_1^{\epsilon_1} \neq x_n^{-\epsilon_n}$. Further, a *subword* of $w = x_1^{\epsilon_1} x_2^{\epsilon_2} \cdots x_n^{\epsilon_n}$ is defined to be either the empty word or a word of the form

$$v = x_i^{\epsilon_i} x_{i+1}^{\epsilon_{i+1}} \cdots x_{i+j}^{\epsilon_{i+j}}$$

where $1 \leq i < i+j \leq n$.

It is clear that the inverse of a reduced word is reduced. Note that v is a subword of w if and only if there are subwords w' and w'' of w with $w = w'vw''$. Furthermore, it is intuitively clear that a nonempty word w is reduced if and only if w contains no subwords of the form $x^\epsilon x^{-\epsilon}$.

Our next aim is to define a multiplication on reduced words. Let

$$w = x_1^{\epsilon_1} x_2^{\epsilon_2} \cdots x_n^{\epsilon_n}$$

and

$$u = y_1^{\delta_1} y_2^{\delta_2} \cdots y_m^{\delta_m}$$

be two reduced words on X . Then the mere concatenation wu need not be reduced as $x_n^{\epsilon_n}$ might be equal to $y_1^{-\delta_1}$. To overcome this, we define a new multiplication as follows.

First we claim that there always exists a subword v (possibly empty) of w with the following properties:

1. $w = w'v$ for some subword w' of w
2. v^{-1} is a subword of u
3. $u = v^{-1}u'$ for some subword u' of u
4. $w'u'$ is reduced.

Case I: If $x_n^{\epsilon_n} \neq y_1^{-\delta_1}$ then set $v = 1$, $w' = w$ and $u' = u$.

Case II: If $u = w^{-1}$ then set $v = w$, $w' = 1$ and $u' = 1$.

Case III: If u^{-1} is a subword of w but $w \neq u^{-1}$ then set

$$\begin{aligned} v &= u^{-1}, \\ w' &= x_1^{\epsilon_1} x_2^{\epsilon_2} \cdots x_{n-m}^{\epsilon_{n-m}}, \\ u' &= 1. \end{aligned}$$

Case IV: If w^{-1} is a subword of u but $w \neq u^{-1}$ then set

$$\begin{aligned} v &= w, \\ w' &= 1, \\ u' &= y_{n+1}^{\delta_{n+1}} y_{n+2}^{\delta_{n+2}} \cdots y_m^{\delta_m}. \end{aligned}$$

Case V: In any other case, let r be the integer such that

$$\begin{aligned} x_n^{\epsilon_n} &= y_1^{-\delta_1}, \\ x_{n-1}^{\epsilon_{n-1}} &= y_2^{-\delta_2}, \\ &\dots\dots\dots, \\ x_{n-r}^{\epsilon_{n-r}} &= y_{r+1}^{-\delta_{r+1}}, \\ x_{n-r-1}^{\epsilon_{n-r-1}} &\neq y_{r+2}^{-\delta_{r+2}}. \end{aligned}$$

Now set

$$\begin{aligned} v &= x_{n-r}^{\epsilon_{n-r}} x_{n-r+1}^{\epsilon_{n-r+1}} \cdots x_n^{\epsilon_n}, \\ w' &= x_1^{\epsilon_1} x_2^{\epsilon_2} \cdots x_{n-r-1}^{\epsilon_{n-r-1}}, \\ u' &= y_{r+2}^{\delta_{r+2}} y_{r+3}^{\delta_{r+3}} \cdots y_m^{\delta_m}. \end{aligned}$$

Then it is routine to check that the above four properties hold as claimed.

Now the new multiplication of w and u called the *juxtaposition* of w and u is defined to be $w'u'$ and is simply denoted by wu .

Thus, juxtaposition wu is the multiplication of w and u with repeated cancellation of adjacent syllables of the form x and x^{-1} .

Now we are in a position to construct a free group.

Theorem 1.4.1: Given a set X , there exists a free group F with basis X .

Proof: Let F be the set of all reduced words on X . We prove that F is a group under juxtaposition. If we try to show that the group axioms are satisfied, we have to deal with tedious case analysis in proving the associativity. Therefore we use an alternative method called van der Waerden trick.

For each $x \in X$, define functions $\phi_x: F \rightarrow F$ and $\phi_{x^{-1}}: F \rightarrow F$ as follows:
for $\epsilon = \pm 1$,

$$\phi_{x^\epsilon}(x_1^{\epsilon_1} x_2^{\epsilon_2} \cdots x_n^{\epsilon_n}) = \begin{cases} x^\epsilon x_1^{\epsilon_1} x_2^{\epsilon_2} \cdots x_n^{\epsilon_n} & \text{if } x^\epsilon \neq x_1^{-\epsilon_1} \\ x_2^{\epsilon_2} \cdots x_n^{\epsilon_n} & \text{if } x^\epsilon = x_1^{-\epsilon_1}. \end{cases}$$

Then, it is easy to check that both $\phi_x \circ \phi_{x^{-1}}$ and $\phi_{x^{-1}} \circ \phi_x$ are equal to the identity function 1_F on F . Hence, ϕ_x is a permutation of F with inverse $\phi_{x^{-1}}$. Let S_F be the symmetric group on F and let $\mathcal{F}$ be the subgroup of S_F generated by $\mathcal{X} = \{\phi_x \mid x \in X\}$. We claim that $\mathcal{F}$ is a free group with basis $\mathcal{X}$.

Let $1 \neq g \in \mathcal{F}$ be arbitrary. Then it can be written in the form of a factorization

$$g = \phi_{x_1}^{\epsilon_1} \circ \phi_{x_2}^{\epsilon_2} \circ \cdots \circ \phi_{x_n}^{\epsilon_n} \quad (1.1)$$

where $\epsilon_i = \pm 1$ and two factors of the form ϕ^ϵ and $\phi^{-\epsilon}$ are never adjacent. This factorization is unique for, if

$$h = \phi_{y_1}^{\delta_1} \circ \phi_{y_2}^{\delta_2} \circ \cdots \circ \phi_{y_m}^{\delta_m}$$

is another factorization of g then $g(1) = h(1)$, i.e.,

$$x_1^{\epsilon_1} \cdots x_n^{\epsilon_n} = y_1^{\delta_1} \cdots y_m^{\delta_m}$$

hence, as syllables of a reduced word is unique, we have $m = n$ and $x_i = y_i$ so that $g = h$.

Let G be any group and let $f: \mathcal{X} \rightarrow G$ be any map. To show that $\mathcal{F}$ is free on $\mathcal{X}$ we will show that there exists a homomorphism $\psi: \mathcal{F} \rightarrow G$ extending f . This ψ is none other than the map defined by

$$\psi(g) = \psi(\phi_{x_1}^{\epsilon_1} \circ \phi_{x_2}^{\epsilon_2} \circ \cdots \circ \phi_{x_n}^{\epsilon_n}) = f(\phi_{x_1})^{\epsilon_1} f(\phi_{x_2})^{\epsilon_2} \cdots f(\phi_{x_n})^{\epsilon_n}.$$

The map ψ is well defined since the factorization in (1.1) is unique. Also it is clear that ψ extends f . If it is shown that ψ is a homomorphism, the uniqueness of ψ follows as $\mathcal{X}$ generates $\mathcal{F}$ and from the fact that two homomorphisms agreeing on a generating set are equal. Hence it remains to show that ψ is a homomorphism.

Let $w = \phi_{x_1}^{\epsilon_1} \circ \phi_{x_2}^{\epsilon_2} \circ \cdots \circ \phi_{x_n}^{\epsilon_n}$ and $u = \phi_{y_1}^{\delta_1} \circ \phi_{y_2}^{\delta_2} \circ \cdots \circ \phi_{y_m}^{\delta_m}$ be two reduced words on $\mathcal{X}$. If the juxtaposition $wu = w \circ u$ is reduced then clearly $\psi(w \circ u) = \psi(w) \circ \psi(u)$. Also, it is easily seen that $\psi(v^{-1}) = \psi(v)^{-1}$ for a reduced word v . Now, to extend this result to any two words w and u , write $w = w' \circ v$ and $u = v^{-1} \circ u'$ as in the definition of juxtaposition. Then,

$$\psi(w) = \psi(w')\psi(v)$$

and

$$\begin{aligned} \psi(u) &= \psi(v^{-1})\psi(u') \\ &= \psi(v)^{-1}\psi(u'). \end{aligned}$$

These imply that

$$\psi(w)\psi(u) = \psi(w')\psi(v)\psi(v)^{-1}\psi(u') = \psi(w')\psi(u').$$

On the other hand,

$$\psi(w \circ u) = \psi(w' \circ u') = \psi(w')\psi(u')$$

and hence

$$\psi(w \circ u) = \psi(w)\psi(u),$$

so that ψ is a homomorphism. Thus, $\mathcal{F}$ is a free group with basis $\mathcal{X}$.

Now it is easily seen that the map $\zeta: \mathcal{F} \rightarrow F$ defined by

$$\phi_{x_1}^{\epsilon_1} \circ \phi_{x_2}^{\epsilon_2} \circ \dots \circ \phi_{x_n}^{\epsilon_n} \mapsto x_1^{\epsilon_1} x_2^{\epsilon_2} \dots x_n^{\epsilon_n}$$

is a bijection with the property that $\zeta(\mathcal{X}) = X$. We can define a binary operation on F to make F into a group isomorphic to $\mathcal{F}$ in the following way. For any two elements w and u in F , define the binary operation $*$ on F by

$$w * u = \zeta \left(\zeta^{-1}(w) \zeta^{-1}(u) \right).$$

It is routine to check that F is a group under $*$ and that ζ is an isomorphism from $\mathcal{F}$ to F . Since we have shown that $\mathcal{F}$ is a free group, we conclude that F is a free group. Further, since $\mathcal{X}$ is a basis for $\mathcal{F}$ and $\zeta(\mathcal{X}) = X$, we have that X is a basis for F . ■

Corollary 1.4.1: The set X in the previous theorem generates F .

Proof: This follows since the set $\mathcal{X}$ generates $\mathcal{F}$.

The following is a very important result on free groups.

Corollary 1.4.2: Every group G is isomorphic to a quotient of a free group.

Proof: Consider the set G and let F be the free group on the set G . The identity map $i: G \rightarrow G$ extends to a homomorphism $\psi: F \rightarrow G$ by the definition of a free group. Hence

$$G = \text{Im}(\psi) = F/\text{Ker}(\psi),$$

and the result follows. ■

Theorem 1.4.2: A free group F on a single generator x is infinite cyclic.

Proof: Clearly F is cyclic as it is generated by a single element. The equation $x^n = 1$, $x \neq 1$, $n \neq 0$ is impossible since every word has a unique representation, hence $F = \langle x \rangle$ is infinite cyclic. ■

We end this section with some important results on free groups and subgroups of free groups followed by a consequence which will be used in Chapter 2. We will not attempt to prove these results because they are way beyond our scope.

Theorem 1.4.3: Any two free groups with bases of the same cardinality are isomorphic.

See [16, page 348] for a proof.

Theorem 1.4.4 (Nielsen Schreier Subgroup Theorem): Every subgroup of a free group is itself free.

See [12, page 95] for a proof.

Theorem 1.4.5: The commutator subgroup F'_2 of the free group F_2 of two generators has countably infinite rank.

See [9, page 13] for a proof.

Corollary 1.4.3: Every free group F with a countably infinite basis is embeddable in F_2 .

Proof: Theorem 1.4.4 and Theorem 1.4.5 say that F'_2 is a free group with a countably infinite basis and Theorem 1.4.3 says that F and F'_2 are isomorphic and hence the Corollary follows. ■

1.5 Presentations of Groups

According to Corollary 1.4.2, any group G is isomorphic to a quotient of a free group. Suppose $G \cong F/N$ where F is free with basis X and N is a normal subgroup of F generated by a subset R of F (i.e., N is the normal closure of R in F). Then we say that the group F/N has *generators* X and *relations* R . The pair $\langle X \mid R \rangle$ is said to be a *presentation* of F/N and written $F/N = \langle X \mid R \rangle$. Sometimes, the elements of X are called generators and that of R are called relators. A presentation of G is a pair $\langle X \mid R \rangle$ together with an isomorphism $\phi: F/N \rightarrow G$. Thus, we may write a group G in the form

$$G = \langle X \mid r = 1, r \in R \rangle.$$

Example 1.5.1: The group G with the presentation

$$G = \langle x, y \mid x^2 = 1, y^2 = 1 \rangle$$

is called the *infinite dihedral group*.

A group $G = \langle X \mid R \rangle$ is called *finitely presented* if both X and R are finite, *finitely generated* if X is finite, and *finitely related* if R is finite.

A group G is called a *one relator group* if G has a presentation with only one relator. We state, without proof, a famous theorem due to Magnus called *The Freiheitssatz* on one relator groups.

Theorem 1.5.1 (The Freiheitssatz): Let $G = \langle a, b, c, \dots \mid r \rangle$ where r is a cyclically reduced relator involving all the generators $a, b, c, \dots$. If L is a subset of $\{a, b, c, \dots\}$ which omits any generator, then the subgroup M of G generated by L is freely generated by L .

See [9, page 11] for a proof. See also, [12, page 252].

An immediate corollary to this theorem is the following.

Corollary 1.5.1: Let $G = \langle a, b \mid r \rangle$ where r is a cyclically reduced relator involving both a and b . Then $\langle a \rangle$ and $\langle b \rangle$ are infinite cyclic.

1.6 Free Products

A free product of groups is a generalization of free groups.

Definition: Let $\{G_i \mid i \in I\}$ be a family of groups. A *free product* of the G_i is a group P and a family of homomorphisms $j_i: G_i \rightarrow P$ such that, for every group G and every family of homomorphisms $f_i: G_i \rightarrow G$, there exists a unique homomorphism $\phi: P \rightarrow G$ with $\phi j_i = f_i$ for all $i \in I$. Diagrammatically,

This condition of extension is called the extension property of free products. In this case, we merely say that P is a free product of the G_i and write $P = *G_i$.

Theorem 1.6.1: A free group F is a free product of infinite cyclic groups.

Proof: Let X be a basis for F . Define, for each $x \in X$, an inclusion map $j_x : \langle x \rangle \hookrightarrow F$. If G is a group and $f_x : \langle x \rangle \rightarrow G$ is a set of homomorphisms indexed by X , we wish to find a unique homomorphism $\phi : F \rightarrow G$ such that $\phi j_x = f_x$ for each $x \in X$.

Let $f : X \rightarrow G$ be the map defined by $f(x) = f_x(x)$. Then, by the universal property of free groups, there is a unique homomorphism $\phi : F \rightarrow G$ extending f . Now, for any $x^n \in \langle x \rangle$, we have

$$\begin{aligned} \phi j_x(x^n) &= \phi(x^n) \\ &= \phi(x)^n \\ &= f_x(x)^n \\ &= f_x(x^n) \end{aligned}$$

so that $\phi j_x = f_x$. The uniqueness follows for, if $\psi : F \rightarrow G$ is another homomorphism such that $\psi j_x = f_x$, then $\phi j_x = \psi j_x$ and hence $\phi = \psi$ as j_x is an inclusion map. ■

Lemma 1.6.1: If P is a free product of $\{G_i \mid i \in I\}$ then the homomorphisms j_i in the definition of free products are injections.

Proof: Fix any $i \in I$ and set $G = G_i$, f_i the identity map and, for $k \neq i$, f_k the trivial map, in the definition of free products. Then, $\phi j_i = 1_{G_i}$, the identity map on G_i , hence j_i is injective. ■

This lemma tells us that $j_i : G_i \rightarrow P$ are embeddings.

The following theorem gives the uniqueness of a free product.

Theorem 1.6.2: Let $\{G_i \mid i \in I\}$ be a family of groups. If (P, j_i) and (Q, k_i) are each a free product of the G_i , then $P \cong Q$.

Proof: Let $j_i: G_i \rightarrow P$ and $k_i: G_i \rightarrow Q$ be two sets of embeddings. Then, by the extension property, there are maps $\phi: P \rightarrow Q$ and $\psi: Q \rightarrow P$ with $\phi j_i = k_i$ and $\psi k_i = j_i$ for all i . Now, considering the embedding $j_i: G_i \rightarrow P$ again and setting $G = P$ and $f_i = j_i$ in the definition of free products, we see that

$$\psi \phi j_i = \psi(\phi j_i) = \psi k_i = j_i$$

and that

$$1_P j_i = j_i.$$

By uniqueness property in the definition of free products, we conclude that $\psi \phi = 1_P$ and similarly we can show that $\phi \psi = 1_Q$. Hence, $\phi: P \rightarrow Q$ is an isomorphism. ■

Next we show, as we did in the case of free groups, that free products really exist.

Theorem 1.6.3: Given a family $\{G_i \mid i \in I\}$ of groups, a free product exists.

Proof: Since the proof is essentially similar to that for free groups, we give only an outline. We may, without loss of generality, assume that $G_j \cap G_k = \emptyset$ since, otherwise, we may replace G_j by an isomorphic copy. Let $U = \bigcup_{i \in I} G_i$. A word $g = g_1 g_2 \cdots g_n$ in U is called *reduced* if either $g = 1$ or any two adjacent syllables belong to different G_i . Let S be the set of all reduced words in U and define the product of two words $g = g_1 \cdots g_n$ and $h = h_1 \cdots h_m$ in U as follows:

If g_n and h_1 belong to different G_i then $gh = g_1 \cdots g_n h_1 \cdots h_m$. If g_n and h_1 are in the same group and $g_n h_1 \neq 1$ then $gh = g_1 \cdots g_{n-1} (g_n h_1) h_2 \cdots h_m$. If g_n and h_1 are in the same group and $g_n h_1 = 1$ then cancel it and repeat the process for $g_1 \cdots g_{n-1}$ and $h_1 \cdots h_{m-1}$. Continuing this way, we should come up to a reduced word at last and let that be the product gh .

It is easy to see that 1 is the identity in S and the inverse of a reduced word is reduced. Now an analogue of the van der Waerden trick used in the case of free groups can be used to show the remaining part of the proof and it will not be repeated here. ■

There is an important way of representing elements in a free product which is given in the following corollary.

Corollary 1.6.1: Let $g \in *G_i$. Then g has a unique factorization $g = g_1 g_2 \cdots g_n$ where adjacent factors lie in distinct G_i .

Proof: In the constructions of free product in Theorem 1.6.3, the set of elements in $*G_i$ was the set of all reduced words and hence the corollary follows. ■

Definition: The form $g_1 g_2 \cdots g_n$ in Corollary 1.6.1 is called the *normal form* of g in $*G_i$ and n is called the *length* of g .

The following theorem gives another way of presenting free products.

Theorem 1.6.4: Let $\{G_i \mid i \in I\}$ be a family of groups and let a presentation of G_i be $\langle X_i \mid \Delta_i \rangle$ where the sets X_i are pairwise disjoint. Then $\langle \bigcup_{i \in I} X_i \mid \bigcup_{i \in I} \Delta_i \rangle$ is a presentation of $*G_i$.

First we prove two preparatory lemmas.

Lemma 1.6.2: For each $i \in I$, let F_i be a free group with basis X_i . Then, $*F_i$ is a free group with basis $\bigcup_{i \in I} X_i$.

Proof: Write $X = \bigcup_{i \in I} X_i$ and $F = *F_i$. Given any group G' and a function $\phi: X \rightarrow G'$, we show that there exists a unique homomorphism $\tilde{\phi}: F \rightarrow G'$ extending ϕ . Since each F_i is free on X_i we have that, for each i , given any map $\phi_i: X_i \rightarrow G'$, there exists a unique homomorphism $\tilde{\phi}_i: F_i \rightarrow G'$ extending ϕ_i . Set $\phi_i = \phi|_{X_i}$. Write any $f \in F$ in its normal form $f = f_1 f_2 \cdots f_n$ where $f_i \in F_{j_i}$ and no two adjacent f_i are in the same F_{j_i} . Put

$$\tilde{\phi}(f) = \tilde{\phi}_{j_1}(f_1) \tilde{\phi}_{j_2}(f_2) \cdots \tilde{\phi}_{j_n}(f_n).$$

Then, $\tilde{\phi}$ clearly extends ϕ . It is routine to check that $\tilde{\phi}$ is a homomorphism (as we did in the case of free groups in Theorem 1.4.1). Furthermore, $\tilde{\phi}$ is unique as any two such homomorphisms should agree on the set $\bigcup_{i \in I} F_i$ of generators of F , and thus F is free on X . ■

Lemma 1.6.3: Let $G = *G_i$ and $H = *H_i$ be free products with given homomorphisms $\phi_i: G_i \rightarrow H_i$. Then there exists a unique homomorphism $\phi: G \rightarrow H$ whose restriction to G_i is ϕ_i . Further, the kernel of ϕ is the normal closure of $\bigcup_{i \in I} \text{Ker}(\phi_i)$.

Proof: The existence and uniqueness of ϕ is immediate from the extension property of free product of $*G_i$. Denote by N the normal closure of $\bigcup_{i \in I} \text{Ker}(\phi_i)$ in $*G_i$ and by K the kernel of ϕ . If $x \in \bigcup_{i \in I} \text{Ker}(\phi_i)$ then $\phi_i(x) = 1$ for some i and hence $\phi(x) = 1$ since ϕ extends ϕ_i . If $y = g^{-1} x^r g$ where $x \in \bigcup_{i \in I} \text{Ker}(\phi_i)$, $g \in *G_i$ and r an integer, then, clearly, $\phi(y) = 1$. Since any element of N is a finite product of such conjugates, which is mapped to 1 in turn under ϕ , we conclude that $N \leq K$.

To show the reverse inclusion, suppose that $N < K$ and then take an element g of minimum length in $K \setminus N$. Let $g = g_1 g_2 \cdots g_r$ be the normal form of g where $g_i \in G_{j_i}$. Now, $1 = \phi(g) = \phi_{j_1}(g_1) \phi_{j_2}(g_2) \cdots \phi_{j_r}(g_r)$ and hence, as the adjacent syllables of this product belong to different groups, at least one of the syllables, say $\phi_{j_i}(g_i)$, must be equal to 1 so that $g_i \in N$. Now, consider the element $g_1 \cdots g_{i-1} g_{i+1} \cdots g_r$ in $*G_i$. Clearly this is in K . Suppose this element is in N . Then, since $N \triangleleft G$,

$$(g_1 g_2 \cdots g_{i-1})^{-1} g_1 \cdots g_{i-1} g_{i+1} \cdots g_r (g_1 g_2 \cdots g_{i-1}) = g_{i+1} \cdots g_r g_1 \cdots g_{i-1} \in N.$$

But, since $g_i \in N$ we have

$$g_i g_{i+1} \cdots g_r g_1 \cdots g_{i-1} \in N.$$

Then,

$$\begin{aligned} (g_1 g_2 \cdots g_{i-1}) g_i g_{i+1} \cdots g_r g_1 g_2 \cdots g_{i-1} (g_1 g_2 \cdots g_{i-1})^{-1} &= g_1 \cdots g_{i-1} g_i g_{i+1} \cdots g_r \\ &= g \\ &\in N, \end{aligned}$$

a contradiction. Hence $g_1 \cdots g_{i-1} g_{i+1} \cdots g_r \in K \setminus N$ contradicting the minimality of length of g . Hence $N = K$ and the lemma is proved. $\blacksquare$

Proof of Theorem 1.6.4: Let F_i be the free group with basis X_i . Also let $\{j_i \mid G_i \hookrightarrow G\}$ be homomorphisms where $G = *G_i$. Denote by R_i the normal closure of Δ_i in F_i . Since $G_i = \langle X_i \mid \Delta_i \rangle$, there is an epimorphism $\phi_i: F_i \rightarrow G_i$ with $\text{Ker}(\phi_i) = R_i$. If $F = *F_i$ then, by Lemma 1.6.3, there is a homomorphism $\phi: F \rightarrow G$ with

$$\text{Ker}(\phi) = \left(\bigcup_{i \in I} R_i \right)^F = \left(\bigcup_{i \in I} \Delta_i \right)^F.$$

Hence, by the definition of a presentation of a group, G has a presentation $\langle \bigcup_{i \in I} X_i \mid \bigcup_{i \in I} \Delta_i \rangle$. $\blacksquare$

1.7 Amalgamated Free Products

We formed the free product of two groups when those two groups are disjoint. If we identify a subgroup of one group which is isomorphic to a subgroup of the other group, then we get a quotient of the original free product.

Definition: Let H, A and B be groups and let $i: H \rightarrow A$ and $j: H \rightarrow B$ be homomorphisms. Call these given collection of groups and homomorphisms *data*. A *solution* (G, α, β) of this data is a commutative diagram:

$$\begin{array}{ccc} H & \xrightarrow{i} & A \\ j \downarrow & & \downarrow \alpha \\ B & \xrightarrow{\beta} & G \end{array}$$

where G is a group and α, β are homomorphisms. A *pushout* of this data is a solution (P, j', i') such that, for every solution (G, α, β) , there exists a unique homomorphism $\phi: P \rightarrow G$ with

$$\alpha = \phi j'$$

$$\beta = \phi i'.$$

Diagrammatically,

Theorem 1.7.1: If a pushout (P, j', i') of the above data exists, then P is unique up to isomorphism.

Proof: Suppose (Q, j'', i'') is another pushout of the data. Then, replacing (G, α, β) in the above definition by (Q, j'', i'') we get that there exist a homomorphism $\phi: P \rightarrow Q$ such that

$$\begin{aligned} j'' &= \phi j' \\ i'' &= \phi i'. \end{aligned}$$

Again, replacing (G, α, β) in the above definition by (P, j', i') and (P, j'', i'') by (Q, j'', i'') we get that there exist a homomorphism $\psi: Q \rightarrow P$ such that

$$\begin{aligned} j' &= \psi j'' \\ i' &= \psi i''. \end{aligned}$$

These equations imply that $j'' = \phi \psi j''$ and $i' = \psi \phi i'$. Now, replacing (G, α, β) in the above definition by (P, j', i') we get there is a unique homomorphism $\theta: P \rightarrow P$ such that $i' = \theta i'$. But the identity homomorphism 1_P on P satisfies this, hence $\theta = 1_P$. Thus, by the uniqueness of θ that

satisfies the equations $i' = 1_P i'$ and $i' = \psi \phi i'$ we have that $\psi \phi = 1$. In a similar way, we can show that $\phi \psi = 1$. Hence, ϕ is an isomorphism and the theorem is proved. ■

Sometimes we merely call P the pushout of the above data.

Next we prove the existence of pushouts.

Theorem 1.7.2: Given homomorphisms $i: H \rightarrow A$ and $j: H \rightarrow B$, a pushout (P, j', i') always exists and is isomorphic to $(A * B)/N$ where N is the normal closure of $\{i(h)j(h^{-1}) \mid h \in H\}$ in $A * B$. Further, if A has a presentation $\langle X \mid \Delta \rangle$ and B has a presentation $\langle Y \mid \Gamma \rangle$ then P has a presentation

$$P = \langle X \cup Y \mid \Delta \cup \Gamma \cup \{i(h)j(h^{-1}) : h \in H\} \rangle.$$

Proof: First we show that (P, j', i') is a solution where $P = (A * B)/N$, $j'(a) = aN$ and $i'(a) = aN$. Then we have $j'i(h) = i(h)N$ and $i'j(h) = j(h)N$. Since $i(h)j(h^{-1}) \in N$ we get $i(h)N = j(h)N$ so that $j'i(h) = i'j(h)$. Hence $j'i = i'j$ and thus (P, j', i') is a solution.

Now, let (G, j'', i'') be a solution of the given data. Then, there exist homomorphisms $j'': A \rightarrow G$ and $i'': B \rightarrow G$ such that $j''i = i''j$. Then, by the extension property of the free product $A * B$, there exists a homomorphism $\psi: A * B \rightarrow G$ such that $\psi \mid A = j''$ and $\psi \mid B = i''$. Then, for $a \in A$ and $b \in B$, we have $\psi(ab) = \psi(a)\psi(b) = j''(a)i''(b)$. Hence, if $h \in H$ then

$$\psi(i(h)j(h^{-1})) = j''i(h)i''j(h^{-1}) = 1 \quad (\text{as } j''i = i''j),$$

and this implies that $N \leq \text{Ker}(\psi)$.

Define a map $\phi: (A * B)/N \rightarrow G$ by $\phi(cN) = \psi(c)$. Then, ϕ is well defined since

$$\begin{aligned} cN = c'N &\iff c^{-1}c' \in N \\ &\iff c^{-1}c' \in \text{Ker}(\psi) \\ &\iff \psi(c) = \psi(c') \\ &\iff \phi(cN) = \phi(c'N) \end{aligned}$$

Further,

$$\phi j'(a) = \phi(aN) = \psi(a) = j''(a) \text{ and } \phi i'(b) = \phi(bN) = \psi(b) = i''$$

so that $\phi j' = j''$ and $\phi i' = i''$. Also, ϕ is unique since any two homomorphisms agree on the generating set $\{aN \mid a \in A\} \cup \{bN \mid b \in B\}$ of $(A * B)/N$. This proves the first statement of the theorem.

The second statement easily follows as the group $A * B$ has a presentation $\langle X \cup Y \mid \Delta \cup \Gamma \rangle$ (by Theorem 1.6.4) and N is generated by $\{i(h)j(h^{-1}) : h \in H\}$. ■

Now we come to the definition of an amalgamated free product.

Definition: Let A and B be groups having isomorphic subgroups H and K respectively. Let $\theta: H \rightarrow K$ be an isomorphism. The *amalgamated free product* (or merely the *amalgam*) of A and B over θ is defined to be the pushout of the data $i: H \rightarrow A$ and $j\theta: H \rightarrow B$ where i and j are the inclusions.

Theorem 1.7.2 implies that, given two groups A , B , and a subgroup H of A with an embedding $\theta: H \rightarrow B$, a unique amalgam always exists. It is $(A * B)/N$ where N is the normal closure of $\{i(h)\theta j(h^{-1}) \mid h \in H\} =$

$\{h\theta(h^{-1}) \mid h \in H\}$ in $A * B$. We denote this amalgam by $A *_\theta B$, or, less precisely, by $A *_H B$. Note that an element $h \in H$ is identified with $\theta(h) \in B$, and, conversely, $k \in \theta(H)$ is identified with $\theta^{-1}(k) \in A$.

As in the case of free products, there is a normal form for each element in an amalgamated free product. For notational convenience, we consider the amalgam $A_1 *_\theta A_2$ of A_1 and A_2 with isomorphic subgroups B_1 and B_2 under the isomorphism $\theta: B_1 \rightarrow B_2$. Furthermore we are going to consider the right cosets of $N \subset A_1 * A_2$ instead of the left cosets we have been dealing with so far. It will enable us to make an easier proof of Theorem 1.7.3 below. Nevertheless, we still adopt the same notation $(A_1 * A_2)/N$ to denote the group of right cosets of N in $A_1 * A_2$. We note that the Theorem 1.7.2 is still valid if we replace left cosets by right cosets.

Call a set of right coset representatives of a group a right transversal. Choose right transversals L_i of B_i in A_i , $i = 1, 2$. For $x \in A_i$, we can write $x = bl$ uniquely, where $l \in L_i$ and $b \in B_i$; indeed, if $x = b'l'$ then $l \in B_i l'$ so that $l = l'$ and hence $b = b'$. We denote by l_x the representative of $B_i x$ in L_i so that $x = bl_x$ for some $b \in B_i$.

Definition: A normal form of an element in $A_1 *_\theta A_2$ is a form $bl_{x_1}l_{x_2} \cdots l_{x_n}$ where $b \in B_1$, $n \geq 0$, the elements l_{x_i} lie in the transversals L_i of B_i in A_i and adjacent l_{x_i} lie in distinct A_i .

Theorem 1.7.3: Let A_1 and A_2 be groups, let B_i be a subgroup of A_i for $i = 1, 2$, and let $\theta: B_1 \rightarrow B_2$ be an isomorphism. Then for each element $Nw \in A_1 *_\theta A_2 = (A_1 * A_2)/N$, there is a unique normal form $F(w)$ of w with $Nw = NF(w)$.

Proof: Recall that $A_1 *_\theta A_2 = (A_1 * A_2)/N$ where N is the normal closure of $\{b\theta(b^{-1}) \mid b \in B_1\}$. For each coset $Nw \in (A_1 * A_2)/N$, consider the representative $w = x_1 y_1 \cdots x_n y_n$ in $A_1 * A_2$ where $x_i \in A_1$, $y_i \in A_2$ and only x_1 and y_n are allowed to be 1. Henceforth, we identify B_1 and B_2 as a common subgroup B of A_1 and A_2 . The following algorithm describes a way of finding a normal form $F(w)$ for each w such that $Nw = NF(w)$.

Case I: $w = x_1$

In this case, $w = x_1 = bl_{x_1} = F(w)$ where $b \in B$ and we are done.

Case II: $w = y_1$

In this case, write $y_1 = bl_{y_1}$ for some $b \in B$ and we are done.

Case III: $w = x_1 y_1$ where $x_1, y_1 \neq 1$

In this case, $w = x_1 bl_{y_1} = (x_1 b)l_{y_1} = b'l_z l_{y_1}$ for $b, b' \in B$ where $z = x_1 b \in A_1$.

By repeating this process, we arrive at a normal form $F(w)$ for any reduced word $w = x_1 y_1 x_2 y_2 \cdots x_n y_n$.

Next we devise a van der Waerden's trick, as we used in the cases of free groups and free products, to prove the uniqueness of the normal form.

Let M be the set of all normal forms. For $a \in A_i$, i fixed, define a map $\phi_a: M \rightarrow M$ by

$$\phi_a(bl_{a_1}l_{a_2} \cdots l_{a_n}) = F(abl_{a_1}l_{a_2} \cdots l_{a_n})$$

Clearly, ϕ_1 is the identity function on M . First we show that $\phi_{a'} \circ \phi_a = \phi_{a'a}$ for any $a, a' \in A_i$.

Let $w = bl_{a_1}l_{a_2} \cdots l_{a_n}$ be an element in M . Write

$$w' = \phi_a(w), \quad w'' = \phi_{a'}(w'), \quad w''' = \phi_{a'a}(w).$$

We wish to show that $w'' = w'''$ and this will be done by considering several cases.

Case I: $n > 0$ and both a and l_{a_1} belong to same group A_i

In this case, since $abl_{a_1} \in A_i$, we can write

$$abl_{a_1} = b'l_x \tag{1.2}$$

for some $b' \in B$, where $x = abl_{a_1}$. Hence,

$$w' = \phi_a(w) = b'l_x l_{a_2} l_{a_3} \cdots l_{a_n}$$

and thus

$$w'' = \phi_{a'}(w') = F(a'b'l_x l_{a_2} l_{a_3} \cdots l_{a_n}).$$

Now, if $y = a'b'l_x$ then $y \in A_i$ and $y = b''l_y$ for some $b'' \in B$, and thus

$$w'' = F(a'b'l_x l_{a_2} l_{a_3} \cdots l_{a_n}) = b''l_y l_{a_2} l_{a_3} \cdots l_{a_n}$$

with

$$a'b'l_x = b''l_y. \tag{1.3}$$

On the other hand, since $a'abl_{a_1} \in A_i$, we have

$$w''' = F(a'abl_{a_1} l_{a_2} \cdots l_{a_n}) = b'''l_z l_{a_2} l_{a_3} \cdots l_{a_n}$$

where $b''' \in B$ and

$$z = a'ab l_{a_1} = b'''l_z. \quad (1.4)$$

The equations (1.2), (1.3) and (1.4) together imply that $b'''l_z = b''l_y$ and hence $w'' = w'''$ and the equality $\phi_{a'a} = \phi_{a'} \circ \phi_a$ follows.

Case II: $w = b$ or a and l_{a_1} belong to different groups.

This case is also easy and we will not give the details.

Thus, ϕ_a is a permutation on M with the inverse $\phi_{a^{-1}}$. Hence, the map $\psi_i: A_i \rightarrow S_M$ defined by

$$\psi_i(a) = \phi_a$$

is a homomorphism. By the extension property of free products, there exists a unique homomorphism $\psi: A_1 * A_2 \rightarrow S_M$ extending the ψ_i and we easily see that

$$\psi(bl_{a_1}l_{a_2} \cdots l_{a_n}) = \phi_b\phi_{l_{a_1}}\phi_{l_{a_2}} \cdots \phi_{l_{a_n}}.$$

Now, if $b \in B$ then clearly $\phi_b = \phi_{\theta(b)}$ so that $\psi(b\theta(b^{-1})) = 1$. Hence $b\theta(b^{-1}) \in \text{Ker}(\psi)$ and thus $N \leq \text{Ker}(\psi)$. Therefore, we have an induced homomorphism $\Phi: (A_1 * A_2)/N \rightarrow S_M$ given by

$$\begin{aligned} \Phi(Nw) = \Phi(Nbl_{a_1} \cdots l_{a_n}) &= \psi(bl_{a_1} \cdots l_{a_n}) \\ &= \phi_b\phi_{l_{a_1}}\phi_{l_{a_2}} \cdots \phi_{l_{a_n}}. \end{aligned}$$

This is well-defined since, if $Nbl_{a_1} \cdots l_{a_n} = Nb'l'_{a'_1} \cdots l'_{a'_m}$ then

$$(bl_{a_1} \cdots l_{a_n})^{-1} b'l'_{a'_1} \cdots l'_{a'_m} \in N \leq \text{Ker}(\psi)$$

and hence $\phi(bl_{a_1} \cdots l_{a_n}) = \phi(b'l_{a'_1} \cdots l_{a'_m})$. Now, to show the uniqueness, suppose $F(w) = bl_{a_1} \cdots l_{a_n}$ and $G(w) = b'l_{a'_1} \cdots l_{a'_m}$ are two normal forms of w . Then $NF(w) = Nw$ and $NG(w) = Nw$ so that $NF(w) = NG(w)$. Now, we have the implications,

$$\begin{aligned}
NF(w) = NG(w) &\iff Nbl_{a_1} \cdots l_{a_n} = Nb'l_{a'_1} \cdots l_{a'_m} \\
&\iff \phi_b \phi_{l_{a_1}} \phi_{l_{a_2}} \cdots \phi_{l_{a_n}} = \phi_{b'} \phi_{l_{a'_1}} \phi_{l_{a'_2}} \cdots \phi_{l_{a'_m}} \\
&\implies \phi_b \phi_{l_{a_1}} \phi_{l_{a_2}} \cdots \phi_{l_{a_n}}(1) = \phi_{b'} \phi_{l_{a'_1}} \phi_{l_{a'_2}} \cdots \phi_{l_{a'_m}}(1) \\
&\iff bl_{a_1} \cdots l_{a_n} = b'l_{a'_1} \cdots l_{a'_m}
\end{aligned}$$

and thus the two normal forms are equal. This completes the proof of the theorem. $\blacksquare$

Corollary 1.7.1: Let $G = A *_H B$ be a free product of two groups A and B amalgamating a subgroup H , and let $A_1 \leq A$ and $B_1 \leq B$ with $A_1 \cap H = B_1 \cap H$. Then the subgroup $\langle A_1, B_1 \rangle$ of G generated by A_1 and B_1 is isomorphic to

$$A_1 *_{{A_1 \cap H}} B_1.$$

Proof: Let T_1 (respectively S_1) be a right transversal of $A_1 \cap H$ in A_1 (respectively B_1). Then, we can write any element w in $A_1 *_{{A_1 \cap H}} B_1$ in a normal form $F(w) = h \cdots t_i s_i \cdots$, where $h \in A_1 \cap H$, $t_i \in T_1$ and $s_i \in S_1$.

Next, we prove that T_1 (respectively S_1) can be extended to a right transversal T (respectively S) of H in A (respectively B). It suffices to prove that for any two distinct $t, t' \in T_1$, $Ht \neq Ht'$. We have that $(A_1 \cap H)t \neq (A_1 \cap H)t'$. Therefore, $t't^{-1} \notin A_1 \cap H$ so that $t't^{-1} \notin H$, i.e., $Ht \neq Ht'$ as claimed. Therefore, $F(w)$ can be regarded as the normal form of w in G with respect

to the transversals T and S . Hence, the natural map

$$\phi: A_1 *_{A_1 \cap H} B_1 \rightarrow A *_{\langle H \rangle} B$$

induced by the inclusions $A_1 \hookrightarrow A$ and $B_1 \hookrightarrow B$ is a monomorphism whose image is $\langle A_1, B_1 \rangle$. Therefore $\langle A_1, B_1 \rangle \cong A_1 *_{A_1 \cap H} B_1$ as desired. $\blacksquare$

Next we are going to list some useful properties of amalgamated free product whose proofs require more effort, time and space. Therefore we omit the proofs giving only references.

Theorem 1.7.4: Let A_1 and A_2 be two groups and let $A = A_1 *_{\langle K \rangle} A_2$ be the free product of A_1 and A_2 amalgamating a subgroup K . If H is a subgroup of A such that $H \cap (y^{-1}Ky) = 1$ for any $y \in A_i$, ($i = 1, 2$), then

$$H = \left(\bigast_{i \in \{1,2\}, x \in X_i} (H \cap x^{-1}A_i x) \right) * F,$$

where, for each i , X_i is a system of double coset representatives for $H \backslash A / A_i$, and F is a free group.

See [17, page 56] for a proof.

Corollary 1.7.2: If H is a normal subgroup of an amalgamated free product $A = A_1 *_{\langle K \rangle} A_2$ such that $H \cap A_i = 1$ for each $i = 1, 2$, then H is a free group.

Proof: First we note that

$$H \cap (x^{-1}A_i x) = (x^{-1}Hx) \cap (x^{-1}A_i x) = x^{-1}(H \cap A_i)x$$

as H is normal in A . Now, from Theorem 1.7.4, we can write,

$$H = \left(\bigast_{i \in \{1,2\}, x \in X_i} x^{-1}(H \cap A_i)x \right) * F.$$

Since each $H \cap A_i$ is the trivial group for each i , we have that $H = F$ so that H is free. ■

Theorem 1.7.5: Let A and B be finite groups and let G be any amalgam of A and B . Then, there is a homomorphism ϕ from G onto a finite group M containing both A and B such that the restrictions $\phi|_A$ and $\phi|_B$ are inclusions.

See [13, page 532] for a proof.

We end this section with the notion of cartesian homomorphism.

Definition: Let $P = \ast_{i \in I} A_i$ be a free product of the groups A_i and $D = \prod_{i \in I} A_i$ be the cartesian product of the groups A_i . Let $\theta_i: A_i \rightarrow D$ be the natural homomorphism that maps each a_i in A_i to $(d_j)_{j \in I}$ in D where $d_i = a_i$ and all other $d_j = 1$. Then, by the extension property of free products, the θ_i are simultaneously extended to a unique homomorphism $\theta: P \rightarrow D$. This θ is called the cartesian homomorphism and the $\text{Ker}(\theta)$, usually denoted by P^* , is called the cartesian group of P .

One thing we notice is that the map θ in this definition is surjective so that $P/P^* \cong D$.

Example 1.7.1: The cartesian group P^* in the above definition is a free group.

Proof: We use Corollary 1.7.2. If $x \in G_i \cap P^*$ then $(1) = \theta(x) = (d_j)$ where $d_i = x$ and all other $d_j = 1$. Hence $x = 1$ and the result follows. ■

1.8 Extension of Groups and Subnormal Series

Definition: A group G is said to be an *extension* of a group A by a group B if G contains a normal subgroup H such that $H \cong A$ and $G/H \cong B$.

For example, the symmetric group S_3 is an extension of $\mathbb{Z}_3$ by $\mathbb{Z}_2$. We note that $\mathbb{Z}_6$ also is an extension of $\mathbb{Z}_3$ by $\mathbb{Z}_2$.

Definition: Let G be a group. Suppose there is a series of subgroups of G such that

$$1 = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_n = G.$$

A series of this form is called a *subnormal series* of G .

Here, we see that G_{i+1} is an extension of G_i by G_{i+1}/G_i . In that sense, the group G is obtained with a succession of extensions by the factor groups starting with the trivial group.

See [4] for an account on subnormal series and related topics.

1.9 HNN extensions

In this section, we define what an HNN extension is and give some examples followed by a theorem on normal forms.

Definition: Let $G = \langle X \mid \Delta \rangle$ be a group with isomorphic subgroups A and B , and let $\phi: A \rightarrow B$ be an isomorphism. Then the group having the

presentation

$$\langle X, t \mid \Delta, t^{-1}at = \phi(a) \text{ for all } a \in A \rangle$$

is called an *HNN extension* of G and is denoted by $G \Omega_\phi A$. The group G is called the *base* and the generator t is called the *stable* letter of $G \Omega_\phi A$.

Example 1.9.1: Consider the infinite cyclic group $G = \langle a \rangle$ and the isomorphic subgroups $A = \langle a^2 \rangle$ and $B = \langle a^3 \rangle$. If $\phi: A \rightarrow B$ is the isomorphism defined by $\phi(a^2) = a^3$ then

$$G \Omega_\phi A = \langle a, t \mid t^{-1}a^2t = a^3 \rangle.$$

Our aim is to state a normal form theorem for HNN extensions, which will not be proven here.

Definition: Let $G \Omega_\phi A$ be an HNN extension with base $G = \langle X \mid \Delta \rangle$ and stable letter t . Denote by g_i ($i = 1, 2, \dots, n-1$) a non-empty word on X (i.e., a non identity element of G), and by g_0 and g_n , any word (including the empty word) on X . A word

$$w = g_0 t^{\epsilon_1} g_1 t^{\epsilon_2} \dots t^{\epsilon_n} g_n \quad (n \geq 0)$$

on $X \cup \{t\}$, where the $\epsilon_i = \pm 1$, is called *reduced* if w does not contain a subword $t^{-1}g_it$ with $g_i \in A$ or tg_it^{-1} with $g_i \in \phi(A)$.

Theorem 1.9.1 (Britton's Lemma): Assume the notation in the above definition. If the word

$$w = g_0 t^{\epsilon_1} g_1 t^{\epsilon_2} \dots t^{\epsilon_n} g_n$$

is reduced and $n \geq 1$, then $w \neq 1$ in $G \Omega_\phi A$.

See [9, page 182] for a proof. See also [16, page 414].

Example 1.9.2: In the HNN extension of Example 1.9.1, the element $c = t^{-1}a^{-1}ta^{-1}t^{-1}ata$ is reduced and hence not equal to the identity. ■

Proof: Neither a nor a^{-1} is in $A \cup \phi(A)$ so that there are no subwords of the form $t^{-1}g_it$ with $g_i \in A$ or tg_it^{-1} with $g_i \in \phi(A)$ in c , and hence the result follows from Britton's Lemma. ■

An account on HNN extensions, including a proof of Britton's Lemma, can be found in [16].

Chapter 2

Residual Properties of Groups

2.1 Definitions and Examples

Definition: Let $\mathcal{C}$ be a class of groups. A group G is called *residually $\mathcal{C}$* if, for any $1 \neq g \in G$, there exists an epimorphism ϕ from G to a group $C \in \mathcal{C}$ such that $\phi(g) \neq 1$.

There are several other equivalent definitions. Some of them are listed in the following theorem.

Theorem 2.1.1: The followings are equivalent:

(a) G is residually $\mathcal{C}$,

(b) For every non-identity element $g \in G$ there exists $N_g \triangleleft G$ such that $G/N_g \in \mathcal{C}$ and $g \notin N_g$,

(c) There is a family $\{N_\lambda\}$ of normal subgroups of G such that $G/N_\lambda \in \mathcal{C}$ for each λ and $\bigcap_\lambda N_\lambda = \{1\}$.

Proof: (a) $\Rightarrow$ (b): Suppose G is residually $\mathcal{C}$. Then, for $1 \neq g \in G$, there exists an epimorphism ϕ from G to a group $C \in \mathcal{C}$ such that $\phi(g) \neq 1$. Then, if we set $N_g = \text{Ker}(\phi)$, we have $N_g \triangleleft G$, $g \notin N_g$ and $G/N_g (\cong C = \text{Im}\phi) \in \mathcal{C}$, and (b) follows.

(b) $\Rightarrow$ (c): Consider the family $\{N_g \mid g \in G, g \neq 1\}$. Let $x \in \bigcap N_g$. If $x \neq 1$ then $x \in N_x$. But by (b), $x \notin N_x$, a contradiction. Therefore, $x = 1$ and (c) follows.

(c) $\Rightarrow$ (a): If the given equality holds, then for any given $1 \neq g \in G$, there exists $N_\mu \triangleleft G$ such that $G/N_\mu \in \mathcal{C}$ and $g \notin N_\mu$. If we define an epimorphism $\phi : G \longrightarrow G/N_\mu$ by $\phi(x) = xN_\mu$, then $\phi(G) = G/N_\mu \in \mathcal{C}$ and $\phi(g) = gN_\mu \neq 1$, so that G is residually $\mathcal{C}$. ■

If the groups of the class $\mathcal{C}$ are characterized by a certain property π then we say that G is residually π . In particular, if $\mathcal{C}$ is the set of all finite groups (i.e., $\pi = \text{finite}$), then we say that G is *residually finite*.

We are mainly concerned with residual finiteness of groups. Not all the groups have this property. First, let us look at some examples.

Example 2.1.1: Every finite group is residually finite

Proof: Set $N_\lambda = \{1\}$ in Theorem 2.1.1(c) and then the result is obvious. ■

Example 2.1.2: The infinite cyclic group $\mathbb{Z}$ is residually finite. Hence, together with Example 2.1.1, any cyclic group is residually finite.

Proof: The family $\{N_\lambda\}_{\lambda=1}^\infty$, where $N_\lambda = \lambda\mathbb{Z}$, of subgroups of $\mathbb{Z}$ satisfies the conditions in Theorem 2.1.1(c). Hence, $\mathbb{Z}$ is residually finite. ■

The following example is due to G. Higman [6].

Example 2.1.3: There exists a finitely generated group which does not contain any subgroup of finite index, hence such a group is not residually finite.

We prove the existence by constructing such a group. First we prove a lemma.

Lemma 2.1.1: If n is an integer greater than 1, the least prime factor of n is less than the least prime factor of $2^n - 1$.

Proof: Let p be a prime factor of $2^n - 1$ and let r be the least positive integer such that p divides $2^r - 1$. Then, clearly, $r > 1$ so that r has a prime factor q . Now consider the group $\{1, 2, \dots, p-1\}$ under the operation multiplication modulo p . This group has $p-1$ elements so that p divides $2^{p-1} - 1$. Since r is the least positive integer such that p divides $2^r - 1$, we conclude, by Lagrange's Theorem for subgroups, that r divides $p-1$ implying that $q \leq r \leq p-1 < p$. From the same theorem, we have that r divides n and hence q is a prime factor of n . This proves the lemma. ■

Proof of Example 2.1.3: Consider the four groups

$$H_i = \langle a_i, b_i \mid a_i^{-1}b_i a_i = b_i^2 \rangle, \quad i = 1, 2, 3, 4.$$

Fix any i . By Corollary 1.5.1, the subgroups $\langle a_i \rangle$ and $\langle b_i \rangle$ of H_i are infinite cyclic. Their intersection contains only the identity. To prove this, consider

an element $x \in \langle a_i \rangle \cap \langle b_i \rangle$. Then $x = a_i^m = b_i^n$ for some m, n . From the relation $a_i^{-1} b_i a_i = b_i^2$, we can prove, by induction, that $a_i^{-1} b_i^n a_i = b_i^{2^n}$. Hence, $a_i^{-1} a_i^m a_i = a_i^{2^m}$, i.e., $a_i^m = 1$, giving $m = 0$ as $\langle a_i \rangle$ is infinite cyclic. Hence $x = 1$ and the intersection is trivial.

Therefore we may form the free product K_{12} , say, of H_1 and H_2 amalgamating the subgroups $\langle a_2 \rangle$ of H_2 and $\langle b_1 \rangle$ of H_1 under the isomorphism $\phi_{12} : a_2 \mapsto b_1$, i.e.,

$$\begin{aligned} K_{12} = H_1 *_{\phi_{12}} H_2 &= \langle a_1, a_2, b_1, b_2 \mid a_1^{-1} b_1 a_1 = b_1^2, a_2^{-1} b_2 a_2 = b_2^2, a_2 = b_1 \rangle \\ &= \langle a_1, a_2, b_2 \mid a_1^{-1} a_2 a_1 = a_2^2, a_2^{-1} b_2 a_2 = b_2^2 \rangle. \end{aligned}$$

Similarly

$$K_{34} = H_3 *_{\phi_{34}} H_4 = \langle a_3, a_4, b_4 \mid a_3^{-1} a_4 a_3 = a_4^2, a_4^{-1} b_4 a_4 = b_4^2 \rangle.$$

Define G to be the free product of K_{12} and K_{34} amalgamating the subgroups $\langle b_2 \rangle$ of K_{12} with $\langle a_3 \rangle$ of K_{34} , and also the subgroups $\langle a_1 \rangle$ of K_{12} with $\langle b_4 \rangle$. Then

$$\begin{aligned} G &= K_{12} *_{\psi_1, \psi_2} K_{34} \\ &= \langle a_1, a_2, a_3, a_4 \mid \\ &\quad a_1^{-1} a_2 a_1 = a_2^2, a_2^{-1} a_3 a_2 = a_3^2, a_3^{-1} a_4 a_3 = a_4^2, a_4^{-1} a_1 a_4 = a_1^2 \rangle. \end{aligned}$$

where $\psi_1 : a_3 \mapsto b_2$ and $\psi_2 : a_1 \mapsto b_4$. Suppose G has a proper normal subgroup N of finite index. Then the quotient group G/N is nontrivial. Also we identify $a_i N$ by a_i in this quotient group. Then, each a_i has finite order, say n_i .

Now, from the equation $a_1^{-1}a_2a_1 = a_2^2$, we can prove, by induction, that $a_1^{-n}a_2a_1^n = a_2^{2^n}$. When $n = n_1$, this gives $a_2^{2^{n_1}-1} = 1$ implying

$$n_2 | 2^{n_1} - 1.$$

Similarly, we can show that

$$n_3 | 2^{n_2} - 1, \quad n_4 | 2^{n_3} - 1, \quad n_1 | 2^{n_4} - 1.$$

If $n_1 = 1$ then these equations imply that $n_1 = n_2 = n_3 = n_4 = 1$ contradicting the non-triviality of G/N . Therefore, we may assume that each $n_i > 1$. Now assume, without loss of generality, that the smallest prime factor p of $n_1n_2n_3n_4$ divides n_2 . Then, since $n_2 | 2^{n_1} - 1$, we have that $p | 2^{n_1} - 1$, but then, according to the lemma, a prime smaller than p divides n_1 , a contradiction. Hence, our initial assumption is false so that G has no proper subgroups of finite index.

Clearly G is finitely generated. We complete the proof by proving that G is infinite.

We note that, in K_{12} , $\langle a_1 \rangle \cap \langle b_1 \rangle = 1$ and $\langle a_2 \rangle \cap \langle b_2 \rangle = 1$. Therefore, by Corollary 1.7.1, $\langle a_1, b_2 \rangle \cong \langle a_1 \rangle * \langle b_2 \rangle$, which is a free group of rank 2 since $\langle a_1 \rangle \cong \mathbb{Z} \cong \langle b_2 \rangle$. Hence, K_{12} contains the free subgroup $\langle a_1, b_2 \rangle$. Similarly, it can be shown that K_{34} contains the free subgroup $\langle a_3, b_4 \rangle$. Now, in the construction of $G = K_{12} *_{\psi_1, \psi_2} K_{34}$, the isomorphisms, ψ_1 and ψ_2 induces an isomorphism

$$\psi: \langle a_1, b_2 \rangle \rightarrow \langle a_3, b_4 \rangle.$$

Therefore, we may regard G to be the free product of K_{12} and K_{34} amalgamating the free subgroups $\langle a_1, b_2 \rangle$ and $\langle a_3, b_4 \rangle$ of K_{12} and K_{34} respectively.

Hence, G contains the free group $\langle a_1, b_2 \rangle$ of rank two which is infinite so that G must be infinite. ■

Example 2.1.4: The additive group $\mathbb{Q}$ of rationals is not residually finite.

Actually, we can prove that $\mathbb{Q}$ has no subgroup of finite index. First we state a lemma whose proof is obvious.

Lemma 2.1.2: Let G be any group and H a normal subgroup in G of finite index n . Then,

$$G^n = \langle g^n \mid g \in G \rangle,$$

the subgroup of G generated by all elements of the form g^n , $g \in G$, is a subgroup of H .

Proof of Example 2.1.4: Suppose there exists $H \triangleleft \mathbb{Q}$ such that $\mathbb{Q}/H$ is finite. Let $[\mathbb{Q} : H] = n$. Then, by Lemma 2.1.2, $n\mathbb{Q} \leq H$ ($n\mathbb{Q}$ is the additive notation for $\mathbb{Q}^n$). But, $n\mathbb{Q} = \mathbb{Q}$ so that $H = \mathbb{Q}$ and hence $\mathbb{Q}$ itself is the only subgroup of $\mathbb{Q}$ of finite index. ■

2.2 Fundamental Properties

Next we investigate some properties of residually finite groups.

Theorem 2.2.1: Every subgroup of a residually finite group is residually finite. Every subgroup of a group which is residually a finite p -group is again residually a finite p -group where p is any prime.

Proof: Suppose G is residually finite and H is a subgroup of G . Let $1 \neq$

$h \in H$. Then, since G is residually finite, there exists $N \triangleleft G$ such that $h \notin N$ and G/N is finite. Then, $h \notin H \cap N \triangleleft H$ and

$$\frac{H}{H \cap N} \cong \frac{HN}{N} \leq \frac{G}{N}$$

and this shows that, being a subgroup of a finite group, $H/(H \cap N)$ is finite. Hence, H is residually finite. The proof when G is residually a finite p -group is just similar: one has to replace the word “finite” by the phrase “finite p -group” appropriately. ■

Theorem 2.2.2: If G and H are two residually finite groups then so is the direct product $G \times H$. If each of G and H is residually a finite p -group then so is the direct product $G \times H$.

Proof: Let $1 \neq gh \in G \times H$ where $g \in G$ and $h \in H$. Then, not both g and h are equal to identity. Suppose, without loss of generality, that $g \neq 1$. Then there exists $K \triangleleft G$ such that $g \notin K$ and G/K is finite. Now, define a map $\phi: G \times H \rightarrow (G/K)$ by $\phi(xy) = xK$. Then, it is routine to check that ϕ is an epimorphism and that $\text{Ker}(\phi) = K \times H$.

Hence, we have,

$$(G \times H)/(K \times H) \cong G/K.$$

This shows that $K \times H$ is a normal subgroup of finite index in $G \times H$ not containing gh , and thus the theorem follows. The proof of the other part is essentially similar with appropriate word changes. ■

2.3 Residual Properties of Free Groups

One of the most important result in the investigation of residual properties of groups is the residual finiteness of free groups. In fact, we prove a stronger property than being residually finite, namely, being residually a finite p -group (a finite group all whose elements have order a power of p). The proof of this theorem and the preceding lemma are from [8, page 92].

Theorem 2.3.1: Let p be any prime. Every free group $F(X)$ is residually a finite p -group.

Lemma 2.3.1: Let m be an integer ≥ 2 . The subgroup of $GL(2, \mathbb{Z})$ generated by the two matrices a and b where,

$$a = \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} \text{ and } b = \begin{pmatrix} 1 & 0 \\ m & 1 \end{pmatrix}$$

is free of rank 2.

Proof: First we note that

$$a^n = \begin{pmatrix} 1 & mn \\ 0 & 1 \end{pmatrix} \text{ and } b^n = \begin{pmatrix} 1 & 0 \\ mn & 1 \end{pmatrix}$$

for any integer n : this can be proved easily using induction.

Any non trivial element w in the group generated by a and b is a finite alternating product of powers of a and b of the form

$$w = a^{\alpha_1} b^{\alpha_2} a^{\alpha_3} \dots b^{\alpha_r}$$

where the α_i are integers, $\alpha_i \neq 0$ for $i = 2, 3, \dots, r-1$ and $r > 0$. We show that $w \neq 1$. Suppose $w = 1$. If w is a non zero integer power of either a or b then, clearly, $w \neq 1$. Therefore, suppose that w contains only non-zero powers of both a and b . If w is of the form

$$b^{\alpha_2} a^{\alpha_3} b^{\alpha_4} \dots$$

then conjugate both side of the equation

$$b^{\alpha_2} a^{\alpha_3} b^{\alpha_4} \dots = 1$$

by b^{α_2} to get an equation of the form

$$a^{\alpha_3} b^{\alpha_4} a^{\alpha_5} \dots = 1.$$

Hence, in any case, we may assume that we get an equation of the form

$$a^{\alpha_1} b^{\alpha_2} \dots c^{\alpha_r} = 1$$

where c is either a or b .

Denote by z_i the first row of the matrix $a^{\alpha_1} b^{\alpha_2} \dots c^{\alpha_i}$ where c again denotes either a or b depending on whether i is odd or even respectively.

Let $z_{2k+1} = (x_{2k+1}, x_{2k+2})$. We show that

$$x_{2k+1} = x_{2k-1} + m\alpha_{2k}x_{2k} \tag{2.1}$$

and

$$x_{2k+2} = x_{2k} + m\alpha_{2k+1}x_{2k+1}. \tag{2.2}$$

We have

$$\begin{aligned} z_{2k} &= z_{2k-1} b^{\alpha_{2k}} \\ &= (x_{2k-1}, x_{2k}) \begin{pmatrix} 1 & 0 \\ m\alpha_{2k} & 1 \end{pmatrix} \\ &= (x_{2k-1} + m\alpha_{2k}x_{2k}, x_{2k}) \end{aligned}$$

and

$$\begin{aligned}
(x_{2k+1}, x_{2k+2}) &= z_{2k+1} \\
&= z_{2k} a^{\alpha_{2k+1}} \\
&= (x_{2k-1} + m\alpha_{2k}x_{2k}, x_{2k}) \begin{pmatrix} 1 & m\alpha_{2k+1} \\ 0 & 1 \end{pmatrix} \\
&= (x_{2k-1} + m\alpha_{2k}x_{2k}, m\alpha_{2k+1}(x_{2k-1} + m\alpha_{2k}x_{2k}) + x_{2k}),
\end{aligned}$$

hence the equations (1) and (2).

Equations (1) and (2) can be combined to get a single equation

$$x_{i+2} = x_i + m\alpha_{i+1}x_{i+1},$$

where $i = 1, 2, \dots, r-1$.

Next we show, by induction, that $|x_{i+1}| > |x_i|$ for $i = 1, 2, \dots, r-1$.

We have $z_1 = (x_1, x_2) = (1, m\alpha_1)$, so that $|x_2| = |m\alpha_1| > 1 = |x_1|$. Hence the result holds for $i = 1$. If the result holds for i then,

$$\begin{aligned}
|x_{i+2}| &\geq m|\alpha_{i+1}||x_{i+1}| - |x_i| \\
&\geq m|x_{i+1}| - |x_i| \\
&= |x_{i+1}| + (|x_{i+1}| - |x_i|) \\
&> |x_{i+1}|.
\end{aligned}$$

Therefore, the first entry of w is never 1 so that $w \neq 1$. Hence, $\langle a, b \rangle$ is freely generated and this completes the proof. ■

Proof of Theorem 2.3.1: We prove the theorem by showing that the free group F_2 is residually a finite p -group. First consider the case when X is

infinite. Let $\hat{X}$ be a finite subset of X . Define a map $\phi: X \rightarrow F(\hat{X})$ by

$$\phi(x) = \begin{cases} x & x \in \hat{X} \\ 1 & x \notin \hat{X}. \end{cases}$$

Then, ϕ extends to an epimorphism $\tilde{\phi}: F(X) \rightarrow F(\hat{X})$ so that

$$F(X)/\text{Ker}(\tilde{\phi}) \cong F(\hat{X}).$$

Denote by $\{H_i \mid i \in I\}$ the collection of the kernels $\text{Ker}(\tilde{\phi})$ of all such epimorphisms $\tilde{\phi}$ (obtained by letting $\hat{X}$ range over all finite subsets of X), where I is a suitable index set. It can easily be proven that

$$\bigcap_{i \in I} H_i = 1.$$

Define a map

$$\psi: F(X) \rightarrow \prod_{i \in I} \left(\frac{F(X)}{H_i} \right)$$

by sending each $g \in F(X)$ to the element in $\prod_{i \in I} F(X)/H_i$ whose i^{th} coordinate is gH_i , $i \in I$. Then it is routine to check that ψ is a monomorphism. Thus, any free group can be embedded in a direct product of free groups of finite rank. Hence, by Theorem 2.2.1, Theorem 2.2.2, Corollary 1.4.3 and Lemma 2.3.1, it suffices to prove that F_2 is residually a finite p -group.

We have, by Lemma 2.3.1, that F_2 is generated by the two matrices

$$a = \begin{pmatrix} 1 & p \\ 0 & 1 \end{pmatrix} \text{ and } b = \begin{pmatrix} 1 & 0 \\ p & 1 \end{pmatrix}.$$

Consider the homomorphism $\psi: SL(2, \mathbb{Z}) \rightarrow SL(2, p)$ defined by

$$\psi \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} = \begin{pmatrix} \bar{a}_1 & \bar{a}_2 \\ \bar{a}_3 & \bar{a}_4 \end{pmatrix},$$

where $\bar{a}_i \equiv a_i \pmod{p}$, $i = 1, 2, 3, 4$.

Clearly, both a and b are in the kernel of ψ . $\text{Ker}(\psi)$ is called a congruence subgroup of $SL(2, \mathbb{Z})$ and denote it by $\Gamma_2(p)$. Then, the free group F_2 is embeddable in $\Gamma_2(p)$. Now consider the kernel of the obvious homomorphism $\chi: SL(2, \mathbb{Z}) \rightarrow SL(2, p^k)$ where k is a positive integer, and denote it by $\Gamma_2(p^k)$. Then, we easily see that

$$\bigcap_{k=1}^{\infty} \Gamma_2(p^k) = 1.$$

Next we show that, for any positive integer k , $\Gamma_2(p)/\Gamma_2(p^k)$ is a p group. Note that any element in $\Gamma_2(p)$ is of the form $1 + pz$ for some $z \in M(2, \mathbb{Z})$, the set of all 2×2 matrices on $\mathbb{Z}$. Now,

$$(1 + pz)^p = \sum_{i=0}^p \binom{p}{i} (pz)^i \equiv 1 \pmod{p^2},$$

so that $(1 + pz)^p = 1 + p^2 z_1$ for some $z_1 \in M(2, \mathbb{Z})$. Now,

$$(1 + p^2 z_1)^p = \sum_{i=0}^p \binom{p}{i} (p^2 z_1)^i \equiv 1 \pmod{p^3},$$

so that

$$(1 + pz)^{p^2} \equiv 1 \pmod{p^3}.$$

Continuing this way, we can show that

$$(1 + pz)^{p^{k-1}} \equiv 1 \pmod{p^k},$$

so that the order of $(1 + pz)\Gamma_2(p^k)$ in $\Gamma_2(p)/\Gamma_2(p^k)$ is a power of p . Hence, by Theorem 2.1.1 (c), $\Gamma_2(p)$ is residually finite and thus, being a subgroup of a residually finite group, F_2 is residually finite. ■

We have shown that every free group is residually finite and that there are groups that are not residually finite. Since every group is a quotient of a free group, we deduce that quotients of residually finite groups need not be residually finite. Nevertheless, the following is an example (see [10, page 307]) that illustrates this situation. It shows that the quotient group of a residually finite group G need not be residually finite even if G is finitely generated.

Example 2.3.1: There is a quotient group of the free group F_2 , which is not residually finite.

Proof: We show that the group

$$G = \langle a, b \mid a^{-1}b^2a = b^3 \rangle,$$

a quotient group of F_2 , is not residually finite.

Suppose G is residually finite. Let ϕ be any homomorphism of G such that $\phi(G)$ is finite. Set $\phi(a) = \alpha$ and $\phi(b) = \beta$. We can prove, using induction, that the equation $a^{-1}b^2a = b^3$ implies

$$a^{-n}b^{2^n}a^n = b^{3^n}. \quad (2.3)$$

If the order of α is n , then, by applying ϕ on both side of the equation (2.3) we get that $\beta^{3^n-2^n} = 1$, hence the order of β divides $k = 3^n - 2^n$. Now, $\text{GCD}(2, k) = 1$ so that $2s + kt = 1$ for some integers s and t . This gives $\beta = \beta^{2^s}$.

Now let $b_1 = a^{-1}ba$. Then, if $\phi(b_1) = \beta_1$, we have $\beta_1^k = \alpha^{-1}\beta^k\alpha$ so that $\beta_1^k = 1$. Hence, as above, $\beta_1 = \beta_1^{2^s}$. On the other hand $b_1^2 = a^{-1}b^2a = b^3$ so that $\beta_1^2 = \beta^3$ and hence $\beta_1 = \beta^{3^s}$. Now consider the element $c = b_1^{-1}b^{-1}b_1b =$

$a^{-1}b^{-1}ab^{-1}a^{-1}bab$ whose image under ϕ is $\beta_1^{-1}\beta^{-1}\beta_1\beta$ which is the identity since β_1 is a power of β . But we proved in Example 1.9.2 that c is not the identity in G . This shows that the non identity element c is mapped to the identity under any epimorphism ϕ from G to a finite group. Hence G is not residually finite. ■

2.4 Further Properties

Now we set off for an investigation of properties of groups which satisfy residual properties.

Given a group by means of a presentation and a word on elements of that group, the problem of deciding whether or not that word is the identity is called the *word problem*. For example, consider the group

$$G = \langle a, b \mid a^2 = 1, aba = b^3 \rangle$$

and the word

$$a^3bab^{-3}.$$

We see that

$$a^3bab^{-3} = a^2(aba)b^{-3} = 1b^3b^{-3} = 1.$$

Given a group G , if there is a procedure to decide whether any given word in G is the identity element or not, then we say that G has a solvable word problem. Otherwise, we say that G has an unsolvable word problem. Some groups have a solvable word problem while others do not. For instance,

every finite group has a solvable word problem. It has been shown that there are finitely presented groups that has an unsolvable word problem (see [16, page 431]. We prove the following. The main sources of the following proof are [15, page 55] and [9, page 195].

Theorem 2.4.1: Every finitely presented residually finite group G has a solvable word problem.

Proof: Let $G = \langle a_1, a_2, \dots, a_n \mid r_1, r_2, \dots, r_m \rangle$ be a presentation of G and w a reduced word in G . We show that there is a procedure to decide, in a finite number of steps, whether or not $w = 1$ in G .

Our procedure consists of two algorithms that act simultaneously.

algorithm 1: Enumerate all possible words on the generators $a_1, a_2, \dots, a_n$ (not necessarily reduced) that are equal to the identity. This can be done as follows:

Assuming that the alphabet is $a_1, a_1^{-1}, a_2, a_2^{-1}, \dots, a_n, a_n^{-1}$, list all words of length 1 in dictionary order, viz.,

$$a_1, a_1^{-1}, a_2, a_2^{-1}, \dots, a_n, a_n^{-1}.$$

List all words length 2 in (dictionary) order, viz.,

$$a_1 a_1, a_1 a_1^{-1}, \dots, a_1 a_n^{-1}, a_1^{-1} a_1, a_1^{-1} a_1^{-1}, \dots, a_1^{-1} a_n^{-1}, \dots, a_n^{-1} a_n^{-1}.$$

Continuing this way, we can enumerate all possible words of all finite lengths on the generators $a_1, a_2, \dots, a_n$. Denote by $u_1, u_2, \dots$ the list of all such words. Also, let us denote, without loss of generality, by $r_1, r_2, \dots, r_m$ the sequence of all relators together with their inverses. Then, create the following table where w_{ij} denotes the conjugate of r_i by u_j , i.e., $u_j^{-1} r_i u_j$.

	u_1	u_2	u_3	$\dots$	u_j	$\dots$
r_1	w_{11}	w_{12}	w_{13}	$\dots$	w_{1j}	$\dots$
r_2	w_{21}	w_{22}	w_{23}	$\dots$	w_{2j}	$\dots$
r_3	w_{31}	w_{32}	w_{33}	$\dots$	w_{3j}	$\dots$
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
r_m	w_{m1}	w_{m2}	w_{m3}	$\dots$	w_{mj}	$\dots$

Now, we can enumerate all elements of this table in the direction of the arrows starting from w_{11} . Let $z_1, z_2, \dots$ be this enumeration. Now, it is clear that we can create another list from this list such that the latter list contains all the words that are equal to the identity in G . If w occurs in this list while enumerating, then stop.

algorithm 2: Enumerate all finite groups. This can be done as follows:

First choose a countably infinite alphabet $y_1, y_2, \dots$. For each positive integer n , construct a multiplication table for each group of order n using the first n letters of the alphabet (i.e., $y_1, y_2, \dots, y_n$). Certainly, there are many different multiplication tables of isomorphic groups on the letters $y_1, y_2, \dots, y_n$ (which can be constructed permuting these letters) for any given group of order n , but we choose any one of them. For example, Klein-4 group can be represented by the multiplication table

$*$	y_1	y_2	y_3	y_4
y_1	y_1	y_2	y_3	y_4
y_2	y_2	y_1	y_4	y_3
y_3	y_3	y_4	y_1	y_2
y_4	y_4	y_3	y_2	y_1

For each such enumerated finite group B , construct all possible homomorphisms $\phi : G \longrightarrow B$. Since B is finite and G is finitely generated, there are only a finite number of such homomorphisms. These homomorphism can be constructed as follows:

To each $a_i \in G$, assign an element b_i in B and then check whether $\phi(r_i) = 1$ for each relator r_i . If it is, then ϕ is a homomorphism. For each such homomorphism, compute $\phi(w)$. If $\phi(w) \neq 1$ for some B and some ϕ , then stop the procedure.

Now we show that one, and only one of these algorithms definitely stops. If the *algorithm 1* does not stop then $w \neq 1$. Then, by the residual finiteness of G , there is a finite group B and an epimorphism ϕ from G to B such that $\phi(w) \neq 1$ in B in which case the *algorithm 2* should stop. On the other hand, if the *algorithm 1* stops then $w = 1$. Hence $\phi(w) = 1$ for homomorphisms ϕ of G in which case *algorithm 2* does not stop. Hence, we conclude that $w = 1$ if and only if *algorithm 1* stops, i.e., $w \neq 1$ if and only if *algorithm 2* stops. Hence, the word problem is solvable for G . ■

Definition: A group G is said to be *hopfian* if every surjective endomorphism of G is an automorphism. An obvious equivalent definition is

$$“\phi : G \xrightarrow{\text{onto endo}} G \implies \text{Ker}(\phi) = \{1}”.$$

The source of the proof of the following theorem is from [15, page 165].

Theorem 2.4.2: A finitely generated residually finite group G is hopfian.

Proof: Suppose G is not hopfian. Then, there exists a surjective endomorphism $\theta : G \rightarrow G$ and an element $x \in G$ such that $1 \neq x \in \text{Ker}(\theta)$.

Since G is residually finite, there exists an epimorphism $\phi: G \rightarrow A$ where A is finite and $\phi(x) \neq 1$. Set $M = \text{Ker}(\phi)$ and $Q = G/M$. Then, $x \notin M$ and Q is finite (actually, $Q \cong A$).

Since G is finitely generated and Q is finite, only finitely many homomorphisms from G to Q are possible. Let them be $\phi_1, \phi_2, \dots, \phi_n$.

Let $\nu: G \rightarrow G/\text{Ker}(\theta)$ be the natural homomorphism defined by $\nu(g) = g\text{Ker}(\theta)$. Define an isomorphism $\bar{\theta}: G/\text{Ker}(\theta) \rightarrow G$ by $\bar{\theta}(g\text{Ker}(\theta)) = \theta(g)$ (it is easy to check that $\bar{\theta}$ is an isomorphism).

Now consider the homomorphisms $\phi_i \bar{\theta} \nu: G \rightarrow Q$ ($i = 1, 2, \dots, n$). We prove that these n homomorphisms are distinct.

Suppose $\phi_i \bar{\theta} \nu = \phi_j \bar{\theta} \nu$. Then, for $g \in G$

$$\begin{aligned} \phi_i(g) &= \phi_i(\theta(g')) \text{ for some } g' \in G \\ &= \phi_i \bar{\theta}(g' \text{Ker}(\theta)) \\ &= \phi_i \bar{\theta}(\nu(g')) \\ &= \phi_i \bar{\theta} \nu(g') \\ &= \phi_j \bar{\theta} \nu(g') \\ &= \phi_j \bar{\theta}(\nu(g')) \\ &= \phi_j \bar{\theta}(g' \text{Ker}(\theta)) \\ &= \phi_j(\theta(g')) \\ &= \phi_j(g) \end{aligned}$$

Hence, $\phi_i = \phi_j$ so that $\phi_i \bar{\theta} \nu: G \rightarrow Q$ ($i = 1, 2, \dots, n$) are distinct. Therefore, they consists of all the homomorphisms from G to Q . Each of them sends

the element x to the identity in Q as,

$$\begin{aligned}
\phi_i \bar{\theta} \nu(x) &= \phi_i \bar{\theta}(x \text{Ker}(\theta)) \\
&= \phi_i \bar{\theta}(1 \text{Ker}(\theta)) \text{ as } x \in \text{Ker}(\theta) \\
&= \phi_i(\theta(1)) \\
&= \phi_i(1) \\
&= 1
\end{aligned}$$

But the natural homomorphism $\lambda: G \rightarrow Q$ defined by $\lambda(g) = gM$ sends x to a non identity element xM as $x \notin M$. This contradiction implies that our initial assumption that G is not hopfian is false. Hence, G is hopfian. ■

The following theorem is due to G. Baumslag [1] and the source of its proof (together with Lemma 2.4.1) is [9] (see page 196).

Theorem 2.4.3: The automorphism group $\text{Aut}(G)$ of a finitely generated residually finite group G is residually finite.

We first prove a lemma.

Lemma 2.4.1: Let G be a finitely generated group. Then the number of subgroups of G having any fixed finite index n is finite. Also if H is a subgroup of finite index in G then H contains a subgroup K characteristic in G with finite index in G .

Proof: Suppose H is of finite index n in G . Then there are n distinct right cosets of H in G . Choose an element (a representative) from each of these cosets. A set of all such representatives containing 1, say $\{c_1, c_2, \dots, c_n\}$ with $c_1 = 1$, is called a complete set of representatives of the right cosets of H in

G . Then the cosets Hc_i are distinct and set $S = \{Hc_1, Hc_2, \dots, Hc_n\}$. For each $g \in G$, define a map $\theta_g: S \rightarrow S$ by $\theta_g(Hc_i) = Hc_i g$. This is clearly a bijection. Hence we can define a homomorphism $\phi_H: G \rightarrow S_n$, where S_n is the symmetric group of degree n , by the equation $\phi_H(g) = \theta_g$ - it is routine to check that this is a homomorphism. We may form these homomorphisms for every subgroup H of index n in G .

Now, $\phi_H(g)$ fixes the element $Hc_1 = H$ in S if and only if $\theta_g(H) = H$, i.e., if and only if $Hg = H$ whence $g \in H$. In other words, $g \notin H$ if and only if $\phi_H(g)$ does not fix the element H .

Let H and K be two distinct subgroups of index n in G . (If there is only one such subgroup then the first part of the lemma is proved.) Then there is an element g which is only in one of H and K . Assume, without loss of generality, that $g \in H$ and $g \notin K$. Then $\phi_H(g)$ fixes 1 while $\phi_K(g)$ does not, hence ϕ_H and ϕ_K are distinct homomorphisms

Since G is finitely generated and S_n is a finite group, there exists only a finite number of homomorphisms from G to S_n (we described in Theorem 2.4.1 how these homomorphisms can be constructed). Since distinct subgroups of finite index n in G give rise to distinct such homomorphisms, the number of subgroups of a finite index n must be finite.

To prove the other part, suppose $[G : H] = n$ and set $K = \bigcap_{i=1}^m H_i$ where $H_1, H_2, \dots, H_m$ are all the subgroups of index n in G . Then, H is one of $H_1, H_2, \dots, H_m$ and $K \leq H$. By Theorem 1.1.1, K is of finite index in G . To prove that this subgroup is characteristic in G , we have to show that $\alpha(K) = K$ for any automorphism α of G . Since the subgroup $\alpha(H_i)$ has

finite index n in G , α permutes all the H_i , i.e.,

$$\alpha(K) = \alpha\left(\bigcap_{i=1}^m H_i\right) = \bigcap_{i=1}^m \alpha(H_i) = \bigcap_{i=1}^m H_i = K$$

and the lemma is proved. ■

Proof of Theorem 2.4.3: Let $1 \neq \alpha \in \text{Aut}G$. Then there is an element $c \in G$ such that $\alpha(c) \neq c$. Hence, if we set $d = \alpha(c)c^{-1}$ then $1 \neq d \in G$. Since G is residually finite, there is a normal subgroup H of finite index in G with $d \notin H$. Let K be the subgroup of H as in Lemma 2.4.1. Since K is characteristic in G , by Theorem 1.3.1, it is normal in G .

Now we can define the quotient group G/K and a map

$$\psi: \text{Aut}(G) \rightarrow \text{Aut}(G/K) \text{ by } \psi(\beta)(Kg) = K\beta(g).$$

To show that the map ψ is well defined, take $\beta \in \text{Aut}(G)$ and $g, g' \in G$ with $Kg = Kg'$. Then, $g' = kg$ for some $k \in K$ so that $\beta(k) \in K$. Hence, $K\beta(g) = K\beta(g')$ and thus $\psi(\beta)$ is well-defined. Therefore, ψ is well-defined. Also, ψ is a homomorphism as

$$\begin{aligned} \psi(\beta\gamma)(Kg) &= K\beta\gamma(g) \\ &= K\beta(\gamma(g)) \\ &= \psi(\beta)(K\gamma(g)) \\ &= \psi(\beta)(\psi(\gamma)(Kg)) \\ &= \psi(\beta)\psi(\gamma)(Kg). \end{aligned}$$

Finally, we have that $\text{Aut}(G/K)$ is finite since G/K is finite and that

$$\psi(\alpha)(Kc) = K\alpha(c) \neq Kc$$

for, if $K\alpha(c) = Kc$ then $d = \alpha(c)c^{-1} \in K \leq H$, a contradiction. Hence $\psi(\alpha) \neq 1$, the identity map on G/K , and thus the theorem is proven. ■

2.5 Subgroups of General Linear Groups

Residual finiteness of a large family of groups is covered by the following theorem due to Malcev. The proof of this theorem (together with the lemmas associated with) is from [3, page 169].

Theorem 2.5.1: Let F be an arbitrary field and let G be a finitely generated subgroup of the general linear group $GL(n, F)$ where n is a positive integer. Then, there is an integer $m > 0$ such that for each $z \neq 1$ in G , there is a finite field F_z and a homomorphism $\psi_z: G \rightarrow GL(m, F_z)$ for which $\psi_z(z) \neq 1$. Moreover, if $\text{char}(F) = q > 0$, then we may take $\text{char}(F_z) = q$ for each z . In particular, every finitely generated subgroup of $GL(n, F)$ is residually finite.

We first prove some lemmas.

Lemma 2.5.1: Suppose that for each prime q , we choose an infinite field $E^{(q)}$ of characteristic q . Let $F = F_0(X_1, X_2, \dots, X_k) = F_0(X)$ be the field of rational functions in k indeterminates over a prime subfield F_0 of arbitrary characteristic. Let G be a finitely generated subgroup of $GL(m, F)$ where m is a positive integer. Then,

(1) If $\text{char}(F) = q > 0$, then for each $1 \neq z \in G$, there is a homomorphism $\psi_1: G \rightarrow GL(m, E^{(q)})$ for which $\psi_1(z) \neq 1$.

(2) If $\text{char}(F) = 0$, then for each $1 \neq z \in G$, there is a bound q_0 (depending on z) such that for each prime $q \geq q_0$, there is a homomorphism $\psi_2: G \rightarrow GL(m, E^{(q)})$ for which $\psi_2(z) \neq 1$.

Proof: By taking a set of generators of G together with their inverses, we can find $x_1, x_2, \dots, x_n \in G$ such that each element in G is a product of the

x_i . We consider two cases.

Case 1: $\text{char}(F) = q > 0$

Let $P = \{p_1, p_2, \dots, p_i\}$ be the set of all polynomials which occur in the denominators and numerators in the non-zero entries of the matrices

$$x_1, x_2, \dots, x_n, z - 1.$$

Since $E^{(q)}$ is infinite, we can find $a_1, a_2, \dots, a_k \in E^{(q)}$ such that

$$a = (a_1, a_2, \dots, a_k)$$

is not a zero of any polynomial in P . Define a map

$$\theta: K \rightarrow E^{(q)} \quad \text{by} \quad \theta(f(x)) = f(a).$$

where K is the subfield of F generated by P . We can easily check that θ is a ring homomorphism. Furthermore, θ induces a group homomorphism

$$\psi_1: G \rightarrow GL(m, E^{(q)})$$

defined by

$$\psi_1(x_{i_1} x_{i_2} \cdots x_{i_r}) = \theta(x_{i_1}) \theta(x_{i_2}) \cdots \theta(x_{i_r}),$$

where $\theta(x_{i_j})$ denotes the matrix in $GL(m, E^{(q)})$ with each entry $f(x)$ in x_{i_j} is replaced by $\theta(f(x))$. It is routine, but cumbersome, to check that ψ_1 is a homomorphism so we avoid it here. According to our choice of a , we have that $\psi_1(z - 1) \neq 0$, i.e., $\psi_1(z) \neq 1$ in $GL(m, E^{(q)})$ and thus part (1) is proven.

Case II: $\text{char}(F) = 0$

Since the prime field of a field whose characteristic is 0 is isomorphic to $\mathbb{Q}$, we may take $F_0 = \mathbb{Q}$. In this case, we note that an element of F is a

quotient of elements of $\mathbb{Z}(X)$. Choose q_0 such that none of the polynomials in $\mathbb{Z}(X)$ which occur as numerator or denominator in the nonzero entries of the matrices $x_1, x_2, \dots, x_n, z - 1$ is divisible by a prime $q \geq q_0$. Then, for such a prime q , the map

$$\psi_0: G \rightarrow GL(m, \mathbb{Z}_q(X))$$

that sends every element $x \in G$ to the matrix y in $GL(m, \mathbb{Z}_q(X))$ such that the entries of y are the entries of x whose coefficients of the polynomials of the numerators and denominators are replaced by taking modulo q : $\mathbb{Z}_q$ denotes the field of integers modulo q . Note that, by the choice of q_0 , we have $\psi_0(z) \neq 1$. Now consider the group $\psi_0(G)$, a finitely generated subgroup of $GL(m, \mathbb{Z}_q(X))$, and the non identity element $\psi_0(z)$ in it. Since $\mathbb{Z}_q(X)$ is an infinite field with $\text{char}(\mathbb{Z}_q(X)) = q > 0$, we can apply Case I. Hence, there exists a homomorphism

$$\psi_1: \psi_0(G) \rightarrow GL(m, E^{(q)})$$

such that $\psi_1(\psi_0(z)) \neq 1$. Now the homomorphism

$$\psi_2 = \psi_1 \circ \psi_0: G \rightarrow GL(m, E^{(q)})$$

has the property that $\psi_2(z) \neq 1$ and thus part (2) is proven. ■

Lemma 2.5.2: If E is a field extension of degree d over a field F , then for each subgroup G of $GL(n, E)$, there is a monomorphism $\theta: G \rightarrow GL(m, F)$ where $m = nd$

Proof: Denote by $\text{Hom}_F(E, E)$ the ring of all F -endomorphisms (i.e., all linear transformations) of E over F . Define a map

$$\alpha: E \rightarrow \text{Hom}_F(E, E)$$

by $\alpha(x) = \bar{x}$ where $\bar{x}(u) = ux$. We can easily check that this is a field monomorphism. Now, $\bar{x}$ is a linear transformation of E over F . Choose a basis S for E over F . Since every linear transformation is associated with a unique matrix under a given basis, we can define a monomorphism

$$\psi: E \rightarrow M(d, F)$$

by $\psi(x) = [\bar{x}]_S$ where $M(d, F)$ denotes the set of all $d \times d$ matrices with entries in F and $[\bar{x}]_S$ denotes the matrix associated with the linear transformation $\bar{x}$. Then for each subgroup G of $GL(n, E)$, ψ induces the homomorphism

$$\theta: G \rightarrow GL(n, M(d, F))$$

defined by

$$\theta([e_{ij}]_{n \times n}) = [[\psi(e_{ij})]_{d \times d}]_{n \times n}.$$

We easily see that θ is injective since ψ is injective. Also the identity

$$GL(n, M(d, F)) = GL(nd, F)$$

gives the required monomorphism $\theta: G \rightarrow GL(m, F)$. ■

Lemma 2.5.3: Suppose that for each prime q , we choose an infinite field $E^{(q)}$ of characteristic q . If G is a finitely generated subgroup of $GL(n, F)$ where F is an arbitrary field, then there is an integer $m > 0$ (depending on n and F , but independent of the choice of $E^{(q)}$) such that

- (1) If $\text{char}(F) = q > 0$, then for each $z \neq 1$ in G , there is a homomorphism $\psi: G \rightarrow GL(m, E^{(q)})$ for which $\psi(z) \neq 1$.
- (2) If $\text{char}(F) = 0$, then for each $1 \neq z \in G$, there is a bound q_0 such that for each prime $q \geq q_0$, there is a homomorphism $\psi: G \rightarrow GL(m, E^{(q)})$ for which $\psi(z) \neq 1$.

Proof: Let $y_1, y_2, \dots, y_s$ be a set of generators for G and let F_1 be the subfield of F generated by the (finite) set of entries of the y_i . Then F_1 is finitely generated over the prime subfield F_0 and there is a transcendence basis $\zeta_1, \zeta_2, \dots, \zeta_k$ for F_1 over F_0 , that is, a maximal set of elements algebraically independent over F_0 . If we put

$$F_2 = F_0(\zeta_1, \zeta_2, \dots, \zeta_k)$$

then F_1 is finitely generated and algebraic over F_2 , and so $[F_1 : F_2] = d$, say, is finite. Now, clearly, $G \leq GL(n, F_1)$ and thus, by Lemma 2.5.2, there is a monomorphism $\theta: G \rightarrow GL(m, F_2)$ where $m = nd$. But, we have that

$$F_2 = F_0(\zeta_1, \zeta_2, \dots, \zeta_k) \cong F_0(X_1, X_2, \dots, X_k)$$

and we can apply Lemma 2.5.1 to $\theta(G)$ to get a homomorphism

$$\psi_i: \theta(G) \rightarrow GL(m, E^{(q)}), \quad (i = 1, 2).$$

Then the Lemma follows when we set $\psi = \psi_i \theta$, $(i = 1, 2)$. ■

Proof of Theorem 2.5.1: We wish to apply Lemma 2.5.3. Choose $E^{(q)}$ as the algebraic closure of the prime subfield of F_q and set $\psi = \psi_z$ in the Lemma 2.5.3. Since $\psi(G)$ is finitely generated, the subfield F_z of $E^{(q)}$ generated by the entries of the matrices in $\psi(G)$ is a finitely generated algebraic extension of the prime subfield. Hence F_z is a finite field thus ψ is a homomorphism from G to a finite group $GL(m, F_z)$ such that $\psi(z) \neq 1$ as desired. ■

2.6 Polycyclic Groups

Next we discuss another family of residually finite groups.

Definition: A group G is said to be polycyclic if there exists a sequence $1 = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_n = G$ such that G_{i+1}/G_i is cyclic for all $0 \leq i < n$. In this case, G is said to have a cyclic series.

An alternative definition says, “a group G is polycyclic if it is an extension of the trivial group by a succession of finite number of cyclic groups”. It is obvious that the two definitions are equivalent.

First, some elementary properties of polycyclic groups.

Theorem 2.6.1: Subgroups and quotient groups of polycyclic groups are polycyclic.

Proof: Let G be a polycyclic group and H a subgroup of G . Then G has a cyclic series, say

$$1 = G_1 \triangleleft G_2 \triangleleft \cdots \triangleleft G_n = G.$$

Consider the series $1 = H \cap G_1 \leq H \cap G_2 \leq \cdots \leq H \cap G_n = H$. This is a subnormal series as

$$H \cap G_i = (H \cap G_{i+1}) \cap G_i \triangleleft H \cap G_{i+1} \text{ for all } i.$$

Now,

$$\frac{H \cap G_{i+1}}{H \cap G_i} \cong \frac{G_i(H \cap G_{i+1})}{G_i} \leq \frac{G_{i+1}}{G_i}$$

and since G_{i+1}/G_i is cyclic, so is its subgroups. Hence, H has a cyclic series and thus H is polycyclic.

To prove the other part, let K be normal in G and consider the quotient group G/K . Consider the natural epimorphism

$$\alpha: G \rightarrow G/K$$

defined by $\alpha(x) = xK$. If G has a cyclic series,

$$1 = G_1 \triangleleft G_2 \triangleleft \cdots \triangleleft G_n = G$$

then we show that

$$1 = \alpha(G_1) \leq \alpha(G_2) \leq \cdots \leq \alpha(G_n) = G/K$$

is a cyclic series of G/K . If $\alpha(x_i) \in \alpha(G_i)$ and $\alpha(x_{i+1}) \in \alpha(G_{i+1})$ then $\alpha(x_{i+1}^{-1}x_i x_{i+1}) \in \alpha(G_i)$ so that $\alpha(G_i) \triangleleft \alpha(G_{i+1})$ for each i so that it is a subnormal series. The map

$$\phi: G_{i+1} \rightarrow \frac{\alpha(G_{i+1})}{\alpha(G_i)}$$

defined by $x_{i+1} \mapsto \alpha(x_{i+1})\alpha(G_i)$ is a surjection for, it is the composite of the surjections $G_{i+1} \rightarrow \alpha(G_{i+1})$ and the natural epimorphism $\alpha(G_{i+1}) \rightarrow \alpha(G_{i+1})/\alpha(G_i)$. Since $G_i \leq \text{Ker}(\phi)$ we can easily show that there exists an epimorphism

$$\theta: \frac{G_{i+1}}{G_i} \rightarrow \frac{\alpha(G_{i+1})}{\alpha(G_i)}$$

namely,

$$\theta(x_{i+1}G_i) = \alpha(x_{i+1})\alpha(G_i).$$

Now, $\alpha(G_{i+1})/\alpha(G_i)$ is a quotient of the cyclic group G_{i+1}/G_i so that it is cyclic. Hence H is polycyclic. ■

The following Theorem is due to K. Hirsch [7], and the proof of the theorem is from [5].

Theorem 2.6.2: Every polycyclic group is residually finite.

Proof: We use induction on the number of cyclic factors of a cyclic series of a polycyclic group. The result is true for a polycyclic group G with a cyclic series of only one cyclic factor since, then, the group G is cyclic. Assume that the theorem is true for polycyclic groups with $n - 1$ cyclic factors. Suppose G is polycyclic and has a cyclic series

$$1 = G_0 \triangleleft \cdots \triangleleft H \triangleleft G$$

with $n > 1$ cyclic factors. Since G/H is a non trivial cyclic group, we may write $G/H = \langle aH \rangle$ for some $a \in G \setminus H$. Then we note that G is generated by H and a since, for any $g \in G$, $gH = a^m H$ for some m and hence $g = a^m h$ for some $h \in H$. Thus, we may write

$$G = \langle a, H \rangle = \langle a \rangle H.$$

Let $1 \neq g \in G$. We will find $K \triangleleft G$ such that $g \notin K$ and G/K is finite.

Case I: $g \notin H$

If G/H is finite then set $K = H$ and we are done. Suppose G/H is infinite. Write $gH = a^m H$ for some $m > 0$. Set $K = \langle a^{2m}, H \rangle = \langle a^{2m} \rangle H$. We prove that K is normal and of finite index in G , and that it does not contain the element g .

If $g \in K$ then $gH = a^{2mr} H$ for some integer r and hence $a^m H = a^{2mr} H$. This implies $(aH)^{m(2r-1)} = 1$ and thus $m(2r - 1) = 0$ since $\langle aH \rangle$ is infinite cyclic. This is a contradiction as none of m and $2r - 1$ are zero and hence $g \notin K$. That $K \triangleleft G$ follows as, for any $a^t h \in G$ and any $a^{2mr} h' \in K$ where

t, r are integers and $h, h' \in H$, we have

$$\begin{aligned}
(a^t h)^{-1} a^{2mr} h' (a^t h) &= h^{-1} a^{-t} a^{2mr} h a^t h \\
&= h^{-1} a^{2mr} h'' h \text{ for some } h'' \in H \\
&= a^{2mr} h''' \text{ for some } h''' \in H \text{ (as } H \triangleleft G) \\
&\in K.
\end{aligned}$$

To prove that it is of finite index, take any left coset $a^t h K$ of K in G . By division algorithm, there exist integers q and r such that $t = 2mq + r$ with $0 \leq r < 2m$. Thus,

$$a^t h K = a^{2mq+r} h K.$$

Therefore,

$$\begin{aligned}
a^t h &= a^{2mq+r} h a^{2ms} h' \text{ for some integer } s \text{ and } h' \in H \\
&= a^r a^{2m(q+s)} h'' \text{ for some } h'' \in H \\
&\in a^r K,
\end{aligned}$$

so that $a^t h K = a^r K$ with $0 \leq r < 2m$. Thus, any left coset of K in G is one of $K, aK, \dots, a^{2m-1}K$ and hence G/K is finite. This completes the proof when $g \notin H$.

Case II: $g \in H$

Since H is a polycyclic group with $n - 1$ cyclic factors, the theorem holds for H , by assumption, and hence there exists $M \triangleleft H$, not containing g , such that H/M is finite. Write $H^k = \langle h^k \mid h \in H \rangle$, i.e., the subgroup of H generated by all k^{th} powers of elements of H where k is an integer. By Lemma 2.1.2, we

have $H^m \leq M$ and clearly, $H^m \triangleleft H$. Next we show that H/H^m is finite. We have, by Theorem 2.6.1, that H/H^m is polycyclic. Set $Q = H/H^m$. Then, Q has a cyclic series

$$1 = Q_1 \triangleleft Q_2 \triangleleft \cdots \triangleleft Q_l = Q.$$

Take any non identity element qQ_i from Q_{i+1}/Q_i . Then, clearly, $Q^m = 1$. Hence,

$$(qQ_i)^m = q^m Q_i = Q_i, \quad \text{the identity element in } Q_{i+1}/Q_i.$$

Therefore each quotient group Q_{i+1}/Q_i is finite cyclic and hence Q is a succession of finite extensions of the trivial group by finite cyclic groups so that Q itself is finite.

Now, if the group $\langle a \rangle$ is finite then we have a subgroup H^m of G not containing g such that $[G : H^m] = [G : H][H : H^m] < \infty$. Hence, we can set $K = H^m$ and we are done. Suppose that $\langle a \rangle$ is infinite cyclic. Since H/H^m is finite, the automorphism ϕ of H/H^m induced by a , i.e.,

$$\phi: H/H^m \rightarrow H/H^m \text{ defined by } \phi(hH^m) = a^{-1}haH^m$$

has finite order e , say, in the automorphism group $\text{Aut}(H/H^m)$. Then

$$\phi^e(hH^m) = a^{-e}ha^eH^m = hH^m,$$

i.e.,

$$ha^eH^m = a^e hH^m. \tag{2.4}$$

Note also that for any integer t ,

$$\phi^{et}(hH^m) = a^{-et}ha^{et}H^m = hH^m$$

so that

$$ha^{et}H^m = a^{et}hH^m. \quad (2.5)$$

If

$$K = \langle a^e, H^m \rangle (= \langle a^e \rangle H^m),$$

then we show that $K \triangleleft G$, G/K is finite and $g \notin K$.

If $g \in K$ then $g = a^{et}h_m$ for some $h_m \in H^m$ and an integer t . This implies $a^{et} = gh_m^{-1} \in H$ so that $et = 0$. Since $e \neq 0$ we have $t = 0$ implying $g = a^0h_m = h_m \in H^m$, a contradiction. Therefore $g \notin K$.

To show that $K \triangleleft G$, take any two elements $a^{et}h_m \in K$ and $a^ih \in G$ where $h_m \in H^m$; t, i are integers and $h \in H$. We have

$$\begin{aligned} (a^ih)^{-1}a^{et}h_m(a^ih) &= h^{-1}a^{-i}a^{et}h_ma^ih \\ &= h^{-1}a^{et}(a^{-i}h_ma^i)h \\ &= h^{-1}a^{et}h'_mh \text{ for some } h'_m \in H^m \\ &= a^{et}h^{-1}h''_mh \text{ for some } h''_m \in H^m \text{ (by equation 2.5)} \\ &= a^{et}h'''_m \text{ for some } h'''_m \in H^m \\ &\in \langle a^e \rangle H^m, \end{aligned}$$

so that $K \triangleleft G$.

It remains to show that G/K is finite. Let j be the order of H/H^m and let $h_1H^m, \dots, h_jH^m$ be all the elements in H/H^m . We know that

$$\frac{G}{K} = \frac{\langle a \rangle H}{\langle a^e \rangle H^m}.$$

Take any element

$$d = a^sh \langle a^e \rangle H^m \in G/K,$$

where s is an integer and $h \in H$. Since we can write $s = eq + r$ for some $0 \leq r < e$, and also since $h \langle a^e \rangle H^m = \langle a^e \rangle h' H^m$ for some $h' \in H$ (which is an obvious consequence of the equation 2.5), we have

$$d = a^{eq+r} \langle a^e \rangle h' H^m = a^r \langle a^e \rangle h_i H^m \text{ for some } 0 \leq i < m.$$

Therefore, every element of G/K is one of $a^r \langle a^e \rangle h_i H^m$ where $0 \leq r < e$ and $0 \leq i < m$, hence G/K is finite and the theorem is proved. ■

2.7 Residual Properties of Free Products

In this section, we pay our attention to a class of special type of residual properties. The notions that follow will be useful in studying the residual properties of free products. The main theorem (Theorem 2.7.2) of this section is due to K.W. Gruenberg and all proofs are basically from his article [5].

Definition: A property P is called a *root property* of groups if:

1. there exists a nontrivial group satisfying property P
2. whenever a group G has property P , all subgroups of G also have property P
3. the direct product of any two groups with property P again has property P
4. given any three groups $G \triangleright H \triangleright K$ such that G/H and H/K have property P , there exists a subgroup N of K which is normal in G such that G/N also has property P .

Theorem 2.7.1: The two properties finiteness and being a group of order a prime power are root properties.

Proof: The two properties clearly satisfy the conditions (1), (2) and (3) of root properties. To prove that condition (4) holds, let

$$N = \bigcap_{g \in G} g^{-1} K g$$

be the core of K in G (cf. Theorem 1.2.1). First consider finiteness. We have that

$$[G : K] = [G : H][H : K] < \infty. \quad (2.6)$$

Let $g_1 K, \dots, g_n K$ be all the left cosets of K in G . Then, for any $g \in G$, $gK = g_i K$, i.e., $g = g_i k$ for some g_i and $k \in K$. Hence, $gK g^{-1} = g_i k K k^{-1} g_i^{-1} = g_i K g_i^{-1}$ so that

$$\bigcap_{g \in G} gK g^{-1} = \bigcap_{i=1}^n g_i K g_i^{-1}.$$

Now,

$$[G : N] = \left[G : \bigcap_{i=1}^n g_i K g_i^{-1} \right].$$

Since

$$[G : g_i K g_i^{-1}] = [G : K] < \infty,$$

we conclude, by Corollary 1.1.1, that $[G : N]$ is finite. Hence, finiteness is a root property. Now consider the other property - being a group of finite prime power order. We can use the results we have just proven since finiteness, in

this case, is a inherent property. First we show that $g^{-1}Kg \triangleleft H$ for any $g \in G$. Since $H \triangleleft G$ we have that $gh = h'g$ for some $h' \in H$ and hence

$$h^{-1}(g^{-1}Kg)h = g^{-1}(h')^{-1}Kh'hg = g^{-1}Kg,$$

implying that $g^{-1}Kg \triangleleft H$. Now, define a map

$$\phi: \frac{H}{N} \rightarrow \prod_{i=1}^n \left(\frac{H}{g_i^{-1}Kg_i} \right) \quad \text{by} \quad \phi(hN) = \prod_{i=1}^n h(g_i^{-1}Kg_i),$$

where $\prod$ denotes the cartesian product. This ϕ is a well-defined injection since

$$\begin{aligned} h_1N = h_2N &\iff h_1^{-1}h_2 \in N = \bigcap_{i=1}^n g_i^{-1}Kg_i \\ &\iff h_1(g_i^{-1}Kg_i) = h_2(g_i^{-1}Kg_i) \quad \text{for all } i \\ &\iff \prod_{i=1}^n h_1(g_i^{-1}Kg_i) = \prod_{i=1}^n h_2(g_i^{-1}Kg_i) \\ &\iff \phi(h_1N) = \phi(h_2N). \end{aligned}$$

Further, we have that, for each i , $[H : g_i^{-1}Kg_i] = [H : K]$ and hence

$$\prod_{i=1}^n \left(\frac{H}{g_i^{-1}Kg_i} \right)$$

is a finite group of prime power order. Since ϕ is an embedding, we conclude that H/N is also a finite group of prime power order. Now, the equality $[G : N] = [G : H][H : N]$ and the supposition that $[G : H]$ is a finite group of prime power order imply that $[G : N]$ is also a finite group of prime power order. This completes the proof of the Theorem. ■

Theorem 2.7.2: If P is a root property, then every free product of residually P groups is itself residually P if and only if every free group is residually P .

First we need some definitions followed by some lemmas which have their own importance.

Definitions: A family $(K_\lambda)_{\lambda \in \Lambda}$ of normal subgroups of G is called a *unit-filter* of G if

1. $\bigcap_{\lambda \in \Lambda} K_\lambda = 1$
2. for each $\mu, \nu \in \Lambda$, there exists $\lambda \in \Lambda$ such that $K_\lambda \leq K_\mu \cap K_\nu$.

If, in addition, G/K_λ is P for every $\lambda \in \Lambda$ where P is any given property, then (K_λ) is called a *P-filter* of G .

Lemma 2.7.1: If P is any property satisfying the conditions (1) and (2) of root properties, then a group G is residually P if and only if G possesses a P -filter.

Proof: A group G is clearly residually P if it possesses a P -filter. To prove the converse, suppose G is residually P . Consider the family (K_λ) of all normal subgroups of G whose quotients have P . Then, an immediate consequence of Theorem 2.1.1(c) is that, $\bigcap_{\lambda \in \Lambda} K_\lambda = 1$. For any $\mu, \nu \in \Lambda$, the mapping

$$\phi: G/K_\mu \cap K_\nu \rightarrow G/K_\mu \times G/K_\nu$$

defined by $\phi(g(K_\mu \cap K_\nu)) = (gK_\mu, gK_\nu)$ is an embedding (it is routine to check this) so that $G/K_\mu \cap K_\nu$ can be considered as a subgroup of $G/K_\mu \times G/K_\nu$, which has property P since it is a direct product of two groups that has property P (by condition (2) of root properties). Then, by condition (1) of root properties, $G/K_\mu \cap K_\nu$, in turn, has property P so that $K_\mu \cap K_\nu$ is a member of the family (K_λ) . Hence, G possesses a P -filter. ■

Lemma 2.7.2: If $1 = x_0, x_1, \dots, x_n$ are distinct elements of G and $(K_\lambda)_{\lambda \in \Lambda}$ is a unit-filter of G , then there exists a $\lambda \in \Lambda$ such that $x_0, x_1, \dots, x_n$ lies in distinct cosets of K_λ .

Proof: By the property (1) of unit filters, we can find $\lambda_{ij} \in \Lambda$, where $0 \leq i < j \leq n$, such that $x_i x_j^{-1} \notin K_{\lambda_{ij}}$. We can easily extend the property (2) of unit-filters inductively to finitely many intersections and hence we can find λ such that $K_\lambda \leq \cap K_{\lambda_{ij}}$ as the intersection is finite. Then, $K_\lambda \leq K_{\lambda_{ij}}$ for each λ_{ij} so that $x_i x_j^{-1} \notin K_\lambda$, i.e., $x_i K_\lambda \neq x_j K_\lambda$ for all i and j . Thus $x_1, x_2, \dots, x_n$ lie in distinct cosets of K_λ . ■

Lemma 2.7.3: Let $F = G_1 * \dots * G_d$ and let $(K_{\lambda_i})_{\lambda_i \in \Lambda_i}$ be a unit filter of G_i ($i = 1, 2, \dots, d$). If S is any finite subset of non unit elements from $G_1, G_2, \dots, G_d$ then, there exist $\lambda_i \in \Lambda_i$ and a transversal T_i of K_{λ_i} in G_i for each $i = 1, 2, \dots, d$ such that $S \subseteq \bigcup_{i=1}^d T_i$.

Proof: Set $S_i = S \cap G_i$. Then, $S = \bigcup_{i=1}^d S_i$ and $S_i \cap S_j = \emptyset$ for $i \neq j$ (as $1 \notin S$). By Lemma 2.7.2, there exists λ_i for each $i = 1, 2, \dots, d$ such that the elements of $\{1\} \cup S_i$ lie in distinct cosets of K_{λ_i} in G_i . Take any transversal T_i of K_{λ_i} containing S_i as a subset. Then $S \subseteq \bigcup_{i=1}^d T_i$. ■

Lemma 2.7.4: Let P be a property satisfying condition (4) of root properties and let H be a normal subgroup of a group G such that G/H is P and H is residually P , Then G is residually P .

Proof: Let $1 \neq g \in G$. We find $K_g \triangleleft G$ such that G/K_g is P and $1 \notin K_g$. If $g \notin H$, then we can take $K_g = H$. If $g \in H$ then, by the residual finiteness of H , there exists $K \triangleleft H$ such that $g \notin K$ and H/K is P . Then, by condition (4) of root properties, there exists $N \triangleleft G$ such that G/N is P and thus we

can take $K_g = N$. ■

Proof of Theorem 2.7.2: Let $F = \bigstar_{\lambda \in \Lambda} G_\lambda$ and suppose that F , as well as every group G_λ , is residually P . Let g_1 and g_2 be two non unit elements belonging to any two distinct free factors G_{λ_1} and G_{λ_2} respectively of F . Consider the cyclic subgroup $\langle g_1 g_2 \rangle$ of F . This is clearly infinite and also is residually P as a subgroup of the residually P group F (root property (1)). Since any free group is a free product of infinite cyclic groups (Theorem 1.6.1), we conclude that every free group is residually P .

Next assume that every free group is residually P . Let $F = \bigstar_{\lambda \in \Lambda} G$ be a free product of residually P groups. We prove that F is residually P . First we prove this when Λ is finite and then extend the result to any free product. Hence we assume that $F = G_1 * \cdots * G_d$. Let $1 \neq g \in F$. Let $(K_{\lambda_i})_{\lambda_i \in \Lambda_i}$ be a P -filter of G_i and let S be the set of all syllables occuring in the normal form of g . As in Lemma 2.7.3, we can find $K_{\lambda_i} \triangleleft G_i$ and transversals T_i of K_{λ_i} for each $i = 1, \dots, d$ such that $S \subseteq \bigcup_{i=1}^d T_i$. Let

$$\phi: F \rightarrow G_1/K_{\lambda_1} * \cdots * G_d/K_{\lambda_d}$$

be the natural homomorphism defined by

$$\phi(g_{\lambda_j} \cdots g_{\lambda_l}) = g_{\lambda_j} K_{\lambda_j} \cdots g_{\lambda_l} K_{\lambda_l}.$$

It is routine to check that this ϕ is the unique extension of the homomorphisms $\phi_i: G_i \rightarrow G_i/K_{\lambda_i}$ defined by $\phi_i(g) = gK_{\lambda_i}$ whose kernels are K_{λ_i} . Thus, by taking $H_i = G_i/K_{\lambda_i}$ in Lemma 1.6.3, we see that the kernel K , say, of ϕ is the normal closure of the K_{λ_i} . We prove that $g \notin K$. If $g \in K$ then $\phi(g) = 1$. If

$$g = g_{\lambda_j} \cdots g_{\lambda_l}$$

is the normal form of g in F , then

$$\phi(g_{\lambda_j} \cdots g_{\lambda_l}) = 1,$$

i.e.,

$$g_{\lambda_j} K_{\lambda_j} \cdots g_{\lambda_l} K_{\lambda_l} = 1.$$

In this case, $g_{\lambda_i} K_{\lambda_i} = 1$ for some i , so that $g_{\lambda_i} \in K_{\lambda_i}$. Since $g_{\lambda_i} \in T_{\lambda_i}$ we have $g_{\lambda_i} = 1$, a contradiction as g_{λ_i} is a syllable of the normal form of g . Thus, our initial assumption that $g \in K$ is wrong and so $g \notin K$. Now, as ϕ is clearly surjective, we have

$$F/K \cong G_1/K_{\lambda_1} * \cdots * G_d/K_{\lambda_d}.$$

First we prove that $G_1/K_{\lambda_1} * \cdots * G_d/K_{\lambda_d}$, hence F/K , is residually P .

Write $H = G_1/K_{\lambda_1} * \cdots * G_d/K_{\lambda_d}$. We have

$$H/H^* \cong \prod_{i=1}^d G_i/K_{\lambda_i},$$

where H^* is the cartesian group of H . Since each G_i/K_{λ_i} has P (as $(K_{\lambda_i})_{\lambda_i \in \Lambda}$ is a P -filter), we have that $\times_{i=1}^d G_i/K_{\lambda_i}$ has P (the condition (2) of root properties). Hence H/H^* has property P . Now, by Example 1.7.1, H^* is a free group and then, by the initial assumption of the theorem, H^* is residually P . Thus, by Lemma 2.7.4, $H (= F/K)$ is residually P . Therefore, as $gK \neq K$ in F/K , there exists a homomorphism ψ_1 from F/K onto a group A with property P such that $\psi_1(gK) \neq 1$. If $\psi_2: F \rightarrow F/K$ is the natural homomorphism then $\psi_1\psi_2$ is a homomorphism from F to A such that the image of g under $\psi_1\psi_2$ is not the identity. Hence, F is residually P . Now

consider the general case that $F = \ast_{\lambda \in \Lambda} G_\lambda$ where Λ is any index set. Take any $1 \neq g \in F$ written in the normal form

$$g = g_{\lambda_1} \cdots g_{\lambda_n}.$$

Let $G = \ast_{i=1}^n G_{\lambda_i}$ and define a set of homomorphisms $\{\theta_\lambda: F \rightarrow G \mid \lambda \in \Lambda\}$ as follows: if λ is one of $\lambda_1, \dots, \lambda_n$ then θ_λ is the identity map; otherwise θ_λ is the trivial map. By the extension property of free products, there exists a unique homomorphism $\theta: F \rightarrow G$ extending all θ_λ . Clearly, θ is a surjection and $\theta(g) \neq 1$ in G . Since G is residually P (the result we have just proved), there is a homomorphism θ' from G to a group A with property P such that $\theta'(\theta(g)) \neq 1$. Hence the map $\theta'\theta: F \rightarrow A$ is a homomorphism such that g is mapped to a non identity element and consequently, F is residually P . ■

2.8 Residual Finiteness of Amalgamated Free Products

In the last section of this chapter, we investigate the residual properties of free products with amalgamations. In this section, our only concern is residual finiteness. We consider only the cases of free product of only two groups with only one amalgamated subgroup. The source of all theorems and lemmas (including their proofs) in this section are from an article by G. Baumslag [2].

We adopt the following notations throughout this section:

$\sigma(A, B)$ denotes the class of all free products of A and B with only one amalgamated subgroup.

$\sigma(A, B; P)$ denotes the class of all free products of A and B with only one amalgamated subgroup which satisfies the condition P .

Theorem 2.8.1: If A and B are finite and $G \in \sigma(A, B)$ then G is residually finite.

Proof: Let H be the amalgamated subgroup of G in which case we may consider $H \leq A$ and $H \leq B$. By Theorem 1.7.4, there is a homomorphism χ from G onto a finite group M containing both A and B such that $\chi|_A$ and $\chi|_B$ are inclusions. Denote $\chi|_A$ by ϕ and $\chi|_B$ by ψ . Then, by the definition of an amalgam, we have that there exists a map $\theta: G \rightarrow M$ with the following commutative diagram:

Let K be the kernel of θ . Since M is finite it follows that G/K is finite. Now, if $x \in K \cap A$ then $1 = \theta(x) = \phi(x)$ so that $x = 1$ as ϕ is injective. Thus, $K \cap A = 1$ and similarly $K \cap B = 1$. Then, by Corollary 1.7.2, K is free and hence, by Theorem 2.3.1, K is residually finite. Now, by and Lemma 2.7.4, we conclude that G is residually finite. $\blacksquare$

The following theorem is a milestone in the investigation of residual finiteness of amalgamated free products.

Theorem 2.8.2: If A and B are residually finite and if $P \in \sigma(A, B; \text{finite})$ then P is residually finite.

We prove this theorem through a series of definitions followed by lemmas. Recall the Lemma 2.7.1 which says that a group is residually finite if and only if it contains a finite-filter: the root property in this case being finiteness.

Definition: Let A and B be two residually finite groups and let $(A_\lambda)_{\lambda \in \Lambda}$ and $(B_\lambda)_{\lambda \in \Lambda}$ be finite-filters, indexed by a same indexing set Λ , of A and B respectively. Also let H be a subgroup of A and K a subgroup of B with an isomorphism $\phi: H \rightarrow K$. Then, $(A_\lambda)_{\lambda \in \Lambda}$ and $(B_\lambda)_{\lambda \in \Lambda}$ are said to be (H, K, ϕ) -compatible if the function

$$\phi_\lambda: HA_\lambda/A_\lambda \rightarrow HB_\lambda/B_\lambda$$

defined by

$$\phi_\lambda(hA_\lambda) = \phi(h)B_\lambda$$

is an isomorphism (called the isomorphism induced by ϕ) for each $\lambda \in \Lambda$. Furthermore, a finite-filter $(A_\lambda)_{\lambda \in \Lambda}$ is called an H -filtration if

$$\bigcap_{\lambda \in \Lambda} (HA_\lambda) = H.$$

Lemma 2.8.1: Let A and B be a given pair of residually finite groups, let H be a subgroup of A , K a subgroup of B and let $\phi: H \rightarrow K$ be an isomorphism. Furthermore, let $(A_\lambda)_{\lambda \in \Lambda}$ and $(B_\lambda)_{\lambda \in \Lambda}$ be finite-filters, indexed by the same indexing set Λ , of A and B respectively. Now, if both $(A_\lambda)_{\lambda \in \Lambda}$ and $(B_\lambda)_{\lambda \in \Lambda}$ are (H, K, ϕ) -compatible, then there exists a free subgroup F of $A *_\phi B$ such that $(A *_\phi B)/F$ is residually finite.

Proof: Put $P = A \star_{\phi} B$. Consider $1 \neq a \in A$. Since filters have the property that $\bigcap_{\lambda} A_{\lambda} = 1$, there exists $\mu \in \Lambda$ such that $a \notin A_{\mu}$. Then, in turn, by another property of finite-filters, the quotient group A/A_{μ} is finite. For the same reason, B/B_{μ} is also finite. Now, by the (H, K, ϕ) -compatibility of the two filters $(A_{\lambda})_{\lambda \in \Lambda}$ and $(B_{\lambda})_{\lambda \in \Lambda}$, the function

$$\phi_{\mu}: HA_{\mu}/A_{\mu} \rightarrow HB_{\mu}/B_{\mu}$$

defined by

$$\phi_{\mu}(hA_{\mu}) = \phi(h)B_{\mu}$$

is an isomorphism. Therefore, we can form the amalgam

$$P_1 = A/A_{\mu} \star_{\phi_{\mu}} B/B_{\mu}$$

identifying $\phi(h)B_{\mu}$ with hA_{μ} .

Let $\nu: A \rightarrow A/A_{\mu}$ and $\eta: B \rightarrow B/B_{\mu}$ be the natural homomorphisms. We note that, for the inclusions $i: H \rightarrow A$ and $j: K \rightarrow B$,

$$\nu i(h) = \eta j\phi(h).$$

Then, by the extension property of the amalgam $A \star_{\phi} B$, there exists a map $\theta: P \rightarrow P_1$ extending ν and η as the following commutative diagram shows:

Here, i', j' are homomorphisms associated with the amalgam P (we may assume i' and j' to be inclusions). Now, we have that

$$\theta j'(a) = \theta(a) = \nu(a) = aA_\mu \neq A_\mu.$$

Since P_1 is residually finite by Theorem 2.8.2, there exists $N_1 \triangleleft P_1$ such that $\theta(a) \notin N_1$ and P_1/N_1 is finite. Set $K = \text{Ker}(\theta)$. Since θ is clearly surjective, we have an isomorphism $\lambda: P/K \rightarrow P_1$ defined by $\lambda(pK) = \theta(p)$. Then, $\lambda^{-1}(N_1) \leq P/K$ and hence $\lambda^{-1}(N_1) = N_a/K$ for some $N_a \leq P$. We note that $a \notin N_a$ since, if it were, then $\lambda(aK) \in N_1$, i.e., $\theta(a) \in N_1$, a contradiction. Next we have,

$$P/N_a \cong (P/K) / (N_a/K) \cong P_1/N_1,$$

so that P/N_a is finite.

Now, let N be the intersection of all normal subgroups of finite index in P . Then,

$$N \cap A \leq \left(\bigcap_{a \in A} N_a \right) \cap A = 1$$

so that $N \cap A = 1$. By symmetry, $N \cap B = 1$ and hence by Corollary 1.7.2, N is free. The group P/N is residually finite by Theorem 2.1.1(c) since P/N has a family (M/N) of normal subgroups of finite index in P/N such that

$$\bigcap_{[P:M] < \infty} M/N = 1.$$

Now, if we set $F = N$ then $A *_\phi B$ contains a free group F such that $(A *_\phi B)/F$ is residually finite as desired. ■

Now we extend this lemma in the case of the filters being H -filtrations.

Lemma 2.8.2: Assume all the hypotheses and notation in Lemma 2.8.1 and in addition to that, assume that $(A_\lambda)_{\lambda \in \Lambda}$ is an H -filtration of A and $(B_\lambda)_{\lambda \in \Lambda}$ is a K -filtration of B . Then, P is residually finite.

Proof: Let $1 \neq u \in P$. If $u \in A$ or $u \in B$ then by Lemma 2.8.1, there is a normal subgroup N_u in P of finite index which does not contain u and hence we are done. Suppose $u \notin A$ and $u \notin B$. Let $u = hl_{u_1}l_{u_2} \cdots l_{u_n}$, $n > 1$, be the normal form of u where $h \in H$ and the l_{u_i} are from a set of representatives of the cosets of A/H and B/K . Here we identify $\phi(h)$ by h . Since the finite-filters $(A_\lambda)_{\lambda \in \Lambda}$ and $(B_\lambda)_{\lambda \in \Lambda}$ are H - and K - filtrations respectively, and also since no l_{u_i} is in $H \cup K$, we can find an index $\mu \in \Lambda$ such that

$$l_{u_i} \notin HA_\mu \text{ and } l_{u_i} \notin KB_\mu.$$

for each l_{u_i} as follows. For each l_{u_i} , choose A_{μ_i} not containing l_{u_i} from the filter. Let

$$A_\mu = \bigcap_{i=1}^n A_{\mu_i}.$$

Then $l_{u_i} \notin HA_\mu$ and A_μ is an element of the filter. Similarly we can find B_μ .

We may, without loss of generality, assume that $l_{u_1} \in A$. Then, since θ extends ν and η , we have

$$\theta(u) = (l_{u_1}A_\mu)(l_{u_2}B_\mu) \cdots.$$

Since none of the $l_{u_i}A_\mu$ and the $l_{u_i}B_\mu$ is equal to the identity and also since adjacent terms in $(l_{u_1}A_\mu)(l_{u_2}B_\mu) \cdots$ are not from the same group A/A_μ or B/B_μ , we conclude that $\theta(u) \neq 1$.

Now, as in the proof of Lemma 2.8.1, since P_1 is residually finite, we can find a normal subgroup N_1 of P_1 of finite index not containing $\theta(u)$, and

then a normal subgroup N_u in P of finite index such that $u \notin N_u$. Now, the sequence (N) of normal subgroups in P of finite index has trivial intersection since

$$\bigcap_{u \in P} N_u = 1,$$

so that, by Theorem 2.1.1(c), P is residually finite. ■

Proof of Theorem 2.8.2: Since H is finite, we have that K is finite and since A and B are residually finite, there are finite-filters $(A'_\lambda)_{\lambda \in \Lambda}$ and $(B'_\lambda)_{\lambda \in \Lambda}$ of A and B respectively. Let

$$H = \{1 = h_0, h_1, h_2, \dots, h_r\}.$$

For each $h_i \in H$, we can find a normal subgroup H_i in A of finite index which does not contain h_i . Set

$$H' = \bigcap_{i=1}^r H_i$$

and define a new sequence of subgroups $(A_\lambda)_{\lambda \in \Lambda}$ in A by

$$A_\lambda = H' \cap A'_\lambda.$$

By Corollary 1.1.1, A/A_λ is finite and

$$\bigcap_{\lambda \in \Lambda} A_\lambda \leq H' \cap \left(\bigcap_{\lambda \in \Lambda} A'_\lambda \right) = 1$$

so that $(A_\lambda)_{\lambda \in \Lambda} = 1$. Also,

$$A_\lambda \cap A_\gamma = H' \cap (A'_\lambda \cap A'_\gamma),$$

therefore $A_\lambda \cap A_\gamma$ is in the sequence $(A_\lambda)_{\lambda \in \Lambda}$. Thus $(A_\lambda)_{\lambda \in \Lambda}$ is a finite-filter.

Note that

$$A_\lambda \cap H \leq H' \cap H = 1$$

so that

$$A_\lambda \cap H = 1$$

In a similar way, we can find a finite-filter $(B_\lambda)_{\lambda \in \Lambda}$ of B such that

$$B_\lambda \cap K = 1.$$

Now,

$$\frac{A_\lambda H}{A_\lambda} \cong \frac{H}{A_\lambda \cap H} \cong H \cong K \cong \frac{K}{B_\lambda \cap K} \cong \frac{B_\lambda K}{B_\lambda}$$

so that the two filters are (H, K, ϕ) -compatible. Next we prove that $(A_\lambda)_{\lambda \in \Lambda}$ and $(B_\lambda)_{\lambda \in \Lambda}$ are respectively H - and K - filtrations.

Once we show that $\bigcap (HA_\lambda) = H$, the other condition $\bigcap (KB_\lambda) = K$ follows by symmetry. Clearly $\bigcap (HA_\lambda) \geq H$. To show the other inclusion, consider $x \in A \setminus H$. We show that $x \notin \bigcap (HA_\lambda)$. This is equivalent to showing that $x \notin HA_\mu$ for some $\mu \in \Lambda$, or equivalently, $h^{-1}x \notin A_\mu$ for all $h \in H$ and for some $\mu \in \Lambda$. Consider the set

$$\{h_0^{-1}x, h_1^{-1}x, h_2^{-1}x, \dots, h_r^{-1}x\}.$$

Clearly 1 is not in this set and thereby, for each $h_i^{-1}x$ there exists an element A_{μ_i} in the filter (A_λ) such that $h_i^{-1}x \notin A_{\mu_i}$. By setting

$$A_\mu = \bigcap_{i=0}^r A_{\mu_i}.$$

we easily see that $h^{-1}x \notin A_\mu$ for all $h \in H$. Now, by Lemma 2.8.2, the theorem follows. ■

Bibliography

- [1] G. Baumslag, *Automorphism groups of residually finite groups*, J. London Math. Soc., **38** (1963) 117-118.
- [2] G. Baumslag, *On the residual finiteness of generalized free products of nilpotent groups*, Trans. Amer. Math. Soc., **106** (1963) 193-209.
- [3] J.D. Dixon, *Structure of Linear Groups*, Van Nostrand-Reinhold, 1971.
- [4] D.S. Dummit and R. M. Foote, *Abstract Algebra*, Prentice Hall, 1991.
- [5] K.W. Gruenberg, *Residual properties of infinite soluble groups*, Proc. London Math. Soc., (3) **7** (1957) 29-62.
- [6] G. Higman, *A finitely generated infinite simple group*, J. London Math. Soc., **26** (1951) 61-64.
- [7] K. Hirsch, *On infinite soluble groups. III*, Proc. London Math Soc., (2) **49** (1946) 184-194.
- [8] M.I. Kargapolov and Ju.I. Merzljakov, *Fundamentals of the Theory of Groups*, Springer-Verlag, New York, 1979.

- [9] R.C. Lyndon and P. E. Schupp, *Combinatorial Group Theory*, Springer-Verlag, Berlin Heidelberg, 1977.
- [10] W. Magnus, *Residually finite groups*, Bull. Amer. Math. Soc., **75** (1969) 305-316.
- [11] W. Magnus, *Noneuclidean tessellations and their groups*, Academic Press, New York, 1974.
- [12] W. Magnus, A. Karrass, D. Solitar, *Combinatorial Group Theory*, John Wiley & Sons, Inc., 1966.
- [13] B.H. Neumann, *An essay on free products of groups with amalgamations*, Philos. Trans. Roy. Soc. London Ser., A **246** (1954) 503-554.
- [14] A. Peluso, *A residual property of free groups*, Comm. Pure Appl. Math., **19** (1967) 435-437.
- [15] D.J.S. Robinson, *A course in the Theory of Groups*, 2nd edition, Springer-Verlag, New York, 1996.
- [16] J.J. Rotman, *An Introduction to the Theory of Groups*, 4th edition, Springer-Verlag, New York, 1995.
- [17] J.P. Serre, *Trees*, Springer-Verlag, Berlin Heidelberg, 1980.