Growth of Groups

Jitendra Rathore

MP14009

A dissertation submitted for the partial fulfilment of

MS degree in Science

Indian Institute of Science Education and Research Mohali

April 2017

Certificate of Examination

This is to certify that the dissertation titled "Growth of Groups " submitted by Mr. Jitendra Rathore (Reg. No. MP14009) for the partial fulfilment of MS degree programme of the Institute, has been examined by the thesis committee duly appointed by the Institute. The committee finds the work done by the candidate satisfactory and recommends that the report be accepted.

Prof. I. B. S. Passi   Prof. Kapil Hari Paranjape   Dr.Pranab Sardar
(Supervisor)

Dated: April 21, 2017

Declaration

The work presented in this dissertation has been carried out by me under the guidance of Prof. I. B. S. Passi at the Indian Institute of Science Education and Research Mohali.

This work has not been submitted in part or in full for a degree, a diploma, or a fellowship to any other university or institute. Whenever contributions of others are involved, every effort is made to indicate this clearly, with due acknowledgement of collaborative research and discussions. This thesis is a bonafide record of original work done by me and all sources listed within have been detailed in the bibliography.

Jitendra Rathore

(Candidate)

Dated: April 21, 2017

In my capacity as the supervisor of the candidate's project work, I certify that the above statements by the candidate are true to the best of my knowledge.

Prof. I. B. S. Passi

(Supervisor)

Acknowledgement

It gives me immense pleasure to thank my advisor Prof. I.B.S. Passi. It is with deep sense of gratitude that I acknowledge the help and constant support, whether mathematical or non-mathematical, I received from him.

I would like to thank my research progress committee members Prof. Kapil Hari Paranjape and Dr. Pranab Sardar for their support and encouragement.

I take this opportunity to thank the Head of the department and faculty members for providing a lively atmosphere for research. I am thankful to the non-academic staff of the department for helping me with administrative formalities.

I would like to thank Dr. Abhay Soman and Swathi Krishna for correcting my thesis. Also, I affectionately thank Sagar Kalane and Pinka Dey. I much appreciate their constant encouragement and the extra effort that they put in for me.

I take this opportunity to thank my classmates, especially Pratyush Mishra. Last but not the least, I owe the greatest debt to my parents for their patience and kind-hearted support.

Contents

Abstract

Let G be a finitely generated group with a finite generating set $\{s_1, s_2, ..., s_n\}$. We define the length ($l(g)$) of $g \in G$ to be the number of generators required in the shortest decomposition of $g = y_1 y_2 ... y_k$, where each y_i is either a generator or the inverse of generator. Then we can define a metric d on G given by $d(g, h) = l(gh^{-1})$. Now, if $B(e, r)$ denotes the ball of radius r centred at identity, then define a function $\gamma_G(r) : \mathbb{N} \to \mathbb{N}$ given by $\gamma_G(r) = |B(e, r)|$, which counts the size of balls. The growth rate of group is the study of the asymptotic behaviour of this function $\gamma_G(n)$. Depending on the nature of this function, we can classify the growth type into polynomial, exponential and intermediate. Here, we try to understand these growth functions and their properties. The asymptotic nature of this function provides us with a lot of information pertaining to the group.

Chapter 1

Introduction

The topic of growth entered group theory, with a geometric motivation, in the middle of the last century. The concept of growth of groups deals with the study of finitely generated groups. This was introduced by A.S. Schwarz and then independently by J. Milnor. The notion of growth seems to be a very natural one, it arose first not in pure group theory, but in a geometric application; when it was noted that the rate of volume growth of the universal cover $\tilde{M}$ of a compact Riemannian manifold M coincides with the rate of growth of the fundamental group $\pi_1(M)$. J.Milnor and J.A.Wolf demonstrated that the growth type of the fundamental group gives some important information about the curvature of the manifold.

Analogously, we can associate a metric space to each finitely generated group and then study the asymptotic behaviour of size of the balls. We define the growth of group to be this asymptotic behaviour of size of these balls.

In 1968, the problems raised by Milnor initiated a lot of activity and opened up new directions in group theory and other areas of its applications.

Problem 1.0.1 *What are the groups of polynomial growth?*

Problem 1.0.2 *Is it true that the growth function of every finitely generated group is necessarily equivalent to a polynomial or to the function* 2^n *?*

In 1968, Milnor [3] and Wolf [9] proved that if a finitely group soluble group G

does not have exponential growth, then G has a nilpotent subgroup of finite index. Then in 1972, H. Bass[2] showed that finitely generated nilpotent groups have polynomial growth. So Bass's result gave a partial answer of 1.0.1. The complete answer was given by M. Gromov in 1981, who proved that groups of polynomial growth have a nilpotent subgroup of finite index. In the light of these results, we can say that a group has polynomial growth if and only if it has a nilpotent subgroup of finite index.

Till 1980, each finitely generated group turned out to be of either polynomial growth or exponential growth. In 1980, Rostislav Grigorchuk [7] constructed a finitely generated infinite torsion group and in 1984 it was proved by Grigorchuk [8] that it has intermediate growth. Along with the intermediate property of the Grigorchuk group, it also gives a negative answer to the *Burnside problem* : *whether a finitely generated group in which every element has finite order must necessarily be a finite group.* Gigorchuck group was first constructed as an example for Burnside problem. Only later was it noted that it has intermediate growth. Later on in 1983, Narain Gupta and Said Sidki constructed, for each odd prime p, a finitely generated infinite torsion group and later on they turned out to be of intermediate growth. The existence of groups of intermediate growth made group theory and other areas of its applications much richer. Eventually it led to the appearance of new directions in group theory: self-similar groups, branch groups, and iterated-monodromy groups etc.

The second chapter includes the notion of growth and properties of growth function. In this chapter, we also discuss some basic results regarding nilpotent groups, soluble and polycyclic groups. In chapter 3, we discuss the growth of finitely generated soluble groups. In the first section, we discuss the following result: a finitely generated soluble group G, which does not have exponential growth, has a nilpotent subgroup of finite index. The second section includes the proof of the theorem of Hymann Bass, which says that a finitely generated nilpotent group has polynomial growth. Chapter 4, includes the proof of Gromov's theorem, which says that groups of polynomial growth have a nilpotent subgroup of finite index and the last chapter discusses the groups of intermediate growth. In the first section of this chapter, we discuss the Grigorchuk group and show that it has intermediate growth. We also look at its properties like, it is a finitely generated infinite 2-group, it is residually finite, has solvable word problem etc. The Second section of this chapter is devoted to Gupta Sidki groups, its properties and intermediate nature of it's growth.

Chapter 2

Growth

2.1 Preliminaries

Definition 2.1.1 *A graph is a pair* $\Gamma = (V, E)$ *, where* V *consisting of a set of vertices and* E*, the set of edges, together with a incidence function* ψ_Γ *that associates with each edge of* Γ *an unordered pair of vertices of* Γ*.*

Definition 2.1.2 ***(Cayley Graph)*** *Let* G *be a finitely generated group and* $S \subset G$ *be a generating set for* G*. The Cayley graph* $\Gamma(G, S)$ *of* G *with respect to the generating set 'S' is the graph "Cay*(G, S)*" whose set of vertices are the elements of* G *and set of edges are* $\{(g, g.s) \mid g \in G, s \in S \cup S^{-1}\}$*.*

Note that, two vertices in a Cayley graph are adjacent if and only if they differ by an element of generating set. Cayley graph of finitely generated group gives us a means by which a finitely generated group can be viewed as a geometric object.

Remark 2.1.3 *Cayley graph is not just a geometric object but we can make it into a topological object(indeed a metric space) by defining a suitable metric.*

So, now we will define a metric on $\Gamma(G, S)$.

2.1.1 Word metric on Cayley graph $\Gamma(G, S)$

First we will define, the length of a word $g \in G$ with respect to some generating set S, if we denote $l(g)$ to be the length of g, then it is defined as follows

$$l(g) = min \{n \in \mathbb{N} \mid \exists\, s_1, s_2, ..., s_n \in S \cup S^{-1} \mid g = s_1 s_2 ... s_n\}$$

Now, let G be a finitely generated group with a finite generating set $S \subset G$. Then a map $d_S : G \times G \to \mathbb{R}$ on G with respect to S is a metric on G associated with the Cayley graph $\Gamma(G, S)$, given by

$$d_S(g, h) = l(gh^{-1}) \quad \forall g, h \in G$$

1. $d_S(g, h) = 0 \Leftrightarrow l(gh^{-1}) = 0 \Leftrightarrow gh^{-1} = e \Leftrightarrow g = h.$

2. $d_S(g, h) = l(gh^{-1})$ since $gh^{-1} = s_1 s_2 ... s_n$, which implies that $hg^{-1} = s_n^{-1} s_{n-1}^{-1} ... s_1^{-1}$ and therefore $l(gh^{-1}) = l(hg^{-1}) = d_S(h, g)$

3. Let $g, h, k \in G$ such that $n = d_S(g, h),\ \ m = d_S(h, k)$ so $gh^{-1} = s_1 s_2 ... s_n$ and $hk^{-1} = s'_1 s'_2 ... s'_m$ therefore $gk^{-1} = (gh^{-1})(hk^{-1}) = s_1 s_2 ... s_n s'_1 s'_2 ... s'_m$
it follows that,

$$d_S(g, k) \leq n + m$$

Therefore, we have

$$d_S(g, k) \leq d_S(g, h) + d_S(h, k)$$

Hence, these three properties shows that d_S gives a metric on G, called word metric on $\Gamma(G, S)$.

Observation 2.1.4 $\Gamma(G, S)$ *is metric space with word metric. In general, the word metric on a given group depends on the chosen set of generators.*

Example 2.1.5 *The word metric on* $\mathbb{Z}$ *corresponding to the generating set* $\{1\}$ *coincide with the metric on* $\mathbb{Z}$ *induced from the standard metric on* $\mathbb{R}$.

Let $B_r^{G,S}(e) = \{g \in G \mid l(g) \leq r\}$ denote the ball of radius r centred at the identity e of G.

2.1.2 Growth Function:

Let G be a finitely generated group and $S \subset G$ be a finite generating set of G. Then the growth function γ_G^S of G with respect to S is defined as $\gamma_G^S : \mathbb{N} \to \mathbb{N}$ given by $\gamma_G^S(r) = |B_r^{G,S}(e)|$, where $|B_r^{G,S}(e)|$ is the number of elements in the ball $B_r^{G,S}(e)$. If we denote $a_G(n)$ be the number of elements of group G having length r and $\gamma_G(r)$ be the number of elements of G of length at most r. i.e..

$$\gamma_G(r) = \sum_{i=0}^{r} a_G(i). \tag{2.1}$$

Example 2.1.6 *If $G = \mathbb{Z}$ and $S = \{1\}$. Now we will calculate $a_G(n)$ and $s_G(n)$*

Take $S = \{1\}$. Clearly $a_G(0) = 1$ and $a_G(1) = 2$, as the generators have length 1. Since every integer n can be written $1 + 1 + 1.. + 1$(n copies) if n is positive and $(-1) + (-1) + ... + (-1)$ (n copies) if n is negative, n and $-n$ are the only numbers which can be formed by using the n copies of generator such that the length is n. Hence $a_G(n) = 2$ for all n except 0. By the equation (1), we have $\gamma_G(0) = 1$ and $\gamma_G(n) = \sum_{i=0}^{n} a_G(i) = 1 + 2 + 2 + ... + 2($ n copies$) = 1 + 2(n) = 2n + 1$. □

Example 2.1.7 *Let $G = \mathbb{Z}$, $S = \{2, 3\}$, then the growth function is given by $\gamma_G^S(r) =$ 1 if $r = 0$, 5 if r= 1 and 6r+1 if $r > 1$.*

□

Proposition 2.1.8 *A group G is finite if and only if $a_G(n)$ is eventually 0, equivalently if and only if $\gamma_G(n)$ is eventually constant.*

Proof: If G is finite group say $G = \{a_1, a_2, ...a_n\}$ then we calculate length of each a_i i.e. $l(a_i)$ and take the maximum of all such length, say k. i.e.

$$k = max\{l(a_i)|i = 1, 2.., n\}$$

and hence $a_G(m) = 0 \ \forall \ m > k$. Then Certainly $\gamma_G(m)$ is constant for all $m > k$. Now conversely if $\gamma_G(n)$ is eventually constant, then $a_G(n)$ must be eventually 0(otherwise

$s_G(n)$ would no longer be eventually constant) as since in equation (1), at each stage n, $\gamma_G(n)$ be the addition of $s_G(n-1)$ with $a_G(n)$. Now assume $a_G(n)$ is eventually 0, i.e. $\exists\ k \in \mathbb{Z}$ such that $a_G(n) = 0\ \forall\ n > k$. If we show that for each integer t there are only finitely many elements of length t, this will complete the proof. Let x be an element of length t and write $x = y_1y_2...y_t$ where each y_i is either s_j or $(s_j)^{-1}$ for some $1 \leq j \leq n$ and $1 \leq i \leq t$. Since choices for such s_j are finite and hence number of elements of length t are finite, So for each $1 \leq t \leq k$ we have only finite numbers of element of length t, and since $a_G(n) = 0\ \forall\ n > k$ which shows that the elements in a group G is finite. Therefore, G is finite group. $\square$

Remark 2.1.9 *In 2.1.6 and 2.1.7, we noticed that growth function of a finitely generated group depends upon the generating set. But we will prove that* ***the growth type*** *of finitely generated group G does not depend upon generating set of a group i.e. the growth type of G remains the same with respect to any finite generating set. Let's make this statement to be more precise. For this we will define the concept of* ***Quasi-isometry*** *between two metric spaces (X, d_X) and (Y, d_Y).*

2.1.3 Quasi-isometry

Let $f : (X, d_X) \to (Y, d_Y)$ be a map between two metric spaces (X, d_X) and (Y, d_Y) is said to be a "quasi-isometric embedding" if there are constants $c, b \in \mathbb{R}_{>0}$ such that

$$\frac{1}{c} d_X(x, x') - b \ \leq d_Y(f(x), f(x')) \leq \ c.d_X(x, x') + b \quad \forall\ x, x' \in X$$

A map $f' : X \to Y$ has finite distance from f if there is a constant $c' \in \mathbb{R}_{\geq 0}$ with $d_X(f(x), f(x')) \leq c'$.

Then the map f is called a *quasi-isometry*, if it is a quasi-isometric embedding for which there is a quasi-inverse i.e. a function $g : Y \to X$ such that $gof : X \to X$ has finite distance from id_X and fog has finite distance from id_Y.

Two metric space X and Y are said to be quasi-isometric if there exists a quasi-isometry between X and Y. In this case, we write $X \sim Y$.

Example 2.1.10 *Let $X = \mathbb{R}$, d_X = Euclidean metric and $Y = \mathbb{Z}, d_Y$ = Euclidean metric, in this case the inclusion map $i : \mathbb{Z} \to \mathbb{R}$ is a quasi-isometric embedding and $g : \mathbb{R} \to \mathbb{Z}$ be defined as $g(x) = [x]$, the greatest integer function, then g is a quasi-inverse of f and hence $\mathbb{Z} \sim \mathbb{R}$.*

$\square$

Observation 2.1.11 *Every non-empty metric spaces of finite diameter is quasi-isometric . Moreover, if a space X is quasi-isometric to space of finite diameter then X must be of finite diameter as well. Hence, Cayley graphs of any two finite groups are quasi-isometric. In other words, if we look at the Cayley graphs of finite groups from far away, they all looks similar in quasi-isometric sense.*

If G is a finite group, then there are finitely many vertices in its Cayley graph which implies that its Cayley graph is quasi-isomteric to a point. Hence, finite groups are of no interest to us. Therefore, we are interested in finitely generated infinite groups.

Now, we will define the *Growth type* and will prove that the *Growth type* is independent of the choice of generating set.

2.2 Growth types

Definition 2.2.1 *(**Quasi-equivalence of generalised growth function**) A generalised growth function is an increasing function from $\mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$. Let $f, g : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ be generalised growth function. we say that g quasi-dominates f if there exist $c, b \in \mathbb{R}_{\geq 0}$ such that*

$$f(r) \leq c.g(c.r + b) + b \quad \forall \ r \in \mathbb{R}_{\geq 0}.$$

If g quasi-dominates f, then we write $f \prec g$. Two generalised growth functions $f, g : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ are quasi-equivalent if $f \prec g$ and $g \prec f$.

Note that a quasi-equivalence defines an equivalence relation on the set of all generalised growth functions.

Growth function yield generalised growth function : Let G be a finitely generated group with a finite generating set S. Then the function $\mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ defined as $r \to \gamma_G^S([r])$, where ($[r]$ is the greatest integer function) associated with the growth function $\gamma_G^S : \mathbb{N} \to \mathbb{N}$ indeed is the generalised growth function.

Equivalence of Growth function: Let G and H be finitely generated groups with finite generating sets S and T respectively. Then we say γ_G^S and γ_H^T are quasi-equivalent if their associated generalised growth function are quasi-equivalent. Hence, we have a notion of quasi-equivalence class of growth function.

Now, In the next proposition, we will prove that this class does not depend upon the generating set.

Proposition 2.2.2 *Let G and H are finitely generated groups with finite generating sets S and T respectively.*
1. *If there exist a quasi-isometric embedding $(G, d_S) \to (H, d_T)$, then $\gamma_G^S \prec \gamma_H^T$.*
2. *In particular, if G and H are quasi-isometric, then the growth functions γ_G^S and γ_H^T are quasi equivalent.*

Proof: Let $f : G \to H$ be a quasi-isometric embedding, hence there is a constant $c \in \mathbb{R}_{\geq 0}$ such that

$$\frac{1}{c} d_S(g, g') - c \leq d_T(f(g), f(g')) \leq c.d_S(g, g') + c \quad \forall \; g, g' \in G$$

We write $e' = f(e)$ and let $r \in \mathbb{N}$. Using the estimates above we obtain the following

If $g \in B_r^{G,S}(e)$ then $d_T(f(g), e') \leq c.d_S(g, e) + c \leq c.r + c$ and thus

$$f(B_r^{G,S}(e)) \subset B_{c.r+c}^{H,T}(e') \quad \forall \; g, g' \in G$$

with $f(g) = f(g')$, we have

$$d_S(g, g') \leq c.(d_T(f(g), f(g') + c) = c^2$$

since the metric d_T on H is invariant under left translation, it follows that

$$\begin{aligned} \gamma_G^S(r) &\leq |B_{c^2}^{G,S}(e)|.|B_{c.r+c}^{H,T}(e')| \\ &= \gamma_G^S(c^2).\gamma_H^T(c.r + c) \end{aligned}$$

which shows that $\gamma_G^S \prec \gamma_H^T$ since $\gamma_G^S(c^2)$ does not depend on the radius r.

Now, interchanging the role of G, S with H, T, we can have $\gamma_H^T \prec \gamma_G^S$. Therefore, we get $\gamma_G^S \sim \gamma_H^T$. □

Corollary 2.2.3 *Let G be a finitely generated group and let S and T be two finite generating sets of G, and γ_G^S, γ_G^T be their respective growth function. Then $\gamma_G^S \sim \gamma_G^T$.*

Proof: Take $c = \max\{d_T(e,s) \mid s \in S \cup T\}$. Since S and T are finite so c is finite. Let $g, h \in G$ and let $n = d_S(g,h)$. Then we can write $g^{-1}h = s_1 s_2 ... s_n$ for certain $s_1, s_2, ... s_n \in S \cup S^{-1}$. Using the triangle inequality and the fact that the metric d_T is left invariant by definition, we obtain

$$\begin{aligned}
d_T(g,h) &= d_T(g, g.s_1.s_2...s_n) \\
&\leq d_T(g, g.s_1) + d_T(g.s_1, g.s_1.s_2) + ... + d_T(g.s_1..s_{n-1}, g.s_1..s_{n-1}.s_n) \\
&= d_T(e, s_1) + d_T(e, s_2) + ... + d_T(e, s_n) \\
&= d_T(e, s_1) + d_T(e, s_2) + ... + d_T(e, s_n) \\
&\leq c.n \\
&= c.d_S(g,h)
\end{aligned}$$

Now, interchange the role of S and T, we will have
$d_S(g,h) \leq c'.d_T(g,h)$ for some $c' > 0$ and hence we conclude that $id_G : (G, d_S) \to (G, d_T)$ is a quasi-isometry. By 2.2.2 we have $\gamma_G^S \sim \gamma_G^T$. □

Our main interest is in the questions related to the order of magnitude of growth functions, and in that connection we are going to define some terms.

First, note that by writing a word of length $m+n$ as a product of a word of length m and a word of length n, we get that $a_G(m+n) \leq a_G(m)a_G(n)$.Therefore

$$\lim_{n\to\infty} (a_G(n))^{1/n} \tag{2.2}$$

exist and it is finite, since G is finitely generated, and we call it $w(G) = \lim_{n\to\infty}(a_G(n))^{1/n}$. Similarly we define, $s(G) = \lim_{n\to\infty}(s(n))^{1/n}$, and since $s_G(n) \geq a_G(n)$, so we have

$s(G) \geq a(G)$. If we take G to be an infinite group G then $a_G(n) \geq 1 \ \forall \ n$ and therefore $w(G) \geq 1$, so given any $\varepsilon > 0$, we have $w(G)+\varepsilon \geq (a_G(n))^{1/n}$ or $(w(G)+\varepsilon)^n \geq a_G(n)$ for large enough n. Hence $s_G(n) = a_G(0) + a_G(1) + ... + a_G(n)$, therefore we have

$$s_G(n) \leq 1 + (w(G) + \varepsilon) + (w(G) + \varepsilon)^2 + ... + (w(G) + \varepsilon)^n$$
$$s_G(n) \leq n(w(G) + \varepsilon)^n$$

So $(s(n))^{1/n} \leq n^{1/n}(w(G) + \epsilon)$ and it follows that

$$s(G) = \lim_{n\to\infty} (s(n))^{1/n} \leq w(G) + \epsilon \ \forall \ \epsilon > 0$$

Thus, $s(G) \leq w(G)$. So we get

$$s(G) = w(G) \tag{2.3}$$

So if a finitely generated group G is generated by d elements, for every $n > 0$, we have $a(n) \leq 2d(2d-1)^{n-1}$. So we have $w(G) \leq 2d - 1$. The exact value of $w(G)$ depends not only on G, but also on the set of generator S, and if that dependence is important, we will use the notation $w_S(G)$.

Definition 2.2.4 *A group G has **exponential growth** if $w(G) > 1$, and **subexponential growth** if $w(G) = 1$, and G is said to be of **polynomial growth** if there exist numbers c and s such that $s_G(n) \leq cn^s$, for all n.*

If $s = 1$ we say that G has *linear growth* and if $s = 2$ then we say that G has *quadratic growth*. In the case of polynomial growth, its degree $d(G)$ is defined as:

$$d(G) = inf\{s \mid \exists \ c \ \mid \ \ s_G(n) \leq cn^s\} = \limsup \frac{logs(n)}{log(n)}$$

Definition 2.2.5 *We say that G has **intermediate growth**, if its growth is neither exponential nor polynomial.*

Proposition 2.2.6 *Let G be a finitely generated group, and let H be a finitely generated subgroup of G. If T and S be finite generating sets of H and G respectively. Then $\gamma_H^T \prec \gamma_G^S$, where γ_H^T and γ_G^S are growth functions of H and G with respect to T and S respectively.*

Proof: Let $S' = S \cup T$, then S' is still a finite generating set of G. If $r \in \mathbb{N}$, then for all $h \in B_r^{H,T}(e)$, we have $d_{S'}(h,e) \leq d_T(h,e) \leq r$,
and so $B_r^{H,T}(e) \subset B_r^{G,S'}(e)$.
In particular, we have

$$\gamma_H^T(r) \leq \gamma_G^{S'}(r)$$

and thus $\gamma_H^T \prec \gamma_G^S$. But we know that (G, d_S) and $(G, d_{S'})$ are quasi-isometric, hence by 2.2.3, we get $\gamma_G^{S'} \sim \gamma_G^S$.

Therefore, $\gamma_H^T \prec \gamma_G^S$. In other words, growth of group dominates the growth of subgroup. $\square$

Basic Properties of growth function : Let G be a finitely generated group and let $S \subset G$ be a finite generating set.

Proposition 2.2.7
1. *If G is an infinite group, then γ_G^S is a strictly increasing function, in particular $\gamma_G^S(r) \geq r \;\; \forall \;\; r \in \mathbb{N}$.*
2. *For all $r \in \mathbb{N}$, we have*

$$\gamma_G^S(r) \leq \gamma_{F(S)}^S(r) = 1 + \frac{|S|}{(|S|-1)}((2.|S|-1)^r - 1)$$

Proof: Let G be an infinite group. In order to prove *(1)*, it is enough to show that

$$\gamma_G^S(r+1) > \gamma_G^S(r).$$

Let us consider the ball of radius $r+1$ around e and consider the ball

$$B_G^S(r+1) = \{g \in G \mid l_S(g) \leq r+1\}$$

So, there exists $g \in B_G^S(r+1)$ such that $l_S(g) = r+1$ (otherwise we can take $B_G^S(r)$) and hence $g \notin B_G^S(r)$ so

$$|B_G^S(r+1)| > |B_G^S(r)|$$

it follows that

$$\gamma_G^S(r+1) > \gamma_G^S(r)$$

So, γ_G^S is strictly monotonically increasing function. Now, $\gamma_S(1) \geq 1$ since $e \in B_G^S(1)$ Assume that $\gamma_G^S(r) \geq r$ then,

$$\gamma_G^S(r+1) > \gamma_G^S(r) \geq r$$
$$\gamma_G^S(r+1) > r.$$

Therefore, we have

$$\gamma_G^S(r+1) \geq r+1$$

2. Let $F(S)$ be the free group on a generating set S of G. So we have a homomorphism $\phi : F(S) \to G$ characterised by $\phi|_S = id_S$. Moreover ϕ is surjective, because any $g \in G$ can be written as combination of $s_1^{\epsilon_1}.s_2^{\epsilon_2}...s_k^{\epsilon_k}$ (say $|S| = k$), and then we can pull back each $s_1^{\epsilon_1}, s_2^{\epsilon_2}, ..., s_k^{\epsilon_k}$ and we will get required word $'w'$ such that $\phi(w) = g$. Therefore, we obtain

$$\begin{aligned}\gamma_G^S(r) &= |B_r^{G,S}(e)| \\ &= |\phi(B_r^{F(S),S}(e))| \\ &= |B_r^{F(S),S}(e)| \\ &= \gamma_{F(S),S}(r)\end{aligned}$$

Therefore, $\gamma_G^S(r) \leq \gamma_{F(S)}^S(r)\ \forall\ r \in \mathbb{N}$ but the growth function of a free group F of finite rank $k = |S|$, where $k \geq 2$, with respect to a free generating set S is

$$\gamma_{F(S)}^S(r) = |B_r^{F(S)}(e)| = |\{g \in F(S) | l(g) \leq r\}$$

i.e. we have to count all the words of length $0, 1, 2...r.$,

Since we are in a free group, there is no non-trivial relation and hence, we have

$$\begin{aligned}\gamma_{F(S)}^S(r) &= 1 + 2|S| + 2|S|(2|S|-1) + 2|S|(2|S|-1)^2 + ... + 2|S|(2|S|-1)^{r-1} \\ &= 1 + 2|S|[1 + 2|S| - 1 + (2|S|-1)^2 + ... + (2|S|-1)^{r-1} \\ &= 1 + 2|S|[\frac{(2|S|-1)^r - 1}{2|S|-1-1} \\ &= 1 + \frac{2|S|}{2(|S|-1)}((2|S|-1)^r - 1)) \\ \gamma_{F(S)}^S(r) &= 1 + \frac{k}{k-1}[(2k-1)^r - 1\end{aligned}$$

Therefore, $\gamma_G^S(r) \leq \gamma_{F(S)}^S(r) = 1 + \frac{|S|}{(|S|-1)}((2|S|-1)^r - 1))$

So, $\gamma_{F(S)}^S(r) = 1 + \frac{|S|}{(|S|-1)}((2|S|-1)^r - 1))$ is an exponential growth function if $r \geq 2$. $\square$

Corollary 2.2.8 *The Free group of rank n has an exponential growth for $n \geq 2$.*

Proposition 2.2.9 *(Submultiplicativity of growth functions) Prove that*

$$\gamma_G^S(r + r') \ \leq \ \gamma_G^S(r).\gamma_G^S(r') \ \forall \ r, r' \in \mathbb{N}$$

Proof: Define a map

$$f : B_G^S(r) \times B_G^S(r') \to B_G^S(r + r')$$

given by $f(g, h) = gh$. Since $l_S(gh) \leq l_S(g) + l_S(h) \leq r + r'$, $gh \in B_G^S(r + r')$, Next we will show that f is surjective. Let $g \in B_G^S(r + r')$ i.e. $l_S(g) \leq r + r'$. $g = s_1.s_2...s_t, \ t \leq r + r'$. If either $t \geq r$ or $t \geq r'$ in either case we can pick a subword out of g of length less than or equal to r and r' respectively say w_1, w_2.
then $f(w_1, w_2) = w_1 w_2 = g$ where $l_S(w_1) \leq r$ and $l_S(w_2) \leq r'$. If $t \leq r$ and $t \leq r'$ then $g = s_1.s_2...s_t$ where $l_S(g) = t \leq r$ so $g \in B_G^S(r)$ and $f(g, e) = g$. In either case, f is surjective.
Hence, we have

$$|B_G^S(r + r')| \leq |B_G^S(r)||B_G^S(r')|$$

which follows that

$$\gamma_G^S(r + r') \leq \gamma_G^S(r).\gamma_G^S(r')$$

$\square$

Observe that, we have

$$m \leq \gamma_G^S(m) = \gamma_G^S(1 + 1 + ... + 1) \leq (\gamma_G^S(1))^m$$
$$m \leq \gamma_G^S(m) \leq (\gamma_S(1))^m$$
$$m^{\frac{1}{m}} \leq (\gamma_G^S(m))^{\frac{1}{m}} \leq \gamma_G^S(1)$$
$$\lim_{m\to\infty} m^{\frac{1}{m}} \leq \lim_{m\to\infty} (\gamma_S(m))^{1/m} \leq \lim_{m\to\infty} \gamma_S(1)$$

and it follows that,

$$1 \leq \lim_{m \to \infty} (\gamma_S(m))^{1/m} \leq \gamma_S(1)$$

and let $\lim_{m\to\infty}(\gamma_S(m))^{1/m} = e_S(\text{say})$. So, $e_S \geq 1$. If $e_S > a > 1$, we have $\gamma_S(m) \geq a^m$ for all sufficiently large m.

Lemma 2.2.10 *Let S and T be finite subsets of a group G and suppose that $< T > \subseteq < S >$. Then there is an integer $a > 0$ such that $\gamma_T(m) \leq \gamma_S(am)$ for all $m \geq 0$. Hence $e_T \leq (e_S)^a$.*

Proof: Let S and T be finite subsets of G and $< T > \subseteq < S >$ and

$$\gamma_T(m) = |\{g \in < T > \mid l_T(g) \leq m\}|$$

also we have

$$\gamma_T(am) = |\{g \in < S > \ |l_S(g) \leq am\}|$$

Choose $a = 1+$ max $\{l_S(t) \mid t \in \mathrm{T}\}$

Let $h \in B_T(m)$, write $h = t_1^{a_1} t_2^{a_2} ... t_n^{a_n}, n \ \leq m,\ t_i \in T$

$$\begin{aligned}
l_S(h) &= l_S(t_1^{a_1} . t_2^{a_2} ... t_n^{a_n}) \\
&\leq |a_1| l_S(t_1) + a_2 | l_S(t_2) + ... + a_n | l_S(t_n) \\
&\leq |a_1|(a-1) + |a_2|(a-1) + ... + |a_n|(a-1) \\
&\leq (a-1)(|a_1| + |a_2| + ... + |a_n|) \\
&\leq (a-1) l_T(h) \\
&\leq (a-1)m \\
&\leq ma.
\end{aligned}$$

which follows that

$$B_T(m) \subset B_S(am)$$

$$\gamma_T(m) \leq \gamma_S(am)$$

Therefore, we have

$$\gamma_T(m)^{1/m} \leq \gamma_S(am)^{1/m} \leq (\gamma_S(am)^{1/am})^a$$

Now applying limit $m \to \infty$, we get $e_T \leq e_S^a$. $\square$

Remark 2.2.11 *If $G =< S >=< T >$, then $e_S > 1 \Leftrightarrow e_T > 1$. In this case we say that G has exponential growth.*

As we have seen that the group $G = \mathbb{Z}$ has polynomial growth. Now we will see that not only $\mathbb{Z}$, but $\mathbb{Z}^n$ also has polynomial growth.

Proposition 2.2.12 *Let $T = \{\tau_1, \tau_2, ...\tau_n\}$ be a minimal generating set for a free abelian group $\mathbb{Z}^n$ of rank n. Then the growth function*

$$\gamma_T(m) = \sum_{l=0}^{n} 2^l \binom{n}{l} \binom{m}{l}.$$

Proof: : Here, $G = \mathbb{Z}^n =< \tau_1, \tau_2, ...\tau_n >$. Let $\gamma_T(m)$ be the growth function of G. For every integer $l \geq 0$, let P_l denote the function on non-negative integers given by $P_0(m) = 1 \, \forall m \geq 0$ and if $l > 0$, then each of the $P_l(m)$ is the number of distinct sequences $(a_1, a_2, .., a_l)$ of positive numbers with $a_1 + a_2 + ... + a_l \leq m$. Observe that $P_0(m) = \binom{m}{0}$ and if $l > 0$ then each of the $P_l(m)$ sequences give rise to a subsets $\{a_1, a_1 + a_2, ..., a_1 + a_2 + ... + a_l\}$ of cardinality l in $\{1, 2, ..., m\}$. Conversely if a subset of cardinality l in $\{1, 2, ..., m\}$ is put in ascending order it is seen to be of the form $\{a_1, a_1 + a_2, ..., a_1 + a_2 + ... + a_l\}$.

Hence, there is a bijection between sequences $(a_1, a_2, .., a_l)$ of positive numbers with $a_1 + a_2 + ... + a_l \leq m$ and subsets of cardinality l in $\{1, 2, ..., m\}$.

Thus, $P_l(m) = \binom{m}{l} = \frac{m!}{l!(m-l)!} = \frac{m(m-1)(m-2)...(m-(l-1))}{l!}$

so, $P_l(m)$ is a polynomial function of degree l with positive leading coefficient on the non-negative integers.

Observe that $\gamma_T(m) = \sum\limits_{l=0}^{n} N_l(m)$, where $N_l(m)$ denote the number of distinct expressions $\tau_1^{a_1}\tau_2^{a_2}...\tau_n^{a_n}$, $\sum|a_i| \leq m$, such that exactly l of the a_i are non-zero.

Let $U = \{u_1, u_2, ..., u_l\}$ be any of the $\binom{n}{l}$ subsets of T with exactly l elements. So by the definition of P_l, there are precisely $P_l(m)$ distinct $u_1^{a_1}u_2^{a_2}...u_l^{a_l}$, $a_i > 0$ and $\sum a_i \leq m$ changing the signs of the a_i at each place, there will be precisely $2^l P_l(m)$ distinct $u_1^{a_1}u_2^{a_2}...u_l^{a_l}$, $a_i > 0$ with $a_i \neq 0$ and $\sum|a_i| \leq m$ (because for each a_i, possibility of choice is 2)

Thus, $N_l(m) = 2^l \binom{n}{l} P_l(m)$ and we have, $\gamma_T(m) = \sum\limits_{l=0}^{n} N_l(m)$

Therefore, $\gamma_T(m) = \sum\limits_{l=0}^{n} 2^l \binom{n}{l} P_l(m) = \sum\limits_{l=0}^{n} 2^l \binom{n}{l}\binom{m}{l}$ □

Hence, we have seen that the free abelian group of rank n has polynomial growth and we also know that finite group has eventually constant growth function.

Corollary 2.2.13 *If G is a finitely generated abelian group then G has polynomial growth.*

□

We know that abelian groups are precisely the nilpotent groups of class 1. So the natural question arises that whether the finitely generated nilpotent group have polynomial growth. We will see in the next chapter that it is indeed the case. Moreover, in 1972, Hymann Bass calculated exactly the degree of that polynomial. So before going into details of the proof, we will look at some interesting properties of nilpotent groups.

2.3 Some Group Theory

2.3.1 Nilpotent Groups

Definition 2.3.1 *: The lower central series $\gamma_i(G)$ of a group G is defined as*

$$G = \gamma_1(G) \supseteq \gamma_2(G) \supseteq ... \supseteq \gamma_n(G) \supseteq ... \tag{2.4}$$

where $\gamma_{i+1}(G) = [G, \gamma_i(G)]$.Then a group G is said to be nilpotent if there exist a positive integer p such that $\gamma_{p+1}(G) = \{1\}$. Moreover if p is the smallest such number then we say that G is a nilpotent group of class p and denote cl(G) = p.

Proposition 2.3.2 *Let G be a finitely generated nilpotent group and H be any subgroup of G. Then H is finitely generated.*

Proof: Let H be a subgroup of finitely generated nilpotent group G. Consider the lower central series

$$G = \gamma_1(G) \supseteq \gamma_2(G) \supseteq ... \supseteq \gamma_n(G) \supseteq ... \tag{2.5}$$

Claim: $\gamma_i(G)/\gamma_{i+1}(G)$ is an abelian group.
First, let's check that $\gamma_{i+1}(G) \triangleleft \gamma_i(G)$. If $g \in \gamma_{i+1}(G), h \in \gamma_i(G)$ and $\gamma_{i+1}(G) = [G, \gamma_i(G)]$. Then $hgh^{-1} = (hgh^{-1}g^{-1})g \in \gamma_{i+1}(G)$

so, $\gamma_{i+1}(G) \triangleleft \gamma_i(G)$. Hence, $\gamma_i(G)/\gamma_{i+1}(G)$ is a group.

Let $x\gamma_{i+1}(G), y\gamma_{i+1}(G) \in \gamma_i(G)/\gamma_{i+1}(G)$, where $x, y \in \gamma_i(G)$

then

$$xyx^{-1}y^{-1} = [x, y] \in \gamma_{i+1}(G)$$
$$x\gamma_{i+1}(G)y\gamma_{i+1} = y\gamma_{i+1}(G)x\gamma_{i+1}$$

Hence, $\gamma_i(G)/\gamma_{i+1}(G)$ is an abelian group, which proves our claim. Since we have lower central series $G = \gamma_1(G) \supseteq \gamma_2(G) \supseteq ... \supseteq \gamma_n(G) \supseteq ..$ where, $\gamma_{i+1}(G) = [G, \gamma_i(G)]$

Now we will prove that H is finitely generated by applying induction on nilpotency class of G.

If $p = 1$, G is an abelian group, hence we know that subgroup of a finitely generated abelian is finitely generated. So assume this holds for all groups with class p or less than p.
Let G be a group of class $p + 1$, then

$$G = \gamma_1(G) \triangleright \gamma_2(G) \triangleright ... \triangleright \gamma_p(G) \triangleright \gamma_{p+1}(G) \triangleright \gamma_{p+2} = \{1\}$$

Given a subgroup H of G, we can obtain

$$H = H \cap \gamma_1(G) \cap H \triangleright H \cap \gamma_2(G) \triangleright ... \triangleright H \cap \gamma_p(G) \triangleright H \cap \gamma_{p+1}(G) \triangleright \{1\}$$

But $H \cap \gamma_2(G)$ is finitely generated, by induction (class $\leq p$), and $\frac{H}{H \cap \gamma_2(G)}$ is isomorphic to a subgroup of $G/\gamma_2(G)$

$$(\because \frac{H}{H \cap \gamma_2(G)} \cong \frac{H.\gamma_2(G)}{\gamma_2(G)} \leq \frac{G}{\gamma_2(G)})$$

But G is finitely generated, so $G/\gamma_2(G)$ is a finitely generated abelian group. Hence, $H \cap \gamma_2(G)$ is finitely generated. Since we know that if we have $N \triangleleft G$ such that both N and G/N are fintely generated, then G is finitely generated.
Therefore, H is finitely generated. □

If G is a finitely generated nilpotent group, then $\gamma_i(G)/\gamma_{i+1}(G)$ is a finitely generated abelian group for each i .

Lemma 2.3.3 *Let X, Y and Z be subgroups of an arbitrary group G, and suppose that $[X, Y, Z] = [[X, Y], Z] = 1$ and $[Y, Z, X] = [[Y, Z], X] = 1$. Then $[Z, X, Y] = [[Z, X], Y] = 1$*

Proof: We want to show that $[\ [Z, X], Y] = 1$ or equivalently, that every element of the group $[Z, X]$ commutes with every elements of Y. So we will show that the commutators $[z, x]$ for every $z \in Z, x \in X$, centralize each element $y \in Y$. This is sufficient because $C_G(y)$ is a subgroup of G, and so it contains all the elements generated by these commutators. It is therefore, enough to show that $[z, x, y] = 1$ for all $x \in X, y \in Y, z \in Z$ Equivalently, it suffices to show that $[z, x^{-1}, y] = 1\ \forall\ x \in X, y \in Y, z \in Z$

Now $[x, y^{-1}] \in [X, Y]$ and so $[x, y^{-1}, z] \in [X, Y, Z] = 1$ and similarly we have $[y, z^{-1}, x] = 1$ so, $[x, y^{-1}, z]^y = y^{-1}[x, y^{-1}, z]y = 1$
Similarly, $[y, z^{-1}, x]^z = z^{-1}[y, z^{-1}, x]z = 1$

Since we have *Hall-Witt Identity*: $[x, y^{-1}, z]^y\ [y, z^{-1}, x]^z\ [z, x^{-1}, y]^x$ =1

$[[x,y^{-1}],z] = [x^{-1}yxy^{-1},z] = yx^{-1}y^{-1}xz^{-1}x^{-1}yxy^{-1}z$

$[[y,z^{-1}],x] = [y^{-1}zyz^{-1},x] = zy^{-1}z^{-1}yx^{-1}y^{-1}zyyz^{-1}x$

$[[z,x^{-1}],y] = [z^{-1}xzx^{-1},y] = xz^{-1}x^{-1}zy^{-1}z^{-1}xzx^{-1}y$

Now $[x,y^{-1},z]^y\ [y,z^{-1},x]^z\ [z,x^{-1},y]^x = 1$

So, using this identity, we get $[z,x^{-1},y]=1$. Hence $[Z,X,Y]=1$ $\square$

Lemma 2.3.4 ***(Three Subgroup Lemma)*** *Let N be a normal subgroup of a group G and let $X,Y,Z \subseteq G$ be arbitrary subgroups. If $[X,Y,Z] \subseteq N, [Y,Z,X] \subseteq N$, then $[Z,X,Y] \subseteq N$.*

Proof: Let $\overline{G} = G/N$ and we know that $\bar{[}H,K] = [\overline{H},\overline{K}]$ for all subgroups H and K of G.
Then,

$$[\overline{X},\overline{Y},\overline{Z}] = [[\overline{X},\overline{Y}],\overline{Z}] = [\overline{[X,Y]},\overline{Z}] = \overline{[X,Y,Z]} = 1$$

Similarly,

$$[\overline{Y},\overline{Z},\overline{X}] = [[\overline{Y},\overline{Z}],\overline{X}] = [\overline{[Y,Z]},\overline{X}] = \overline{[Y,Z,X]} = 1$$

So, by the previous lemma, we have $[\overline{Z},\overline{X},\overline{Y}]=1$, which follows that $\overline{[Z,X,Y]}=1$ and $[Z,X,Y]N = N$

$$[Z,X,Y] \subseteq N$$

$\square$

Theorem 2.3.5 *If G^i and G^j denote the i^{th} and j^{th} term of the lower central series of a group G. Then [G^i,G^j] $\subseteq G^{i+j}$ for integers $i,j \geq 1$.*

Proof: We proceed by induction on j, which is the superscript on the right in the commutator $[G^i,G^j]$. Since $G^1=G$, we see that if $j=1$, the formula we need is

$[G^i, G] = G^{i+1} \subseteq G^{i+1}$. We can assume that, therefore that $j > 1$ and so we can write $G^j = [G^{j-1}, G]$. Then

$$[G^i, G^j] = [G^j, G^i] = [G^{j-1}, G, G^i]$$

and to show that this triple commutator is contained in the normal subgroup G^{i+j} it suffices to prove that by 2.3.4, $[G, G^i, G^{j-1}] \subseteq G^{i+j}$ and $[G^i, G^{j-1}, G] \subseteq G^{i+j}$ we have

$$[G, G^i, G^{j-1}] = [G^i, G, G^{j-1}][G^{i+1}, G^{j-1}] \subseteq G^{(i+1)+(j-1)} = G^{i+j}$$

where the containment is valid by the inductive hypothesis. Also, $[G^i, G^{j-1}, G] \subseteq [G^{i+j-1}, G] = G^{i+j}$
Hence, by 2.3.4, we have $[G^i, [G, G^{j-1}]] = [G^i, G^j] \subseteq G^{i+j}$, and it follows that

$$[G^i, G^j] \subseteq G^{i+j}.$$

□

Proposition 2.3.6 *Let G be a finitely generated nilpotent group. Then we can choose a finite set T of generators of G such that if $s, t \in T$ then $s^{-1} \in T$ and $[s, t] \in T$.*

Proof: Let G be finitely generated nilpotent group. So we have finite generating set $S = \{s_1, s_2, ...s_n\}$. Take $S' = S \cup S^{-1}$ is finite set that generates G, where S^{-1} is the set of inverse of elements of S. So $S' = \{s_1, s_2, ...s_n, s_1^{-1}, s_2^{-1}, ...s_n^{-1}\}$. Since G is a nilpotent group, so $\exists\, k \in \mathbb{N}$ such that $\gamma_{k+1}(G) = (1)$ where $\gamma_{k+1}(G) = [G, \gamma_k(G)]$.

i.e. $[G, [G, [G, ...[G, G]]..] = (1)$ where number of brackets are k. For each $1 \leq i \leq k$, if we use i square brackets then number of all possible pairing of brackets is finite, and for each $1 \leq i \leq k$ we have i empty places and we have $2n$ elements to fill these i places which can be done in finite number of ways. Since if we use number of brackets more than k, then the resultant element would be identity. Hence, if we include all such elements for each $1 \leq i \leq k$ in S, we call such a set T which has the following property that $s, t \in T \Rightarrow s^{-1} \in T$ and $[s, t] \in T$ □

2.3.2 Soluble and Polycyclic Groups

A group G is *soluble* if it has a normal series

$$1 = G_n \lhd G_{n-1} \lhd ... \lhd G_1 = G \tag{2.6}$$

with abelian factor groups G_i/G_{i+1}. A group G is said to be *polycyclic* if each factor G_i/G_{i+1} is cyclic.

Remark: Polycyclic groups are soluble groups but not conversely. If we take

$$G =< a, b|ab = b^2a >$$

then G is soluble but not polycyclic.

Now we prove some important properties of polycyclic groups and soluble groups.

Proposition 2.3.7 *Let G be a finitely generated nilpotent group then G is polycyclic.*

Proof: Let G be a finitely generated nilpotent group. Then G has a lower central series of the form

$$G = \gamma_1(G) \rhd \gamma_2(G) \rhd ... \rhd \gamma_p(G) \rhd \gamma_{p+1}(G) = \{1\}$$

such that $\gamma_i(G)/\gamma_{i+1}(G)$ is a finitely generated abelian group. So each quotient can be refined in such a way that the quotient of the new series becomes cyclic. Hence, G is polycyclic. □

Proposition 2.3.8 *A group G is polycyclic iff G is soluble and all of its subgroups are finitely generated.*

Proof: If G is polycyclic, then certainly, it is soluble. Suppose, we have

$$G = G_0 \geq G_1 \geq G_2 \geq ... \geq G_r = 1$$

Let H be any subgroup of G and $H_i = H \cap G_i$ So, we have

$$H = H_0 \geq H_1 \geq H_2 \geq ... \geq H_r = 1$$

Using third isomorphism theorem of groups[17], we have

$$\frac{H_{i-1}}{H_i} \cong \frac{H_{i-1}}{H \cap G_i} \cong \frac{H_{i-1}}{G_i \cap H_{i-1}} \cong \frac{G_i H_{i-1}}{G_i}$$

is cyclic. ($\because G_i \cap H_{i-1} = G_i \cap (G_{i-1} \cap H) = G_i \cap H$). So we can choose $x_i \in H_{i-1}$ so that $H_{i-1} = < H_i, x_i >$. Thus $T = \{x_1, x_2, ...x_r\}$ is a finite generating set for H. Hence, our claim is proved.

Conversely, suppose G is soluble and all its subgroups are finitely generated. So, we have a series

$$G = G_0 \geq G_1 \geq G_2 \geq ... \geq G_r = 1$$

with $G_i \lhd G_{i-1}$ and G_{i-1}/G_i is abelian. Since each subgroup is finitely generated, so G_{i-1} is finitely generated and hence G_{i-1}/G_i is finitely generated abelian group. So we can interpolate between each G_{i-1} and G_i a finite number of subgroups to produce a series with cyclic factor groups. Hence, G is polycyclic. $\square$

Proposition 2.3.9 *If G is a group with a subgroup H such that H is normal in G, H and G/H is polycyclic group, then G is polycyclic.*

Proof: Given that,H be a normal and polycyclic subgroup of G. So we have

$$\{1\} \leq H_1 \lhd H_2 \lhd ...H_{r-1} \lhd H_r = H$$

with H_{i+1}/H_i is cyclic. Since G/H is polycyclic so, we have

$$H \lhd H^1/H \lhd H^2/H \lhd H^3/H \lhd ... \lhd H^s/H = G/H$$

with

$$\frac{H^{i+1}/H}{H^i/H} \cong \frac{H^{i+1}}{H^i}$$

is cyclic. By subgroup correspondence theorem[17]

$$H \lhd H_1^{(1)} \lhd H_2^{(2)} ... \lhd H_s^{(s)} = G$$

and

$$\frac{H_{i+1}^{(i+1)}}{H_i^{(i)}} \cong \frac{H_{i+1}^{(i+1)}/H}{H_i^{(i)}/H}$$

is cyclic. Hence, we have a series for G.

$\{1\} \leq H_1 \triangleleft H_2 \triangleleft ... H_{r-1} \triangleleft H_r = H \triangleleft H_1^{(1)} \triangleleft H_2^{(2)}, ... \triangleleft H_s^{(s)} = G$ with successive cyclic quotient. Therefore, G is polycyclic. $\square$

Proposition 2.3.10 *If G is polycyclic group. Then G is finitely presented.*

Proof: If G is polycyclic, then we have $G = G_0 \triangleright G_1 \triangleright G_2 \triangleright ... \triangleright G_r = \{1\}$ such that G_i/G_{i+1} is cyclic. Also, $G_{r-1}/G_r \cong= G_{r-1}$ is cyclic. so $G_{r-1} = < a_{r-1} \mid R_{r-1} >$ and also G_{r-2}/G_{r-1} is a cyclic group. Therefore, we have

$$G_{r-2}/G_{r-1} = < a_{r-2}G_{r-1} \mid R_{r-2}G_{r-1} >$$

Let $g \in G_{r-2}/G_{r-1}$, so we have

$$gG_{r-1} = a_{r-2}^{\alpha_{r-2}} G_{r-1}$$

$$\therefore g^{-1} a_{r-2}^{\alpha_{r-2}} \in G_{r-1}$$

hence, we can write $g^{-1} a_{r-2}^{\alpha_{r-2}} = a_{r-1}^{\alpha_{r-1}}$

$$g = a_{r-2}^{\alpha_{r-2}} a_{r-1}^{\alpha_{r-1}}$$

with relations R_{r-1}, R_{r-2}. So continuing in this way, we will get

$$G = < a_0, a_1, a_2, ... a_{r-1} \mid R_0, R_1, ... R_{r-1} >$$

Hence, G is finitely generated and finitely related. So, G is finitely presented. $\square$

Now we will define some terminologies which will be used in further discussion.

Definition 2.3.11 *(Virtually P): A group G is said to be virtually P if G has a subgroup H of finite index such that H has property P.*

Definition 2.3.12 *: A group G is said to be virtually nilpotent if G has a nilpotent subgroup of finite index. G is said to be virtually solvable if G has solvable subgroup of finite index.*

Since we know that nilpotent groups are solvable, so virtually nilpotent groups are virtually solvable groups. If G is finite group. Then G is both virtually nilpotent and virtually solvable because we can take trivial subgroup to be of finite index subgroup.

Example 2.3.13 *If G is nilpotent, then certainly G is virtually nilpotent but not conversely. Take $G = S_3$, the symmetric group of order 6 is not nilpotent but G is virtually nilpotent. Similarly each solvable group is virtually solvable but not conversely. Take, $G = \mathbb{Z} \times S_5$ is virtually solvable but G is not solvable.*

Now we will prove one interesting fact about finitely generated group that we will use in later.

Proposition 2.3.14 *If G is a finitely generated group, then G has only finitely many subgroups of a given index.*

Proof: Let G be a finitely generated group and let $d(G)$ be the minimal cardinality of a generating set for G. Let $a_n(G)$ be the number of subgroups $H \subset G$ such that $|G : H| = n$. Let H be any subgroup of index n and

$$G/H = \{H, g_2H, g_2H, ..., g_nH\}$$
$$\Omega = \{g_iH \mid g_i \in G, 1 \leq i \leq n, g_1 = 1\}$$

set of all left cosets such that $|\Omega| = n$. We can define a action $G \times \Omega \to \Omega$ given by $(g, g_iH) \to gg_iH$ and label H by 1 and the other elements of Ω by $2, ..., n$. So this action induces a homomorphism $\phi : G \to S_n$ and $\phi(G)$ is a transitive subgroup ($\because$ action is transitive) and $stab_G(1) = H$. Keep the label of H to be 1, and vary the other labelling of Ω. So there are $(n-1)!$ such labelling, and each labelling gives a homomorphism $\phi : G \to S_n$ such that $\phi(G)$ is a transitive subgroup and $stab_G(1) = H$. So, a subgroup H of index n leads to $(n-1)!$ homomorphism $\phi : G \to S_n$ such that $\phi(G)$ is transitive subgroup and $stab_G(1) = H$.

Conversely, let $\phi : G \to S_n$ be any homomorphism such that $\phi(G)$ is transitive subgroup i.e. we have action of G on $\Omega(|\Omega| = n)$, such that action $G \times \Omega \to \Omega$ is transitive. i.e. $orb_G(1) = n$ and $|G/stab_G(1)| = |orb_G(1)|$ so $H = stab_G(1)$ is a subgroup of index n. Hence if we denote $t_n(G) = |\{\phi : G \to S_n, \phi(G)$ is transitive subgroup$\}|$ then, $a_n(G) = \frac{t_n(G)}{(n-1)!}$. If G is finitely generated then number of all possible homomorphisms from $G \to S_n$ is finite. Because G has d minimal generating set, a homomorphism ϕ will be completely determined by the value of ϕ at the generators. Hence, number of such maps will be at most $(n!)^d$. So, $t_n(G) \leq (n!)^d$

$$a_n(G) \leq \frac{(n!)^d}{(n-1)!}$$

which is finite. $\square$

Corollary 2.3.15 *If $|G : H| = s$ is finite, then H contains a finite index subgroup K that is normal in G, and if G is finitely generated, we can take K to be characteristics in G.*

Proof: Let K be the intersection of all the conjugates of H, or, if G is finitely generated, the intersection of all subgroup of G of index s. $\square$

Proposition 2.3.16 *If G is a finitely generated group and H is a subgroup of G of finite index, then H is finitely generated.*

Proof: Let G be a finitely generated group say by finite generating set $\{x_1, x_2, ..., x_d\}$ and $H \leq G$ with $|G : H| = s$, and let $\{a_1 = 1, ..., a_s\}$ be a set of representatives for right cosets of H in G. Let $x = y_1...y_n$ be any element of G, where each y_i is one of the generators or their inverses. Let a_{i_1} be the representatives of Hy_1, and write $x = y_1 a_{i_1}^{-1} a_{i_1} y_2...y_n$, then let a_{i_2} be the representatives of $Ha_{i_1}y_2$, and write $x = y_1 a_{i_1}^{-1}.a_{i_1} y_2 a_{i_2}^{-1}.a_{i_3} y_3...y_n$, etc., finally obtaining $x = y_1 a_{i_1}^{-1}.a_{i_1} y_2 a_{i_2}^{-1}....a_{i_{n-1}} y_n a_{i_n}^{-1}.a_{i_n}$.. Here the terms $a_j y_k a_l^{-1}$ lie in H, so if $x \in H$, we have $a_{i_n} = 1$, and x is written as a product of the finitely many triple product $a_j y_k a_l^{-1}$

$\square$

Corollary 2.3.17 *Let H be a subgroup of G of finite index and r be the maximal length of coset representatives, then*

$$s_G(n) \leq |G : H| s_H(n + r) \leq |G : H| s_H((r + 1)n)$$

Proof: Let H be a subgroup of G of finite index, let r be the maximal length of the elements in a system of representatives for the cosets of H. Given an element in G of length at most n, write it as xu, where $x \in H$ and u belongs to our system of representatives. Then $k = l(x) \leq n + r$. Write $x = y_1...y_k$, where each y_j is either a generator or an inverse of a generator. Then

$$x = y_1 u_1^{-1}.u_1 y_2 u_2^{-1}.u_2 y_2...y_k u_k^{-1}.$$

, for some u_j in our system of representatives. This shows that relative to the generators of the form (by 2.3.16) of H, we have $l(x) \leq k$, and therefore

$$s_G(n) \leq |G : H| s_H(n + r) \leq |G : H| s_H((r + 1)n)$$

□

Theorem 2.3.18 *Let G be a finitely generated group of polynomial growth. Then the commutator subgroup G' of G is also finitely generated.*

Proof: Suppose G be a finitely generated group, therefore G/G' is a finitely generated abelian group, it is a direct product of finitely many cyclic groups and we can refine this quotient so that quotient becomes cyclic. It will thus suffice to show that if $N \triangleleft G$ and G/N is cyclic, then N is finitely generated.
If G/N is finite group, then by 2.3.16, N is finitely generated. So we can assume that G/N is an infinite cyclic group.

$$G/N = < xN > \cong \mathbb{Z}$$

Given any generators $\{x_1, x_2, ..., x_d\}$ of G, we can write them in the form $x_i = x^{e_i} y_i$, where $y_i \in N$, and then $x, y_1, ..., y_d$ generate G. If we denote the normal closure of y_i for $1 \leq i \leq d$. Then it is clear that $K \subseteq N$.
Since we have a natural map $\eta : G \to G/K$, So G/K is generated by the set $\{\eta(x), \eta(y_1), ..., \eta(y_d)\} = \{1, xK\}$, if suppose xK has finite order and $K \subseteq N$, then xN has finite order, which is contradiction. So G/K is infinite cyclic and G/N is an infinite cyclic factor group of it, which is possible only if $K = N$.
Let K_i be the subgroup generated by all the conjugates $x^{-n} y_i x^n$, then $N \geq < K_1, ..., K_d >$, and the latter subgroup contains $y_1, ..., y_d$ and is invariant under conjugation by all

the generators of G, hence it is equal to N. It will thus suffice to prove that each K_i is finitely generated. If we denote y for y_i, and consider the products $xy^{e_1}xy^{e_2}x...y^{e_n}$, where each e_i is 0 or 1. There are 2^n such words, all of length $2n$ or less, and the polynomial growth implies that if n is large enough, two of these words are equal. Let us consider the minimal n at which equality occurs, say, the word above equals a similar one with exponents f_i. By minimality, $e_n \neq f_n$. Write $y(k) = x^k y x^{-k}$, and write the equality in the form

$$y(1)^{e_1}y(2)^{e_2}...y(n)^{e_n}x^n = y(1)^{f_1}y(2)^{f_2}...y(n)^{f_n}x^n$$

Since $e_n \neq f_n$, this shows that $y(n)$ can be expressed as a product of $y(1), ..., y(n-1)$. Therefore $y(n+1) = xy(n)x^{-1}$ can be expressed in terms of $y(2), ...y(n)$, and substituting the expression of $y(n)$ we see that $y(n+1)$ also belongs to the subgroup generated by $y(1), ..., y(n-1)$, and an obvious induction shows that all the $y(n)$, for $n > 0$, belongs to the same subgroup. Replacing x by its inverse, we see that the subgroup generated by the $y(n)$ for negative n is also finitely generated, hence so k_i and hence N is finitely generated.

$\square$

Chapter 3

Growth of finitely generated Solvable groups

Now, in this chapter we will discuss the growth of finitely generated solvable groups and finitely generated nilpotent groups and will prove the main theorem of this chapter, which was given by J. Milnor[3] and J. Wolf[9]

Theorem 3.0.19 ***(Milnor-Wolf)*** *If G be a finitely generated soluble group not of exponential growth then G is virtually nilpotent.*

We will prove this theorem in two steps: First, we will prove theorem 3.0.20.

Theorem 3.0.20 *[3] If G is finitely generated group not of exponential growth and if G is solvable then G must be polycyclic*

and then we will prove the theorem 3.0.21

Theorem 3.0.21 *[2] If G is finitely generated polycyclic group not of exponential growth then G must be virtually nilpotent*

So the proof of the theorem 3.0.19 directly follows from 3.0.20 and 3.0.21. So we will devote this chapter in proving theorms 3.0.20 and 3.0.21. In order to prove these results, we need several theorems and lemmas:-

Lemma 3.0.22 *Let $1 \to A \to B \xrightarrow{\phi} C \to 1$ be a short exact sequence of groups, where A is abelian group and B is finitely generated. If B does not have exponential* *growth, then for an each $\alpha \in A$ and $\beta \in B$, the set of all conjugates $\beta^k\alpha\beta^{-k}$ for $k \in \mathbb{Z}$, spans a finitely generated subgroup of A .*

Proof: For each sequence $i_1, i_2, ...i_m$ of $0's$ and $1's$. consider the expression $\beta\alpha^{i_1}\beta\alpha^{i_2}...\beta\alpha^{i_m} \in B$. In this way, we have 2^m expressions. If these 2^m expressions all represent distinct elements of B, then the growth function g_S of B with respect to any generating set S for B which containing both β and $\beta\alpha$, would satisfy: $g_S(m) \geq 2$, but this leads to B having exponential growth, which is a contradiction to our hypothesis. Hence, there must exist a non-trivial relation of the form $\beta\alpha^{i_1}\beta\alpha_{i_2}...\beta\alpha_{i_m} = \beta\alpha^{j_1}\beta\alpha_{j_2}...\beta\alpha_{j_m}$ for some integer m. Now, we will introduce a convenient abbreviation $\alpha_k = \beta^k\alpha\beta^{-k}$, hence using this abbreviation we have

$$\begin{aligned}\alpha_1^{i_1}\alpha_2^{i_2}...\alpha_2^{i_2}\beta^m &= (\beta\alpha^{i_1}\beta^{-1})(\beta^2\alpha^{i_1}\beta^{-2})(\beta^3\alpha^{i_1}\beta^{-3})...(\beta^m\alpha^{i_1}\beta^{-m}) \\ &= \beta\alpha^{i_1}\beta\alpha^{i_2}...\beta\alpha^{i_m}\end{aligned}$$

Therefore, we have the relations

$$\begin{aligned}\alpha_1^{i_1}\alpha_2^{i_2}...\alpha_m^{i_m}\beta^m &= \alpha_1^{j_1}\alpha_2^{j_2}...\alpha_m^{j_m}\beta^m \\ \alpha_1^{i_1}\alpha_2^{i_2}...\alpha_m^{i_m} &= \alpha_1^{j_1}\alpha_2^{j_2}...\beta\alpha_m^{j_m}\end{aligned}$$

in A. Since A is abelian, so we can put $a_i's$ together i.e.

$\alpha_1^{i_1-j_1}\alpha_2^{i_2-j_2}...\alpha_m^{i_m-j_m} = 1$, $i_k, j_k \in \{0, 1\}$ for $1 \leq k \leq m$ and $i_k - j_k \in \{0, 1, -1\}$ and all $i_k - j_k$ are not zero. In fact we can choose a small m so that we may assume that $i_1 \neq j_1$ and $i_m \neq j_m$. It follows that α_m can be expressed as a word in $\alpha_1, \alpha_2, ...\alpha_{m-1}$. Conjugating by β it follows that α_{m+1} can be expressed aa a word in $\alpha_2, ...\alpha_m$ and hence as a word in $\alpha_1, \alpha_2, ...\alpha_{m-1}$. ($\because$ $\alpha_{m+1} = \beta^{m+1}\alpha\beta^{-(m+1)} = \beta(\beta^m\alpha\beta^{-m})\beta^{-1} = \beta\alpha_m\beta^{-1}$)

Continuing inductively we see that every α_k with $k \geq m$ can be expressed as a word in $\alpha_1, \alpha_2, ...\alpha_{m-1}$. Similarly, every α_k with $k \leq 0$ can be expressed in terms of $\alpha_1, \alpha_2, ...\alpha_{m-1}$($\because$ $k = -l, l \geq 0, \alpha_k = \beta^k\alpha\beta^{-k} = \beta^{-l}\alpha\beta^l = (\beta^{-l}\alpha^{-1}\beta^l)^{-1} = (\gamma^l\alpha^{-1}\gamma^{-l})^{-1}$ where $\beta = \gamma^{-1}$) Hence, $T = \text{span } \{\beta^k\alpha\beta^{-k} \mid k \in \mathbb{Z}\}$ is finitely generated. □

Lemma 3.0.23 *Let $1 \to A \to B \xrightarrow{\phi} C \to 1$ be a short exact sequence of groups, where A is abelian group and B is finitely generated. If $C = B/A$ has a finite presentation,* *then there exists finitely many elements $\alpha_1, ...\alpha_l \in A$ so that every element of A can be expressed as a product of conjugates of the α_j.*

Proof: Since $C = B/A$ has finite presentation, so C has finitely many generators and finitely many defining relators.
$C =< \phi(\beta_1), ..., \phi(\beta_k) \mid \gamma_1, \gamma_2, ...\gamma_l >$. Since we chose $\beta_1, ..., \beta_k$ be a generator for B so, $\phi(\beta_1), ..., \phi(\beta_k)$ be generator for $c = B/A, C$ has finite number of defining relations.

$$\gamma_1(\phi(\beta_1)...\phi(\beta_k)) = ... = \gamma_l(\phi(\beta_1...\phi(\beta_k)) = 1$$

Setting $\alpha_j = \gamma_j(\beta_1, ...\beta_k)$. Let $a \in A \subseteq B$ and $\phi(a) = 1$. Since $\gamma_1, ...\gamma_l$ are defining relators $\phi(a)$ can be written as product of conjugates $\gamma_1(\phi(\beta_1), ..., \phi(\beta_k)), ..., \gamma_l(\phi(\beta_1), ..., \phi(\beta_k))$.
$\therefore$ a can be written as product of conjugates of $\gamma_1(\beta_1, ..., \beta_k), ..., \gamma_l(\beta_1, ..., \beta_k)$.
Hence, $\alpha_1, \alpha_2, ..., \alpha_l$ are the required elements. $\square$

Lemma 3.0.24 *Let $1 \to A \to B \xrightarrow{\phi} C \to 1$ be a short exact sequence of groups, where A is an abelian group and B is finitely generated. If C is polycyclic and B does not have exponential growth, then B must be polycyclic.*

Proof: Since C is polycyclic group so by 2.3.10 , C is finitely presented. Choose generators $\gamma_1, \gamma_2, ..., \gamma_p$ for C so that each element of C can be expressed as a product $\gamma_1^{i_1}\gamma_1^{i_1}...\gamma_p^{i_p}$ with $i_1, i_2, ..., i_p \in \mathbb{Z}$. choose elements $\beta_1, ..., \beta_p \in B$ so that $\phi(\beta_1) = \gamma_1, \phi(\beta_2) = \gamma_2, ..., \phi(\beta_p) = \gamma_p$.($\phi$ is onto). Now according to 3.0.23, there exist elements $\alpha_1, \alpha_2, ..., \alpha_l \in A$ so that every element of A can be expressed as a product of conjugates of the α_j. Let $b \in B$, $\phi(b) = \gamma_1^{i_1}\gamma_1^{i_1}...\gamma_p^{i_p} = \phi(\beta_1^{i_1}...\beta_p^{i_p})$

So, $b(\beta_1^{\gamma_1}...\beta_p^{\gamma_p})^{-1} \in \ker\phi = Im(A)$
and it follows that

$$b(\beta_1^{\gamma_1}...\gamma_p^{\gamma_p})^{-1} \in A$$
$$b = a(\beta_1^{\gamma_1}...\beta_p^{\gamma_p})^{-1})$$

Now,

$$b^{-1}\alpha_j b = (\beta_1^{\gamma_1}...\beta_p^{\gamma_p})a^{-1}\alpha_j a(\beta_1^{\gamma_1}...\beta_p^{\gamma_p})^{-1})$$

, where $a \in A$ and since A is abelian, therefore

$$= (\beta_1^{\gamma_1}...\beta_p^{\gamma_p})^{-1}\alpha_j(\beta_1^{\gamma_1}...\beta_p^{\gamma_p})$$

so clearly each conjugate of α_j can be written as in the above form. Let A_0 denote the subgroup of A spanned by $\alpha_1, ..., \alpha_l$. Applying 3.0.23 to the elements α_j and β_1, we see that there exist a finitely generated group A_1 which is spanned by all conjugates of the form $\beta_1^{-i_1}\alpha_j\beta_1^{i_1}$ with $1 \leq j \leq l, i_1 \in \mathbb{Z}$. Similarly applying 3.0.23 to each generator of A_1 and β_2 we see that all of $\beta_2^{-i_2}(\beta_1^{-i_1}\alpha_j\beta_1^{i_1}\beta_2^{i_2})$ span a finitely generated group A_2. Continuing inductively we can construct $A_1 \subset A_2 \subset ... \subset A_p$ and it follows that $A = A_p$ is also a finitely generated abelian group. Since we have already prove that each conjugate of α_j can be written as $(\beta_1^{i_1}...\beta_p^{i_p})^{-1}\alpha_j(\beta_1^{i_1}...\beta_p^{i_p}))$, So A is a finitely generated abelian group, so by 2.3.7, A is polycyclic group. Since $C = B/A$ is polycyclic so by 2.3.9, we conclude that B is polycyclic group. □

Now we will prove our theorem 3.0.20

Proof: Since G is a solvable group, we have derived series $G = G_0 \supset G_1 \supset ... \supset G_k = \{1\}$ where $G_1 = [G, G], G_{i+1} = [G_i, G_i]$. Consider a short exact sequence

$$1 \to G_1/G_2 \to G/G_2 \to G/G_1 \to 1$$

Since quotient of the derived series G_1/G_2 is an abelian group and G is finitely generated, G/G_2 is finitely generated and $G/G_1 = G/[G, G]$ is finitely generated abelian group. So G/G_1 is polycyclic. Suppose we assume that G is not of exponential growth, then G/G_2 can not have exponential growth. Since we know that G/N has exponential growth, G has exponential growth. Then by 3.0.24, G/G_2 must be polycyclic. Now take another short exact sequence:

$$1 \to G_2/G_3 \to G/G_3 \to G/G_2 \to 1$$

Again, G_2/G_3 is abelian ($\because$ successive quotient of derived series is an abelian group) and G/G_2 is a finitely generated abelian group so it is polycyclic. So by 3.0.24, either G/G_3 has exponential growth or G/G_3 is polycyclic. By the same argument above, we have G/G_3 is polycyclic. Continuing in this way, we will get $G/G_k \cong G$ is polycyclic but this is contradiction to our hypothesis. Hence, G must be of exponential growth, which is again contradiction which proves our result. $\square$

Therefore, if G is finitely generated solvable group which is not of exponential growth. Then G must be polycyclic. Next we will prove theorem 3.0.21.

Proof: Let G be a finitely generated polycyclic group. By 2.3.8, G is solvable and all of its subgroups are finitely generated. So consider the derived series of a group G

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq ... \supseteq G_{p+1} = \{1\}$$

Each subgroup is finitely generated and so its successive quotient is finitely generated abelian group. Let r denote the sum of their (torsion-free) ranks and it is called rank of group G. We will prove our result by induction on r. If $r = 0$, then successive quotient is finite abelian. Hence G is finite group. Therefore G is virtually nilpotent. Suppose $r > 0$, i.e. some quotient has copy of $\mathbb{Z}$, if $G/G_1 \cong \mathbb{Z}^s \oplus T$, $\mathbb{Z}^s$ is free abelian group and T is torsion-part. Then by Subgroup-correspondence theorem [17], there exist a subgroup H of G such that, we have

$$\begin{aligned} H/G_1 &\cong \mathbb{Z}^{s-1} \oplus T \\ G/H &\cong \frac{G/G_1}{H/G_1} \cong \frac{\mathbb{Z}^s \oplus T}{\mathbb{Z}^{s-1} \oplus T} \cong \mathbb{Z} \end{aligned}$$

So we have found a subgroup H such that $G/H \cong \mathbb{Z}$. If $G/G_1 \cong T$, where T is the finite part and $G_1/G_2 \cong \mathbb{Z}^s \oplus T_1$. Then again, $H_1/G_2 \cong \mathbb{Z}^{s-1} \oplus T_1$ and

$$G_1/H_1 \cong \frac{G_1/G_2}{H_1/G_2} \cong \frac{\mathbb{Z}^s \oplus T_1}{\mathbb{Z}^{s-1} \oplus T_1} \cong \mathbb{Z}$$

and $|G : G_1| < \infty$. So this time, we have a subgroup G_1 of finite index in G such that $G_1/H_1 \cong \mathbb{Z}$ and a subgroup H_1 of G. Since $r > 0$, replacing G by a subgroup of finite index, if necessary we can find an infinite cyclic quotient G/H of G i.e. $G/H \cong \mathbb{Z}$. So we have a short exact sequence

$$1 \to H \to G \xrightarrow{\lambda} \mathbb{Z} \to 1$$

If $t \in G$ maps onto a generator of $G/H \cong \mathbb{Z}$. If define $\mu : \mathbb{Z} \to G$ given by $\mu(1) = t$, μ is a homomorphism and also $\lambda \circ \mu(1) = \lambda(t) = 1$, so $G \cong H \rtimes < t >$. So G is the semidirect product of H with the cyclic group $< t >$ generated by t. Since rank(H)=

$r-1$, because one copy of $\mathbb{Z}$ is outside H. It follows by induction that H contains a nilpotent subgroup N of finite index i.e. $|G : N| < \infty$. Since, we know that H is finitely generated and by 2.3.14, we know that H has only finitely many subgroups of index $[H : N]$. So it follows that N has only finitely many conjugates in G. Because conjugates subgroups have same index as N has, since there are only finite subgroups of index $[H : N]$ say $Ng_1, Ng_2, ...Ng_t$. If we take their intersection $N' = \cap_{i=1}^{t} Ng_i$ which is still of finite index, since each Ng_i has finite index in H, because if we have N_1, N_2 such that $|H : N_1| < \infty$ and $|H : N_2| < \infty$, then $|H : N_1 \cap N_2| = |H : N_1||H_1 : N_1 \cap N_2|$

$$\frac{N_1}{N_1 \cap N_2} \cong \frac{N_1 N_2}{N_2}$$

Since $|H : N_2| < \infty$ so $|N_1N_2 : N_2| < \infty$ it implies that $|H : N_1 \cap N_2| < \infty$. Similarly hold for any finite intersection. Hence N' is normal subgroup of G which has finite index in H. So we may therefore assume N is normal in G which has finite index in H. Note that $N. < t >$ has finite index $[H : N]$ G, since we have $G \cong H. < t >$ and therefore $|G : N. < t >| = |H. < t >: N. < t >| = |H : N| < \infty$ so we may assume that $G = N. < t >$($\because$ upto finite index). Because in order to prove G is virtually nilpotent if we are able to show that G has a subgroup H of finite index such that H is virtually nilpotent. Then we are done since in that case we have $|G : H| < \infty$ and $|H : N| < \infty$ which implies that $|G : N| < \infty$. Now our $G = N. < t >$. So N has lower central series

$$N = \gamma_1(N) \supseteq \gamma_2(N) \supseteq ... \supseteq \gamma_{s+1}(N) = \{1\}$$

. Refine this lower central series of N to chain $N = N_1 \supseteq N_2 \supseteq ... \supseteq ..$ of G-invariant subgroups such that N_h/N_{h+1} is either finite or else such that N_L/L is finite for any G-invariant subgroup L with

$$N_{h+1} \subseteq L \subseteq N_h$$

$N_h/N_{h+1} \cong \mathbb{Z}^r \oplus T$, there exists a subgroup H/N_{h+1} of N_h/N_{h+1} such that $H/N_{h+1} \cong \mathbb{Z}^r$ and $|N_h : H| < \infty$ The latter condition just means that the G-module $M_h = N_h/N_{h+1}$ is torsion free and $\mathbb{Q} \otimes_{\mathbb{Z}} M_h$ is an irreducible $\mathbb{Q}[G]$-module. $\square$

Lemma 3.0.25 *Let $< t >$ be an infinite cyclic group . Let M be a $< t >$-module which is finitely generated and torsion free and such that $\mathbb{Q} \otimes_{\mathbb{Z}} M$ is irreducible.*

Suppose that the semi-direct product M with $< t >$ does not have exponential growth. Then some power of t acts trivially on M.

Proof: Here, we have $< t > \cong \mathbb{Z}$ be an infinite cyclic group. Let M be $< t >$ module which is finitely generated torsion free and such that $\mathbb{Q} \otimes_{\mathbb{Z}} M$ is irreducible. Let α be an automorphism of M induced by t: $< t > \times M \to M$ so $\phi_t : M \to M$ is given by $\phi_t(m) = t.m$. Since, $\mathbb{Q} \otimes_{\mathbb{Z}} M$ is irreducible, $\mathrm{End}(\mathbb{Q} \otimes_{\mathbb{Z}} M)$ is a division $\mathbb{Q}$-algebra. Now consider the subalgebra of $\mathrm{End}(\mathbb{Q}\otimes_{\mathbb{Z}} M)$ generated by α, which is $\mathbb{Q}[\alpha]$, α induces a endomorphism at the level of $\mathbb{Q} \otimes_{\mathbb{Z}} M$ namely

$$1 \otimes \phi : \mathbb{Q} \otimes_{\mathbb{Z}} M \to \mathbb{Q} \otimes_{\mathbb{Z}} M$$

given by

$$1 \otimes \phi(\sum \alpha_i \otimes m) = \sum \alpha_i \otimes \alpha(m)$$

Since, we know that M be a $< t > \cong \mathbb{Z}$ module which is finitely generated and torsion-free i.e. $(M \cong \mathbb{Z}^d)$ so

$$\mathbb{Q} \otimes_{\mathbb{Z}} M \cong \mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}^d \cong \mathbb{Q}^d$$

i.e. $\alpha \in \mathrm{End}(\mathbb{Q}\otimes_{\mathbb{Z}} M \cong \mathbb{Q}^d)$ i.e. there are scalars, not all zero, such that $\sum_{i=0}^{d+1} \beta_i \alpha^i = 0$ for $\beta_i \in \mathbb{Q}$, it follows that

$$\beta_0 + \beta_1 \alpha + ... + \beta_{d+1} \alpha^{d+1} = 0$$

We can always choose a constant $\beta_i \neq 0$ such that $\beta_i + \beta_{i+1}\alpha^{i+1} + ... + \beta_{d+1}\alpha^{d+1} = 0$. So without loss of generality, choose $\beta_0 \neq 0$

$$\begin{aligned}
&\beta_0 = -(\beta_1 \alpha + ... + \beta_{d+1}\alpha^{d+1}) \\
&1 = -(\beta_0^{-1}\beta_1 \alpha + ... + \beta_0^{-1}\beta_{d+1}\alpha^{d+1}) \\
&\alpha^{-1} = -(\beta_0^{-1}\beta_1 + ... + \beta_0^{-1}\beta_{d+1}\alpha^{d}) = -\sum_{i=0}^{d} c_i \alpha^i \in \mathbb{Q}[\alpha]
\end{aligned}$$

So, $\mathbb{Q}[\alpha] = \mathbb{Q}(\alpha)$. Hence, the subalgebra generated by α is a field namely $\mathbb{Q}(\alpha)$. Since, $\alpha \in \mathrm{End}(\mathbb{Q} \otimes_{\mathbb{Z}} M)$, we can view α as a $d \times d$ matrices over $\mathbb{Z}$. So it satisfy its characteristic equation. Hence α, is an algebraic integer. Also, α satisfies some monic polynomial, therefore so $\mathbb{Q}(\alpha)$ is a finite extension over $\mathbb{Q}$ and we can embed $\mathbb{Q}(\alpha)$ in

$\mathbb{C}$. Now we wish to prove that α is a root of unity. Suppose α is not a root of unity. Then we can see α as an embedding of $\mathbb{Q}(\alpha)$ in $\mathbb{C}$ such that $|\alpha| \neq 1$. Now replacing α by a power of α (and t by the same power of t), we can further arrange that $|\alpha| > 2$ (if $|\alpha| > 1$) otherwise we can consider $\mathbb{Q}(\alpha^{-1})(\ |\alpha^{-1}| < 1)$. Now, choose $x \neq 0$ in M. Since, $\mathbb{Q}(\alpha)$ is the subalgebra generated by α of $\mathrm{End}(\mathbb{Q} \otimes_{\mathbb{Z}} M)$. So $\mathbb{Q}(\alpha).x$ is a submodule of $\mathbb{Q} \otimes M$ but $\mathbb{Q} \otimes_{\mathbb{Z}} M$ is irreducible. Therefore, $\mathbb{Q} \otimes_{\mathbb{Z}} M = \mathbb{Q}(\alpha).x$
Now, by our given hypothesis that the semi-direct product of M with $< t >$ does not have exponential growth, we can apply 3.0.23 by interchange the role of t, x in the place of β and α. Hence, we have a relation of the form

$$0 = e_0 x + e_1 \alpha x + ... + e_{m-1} \alpha^{m-1} x + \alpha^m x$$

where each $e_i = 0, 1$ or -1. This implies that,

$$\begin{aligned} \alpha^m x &= -(e_0 x + e_1 \alpha x + ... + e_{m-1} \alpha^{m-1} x) \\ \alpha^m &= -(e_0 + e_1 \alpha + ... + e_{m-1} \alpha^{m-1}) \end{aligned}$$

Therefore,

$$\begin{aligned} &|\alpha^m| = |e_0 + e_1 \alpha + ... + e_{m-1} \alpha^{m-1}| (\because e_i \in \{0, 1, -1\}) \\ &|\alpha^m| \leq 1 + |\alpha| + ... + (|\alpha|)^{m-1} \\ &= \frac{(|\alpha|)^m - 1}{|\alpha| - 1} \end{aligned}$$

,Since $|\alpha| > 2$, we have $|\alpha| - 1 > 1$ it follows that $\frac{1}{|\alpha|-1} < 1$

$$\frac{(|\alpha|)^m - 1}{|\alpha| - 1} < (|\alpha|)^m - 1 < (|\alpha|)^m$$

So, $|\alpha|^m < |e_0 + e_1 \alpha + ... + e_{m-1} \alpha^{m-1}| < |\alpha|^m$ which is contradiction, because $|\alpha| > 2$. Hence, α is a root of unity. Since α is an automorphism of M induced by t, some power of t acts trivially on M. Now, let's apply the above lemma to finish our proof. Now, note that N acts trivially on N_h because N_h is a $G-$invariant subgroup. Since N is nilpotent group by 3.0.25, some power of t likewise acts trivially on M_h. Thus there is a power t^q of t which acts trivially on all the M_h. If we take $G' = N'. < t^q >$, then

$$[G', N_h] = [N. < t^q, N_h] \subseteq N_{h+1} \forall h$$

Since t^q acts trivially on $M_h = N_h/N_{h+1}$ and N acts trivially on $M_h \forall h$. Since

$$[G', G'] = [N. < t^q, N. < t^q] \subseteq N = N_1$$

and

$$G'_{(2)} = [G', [G', G']] \subseteq [G', N_1] \subseteq N_2$$
$$G'_{(3)} = [G', [G', [G', G']]] \subseteq [G', N_2] \subseteq N_3$$
$$\ldots$$

We proceed like this and since N is nilpotent group so there exist $k \in \mathbb{N}$ such that $G'_{(k)} = \{1\}$.

Now, $|G : G'| = |\frac{N.<t>}{N.<t^q>}| = \frac{|<t>|}{|<t^q>|} = q$. So, G' is a nilpotent subgroup of G of finite index q. □

3.0.3 Growth of finitely generated nilpotent groups

In this section, we will prove our main result which says that if G is finitely generated nilpotent group then the growth type of G is polynomial, not only that we will calculate the degree of that polynomial.

To prove this, first let's make the definition of polynomial growth to be more precise.

Definition 3.0.26 ***(Polynomial growth)*** *Let G be a group, S a finite generating set of G. Suppose that there are polynomials P, Q with positive leading coefficients such that $P(m) \leq \gamma_S(m) \leq Q(m)$ for all $m >> 0$.*

If $d = \deg(P)$ and $e = \deg(Q)$, then it is clear that there exist constants $A, B > 0$ such that $Am^d \leq \gamma_S(m) \leq Bm^e$ for all $m >> 0$. Suppose that T is another finite generating set of G. By 2.2.10, there are integers $a, b > 0$ such that $\gamma_S(m) \leq \gamma_T(am)$ and $\gamma_T(m) \leq \gamma_S(bm)$ for all m. The latter condition implies that $\gamma_T(m) \leq (Bb^e)m^e$ for $m >> 0$ and the former condition implies that $\gamma_T(m) \geq \gamma_T(a[\frac{m}{a}]) \geq A([\frac{m}{a})^d(\because m \geq a[\frac{m}{a}] \geq \gamma_S([\frac{m}{a}])$ Since, $[\frac{m}{a}]^d = [\frac{m}{a} - 1 + 1]^d$, where $[x]$ is the greatest integer function. As we know $[x]-1 \leq x \leq [x]+1$

$\therefore \quad A[\frac{m}{a}]^d \geq A(\frac{m}{a}-1)^d$.
($\because$ if $\frac{m}{a} \in \mathbb{Z}$ then $[\frac{m}{a}]^d \geq (\frac{m}{a}-1)^d$

and if $\frac{m}{a} \notin \mathbb{Z}$ then $[\frac{m}{a}]^d \geq (\frac{m}{a}-1)^d$)

So, we have $\gamma_T(m) \geq \frac{A}{a^d}(m-a)^d$ for $m >> 0$. Thus γ_T is bounded above and below by polynomials of the same degree with positive leading coefficients.

Let d be a positive integer. We say that G has polynomial growth of degree d if there exists constants $A, B > 0$ such that $Am^d \leq \gamma_S(m) \geq Bm^d$ for all $m >> 0$ and this notion does not depend upon the choice of S.
Now, just before writing a main theorem, we fix some notations which we will use throughout this section.

Let G be a finitely generated nilpotent group with lower central series

$$G = G_1 \supseteq G_2 \supseteq ... \supseteq G_p \supseteq G_{p+1} = \{1\}$$

Let r_h denote the rank of the finitely generated abelian group G_h/G_{h+1} and write $d(G) = \sum_{h\geq 1} hr_h$. Then the theorem says that:

Theorem 3.0.27 *[**H. Bass**, [2]] Let G be a finitely generated nilpotent group with lower central series*

$$G = G_1 \supseteq G_2 \supseteq ... \supseteq G_p \supseteq G_{p+1} = \{1\}.$$

Let r_h denote the rank of finitely generated abelian group G_h/G_{h+1} and write $d(G) = \sum_{h\geq 1} hr_h$. Then G has polynomial growth of degree $d(G)$. In other words there is finite generating set T of G and polynomial P and Q of degree $d(G)$ such that $P(m) \leq \gamma_T(m) \leq Q(m)$.

We will prove this theorem in two steps. Our first step will be to prove $P(m) \leq \gamma_T(m)$ and second step will be to prove $\gamma_T(m) \leq Q(m)$. Let's start with first step. In order to prove it, we need a small proposition.

Proposition 3.0.28 *If A and B are subgroup of G whose commutator $[A, B]$ lies in the centre $Z(G)$, then the commutator map $A \times B \to [A, B]$ is bimultiplicative.*

Proof: Let $A, B \leq G$ such that $[A, B] \subseteq Z(G)$, and a map $\phi : A \times B \to [A, B]$ given by $\phi(a, b) = a^{-1}b^{-1}ab$.

$$\phi(aa', b) = (aa')^{-1}b^{-1}aa'b = a'^{-1}a^{-1}b^{-1}aa'b$$

$$\phi(a, b)\phi(a', b) = a^{-1}b^{-1}aba'^{-1}b^{-1}a'b$$

Now,

$$\begin{aligned}
\phi(aa', b) &= a'^{-1}a^{-1}b^{-1}aa'b \\
&= a'^{-1}(a^{-1}b^{-1}ab)b^{-1}a'b (\because a^{-1}b^{-1}ab \in Z(G)) \\
&= a^{-1}b^{-1}aba'^{-1}b^{-1}a'b \\
&= \phi(a, b)\phi(a', b)
\end{aligned}$$

Similarly, we have $\phi(a, bb') = a^{-1}b'^{-1}b^{-1}abb'$

$$\phi(a, b)\phi(a, b') = a^{-1}b^{-1}aba^{-1}b'^{-1}ab'$$

Now, $\phi(a, bb') = a^{-1}b'^{-1}a(a^{-1}b^{-1}ab)b' = a^{-1}b^{-1}aba^{-1}b'^{-1}ab' = \phi(a, b)\phi(a, b')$ $[\because a^{-1}b^{-1}ab \in Z(G)]$. So, ϕ is bimultiplicative. $\square$

Now, let's start the proof of first step. Since we know that by 2.3.5, we have $[G_h, G_k] \subseteq G_{h+k}$. Now, we will apply 3.0.28 to $A = G_h/G_{h+1}$ and $B = G_k/G_{k+1}$, Now,

$$Z(G/G_{h+k+1}) = \{gG_{h+k+1} \in G/G_{h+k+1} : gG_{h+k+1}hG_{h+k+1} = hG_{h+k+1}gG_{h+k+1} \forall hG_{h+k+1} \in G/G_{h+k}$$

$$= \{gG_{h+k+1} \in G/G_{h+k+1} : ghg^{-1}h^{-1} \in G_{h+k+1}\}$$

$Z(G/G_{h+k+1}) = \{g \in G : [g,h] \in G_{h+k+1} \forall h \in G$

Claim: $[G_h/G_{h+1}, G_k/G_{k+1}] \subseteq Z(G/G_{h+k+1})$

Now,

$$[G_h/G_{h+1}, G_k/G_{k+1}] = \frac{[G_h, G_k]G_{h+k+1}}{G_{h+k+1}} \leq \frac{G_{h+k}G_{h+k+1}}{G_{h+k+1}} = \frac{G_{h+k}}{G_{h+k+1}}$$

Let $gG_{h+k+1} \in G/G_{h+k+1}$, and $h \in G$, since we have $[G_1, G_{h+k}] \subseteq G_{h+k+1}]$, $[g,h] \subseteq G_{h+k+1}$. So by 3.0.28, we have

$$\phi : G_h/G_{h+1} \times G_k/G_{k+1} \to [G_h/G_{h+k+1}, G_k/G_{h+k+1}]$$

given by

$\phi(gG_{h+k+1}, hG_{h+k+1}) = [g,h]G_{h+k+1}$ is bimultiplicative. So by the universal property of tensor product , we have a map:

$$\psi : G_h/G_{h+1} \otimes G_k/G_{k+1} \to [G_h/G_{h+k+1}, G_k/G_{h+k+1}] \subseteq \frac{G_{h+k}}{G_{h+k+1}}$$

and therefore we have a map

$$\psi : G_h/G_{h+1} \otimes G_k/G_{k+1} \to [G_h/G_{h+k+1}, G_k/G_{h+k+1}]$$

Since $\frac{G_h}{G_{h+1}} \cong \frac{G_h/G_{h+k+1}}{G_k/G_{h+k+1}}$ and $\frac{G_k}{G_{k+1}} \cong \frac{G_k/G_{h+k+1}}{G_{k+1}/G_{h+k+1}}$, so we define

$$\psi : G_h/G_{h+1} \otimes G_k/G_{k+1} \to [G_h/G_{h+k+1}, G_k/G_{h+k+1}]$$

given by $\psi(gG_{h+1}, g'G_{k+1}) = [g,g']G_{h+k+1}$: if k = 1 , $\psi : G_h/G_{h+1} \otimes G_1/G_2 \to G_{h+1}/G_{h+2}$ .Then ψ' is surjective, because if $gG_{h+2} \in G_{h+1}/G_{h+2}$, where $g \in G_{h+1} = [G, G_h]$, write

$$g = [x_1, y_1]^{\epsilon_1}[x_2, y_2]^{\epsilon_2}...[x_r, y_r]^{\epsilon_r}$$

where $x_i \in G, y_i \in G_h$. Now each $[x_i, y_i]$ has preimage $x_iG_{h+1} \otimes y_iG_2$ such that

$$\psi(x_iG_{h+1} \otimes y_iG_2) = [x_i, y_i]G_{h+2}$$

Since ψ is bimultiplicative, $\psi(x_i^{\epsilon_1}G_{h+1} \otimes y_iG_2) = [x_i, y_i]^{\epsilon_1}G_{h+2}$

Similarly,

$$\psi(\sum_{i=1}^{r}(x_i^{\epsilon_i}G_{h+1}\otimes y_iG_2)) = [x_1,y_1]^{\epsilon_1}[x_2,y_2]^{\epsilon_2}...[x_r,y_r]^{\epsilon_r}G_{h+2}$$

Hence for $k = 1$, f is an onto homomorphism. It follows by induction that if T_1 is a finite set in G, whose image generates G_1/G_2 and if we define T_h inductively : $T_{h+1} = \{[s,t] = sts^{-1}t^{-1} \mid s \in T_1, t \in T_h\}$. Then T_h is a finite subset of G_h whose image generates G_h/G_{h+1}, Now we have $G_h \to G_h/G_{h+1}$ given by $T_h \to G_h/G_{h+1}$ similarly $G_1 \to G_1/G_2$, So,

$$G_h/G_{h+1} \otimes G_1/G_2 \xrightarrow[onto]{f} G_{h+1}/G_{h+2}.$$

Here,

$$gG_2 = t_1^{\alpha_1}.t_2^{\alpha_2}...t_r^{\alpha_r}G_2$$

therefore $g^{-1}(t_1^{\alpha_1}.t_2^{\alpha_2}...t_r^{\alpha_r}) \in G_2$

$$g = t_1^{\alpha_1}.t_2^{\alpha_2}...t_r^{\alpha_r}(\prod[t_i,t_j])(\prod_{i,j}[t_i,[t_i,t_k]]) \in T_1.$$

$$\therefore G = < T_1 >$$

Lemma 3.0.29 *Let h, m and n be integers such that $h \geq 1, m > 0$ and $\mid n \mid \leq m^h$. Let $t \in T_h$. Then there is an element $t^{(n)} \in G_h$ such that $t^{(n)} \equiv t^n mod\ G_{h+1}$ and $l_{T_1}(t^{(n)}) \leq 8^{h-1}m$.*

Proof: We will treat only the case $n \geq 0$. If $n < 0$, $m = -n > 0$, then $t^{(m)} = t^{(-n)} = (t^{(n)})^{-1}$. Now if $h = 1$, we put $t \in T$ and $|n| \leq m$ then $t^{(n)} = t^n$. Clearly $l_{T_1}(t^{(n)}) \leq n$ and $n \leq 8^{1-1}m = 8^0m$, by hypothesis.

Suppose by induction, the lemma holds for $h \geq 1$. We wish to prove it for $h+1$. Given $u \in T_{h+1}$ and $0 \leq n \leq m^{h+1}$, we seek $u^{(n)} \equiv u^n \text{mod } G_{h+2}$ with $l_{T_1}(u^{(n)}) \leq 8^hm$. Let $n = am + b$ with $0 \leq b < m$ and then $0 \leq a < m^h$. (Otherwise, $n \leq m^{h+1}$ so $a \leq m^h$, if $a > m^h \Rightarrow ma > m^{h+1}$ a contradiction). Now $u \in T_{h+1} = \{[s,t] \mid s \in T_1, t \in T_h\}$, say $u = [s,t]$, $\phi : G_1 \times G_h \to G_{h+1}/G_{h+2}$, given by $\phi(a,b) = [a,b]G_{h+2}$ and the map ϕ is bilinear. So using the bilinearity of ϕ, we have $\phi(aa',b) \equiv [a,b][a',b]$ ($\equiv$:modG_{h+2})

i.e. $[a^2,b] \equiv [a,b][a,b](\text{mod } G_{h+2}) \Rightarrow [a^2,b] \equiv [a,b]^2(\text{mod } G_{h+2})$

Similarly,

$$\begin{aligned}[a^2,b^2] &\equiv [a,b^2]^2(modG_{h+2})\\ &\equiv [a,b]^4(modG_{h+2})\end{aligned}$$

Hence, we have $u^n = [s,t]^{am+b}$

Now,

$$\begin{aligned}[s^m,t^a][s^b,t] &\equiv [s^m,t^a][s,t]^b(modG_{h+2}))\\ &\equiv [s,t^a]^m[s,t]^b(modG_{h+2}))\\ &\equiv [s,t]^{am}[s,t]^b(modG_{h+2}))\\ &\equiv [s,t]^{am+b}(modG_{h+2}))\\ &\equiv u^n = [s,t]^{am+b} \equiv [s^m,t^a][s^b,t]\\ &\equiv [s^m,t^{(a)}][s^b,t](modG_{h+2}))\end{aligned}$$

Since, $0 \leq a \leq m^h$, by induction, we have

$$\begin{aligned}\equiv u^n &\equiv [s^m,t^a][s^b,t]\\ &\equiv u^n(modG_{h+2}))\end{aligned}$$

Then,

$$\begin{aligned}l_{T_1}(u^{(m)}) &\leq 2m + 2l_{T_1}(t^{(m)}) + 2b + 2l_{T_1}(t)\\ &\leq 2m + 2m + 2l_{T_1}(t^{(a)}) + 2l_{T_1}(t)[\because l_{T_1}(t^{(a)}) \leq 8^{h-1}m]\\ &\leq 4m + 2.8^{h-1}m + 2.8^{h-1}m\\ &\leq 4m + 4.8^{h-1}m = 4m(1+8^{h-1}) \leq 8^hm\end{aligned}$$

Hence, $u^{(n)}$ is the required element in the lemma, which completes the proof. $\square$

Now, fix an integer $m > 0$, for each $h \geq 1$ choose elements $t_{h_1}, t_{h_2}, ..., t_{h_{r_h}} \in T_h$ which are linearly independent modulo G_{h+1}. Since, r_h = rank of finitely generated abelian groups G_h/G_{h+1}(torsion-free part), we can choose elements $t_{h_1}, t_{h_2}, ..., t_{h_{r_h}} \in T_h$ which are linearly independent modulo G_{h+1}. i.e. whenever $t_{h_1}^{\alpha_1}, t_{h_1}^{\alpha_2}, ..., t_{h_1}^{\alpha_h} \in G_{h+1}$

which imply that $\alpha_1 = 0, \alpha_2 = 0, ..., \alpha_{r_h} = 0$. Consider the set S_h of elements $t_{h_1}^{(q_1)}, t_{h_2}^{(q_2)}, ..., t_{h_{r_h}}^{(q_{r_h})}$ with $|q_i| \leq m^h$ for $1 \leq i \leq r_h$ and there are $(2m^h + 1)^{r_h}$ distinct elements in S_h. Suppose

$$t_{h_1}^{(q_1)}, t_{h_2}^{(q_2)}, ..., t_{h_{r_h}}^{(q_{r_h})} = t_{h_1}^{(q_1^*)}, t_{h_2}^{(q_2^*)}, ..., t_{h_{r_h}}^{(q_{r_h}^*)}(modG_{h+2}))$$
$$t_{h_1}^{(q_1 - q_1^*)}, t_{h_2}^{(q_2 - q_2^*)}, ..., t_{h_{r_h}}^{(q_{r_h} - q_{r_h}^*)} \equiv 1(modG_{h+2}))$$

but $\{t_{h_1}, t_{h_2}, ..., t_{h_{r_h}}\}$ is a linearly independent set modulo G_{h+2}. So, $q_1 = q_1^*, ..., q_{r_h} = q_{r_h}^*$. So there are $(2m^h+1)^{r_h}$ distinct elements in S_h, because q_i has $(2m^h+1)^{r_h}$ choices and each of T_1- length $\leq r_h.8^{h-1}m$ or less 3.0.29. Now consider the sets $S_1, S_2, ...S_p$ for each $h = 1, 2, ..., p$ and

$$S_h = \{t_{h_1}^{(q_1)}, t_{h_2}^{(q_2)}, ..., t_{h_p}^{(q_p)}\}$$

Claim: The product map is $S_1 \times S_2 \times ... \times S_p \to G$ is injective.

Suppose

$$(t_{11}^{q_1^{(1)}} ... t_{1r_1^{(1)}}^{q_{1r_1}})(t_{21}^{q_1^{(2)}} ... t_{2r_2}^{q_{r_2}^{(2)}})...(t_{p1}^{q_1^{(p)}} ... t_{pr_p}^{q_{r_p}^{(p)}}) = \{1\}$$

and also we have $G_1 \supset G_2 \supset G_3 \supset ...G_p \supset G_{p+1} = \{1\}$ Reducing the equation over G_2, we get

$$(t_{11}^{q_1} ... t_{1r_1}^{q_{1r_1}})G_2(t_{21}^{q_1^{(2)}} ... t_{2r_2}^{q_{r_2}^{(2)}})G_2...(t_{p1}^{q_1^{(p)}} ... t_{pr_p}^{q_{r_p}^{(p)}})G_2 = G_2,$$

since, we have

$$(t_{21}^{q_1^{(2)}} ... t_{2r_2}^{q_{r_2}^{(2)}}) \subset G_2, T_3 \subset G_3 \subset G_2 ... T_p \subset G_p \subset G_2$$

we get $t_{11}^{q_1} ... t_{1r_1}^{q_{1r_1}} G_2 = G_2$, since $\{t_{11}, t_{12}, ..., t_{1r_1}\}$ is a linearly independent set modulo G_2. So $q_1 = 0, q_2 = 0, ..., q_{r_1} = 0$. Now we have left

$$(t_{21}^{q_1^{(2)}} ... t_{2r_2}^{q_{r_2}^{(2)}})...(t_{p1}^{q_1^{(p)}} ... t_{pr_p}^{q_{r_p}^{(p)}}) = \{1\}$$

Now reduce the equation over G_3, we get $q_1^{(2)} = 0 ... q_{2r_2}^{(2)} = 0$. Similarly, $q_i^{(r_i)} = 0 \ \forall \ 1 \leq i \leq r_h$. Therefore, the product map

$S_1 \times S_2 \times ... \times S_p \to G$ is injective. So its image consists of

$$P(m) = \prod_{h \geq 1} (2m^h + 1)^{r_h}$$

distinct elements and each of T_1-length at most

$$\sum_{h \geq 1} 8^{h-1} r_h m = m(\sum_{h \geq 1} 8^{h-1} r_h) = cm$$

for some c.

Thus, $P(m) \leq \gamma_{T_1}(cm)$

Since, $P(m) = \prod_{h \geq 1}(2m^h + 1)^{r_h}$. So $P(m)$ is a polynomial of degree $\sum_{h \geq 1} hr_h = d(G)$ with leading term $2^e m^d$, $e = \sum_{h \geq 1} r_h$. Since the notion of growth does not depend upon choice of generator, $P(m) \leq \gamma_T(m)$, where deg$P(m) = d(G)$, which completes the proof of first step.

Now we will prove the second part of theorem 3.0.27 i.e. $\gamma_T(m) \leq Q(m)$, where $Q(m)$ is a polynomial of degree $d(G)$.

Proof: Since G is finitely generated and a nilpotent group, so by 2.3.6, we can choose a finite set T of generators of G such that $s, t \in T \Rightarrow s^{-1} \in T$ and $[s, t] \in T$. We have the lower central series $G = G_1 \supseteq G_2 \supseteq G_3 .... \supseteq G_p \supseteq G_{p+1} = \{1\}$. We put $T_h = T \cap G_h$, for $h \geq 1$, so that

$T = T_1 \supseteq T_2 \supseteq ... \supseteq T_p \supseteq T_{p+1} = \{1\}$, and $G_h =< T_h >$ for all $h \geq 1$ because our T is the set of all possible commutators. Let's recall 2.2.12, $P_r(m)$ be the growth function of a free abelian group of rank r with respect to a standard basis i.e. Therefore, $P_r(m) = \sum_i^r 2^i \binom{r}{i} \binom{m}{i}$ is a polynomial of degree r with positive leading coefficient.

To prove $\gamma_T(m) \leq Q(m)$, where $Q(m)$ is a polynomial of degree $d(G)$, we need a proposition from which it will directly follow:

Proposition 3.0.30 *There exist constants $A_1, A_2, ..., A_p$ with the following property: given integers $c \geq 1$ and h with $1 \leq h \leq p$, there exist integers $c_j \geq 1$, for $h \leq j \leq p$, such that $\gamma_{T_h}(cm^h) \leq A_h. \prod_{j \geq h} P_{r_j}(c_j m^j)$ for all m.*

Proof: Suppose $h = 1$, since $m \leq cm$ $(c \geq 1)$ and $T = T_1$, $(T_1 = T \cap G_1 = T \cap G = T)$ we conclude from the proposition that $\gamma_T(m) \leq A_1. \prod_{j \geq 1} P_{r_j}(c_j m^j)$. Since we know that

$$P_r(m) = \sum_{i=0}^{r} 2^i \binom{r}{i} \binom{m}{i}$$
$$P_{r_j}(m) = \sum_{i=0}^{r_j} 2^i \binom{r_j}{i} \binom{m}{i}$$
$$P_{r_j}(c_j m^j) = \sum_{i=0}^{r_j} 2^i \binom{r_j}{i} \binom{c_j m^j}{i}$$

So, $P_{r_j}(c_j m^j)$ is polynomial of degree jr_j and $A_1 \prod_{j \geq} P_{r_j}(c_j m^j)$ is polynomial of degree $\sum jr_j = 1.r_1 + 2.r_2 + ...$ it implies that

$\sum_{j \geq 1} jr_j = d(G)$. Hence, $A_1. \prod_{j \geq h} P_{r_j}(c_j m^j)$ is a polynomial with positive leading coefficient of degree $\sum_{j \geq 1} jr_j = d(G)$. So it follows that $\gamma_T(m) \leq Q(m)$, where $Q(m)$ is a polynomial of degree $d(G)$.

Now fix, $1 \leq h \leq p$. List the elements of T_h/T_{h+1} : $t_1, t_2, ..., t_l$ so that $t_1, t_2, ..., t_{r_h}$ are linearly independent modulo G_{h+1} because rank$(G_h/G_{h+1}) = r_h$. Therefore, $G_h/G_{h+1} \cong \mathbb{Z}^{r_h} \oplus T$ where $\mathbb{Z}^{r_h}$ is the free part and T is torsion part. So, $< t_1, t_2, ..., t_{r_h} > \cong \mathbb{Z}^{r_h}$ and $< t_1, t_2, ..., t_{r_h} > G_{h+1}$ has finite index, say N, in G_h. ($\because \exists$ subgroup H of G_h such that $H/G_{h+1} \cong \mathbb{Z}^{r_h}$, $G_h/H \cong T$ with $|G_h : H| < \infty$). Now we will define some terminology:

By a word in T_h, we mean a finite sequence $w = (s_1, s_2, ...s_n)$ of elements of T_h. It is said to represent $|w| = s_1 s_2 ... s_n \in G_h$. We say w is prenormalized if it is of the form

$$w = (t_1, t_1, ..t_1, ...t_l, t_l, ..t_l, v) \tag{3.1}$$

where first a_i coordinates are of t_i, for $1 \leq i \leq l$, and v is a word in T_{h+1}. We say w is normalized if further $a_j < N$ for $r_h < j \leq l$. Now, let $w = (s_1, s_2, ..s_n)$ be a word in T_h. If $S \subseteq T_h$, let $deg_S(w)$ be the number of $i's$ for which $s_i \in S$. Put $q = p - h + 1$

and let $d = (d_h, ..., d_p) \in \mathbb{Z}^q$, we write $deg(w) \leq d = (d_h, ..., d_p)$ if $deg_{T_h \setminus T_{h+1}}(w) \leq d_i$ for $h \leq i \leq p$.

Let $G_h(d) = G_h(d_h, ..., d_p)$, denote the set of words w such that $\deg(w) \leq d$, and let $G'_h(d)$ be the set of words in $G_h(d)$ that are normalized and elements of G_h represented by these sets will be denoted $|G_h(d)|$ and $|G'_h(d)|$, respectively. If $w \in G'_h(d_h, ..., d_p)$ is normalized word as above with $a_j = deg_{t_j}(w)$, then

$$a_1 + a_2 + ... + a_l = deg_{t_1}(w) + deg_{t_2}(w) + ... + deg_{t_l}(w)$$

since, $t_1, t_2, ..., t_l \in T_h \setminus T_{h+1}$ and $deg_{T_h \setminus T_{h+1}}(w) = a_1 + a_2 + ... + a_l$ ($\because$ $deg_{T_h \setminus T_{h+1}}(w)$ be the number of elements t_j such that $t_j \in T_h \setminus T_{h+1}$ and since $a_j = deg_{t_j}(w)$ and $v \notin T_h \setminus T_{h+1}$ so v would not contribute to $deg_{T_h \setminus T_{h+1}}(w)$). So, $a_1 + a_2 + ... + a_l = deg_{T_h \setminus T_{h+1}}(w) \leq d_h$ ($w \in G'_h(d_h, ..., d_p)$ also $deg(w) \leq d$ i.e. $deg_{T_h \setminus T_{h+1}}(w) \leq d_i, h \leq i \leq p$, In particular, $i = h$ and $deg_{T_h \setminus T_{h+1}}(w) \leq d_h$). Hence, we have $a_1 + a_2 + ... + a_l = deg_{T_h \setminus T_{h+1}}(w) \leq d_h$. It follows that

$$Card|G'_h(d_h, ..., d_p) | \leq A'_h P_{r_h}(d_h).Card \mid G_{h+1}(d_{h+1}, ..., d_p)| \tag{3.2}$$

where $A'_h = (l - r_h)^N + 1$. Let $\tau : \mathbb{Z}^q \to \mathbb{Z}^q$ be the endomorphism defined by :

$$\tau(d_h, d_{h+1}, ..., d_p) = (0, d_h, ..., d_{p-1})$$

$$\begin{aligned} \tau((d_h, ..., d_p) + (d'_h, d'_{h+1}, ..., d'_p)) &= \tau(d_h + d'_h, ..., d_p + d'_p) \\ &= \tau(0, d_h + d'_h, ..., d_{p-1} + d'_{p-1}) \\ &= (0, d_h, ..., d_{p-1}) + (0, d'_h, ..., d'_{p-1}) \\ &= \tau(d_h, ..., d_p) + \tau(d'_h, d'_{h+1}, ..., d'_p) \end{aligned}$$

Hence, τ is an endomorphism.

Lemma 3.0.31 *Let $d = (d_h, ..., d_p) \in \mathbb{Z}^q$ and put $d' = (I + \tau^h)^{d_h}(d), w \in G_h(d)$. Then there is a word $w_1 \in G_h(d')$ such that $|w_1| = |w|$, $deg_{t_j}(w_1) = deg_{t_j}(w)$ for $1 \leq j \leq l$ and w_1 is prenormalized.*

Proof: Consider an occurence of t_1 in w, say $(..., s, t_1, ..)$. We have $st_1 = t_1s[s^{-1}, t^{-1}]$ so we can write $st_1 = t_1s[s^{-1}, t^{-1}]$ and $[s^{-1}, t^{-1}] \in T_{2h}$ ($\because s \in T_h = G_h \cap T, s \in G_h$ and $t_1 \in T_h \subset G_h$), since $[G_h, G_h] \subseteq G_{2h}$ and $[s^{-1}, t^{-1}] \in G_{2h}, T_{2h} = T \cap G_{2h}$. since $s, t_1 \in T_h = T \cap G_h$ where $s, t_1 \in T$ but T has the property $s^{-1}, t_1^{-1} \in T \Rightarrow [s^{-1}, t_1^{-1}] \in T$, hence $[s^{-1}, t_1^{-1}] \in T \cap G_{2h} = T_{2h}$.

$\therefore [s^{-1}, t_1^{-1}] \in T_{2h}$.

we can replace (s, t_1) in w by $(t_1, s, [s^{-1}, t_1^{-1}])$ so t_1 occurs before s.

So we do not alter the group element represented and we move t_1 one step towards the left at the cost of an extra term $[s^{-1}, t_1^{-1}]$). Note that we have not changed the degree in the $t_j 1 \leq j \leq l$. ($\because [s^{-1}, t_1^{-1}] \in T_{2h} \Rightarrow [s^{-1}, t_1^{-1}] \notin T_h \setminus T_{h+1}$). Moving t_1 all the way to the left therefore yields a new word w' such that $|w'| = |w|$, $deg_{t_j}(w') = deg_{t_j}(w')$ for $1 \leq j \leq l$ and such that the term of w' are those of w plus one extra term of the form $[u^{-1}, t_1^{-1}]$), for each u in w originally occurring to the left of our t_1. If $u \in T_k$ then $[u^{-1}, t_1^{-1}] \in T_{h+k}$.

$\because u \in T_k = T \cap G_k, u \in G_k, t_1^{-1} \in T_h = T \cap G_h[u^{-1}, t_1^{-1}] \in G_{h+k}, u, t \in T[u, t] \in T$ and $[u^{-1}, t_1^{-1}] \in T \cap G_{h+k} = T_{h+k}$). It follows that $\deg(w') \leq (d_h, ..., d_p) + (0, .., d_h, .., d_{p-h})$, Since $\tau : \mathbb{Z}^d \to \mathbb{Z}^d$

$\tau(d_h, ..., d_p) = (0, d_h, .., d_{p-1})$

$\tau^h(d_h, ..., d_p) = (0, ..., 0, d_h, .., d_{p-h})$, where first h coordinate are 0.

Also $I(d_h, ..., d_p) = (d_h, ..., d_p)$, where I is the identity map.

So

$$deg(w') \leq (d_h, ..., d_p) + (0, ..., d_h, ..., d_{p-h}) \leq (I + \tau^h)(d) \tag{3.3}$$

This is because $T_i \setminus T_{i+1}$ degree of w' is augmented over that of w by the terms $[u^{-1}, t^1]$ by at most d_{i-h} in number, where $u \in T_h \setminus T_{i-h+1}$. Put $a_j = deg_{t_j}(w)$. By the above procedure we first move all a_1 occurrences of t_1 to the left, then all a_2 occurrences of t_2, and a_l occurrences of t_l. The result will be a prenormalized word w_1 such that $|w_1| = |w|$ and $\deg(t_j(w_1) = a_j$ for $1 \leq j \leq l$. Moreover it follows from above that deg

$$\begin{aligned}(w_1) &\leq (I+\tau^h)(a_1)...(I+\tau^h)(a_l)(d)\\ &\leq (I+\tau^h)(d_h)d = d'\end{aligned}$$

($\because a_1 + a_2 + ... + a_l \leq d_h$) which proves the lemma's proof. Hence, we have a word w_1 which is prenormalized and $deg_{t_j}(w_1) = deg_{t_j}(w)$ and they represent the same word. i.e. $|w_1 rvert = |w|$.

Now, in order to normalize prenormalized words, for each $j = r_h + 1, r_h + 2, ...l$, we choose a word s_j in $\{t_1, ..., t_{r_h}\} \cup T_{h+1}$ representing t_j^N. Choose a constant $k > 0$ such that that deg $(s_j) \leq k = (k, k, ..., k)\ \forall j$. Now let w and w_1 be as in the previous lemma, $w_1 = (t_1, t_1, ..., t_1 .....t_l, ..t_l, v)$ is prenormalized, $a_j = deg_{t_j}(w)$ and $|w_1| = |w|$ for $r_h < j \leq l$, we divide a_j by N.
We may write $a_j = b_j N + c_j$ with $0 \leq c_j < N$. Then replace $(t_j, t_j, ..., t_j)$ in w_1 by $(s_j, s_j, ..., s_j, t_j, ..t_j)$ where b_j, c_j are the number of s_j and t_j copies for $r_h < j \leq l$ ($\because$ where $|s_j s_j ... s_j t_j ... t_j| = s_j^{b_j} t_j^{c_j}$ but s_j represent t_j^N. So, $|s_j s_j ... s_j t_j ... t_j| = t_j^{Nb_j + c_j} = t_j^{a_j}$. So the result is a new word w_2 with the following properties : $|w_2| = |w_1|$, and $deg_{t_j}(w_2) < N$ for $r_h < j \leq l$ and

$$\begin{aligned}deg(w_2) &\leq d' + (\sum_{r_h} < j \leq l b_j)k\\ &\leq d' + (\sum_{1\leq j\leq l} a_j)k\\ &\leq d' + d_h k\end{aligned}$$

Now if $e, e' \in \mathbb{Z}^q$, we denote $e \leq e'$, if $e_j \leq e'_j \forall j$. In this case, when $d_h \leq d_j$ for $j \geq h$.

$d_h k = (d_h k, d_h k, ..., d_h k)$

$kd = (kd_h, kd_{h+1}, ..., kd_p)$ since $d_h \leq d_j$ for $j \geq h$ and $kd_h \leq kd_j \forall j \geq h$ $\Rightarrow d_h k \leq kd$. Since $\tau^h(d)(0, ..., 0, d_h, .., d_{p-h})$

$(I+\tau^h)(d) = (d_h, ..., d_p) + (0, ..., d_h, ..., d_{p-h})$

$= (d_h, d_{h+1}, ..., d_{2h-1}, d_{h+h}, ..., d_{p+p-h})$
so, $d_h k \le kd \le (I+\tau^h)^{d_h}(kd)$ and since $d' = (I+\tau^h)^{d_h}(d)$, we have $d' + d_h k = (I+\tau^h)^{d_h}(d) + d_h k$

$\le (I+\tau^h)^{d_h}(d) + dk$

$\le (I+\tau^h)^{d_h}(d) + (I+\tau^h)^{d_h}(kd)$

$\le (1+k)(I+\tau^h)^{d_h}(d)$. We conclude therefore, if $d_j \ge d_h$ for $j \ge h$, then

$$deg(w_2) \le (1+k)(I+\tau^h)^{d_h}(d) = d"(say) \tag{3.4}$$

Next we again apply 3.0.31 to w_2 ,to obtain a new prenormalized word w_3 with the following properties: $|w_3| = |w_2| = |w_1| = |w|$, $deg_{t_j}(w_3) = deg_t(w) < N$ for $r_h < j \le l$. From the equation(4), $deg(w_3) \le (I+\tau^h)^{d"_h}(d") = d'''$. Note in particular that w_3 is normalized, then $d"_h = (1+k)d_h$ and so, $d''' = (1+k)(I+\tau^h)^{(2+k)d_h}(d)$.

$(\because deg(w_3) \le (I+\tau^h)^{(1+k)d_h}(d) \le (I+\tau^h)^{(1+k)d_h}(I+k)d_h \le (1+k)(I+\tau^h)^{(2+k)d_h}(d))$.
Then, we have shown that $w \in G_h(d)$, there exist $w_3 \in G'_h(d''')$ such that $|\ w_3| = |\ w|$, provided that $d_j \ge d_h$ for $j \ \ge \ h$.

One can say that, given $d = (d_h, .., d_p)\mathbb{Z}^q$ with that $d_j \ge d_h$ for $j \ge h$, we have

$$|G_h(d)| \subset |\ G'_h(e)\ |, wheree = (1+k)(I+\tau^h)^{(2+k)d_h}(d) \tag{3.5}$$

Now, let c be a positive constant and assume that $d = (cm^h, ..., cm^p)$ $(d_h = cm^h)$.
Put $M = (2+k)d_h = (2+k)cm^h$
Then, $e = (1+k)(I+\tau^h)^{(2+k)d_h}(d)$

$e = (1+k)(I+\tau^h)^M(d)$

$e = (1+k)(I+ \binom{M}{1}\ \tau^h + \binom{M}{2}\ \tau^{2h} + ...)(d)$

$[\because \binom{M}{1} = \frac{M!}{(M-1)!} = M, \binom{M}{j} = \frac{M!}{j!(M-j)!} = \frac{M(M-1)(M-2)...(M-(j-1))}{j!} \le \frac{M^j}{j!}]$

So, $e \le (1+k)(I + M\tau^h + \frac{M^2}{2!}\tau^{2h} + ...)(d)$ since, $\tau : \mathbb{Z}^q \to \mathbb{Z}^q$ $\tau(d) = (0, d_h, ..., d_{p-1})$ and therefore $\tau^h(d) = (0, 0, ...d_h, ..., d_{p-h})$ and $(\tau^h(d))_h = 0$, $(\tau^h(d))_{h+1} = d_h$ and similarly we have $(\tau^h(d))_{p-h} = d_{p-h}$. In general, $(\tau^h(d))_i = d_{i-h}$ for $h \ \le i \le p$. Then we have

$e \le (1+k)(I + M\tau^h + \frac{M^2}{2!}\tau^{2h} + ...)(d)$

$e_i \le (1+k)(d_i + Md_{i-h} + \frac{M^2}{2!}d_{i-2h} + ...)(d)$

the term $\frac{M^j}{j!}d_{i-jh}$ being understand to be zero if $i - jh < h$ and is otherwise equal to $\frac{1}{j!}[(2+k)cm^h]^j cm^{i-jh} = \frac{cm^i[(2+k)c]^j}{j!}$

$[\because \tau^h(d) = (0, , , 0, d_h, , , d_{p-h})$

$\frac{1}{j!}[(2+k)cm^h]^j cm^{i-jh} = \frac{1}{j!}[(2+k)c]^j m^{jh} cm^{i-jh}$

$= \frac{1}{j!}[(2+k)c]^j cm^i$

$= \frac{cm^i}{j!}[(2+k)c]^j$, and put $M = (2+k)cm^h]$. Then put $x = (2+k)c$, we have

$e_i \le (1+k)cm^i(1 + x + \frac{x^2}{2!} + ...)$

$\le (1+k)(ce^x)m^i$. This proves that if c is a constant $(c > 0)$ and if $d = c\delta$, $\delta = (m^h, ..., m^p)$, then

$$(1+k)(I+\tau^h)^{(2+k)d_h}(d) \le c'\delta, where c' = (1+k)ce^{(2+k)}c \tag{3.6}$$

It is just by looking at equation no.(3.5), Now from equation (3.5) and (3.6), we obtain

$$|G_h(cm^h, ..., cm^p)| \subset |G'_h(c'm^h, ..., c'm^p)| \tag{3.7}$$

and from equation (3.2), we have

$$Card|G'_h(c'm^h, ..., c'm^p)| \le A'_h P_{r_h}(c'm^h) Card|G_{h+1}(c'm^{h+1}, ...c'm^p)| \tag{3.8}$$

where A'_h is a positive constant. Now, we will prove our main result $\gamma_T(m) \le Q(m)$, just by using these result which mentioned in equations (3.2),(3.5),(3.6),(3.7) and induction.

Claim: There is a constant $A_h > 0$ such that given $c > 0$, there are constants $c_h, ..., c_p > 0$ such that

$$Card \mid G_h(cm^h, ..., cm^p) \mid \leq A_h \prod_{j \geq h} P_{r_j}(c_j m^j) \ \forall m \tag{3.9}$$

Since by equation (3.7), we have

$Card \mid G_h(cm^h, ..., cm^p) \mid \subset \mid G'_h(c'm^h, ..., c'm^p) \mid$ and from equation (3.8), we have $Card \mid G'_h(c'm^h, ..., c'm^p) \mid \leq A'_h P_{r_h}(c'm^h) Card \mid G_{h+1}(c'm^{h+1}, ...c'm^p \mid$. So, we obtain from these two equation; there are constants $A'_h > 0$ and c' such that

$$Card|G_h(cm^h, ..., cm^p)| \leq A'_h P_{r_h}(cm^h) Card \mid G_{h+1}(c'm^{h+1}, ...c'm^p \mid$$

if $h = p$, $A_p = A_h = A'_p c_p = c'$. In that case $A_h \prod_{j \geq p} P_{r_j}(c_j m^j) = A_p P_{r_p}(c_p m^p)$,

$$Card|G_p(cm^p)| \leq A'_P P_{r_p}(c'm^p) = A_p . P_{r_p}(c_p m^p)$$

Hence $h = p$ proves our claim. If $h < p$, then we apply induction to $h + 1$ and c' to obtain $A_{h+1} > 0$ and $c_{h+1}, ..., c_p > 0$ such that

$$Card|G_{h+1}(c'm^{h+1}, ..., c'm^p)| \leq A_{h+1} \prod_{j \geq h+1} P_{r_j}(c_j m^j)$$

Therefore, the claim follows by taking $A_h = A'_h . A_{h+1} c_h = c'$ and

$$\begin{aligned} Card|G_h(cm^h, ..., cm^p)| &\leq A'_h P_{r_h}(c'm^h) A_{h+1} \prod_{j \geq h+1} P_{r_j}(c_j m^j) \\ &\leq A'_h . A_{h+1} \prod_{j \geq h} P_{r_j}(c_j m^j) \end{aligned}$$

Call $A_h = A'_h A_{h+1}$ new constant. So, our claim is proved i.e. there is a constant $A_h > 0$ such that given $C > 0$, there are constants $c_h, ..., c_p > 0$ such that

$$Card|G_h(cm^h, ..., cm^p)| \leq A_h \prod_{j \geq h} P_{r_j}(c_j m^j) \forall m$$

To prove 3.0.30, it suffices to show that $\gamma_{T_h}(cm^h) \leq Card|(G_h(cm^h, ..., cm^p)|$. But this is clear, because each element of T_h length $\leq cm^h$ is represented by a word w in

T_h of length $\leq cm^h$ and evidently, $w \in G_h(cm^h, ..., cm^p)$. ($w \in G_h h \leq ... \leq p$ and $cm^h \leq cm^i h \leq i \leq p$ so,

$$deg_{T_h \setminus T_{h+1}}(w) \leq cm^h$$
$$deg(w) \leq cm^h$$
$$w \in G_h(cm^h, ..., cm^p)$$

So,

$$\gamma_{T_h}(cm^h) \leq Card|G_h(cm^h, ..., cm^p)|....eq(10) \tag{3.10}$$

Hence from (3.9) and (3.10), we have

$$\gamma_{T_h}(cm^h) \leq Card \mid G_h(cm^h, ..., cm^p) \mid \leq A_h \prod_{j \geq h} P_{r_j}(c_j m^j)$$
$$\gamma_T(cm^h) \leq A_h. \prod_{j \geq h} P_{r_j}(c_j m^j)$$

which proves the proposition 3.0.30. Now, $T_1 = T \cap G = T$

$$\gamma_T(m) = \mid \{g \in G : l_T(g) \leq m\} \mid$$

Claim: $\gamma_T(m) \leq \gamma_{T_h}(cm^h)$ so if $h = 1, m \leq cm, T = T_1$

$$\gamma_T(m) \leq \gamma_{T_1}(cm) \leq A_1. \prod_{j \geq h} P_{r_j}(c_j m^j)$$
$$\gamma_T(m) \leq A_1. \prod_{j \geq 1} P_{r_j}(c_j m^j)$$

Now, let $Q(m) = A_1. \prod_{j \geq 1} P_{r_j}(c_j m^j)$ be a polynomial of degree $\sum_{h \geq 1} hr_h = d(G)$. Then we have $\gamma_T(m) \leq Q(m)$, where $Q(m)$ is polynomial of degree $d(G)$, which completes the proof. Now, from first step of theorem 3.0.27, we have $P(m) \leq \gamma_T(m)$, where $P(m)$ is a polynomial of degree $d(G)$ and from second part, we have $\gamma_T(m) \leq Q(m)$. Hence $\gamma_T(m)$ is polynomial function. Hence we have our main result that if G is finitely-generated nilpotent group, then G has polynomial growth and degree of growth is $d(G)$, where $d(G) = \sum_{h \geq 1} hr_h$ and $r_h = rank(G_h/G_{h+1})$.

3.0.4 Classification of Growth type of finitely generated solvable groups

In this section, we will completely classify the growth types of finitely generated solvable groups by using the results in previous section. Let G be a finitely generated solvable group. Then G may have a exponential growth or not. Suppose G does not have exponential growth. Then by 3.0.24, G must be polycyclic. Now , if G is a finitely generated polycyclic group which does not have exponential growth, then by 3.0.21, G must be virtually nilpotent i.e. G has a nilpotent subgroup(say H) of finite index and $|G : H| < \infty$. We know that by Milnor-Svarc lemma [19, 91], H is finitely generated, G and H are quasi-isometric. So, H is finitely-generated nilpotent group. So by 3.0.27, H has polynomial growth. Now, since by 2.2.3, we know that Quasi-isometric groups have same growth type. So G and H have same growth type. Hence, G is of polynomial growth. i.e. if G is finitely generated solvable group and G is not of exponential growth then G must be of polynomial growth. So, we have classified the growth type of finitely generated solvable groups. Hence, the possible type of growth of a finitely generated solvable is either polynomial or exponential. Hence finitely generated solvable group can not have Intermediate growth.

Chapter 4

Groups of Polynomial growth

So far, we have seen that finitely generated nilpotent groups have polynomial growth, but we still don't have the complete answer for Milnor's question (What are the groups with polynomial growth?). In this section, we will answer this question in more generality. In 1981, M. Gromov completely classified the groups with polynomial growth and proved that if a finitely generated group has polynomial growth then it must have a nilpotent subgroup of finite index. In light of the previous result and Gromov's result, we have: *A finitely generated group has polynomial growth if and only if it is virtually nilpotent.* In this section we will prove our major theorem namely Gromov's theorem:

Theorem 4.0.32 ***(Gromov's)*** *[4] Let G be a finitely generated group of polynomial growth, then G has a nilpotent subgroup of finite index.*

We know that we have a metric space associated with any finitely generated group. Gromov's idea was to construct a sequence (X_n) of metric space such that distance between two points in X_{n+1} is closer than the distance between the same points in X_n, and then he constructed a limit space of that sequence, called the asymptotic cones(in which two points are too close). Not only did he define that space, he also gave a very nice action of a group G on that space X and deduced many interesting properties of the group. In particular if the limiting space is nice (homogenous, path-connected, locally connected, complete, finite dimensional , locally compact) and our group G has polynomial growth then from that action we can deduce that G is virtually nilpotent.

This proof involves techniques of non standard analysis namely filters, ultrafilters, ultraproduct, asymptotic cone etc. and it stimulated a lot of activity in different areas of mathematics. His proof used the idea of the limit of a sequence of metric spaces, as well as Montgomery and Zippin's solution of Hilbert's 5^{th} problem[11] and Tits Alternative[15].

Later on, there are various proofs given by many people namely Van den Dries and Wilkies in 1984, who used the same approach but a slightly improved version, and then by Bruce Kleiner in 2010, whose proof relies on harmonic analysis without using Zippin's solution of Hilbert 5^{th} problem. Y. Shalom and Terrence.Tao in 2010 gave another proof which also depends harmonic analysis. Here, I present the proof of Gromov's which uses the theory of Asymptotic cones.

4.0.5 Asymptotic cone of a finitely generated group

Let's start with the definitions of filters, ultrafilters etc,

Definition 4.0.33 *Let S be any non-empty set. A filter on S is a family $\mathcal{F}$ of subsets of S with the following properties:*
(i) $\emptyset \notin \mathcal{F}$
(ii) if $A, B \in \mathcal{F}$ then $A \cap B \in \mathcal{F}$ (closed under intersection)
(iii) if $A \in \mathcal{F}$ and $A \subseteq B$ then $B \in \mathcal{F}$ (closed under superset inclusion).

Example 4.0.34 *Let $S = \{1, 2, 3\}$. Consider $\mathcal{F}_1 = \{\{1\}, \{1, 2\}, \{1, 2, 3\}, \{1, 3\}\}$ is a filter on S but $\mathcal{U} = \{\{1\}, \{2\}, \{3\}, \{1, 2\}, \{2, 3\}, \{1, 3\}, \{1, 2, 3\}\}$ is not a filter on S because $\{1\} \cap \{2\} = \emptyset$.*

Observation 4.0.35 *1. Filter can not contain two disjoints subsets.*
2. Filter always contains at least one element (namely set itself).
3. Union of two filters need not be a filter on S. Take $\mathcal{F}_2 = \{\{2\}, \{1, 2\}, \{2, 3\}, \{1, 2, 3\}\}$ and $\mathcal{F}_3 = \{\{3\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$, and $\mathcal{F}_2 \cup \mathcal{F}_3 = \{\{2\}, \{3\}, \{1, 2\}, \{2, 3\}, \{1, 3\}, \{1, 2, 3\}\}$ is not a filter on S.
4. Symmetric difference of two filters need not be a filter.
Consider $\mathcal{F}_2 \triangle \mathcal{F}_3 = \{\{2\}, \{3\}, \{1, 2\}, \{1, 3\}\}$ is not a filter.

Proposition 4.0.36 *The Intersection of two filters on a set S is always a filter on a set S.*

Proof: Let $\mathcal{F}', \mathcal{F}''$ be two filters on S. Since, $S \in \mathcal{F}', \mathcal{F}'' \Rightarrow S \in \mathcal{F}' \cap \mathcal{F}''$. i.e. $\mathcal{F}' \cap ''$ is a non-empty set. Also, $\emptyset$ does not belongs to both so $\emptyset \notin \mathcal{F}' \cap \mathcal{F}''$. Let $A, B \in \mathcal{F}' \cap \mathcal{F}'' \Rightarrow A, B \in \mathcal{F}', \mathcal{F}'' \Rightarrow A \cap B \in \mathcal{F}', \mathcal{F}''$ and hence $A \cap B \in \mathcal{F}' \cap \mathcal{F}''$. Suppose $A \in \mathcal{F}' \cap \mathcal{F}''$ and $A \subseteq B$, since $A \in \mathcal{F}' \Rightarrow B \in \mathcal{F}'$ and similarly we have $A \in \mathcal{F}'' \Rightarrow B \in \mathcal{F}''$ and hence we get $B \in \mathcal{F}' \cap \mathcal{F}''$. Thus, $\mathcal{F}' \cap \mathcal{F}''$ is a filter on S.

Definition 4.0.37 *A maximal filter on a set S is called an ultrafilter.*

Example 4.0.38 *$\mathcal{F}_1, \mathcal{F}_2$ and $\mathcal{F}_3$ are ultrafilters on $S = \{1, 2, 3\}$ but $\mathcal{S} = \{\{1, 2, 3\}\}$ is not an ultrafilter on S($\mathcal{S} \subset \mathcal{F}_1$).*

We have seen in the above example that ultrafilter on a set is not unique.

Definition 4.0.39 *The family of all subsets of S containing a fixed element $s \in S$, is termed as a principal filter.*

Remark 4.0.40 *Our definition of principal ultrafilter demands that the set of all subsets containing a particular element forms a filter. Infact, we can easily prove that this set forms a filter and indeed an ultrafilter.*

Example 4.0.41 *Consider the all subsets of $S = \{1, 2, 3\}$ which contains 1 say $\mathcal{F}_1 = \{\{1\}, \{1, 2\}, \{1, 2, 3\}, \{1, 3\}\}$. Similarly we can define $\mathcal{F}_i$ for $i = 1, 2, 3$. and these are all examples of principal filters on S.*

It is clear that the set of all subsets containing a particular element $s \in S$ forms a filter say $\mathcal{F}_s$. Now we will prove that it is indeed an ultrafilter on S.
Suppose $\mathcal{F}_s$ is not an ultrafilter on S i.e. there exist a filter $\mathcal{Y}$ which contains $\mathcal{F}_s$ as a proper subset i.e. $\exists\, A \in \mathcal{Y}$ such that $A \notin \mathcal{F}_s$ but by the definition of $\mathcal{F}_s$, $s \notin A$ and since $\{s\} \in \mathcal{F}_s \subset \mathcal{Y} \Rightarrow \{s\} \cap A = \emptyset$, which contradicts that $\mathcal{Y}$ is a filter on S. Hence, $\mathcal{F}_s$ is an ultrafilter on a set S.

Now, we have seen that all principal filters on a set S are ultrafilters but the natural question arises that whether the converse holds? We will see in the next proposition, that converse holds if S is a finite set.

Proposition 4.0.42 *If S is a finite set, then all ultrafilters are of principal type.*

Proof: L.et $\mathcal{F}$ be an ultrafilter on $S = \{a_1, a_2, .., a_n\}$, then certainly $S \in \mathcal{F}$. Consider a set T is the set of all those subsets of S which contains a_i, where $a_i \in T = \bigcap_{J \in \mathcal{F}} J$ since T is non-empty so we can pick some $a_i \in T$ and consider the filter $\mathcal{F}_{a_i}$, the set of all subsets of S which contains a_i. Consider $\mathcal{F}_{a_i} \cup T$. First we will prove that $\mathcal{F}_{a_i} \cup T$ is a filter. Clearly $\emptyset \notin \mathcal{F}_{a_i} \cup T$. If $A \in \mathcal{F}_{a_i} \cup T$ and $A \subseteq B$, if

$A \in \mathcal{F} \Rightarrow B \in \mathcal{F} \Rightarrow B \in \mathcal{F}_{a_i} \cup T$ and similarly if $B \in \mathcal{T} \Rightarrow B \in B \in \mathcal{F}_{a_i} \cup T$ and if $A, B \in \mathcal{F}_{a_i} \cup T$. Since $a_i \in A, B \Rightarrow a_i \in A \cap B$ and $\mathcal{T}$ contains all those subsets which contains $a_i \in \mathcal{T}$ so, $A \cap B \in \mathcal{T} \subseteq \mathcal{F}_{a_i} \cup T$. So $\mathcal{F}_{a_i} \cup T$ is filter on S. But since $\mathcal{F}_{a_i} \subseteq \mathcal{F}_{a_i} \cup T$ and $\mathcal{F}_{a_i}$ is an ultrafilter on S so we have $\mathcal{F}_{a_i} \subseteq \mathcal{F}_{a_i} \cup T = \mathcal{F}_{a_i} \Rightarrow \mathcal{T} \subseteq \mathcal{F}_{a_i}$ and since $\mathcal{F}_{a_i}$ is principal ultrafilter and so we get $\mathcal{T} = \mathcal{F}_{a_i}$.

Now, if $S = \{a_1, a_2, ..., a_n\}$, then all ultrafilters on S are of the form $\mathcal{F}_{a_i}$ for $i = 1, 2, ..., n$ and these are the only n ultrafilters on S but if S is an infinite set then it is possible for ultrafilter to be non-principal.

Example 4.0.43 *If S is an infinite set, then the family of all cofinite sets is a filter.*

Consider $\mathcal{F} = \{A \in P(S) \mid A = B^c$, where B is a finite set$\}$. Clearly $\emptyset \notin \mathcal{F}$ because $\emptyset^c = S$ is not finite set. Now, if $A, B \in \mathcal{F}, i.e. A = A_1^c, B = B_1^c$, where $\mid A_1 \mid < \infty$ and $\mid B_1 \mid < \infty$, then $A \cap B = A_1^c \cap B_1^c = (A_1 \cup B_1)^c$ and since A_1, B_1 are finite set so is $A_1 \cup B_1$, therefore $A \cap B \in \mathcal{F}$, and if $A \in \mathcal{F}$, $A \subseteq C$ for some $C \in P(S)$ then since we have $A = A_1^c$ where $\mid A_1 \mid < \infty$, so $A_1^c \subseteq C \Rightarrow A_1 \supseteq C^c$ since A_1 is finite and so is $C^c \Rightarrow C \in \mathcal{F}$. Hence, $\mathcal{F}$ is a filter on S and this filter is called the *cofinite filter.* $\square$

Now we will construct a non-principal ultrafilter on the infinite set S. Now consider $\mathcal{A} = \{\mathcal{U} \mid \mathcal{U}$ is a filter on S s.t. $\mathcal{F} \subseteq \mathcal{U}$, where $\mathcal{F}$ is the cofinite filter on $S\}$. Since the cofinite filter $\mathcal{F} \in \mathcal{A}$, $\mathcal{A}$ is a non-empty set. Let's define an ordering on $\mathcal{A}$ as $\mathcal{U}_1 \leq \mathcal{U}_2$ if $\mathcal{U}_1 \subseteq \mathcal{U}_2$. It is clear that $\mathcal{A}$, with this ordering becomes a partially ordered set. Let $\mathcal{S}$ be a partial ordered subset of $\mathcal{A}$ and take $X = \bigcup_{\mathcal{U} \in \mathcal{S}} \mathcal{U}$, which is a filter on S and it contains the cofinite filter $\mathcal{F}$ i.e. $\mathcal{F} \subseteq X$. So, $\mathcal{S}$ satisfies the condition of Zorn's lemma and hence $\mathcal{S}$ has a maximal element say $\mathcal{Z}$, which is filter on S containing $\mathcal{F}$. Since $\mathcal{Z}$ is a maximal filter on S, it is an ultrafilter. But $\mathcal{Z}$ cannot be a principal filter, otherwise there exists $s \in S$ such that $\{s\} \in \mathcal{Z}$ and since $\mathcal{F} \subseteq \mathcal{Z}$, $(\{s\})^c \in \mathcal{F}$, $\{s\}^c \in \mathcal{Z}$ it follows that $\{s\} \cap (\{s\})^c = \emptyset$, which is a contradiction. Hence, $\mathcal{Z}$ is a *non-principal ultrafilter* on S.

Remark 4.0.44 *The above result guarantees only the existential part of such a filter,* *but we don't have any explicit non-principal ultrafilter on infinite set, not even an explicit construction of any non-principal ultrafilter is known.*

Lemma 4.0.45 *If $\mathcal{U}$ is a family of non-empty subsets of S which have finite intersection property, then $\mathcal{U}$ is contained in some filter on S.*

Proof: Consider $\mathcal{F} = \{B \subseteq P(S) \mid B \supseteq \bigcap_{i=1}^{n} A_i$ for some $n \in \mathbb{N}$ and for some $A_i \in \mathcal{U}\}$. Clearly, any finite intersection of members of $\mathcal{U}$ is non-empty. So, the sets containing these intersection are also non-empty and therefore $\emptyset \notin \mathcal{F}$. If $A, B \in \mathcal{F}$ i.e. $A \supseteq \bigcap_{i=1}^{n} C_i$ for some $C_i \in \mathcal{U}$ and $B \supseteq \bigcap_{i=1}^{m} D_i$ for some $D_i \in \mathcal{U}$, then $A \cap B \supseteq (\bigcap_{i=1}^{n} C_i) \cap (\bigcap_{i=1}^{m} D_i)$. Also, if $A \in \mathcal{F}$ and $A \subseteq B$ then $B \supseteq A \supseteq \bigcap_{i=1}^{n} E_i$ for some $E_i \in \mathcal{U}$. Therefore, $B \in \mathcal{F}$. Hence, $\mathcal{F}$ is a filter containing $\mathcal{U}$. $\square$

Roughly speaking, a filter contains all large subsets and an ultrafilter divide the set into large and colarge sets.

Proposition 4.0.46 *A filter is an ultrafilter if and only if it satisfiesthe following whenever $A \subseteq S$, then either A or the complement $S - A$ is in $\mathcal{F}$.*

Proof: Assume that for any $A \subseteq S$, either A or $S - A$ is in $\mathcal{F}$, but $\mathcal{F}$ is not an ultrafilter i.e. $\exists$ another filter $\mathcal{F}'$ such that $\mathcal{F} \subseteq \mathcal{F}'$, i.e. $\exists$ some $B \in \mathcal{F}'$ such that $B \notin \mathcal{F}$ but by given condition $S \setminus B \in \mathcal{F} \subseteq \mathcal{F}'$ which implies that $B \cap (S \setminus B) = \emptyset$, a contradiction. So $\mathcal{F}$ is an ultrafilter. Conversely, suppose if $\mathcal{F}$ is an ultrafilter. Let $A \subseteq S$. If $A \in \mathcal{F}$, then we are done. So suppose $A \notin \mathcal{F}$. Then $\mathcal{F} \cup A$ can not be filter because $\mathcal{F}$ is an ultrafilter. So $\mathcal{F} \cup A$ can not have finite intersection property, because if it had, then it would be contained in some filter which would contradict the maximality of $\mathcal{F}$. So $\exists\, C \subseteq \mathcal{F}$ such that $A \cap C = \emptyset$ which implies that $C \subseteq S \setminus A$ ($\because C \in \mathcal{F}$) it follows that $S \setminus A \in \mathcal{F}$, which completes the proof. $\square$

Proposition 4.0.47 *Let $\mathcal{F}$ be an ultrafilter with $T \in \mathcal{F}$ and $T = A_1 \cup A_2 \cup ... \cup A_n$. Then $A_i \in \mathcal{F}$ for some $i \in \{1, 2, .., n\}$.*

Proof: Let $T \in \mathcal{F}$, where $\mathcal{F}$ is an ultrafilter and $T = A_1 \cup A_2 \cup ... \cup A_n$. Suppose $A_i \notin \mathcal{F}$ for any $1 \leq i \leq n$. Then $(A_i)^c \in \mathcal{F}$ (by Prop) $\Rightarrow T^c = (A_1)^c \cap (A_2)^c \cap ... \cap (A_n)^c \in \mathcal{F}$. This implies that $T, T^c \in \mathcal{F}$, which is not possible.

Roughly speaking, last two propositions say that every element of an ultrafilter is either a large set or its complement is a large set, and we can not write a large set as a union of colarge sets.

Lemma 4.0.48 *Cofinite filter on an infinte set S is the intersection of all non-principal ultrafilters on S.*

Proof: Let $\mathcal{F}$ be a cofinite filter and let $\mathcal{F}_\alpha$ be any non-principal ultrafilter on S. Let $x \in S$ such that $\{x\} \notin \mathcal{F}_\alpha$ ($\because \mathcal{F}_\alpha$ is non-principal). Then $S \setminus \{x\} \in \mathcal{F}_\alpha \; \forall \alpha \in \triangle$. Let F be any finite subset of S say $F = \{x_1, x_2, ..., x_n\}$ and we have $S \setminus F = \bigcap_{i=1}^{n} S \setminus \{x_i\} \in \mathcal{F}_\alpha \; \forall \alpha \in \triangle$ so, $\mathcal{F} \subseteq \mathcal{F}_\alpha \; \forall \alpha \in \triangle \Rightarrow \mathcal{F} \subseteq \bigcap_{\alpha \in \triangle} \mathcal{F}_\alpha$.
Converse is easy to check. □

Now, we are going to define some notions of limit in the sense of filter. We now fix a non-principal ultrafilter $\mathcal{F}$ on $\mathbb{N}$. Let T be any topological space and let $\{x_n\}$ be a sequence in T. For each $x \in T$, and each neigbhourhood U of x, we write $O(x, U) = \{n \in \mathbb{N} : x_n \in U\}$.

Definition 4.0.49 *We say x is the $\mathcal{F}$-limit of the sequence $\{x_n\}$, if for each neighbourhood U of x, the subset $O(x, U) \in \mathcal{F}$. Then we write $x = \mathcal{F} \lim x_n$*

Remark 4.0.50 *This notion of $\mathcal{F}$-limit is not arbitrary, but it has familiarity with the notion of convergence in real analysis sense. In real analysis, a sequence $y_n \to y$ if for any small neighbourhood containing y, almost(except finite) all of x_n lie in that neighbourhood. We say y_n converge to y. We have the same analogy here, i.e. for any neighbourhood U of y, if almost (belongs to $\mathcal{F}$ i.e large set) all the terms of x_n belong that neighbourhood, then we say $x = \mathcal{F}lim\ x_n$.*

Proposition 4.0.51 *Let x_n be a sequence in $\mathbb{R}$. Then x_n convergent to x if and only if $x = \mathcal{F}limx_n$ for all non-principal ultrafilter $\mathcal{F}$ on $\mathbb{N}$.*

Proof: Let $\mathcal{F}$ be any non-principal ultrafilter on $\mathbb{N}$ and suppose x_n converges to x in the real analysis sense. Then for any neighbourhood U of x, $\exists\, m \in \mathbb{N}$ such that

$x_n \in U$ for all $n \geq m$ i.e. $O(x,U) = \{m, m+1, m+2, ...\} = (\{1,2,..m-1\})^c$ is a cofinite set and since the cofinite filter is contained in every non-principal ultrafilter on $\mathbb{N}$, $O(x,U) \in \mathcal{F}$. Hence $x = \mathcal{F}$ lim x_n.

Conversely, let $x = \mathcal{F}_\alpha$lim x_n for all $\alpha \in \triangle$. Then for any neighbourhood U_α of x we have $O(x,U_\alpha) = \{n \in \mathbb{N} : x_n \in U_\alpha\} \in \mathcal{F}_\alpha$. Suppose x_n does not converge to x in the real analysis sense i.e. $\exists$ a neighbourhood U_0 of x such that for any $n_0 \in \mathbb{N}$, $\exists m \in \mathbb{N}$ such that $x_m \notin U_0$ for $m > n_0$(similarly we can choose some integer after m). So we will have infinitely many integers j such that $x_j \notin U_0$. Consider $O(x,U_0) = \{n \in \mathbb{N} \mid x_n \in U_0\} \in \mathcal{F} \Rightarrow \mathbb{N} \setminus S' \in \mathcal{F}$ where S' is an infinite set of $\mathbb{N}$, but by 4.0.48, for a cofinite filter on $\mathcal{F} = \bigcap_{\alpha \in \triangle} \mathcal{F}_\alpha$, where $\mathcal{F}_\alpha$ are non-principal ultrafilters. So $\mathbb{N} \setminus S' \in \mathcal{F}_\alpha \, \forall \alpha \in \triangle \Rightarrow \mathbb{N} \setminus S' \in \bigcap_{\alpha \in \triangle} \mathcal{F}_\alpha \Rightarrow \mathbb{N} \setminus S' \in \mathcal{F} \Rightarrow S'$ must be finite, which is a contradiction. Therefore x_n converges to x in real analysis sense. □

Proposition 4.0.52 *1).If T is a Hausdorff space, the $\mathcal{F}-$limit is unique.*
2). If T is compact, then each sequence $\mathcal{F}-$converges.

Proof: 1). Let $x, y \in T$ be two $\mathcal{F}$-limit of a sequence x_n. Since T is Hausdorff space, there exist disjoint open sets U_x and U_y containing x and y respectively. Since $x = \mathcal{F}$lim x_n, $O(x,U_x) = \{n : x_n \in U_x\} \in \mathcal{F}$ and similarly for y, we have $O(y,U_y) = \{n : x_n \in U_y\} \in \mathcal{F}$ but $O(x,U_x)$ and $O(y,U_y)$ are disjoint elements of $\mathcal{F}$, which gives us a contradiction. Hence $\mathcal{F}$-limit is unique.
2). Suppose there exists a sequence $\{x_n\}$ that does not converge to any point $x \in T$, i.e. for each x $\in T$ there exists a neighbourhood U_x of x , such that $O(x,U_x) \notin \mathcal{F}$. Then $O^*(x,U_x) = \{n : x_n \notin U_x\} \in \mathcal{F}$. Since $\{U_x : x \in T\}$ is a cover of T and since T is compact, there exists finitely many $x_i \in T$ for $1 \leq i \leq n$ such that $\{U_{x_i} : 1 \leq i \leq n\}$ covers T i.e. Consider $Y = \bigcap_{i=1}^{n} O^*(x_i, U_{x_i})$, so Y is non-empty and hence there exist $j \in \mathbb{N}$ such that such that $x_j \notin U_{x_i}$ for $1 \leq i \leq n$, which contradicts to the fact $\{U_{x_i} : 1 \leq i \leq n\}$ is a finite cover of T. Hence, each sequence $\mathcal{F}$- converges. □

Corollary 4.0.53 *Any bounded sequence of real numbers $\mathcal{F}$-converges and its $\mathcal{F}-$limit is unique.*

Proof: Let x_n be a real bounded sequence i.e. $x_n \in [m, M]$ for some $m, M \in \mathbb{R}$. Since $[m, M]$ is a compact Hausdorff space and by above proposition, we get x_n

converges to a unique point. $\square$

There are certain properties which is very easy to prove.

Proposition 4.0.54 *Let x_n and y_n be two bounded real sequences, and c be a real number:*
a). $\mathcal{F}lim(x_n + y_n) = \mathcal{F}lim(x_n) + \mathcal{F}lim(y_n)$
b). $\mathcal{F}lim(cx_n) = c\mathcal{F}lim(y_n)$
c). If $x_n \leq y_n$ for all n, then $\mathcal{F}lim(x_n) \leq \mathcal{F}lim(y_n)$.

We are now heading to define Asymptotic cone. So we now consider a metric space (T, d_T) and fix some base point $e \in T$. Let $\mathcal{F}$ be a non-principal ultrafilter on $\mathbb{N}$.

Definition 4.0.55 *A sequence $\{x_n\} \in T$ is said to be moderate if it satisfies $d(x_n, e) \leq A.n$ for some constant A.*

Example 4.0.56 *Let $\mathbb{R}$ be a Euclidean metric space with distance d and base point $e = 0$. Consider $x_n = \frac{1}{n}$, we have $d(x_n, 0) = |\frac{1}{n} - 0| \leq 1 \leq 1.n$ (choose $A = 1$). More generally, this sequence is moderate with respect to any point $e \in \mathbb{R}$. Take $y_n = n$, and $d(y_n, 0) = |n - 0| \leq 1.n$ and hence $\{y_n\}$ is also a moderate sequence, But if we take $z_n = n^2$ then $d(z_n, 0) = n^2$ and there does not exist any constant $A \in \mathbb{R}$ such that $n^2 \leq A.n$ holds for all $n \in \mathbb{N}$. Hence $\{z_n\}$ is not a moderate sequence.*

Remark 4.0.57 *we observed that a moderate sequence does not mean that it cannot go to infinity, it can but in a very controlled manner.*

Let M denote the set of all moderate sequences in T. So given two moderate sequences $\alpha = \{x_n\}$ and $\beta = \{y_n\}$ we define the distance between them is as :

$$d(\alpha, \beta) = \mathcal{F}lim(\frac{d_T(x_n, y_n)}{n})$$

Take $T = \mathbb{R}$ with Euclidean metric space and $e = 0$ and $\mathcal{F}$ be a non-principal ultrafilter on $\mathbb{N}$. Let $\alpha = \{x_n\} = \{n\}$ and $\beta = \{y_n\} = \{n + 1\}$, then

$$d(\alpha, \beta) = \mathcal{F}lim(\frac{d_T(x_n, y_n)}{n}) = \mathcal{F}lim(\frac{d_T(n, n + 1)}{n}) = \mathcal{F}lim(\frac{1}{n})$$

and since 0 is the limit of $\frac{1}{n}$ in the real analysis sense, by 4.0.51, we have $0 = \mathcal{F}\text{lim}(\frac{1}{n}$, it follows that $d(\alpha, \beta) = 0$. So it is possible to have two different moderate sequences which are zero distance apart. Now we can define a relation on M for α, $\beta \in M$, we say $\alpha \sim \beta$ (equivalent) if $d(\alpha, \beta) = 0$. We can easily show that $\sim$ is an equivalence relation. Clearly, it is reflexive, and suppose α and β are represented by $\{x_n\}$ and $\{y_n\}$ respectively, then

$$d(\alpha, \beta) = \mathcal{F}lim(\frac{d_T(x_n, y_n)}{n}) = \mathcal{F}lim(\frac{d_T(y_n, x_n)}{n}) = d(\beta, \alpha)$$

and if $\gamma \in M$, represented by $\{z_n\}$, is another moderate sequence, then if

$$\alpha \sim \beta \Rightarrow d(\alpha, \beta) = \mathcal{F}lim(\frac{d_T(x_n, y_n)}{n}) = 0$$

and $\beta \sim \gamma \Rightarrow d(\beta, \gamma) = \mathcal{F}\mathrm{lim}(\frac{d_T(y_n, z_n)}{n}) = 0$, then

$$d_T(x_n, z_n) \leq d_T(x_n, y_n) + d_T(y_n, z_n)$$

and we have

$$\begin{aligned} &\frac{d_T(x_n, z_n)}{n} \leq \frac{d_T(x_n, y_n)}{n} + \frac{d_T(y_n, z_n)}{n} \\ &\Rightarrow \mathcal{F}lim\frac{d_T(x_n, z_n)}{n} \leq \mathcal{F}lim\frac{d_T(x_n, y_n)}{n} + \mathcal{F}lim\frac{d_T(y_n, z_n)}{n} = 0 + 0 = 0 \end{aligned}$$

Hence $\alpha \sim \gamma$. Therefore, $\sim$ is an equivalence relation on M and it divides the set M into disjoint equivalence classes. Let K denote the set of all equivalence classes of M and now we can define a distance on the elements of K as

$$d([\alpha], [\beta]) = \mathcal{F}lim(\frac{d_T(x_n, y_n)}{n})$$

First, we will prove that this notion of distance does not depend upon the choice of representatives. Let $\alpha \sim \alpha_1$ and $\beta \sim \beta_1$ i.e. $d(\alpha, \alpha_1) = 0$ and $d(\beta, \beta_1) = 0$. Then,

$$d(\alpha, \beta) \leq d(\alpha, \alpha_1) + d(\alpha_1, \beta_1) + d(\beta_1, \beta) \leq 0 + d(\alpha_1, \beta_1) + 0 = d(\alpha_1, \beta_1)$$

Similarly, if we change the role of α by α_1 and β by β_1, we will have $d(\alpha_1, \beta_1) \leq d(\alpha, \beta)$. Therefore, we get $d(\alpha, \beta) = d(\alpha_1, \beta_1)$. Since the distance d on M is metric so this is also a metric on K.

The space K with this distance d is called an *Asymptotic cone* of (T, d_T) with base point $e \in T$.

Definition 4.0.58 *Let $\mathcal{F}$ be a filter on S, and let A be any set. Consider the set $A^S = \{f : f \text{ is function from } S \text{ to } A\}$. Two functions f, g are said to be related($f \sim g$) (or almost equal) if the set $\{s : f(s) = g(s)\} \in \mathcal{F}$. Then the set of equivalence classes, $A^S/\sim$ is called the reduced power of A mod $\mathcal{F}$, and if $\mathcal{F}$ is an ultrafilter, we call it the reduced power set to be an ultraproduct.*

In particular, if $S = \mathbb{N}$, and $A = \mathbb{R}$, then two sequence $\alpha = \{x_n\}$ and $\beta = \{y_n\}$ represent the same element in ultraproduct if $\{n \in \mathbb{N} : x_n = y_n\} \in \mathcal{F}$. In other words,

$$d(\alpha, \beta) = \mathcal{F}lim \frac{d_T(x_n, y_n)}{n} = 0$$

because if

$$X = \{n \in \mathbb{N} : x_n = y_n\}, \quad Y = \{n \in \mathbb{N} : d(x_n, y_n) = 0\}$$

then $X \subseteq Y$ and $X \in \mathcal{F}$, therefore $Y \in \mathcal{F}$ and hence $d(\alpha, \beta) = 0$. It says that if we change the elements of a sequence $\{x_n\}$ on a set $B \notin \mathcal{F}$, then its equivalence class does not change in Asymptotic cone K.

Now, we will define the asymptotic cone of a finitely generated group. Let G be a finitely generated group and S be a finite set of generators. Let (G, d_S) be a metric space, where d_S is the word metric on G and take the identity $e \in G$ as the base point of the space and let $\mathcal{F}$ be a non-principal ultrafilter on $\mathbb{N}$. Then the space K obtained from the metric space (G, d_S) is called the *asymptotic cone* of a finitely generated group G.

Let $x_n = s$ be a constant sequence of in $G =< S >$, where S is finite set and $s \in S$. Then

$$d(x_n, e) = \mathcal{F}lim(\frac{d(x_n, e}{n}) = \mathcal{F}lim(\frac{l(s)}{n}) = \mathcal{F}lim(\frac{1}{n}) = 0$$

Now take $G = \mathbb{F}_2$, the free group of rank 2 and $S = \{a, b\}$. Consider $x_n = a^n$ and $y_n = e$ (constant sequence). Then

$$d(x_n, y_n) = \mathcal{F}lim(\frac{d(x_n, y_n)}{n}) = \mathcal{F}lim(\frac{d(a^n, e)}{n}) = \mathcal{F}lim(\frac{l(a^n)}{n}) = \mathcal{F}lim(\frac{n}{n}) = \mathcal{F}lim(\frac{1}{n}) = 0$$

So the sequence x_n and y_n represent the same element in the asymptotic cone.

First, we can observe that the word metric on G depends upon the chosen set of generators and so the asymptotic cone of a finitely generated group G depends upon the chosen generators. But we will prove in the next proposition that geometry of the space is independent of the choice of generating set.

Proposition 4.0.59 *Let G be a finitely generated group and S_1 and S_2 be two finite generating sets of G and let $\mathcal{F}$ be non-principal ultrafilter on $\mathcal{N}$. Let K_1 and K_2 be two asymptotic cones of G with respect S_1 and S_2 respectively. Then K_1 and K_2 are quasi-isometric.*

Proof: We need to define a map

$$f : (K_1, d_1) \to (K_2, d_2)$$

such that

$$\frac{-1}{A} d_1(\alpha, \beta) - B \leq d_2(f(\alpha), f(\beta) \leq A d_1(\alpha, \beta) + B$$

for some constant $A, B \in \mathbb{R}$ with $A \neq 0, \forall \alpha, \beta \in K1$.

Let d_{S_1} and d_{S_2} be the word metrics on G corresponding to S_1 and S_1 respectively. So the space (G, d_{S_1}) and (G, d_{S_2}) are quasi isometric i.e. $\exists$ and quasi-isometry $\phi : (G, d_{S_1}) \to (G, d_{S_2})$ such that we have $\frac{-1}{A} d_{S_1}(x, y) - B \leq d_{S_2}(\phi(x), \phi(y)) \leq A d_{S_1}(x, y) + B$ for some constant $A, B \in \mathbb{R}$ with $A \neq 0$ for all $x, y \in G$. If α and β are represented by $\{x_n\}$ and $\{y_n\}$ then we have

$$\frac{-1}{A} d_{S_1}(x_n, y_n) - B \leq d_{S_2}(\phi(x_n), \phi(y_n)) \leq A d_{S_1}(x_n, y_n) + B$$

for some constants $A, B \in \mathbb{R}$ with $A \neq 0$ for all $x_n, y_n \in G$

$$\Rightarrow \frac{-1}{A} \frac{d_{S_1}(x_n, y_n)}{n} - \frac{B}{n} \leq \frac{d_{S_2}(\phi(x_n), \phi(y_n))}{n} \leq A \frac{d_{S_1}(x_n, y_n)}{n} + \frac{B}{n} \forall n \in \mathbb{N}$$

$$\Rightarrow \mathcal{F}lim(\frac{-1}{A} \frac{d_{S_1}(x_n, y_n)}{n} - \frac{B}{n}) \leq \mathcal{F}lim(\frac{d_{S_2}(\phi(x_n), \phi(y_n))}{n}) \leq \mathcal{F}lim(A \frac{d_{S_1}(x_n, y_n)}{n} + \frac{B}{n}) \forall n \in \mathbb{N} \Rightarrow \frac{-1}{A} \mathcal{F}$$
$$\Rightarrow \frac{-1}{A} \mathcal{F}lim(\frac{d_{S_1}(x_n, y_n)}{n}) \leq \mathcal{F}lim(\frac{d_{S_2}(\phi(x_n), \phi(y_n))}{n}) \leq A \mathcal{F}lim(\frac{d_{S_1}(x_n, y_n)}{n}) \forall n \in \mathbb{N} (\because \mathcal{F}lim(\frac{1}{n}) = 0)$$
$$\Rightarrow \frac{-1}{A} d_1(\alpha, \beta) \leq d_2(f(\alpha), f(\beta) \leq A d_1(\alpha, \beta).$$

Definition 4.0.60 *A homogeneous space for a group G is a non-empty topological space X on which G acts transitively. Elements of G are called the symmetries of X.*

Now we will see that G acts on K by isomteries.

Define, $G \times K \to K$ by $(g, \alpha) = g\alpha$ where $\alpha = \{x_n\}$, $g\alpha = \{gx_n\}$. This is clearly a group action and it induces a homomorphism

$$\phi_g : K \to K$$

by $\phi_g(\alpha) = g\alpha$.

Now,

$$d_1(\phi_g(\alpha), \phi_g(\beta)) = d_1(g\alpha, g\beta) = \mathcal{F}lim(\frac{d(gx_n, gy_n)}{n}) = \mathcal{F}lim(\frac{d(x_n, y_n)}{n}) = d(\alpha, \beta) = d_1(\alpha, \beta)$$

So ϕ_g is an isometry. So this action gives a homomorphism $\psi : G \to$Iso(K), where Iso(K) is group of isometries of metric space K and the map ψ need not be injective so let N denote the kernel of this map.

Proposition 4.0.61 *The asymptotic cone(K) of finitely generated group G is a homogeneous space.*

Proof: Let's take α and β are two elements of K that are represented by the sequences $\{x_n\}$, $\{y_n\}$. Then consider the elements γ of K represented by $\{y_n x_n^{-1}\}$. Then $\phi_g(\alpha) = g\alpha = \{y_n x_n^{-1}\}\{x_n\} = \{y_n x_n^{-1} x_n\} = \{y_n\} = \beta$. Hence K is homogeneous space. □

Define, for each $x \in G$, the displacement of x by

$$D(x; r) = max(d(a, xa)) = max\{l(a^{-1}xa) \mid a \in G, l(a) \leq r\}$$

Here r be any natural number. If $x = e$, then $D(x, r) = 0$. More generally if x is an element in the center of G, then $D(x, r) = 0$.

Example 4.0.62 *$G = \mathbb{Z}$, $x = 1$, $r = 2$. Then $D(0, 2) = max\ \{l(a^{-1}xa) \mid l(a) \leq 2\}$ $=l(1) = 1$. Now consider $G = \mathbb{F}_2 =< x_1, x_2 >$, the free group of rank 2, and take $x = x_1$, $r = 2$, then $D(x_1, 2) =max\ d(a, x_1a)\ =max\ \{l(a^{-1}x_1a) \mid a \in G, l(a) \leq 2\} = 5$.*

If $x \in H \leq G$, and we restrict a from above to lie in H, we write $D_H(x, r) =$max$\{l(a^{-1}xa) : l(a) \leq r; x, a \in H\}$. Consider $G = \mathbb{F}_2 =< a, b >$, the free group of rank 2, and take

$x = a$, $r = 2$, and $H =< a >$, then $D_H(x, 2)$ =max$\{l(g^{-1}xg) : l(g) \leq r; x, g \in H\}$. = $l(a)$ =1.(because $b \in H$ and hence commutes with a.)

Proposition 4.0.63 *If $x \in N$, then $\mathcal{F}lim_{r\to\infty}\frac{D(x,r)}{r} = 0$.*

Proof: For each r, choose an a_r such that $l(a_r) \leq r$ and $l(a_r^{-1}xa_r) = D(x, r)$. The sequence $\alpha = \{a_r\}$ is moderate. If $x \in N$, since we have a map $\Phi : G \to I$ with kernel N given by $\Phi(x)(\alpha) = x\alpha$, $x\alpha = \alpha$.
Therefore, $\frac{D(x,r)}{r} = \frac{l(a_r^{-1}xa_r)}{r} = \frac{d(a_r,xa_r)}{r}$.

Now,

$$\mathcal{F}lim\frac{D(x,r)}{r} = \mathcal{F}lim(\frac{d(a_r, xa_r}{r}) = d(\alpha, x\alpha) = d(\alpha, \alpha) = 0$$

Proposition 4.0.64 *The function $D(x, r)$ is bounded if and only if x has only finitely many conjugates in G, and in that case $x \in N$.*

Proof: If x has only finitely conjugates in G say $y_1, y_2, ..., y_l$, then

$$D(x, r) = max\{l(a^{-1}xa) \mid l(a) \leq r\} \leq max\{l(y_1), l(y_2), ..., l(y_l)\}$$

is bounded. Conversely if $f(r) = D(x, r)$ is bounded, i.e. $\exists\ M > 0$ such that $D(x, r) \leq M\ \forall r \in \mathbb{N}$ i.e. max$\{l(a^{-1}xa \mid l(a) \leq r\} \leq M\ \forall\ r \in \mathbb{N}$. Suppose x has infinitely many conjugates say $z_1, z_2, ...$ We know that a finitely generated group can have only finitely many words of given length. So let k_n denote the number of conjugates of length n. Then there exists a conjugate of length greater than M(because, number of conjugates is infinite and K_n is finite for each n), which is contradiction. Therefore, x has only finitely conjugates.

Definition 4.0.65 *An element $g \in G$ is said to be an FC element if g has finitely many conjugates in G. The set of all FC elements of a finitely generated group G forms a normal subgroup of G and this subgroup is called the FC centre of G.*

It is clear that if $x \in H \leq G$ is an FC element of G then x is also a FC element element of H but converse need not be true. We will show that if H is subgroup of

G of finite index then any FC element of H is also an FC element of G.

Proposition 4.0.66 *Suppose that* $\mid G : H \mid < \infty$ *and* $x \in H$. *Then* $D(x, r)$ *is bounded if and only if* $D_H(x, r)$ *is bounded.*

Proof: It is clear that, if $D(x, r)$ is bounded then $D_H(x, r)$ is bounded. Conversely, suppose x has finitely many conjugates in H i.e. $\mid \{h^{-1}xh \mid h \in H\} \mid < \infty$. Since we know that

$$G = a_1H \cup a_2H \cup ... \cup a_kH, \;\; g \in G \;\; and \;\; g = a_ih_j$$

$\mid \{(ga_i^{-1})^{-1}x(ga_i^{-1}) : g \in G, i = 1, 2, .., k\} \mid < \infty$
$\Rightarrow \mid \{a_i(g^{-1}xg)a_i^{-1} : i = 1, 2, .., k, g \in G\} \mid < \infty$
i.e. for each i, $\mid \{a_i(g^{-1}xg)a_i^{-1} : g \in G\} \mid < \infty$
Claim: $\mid \{g^{-1}xg : g \in G\} \mid < \infty$.
Suppose, $\{g^{-1}xg\} = \{t_1, t_2, ..., t_r, ...\}, say$
Fix i, Then $\{a_i(g^{-1}xg)a_i^{-1} : g \in G\} = \{a_it_1a_i^{-1}, a_it_2a_i^{-1}, ..., a_it_ra_i^{-1}, ...\}$
$\Rightarrow$ i.e. $a_it_ja_i^{-1} = a_it_la_i^{-1}j, l > r \Rightarrow t_j = t_l$
$\Rightarrow \mid \{g^{-1}xg : g \in G\} \mid < \infty$

$\Rightarrow x$ has only finitely many conjugates in G. Therefore $D(x, r)$ is bounded.

Proposition 4.0.67 *For* $x, y \in G$ *and integer* r, s, *we have* $D(x, r+s) \leq D(x, r)+2s$ *and* $D(y^{-1}xy, r) \leq D(x, r) + 2l(y)$.

Proof: Let $l(a) \leq r + s$. Then we can write $a = bc$ with $l(b) \leq r$, $l(c) \leq s$. Then

$$\begin{aligned} d(xa, a) = d(xbc, bc) &\leq d(xbc, xb) + d(xb, b) + d(b, bc) \\ &\leq d(bc, b) + d(xb, b) + d(b, bc) \\ &\leq d(xb, b) + 2d(bc, b)(\because d(bc, b) = l(c) \leq s) \end{aligned}$$

$Therefore \;\; d(xa, a) \leq D(x, r) + 2s \leq D(x, r) + 2s$

Therefore, we have

$$D(x, r + s) \leq D(x, r) + 2s$$

ii). if $l(a) \leq r$, then

$$d(y^{-1}xya, a) = d(x(ya), (ya)) \leq D(x, r + l(y))$$
$$\leq D(x, r) + 2l(y)$$

$\therefore D(y^{-1}xy, r) \leq D(x, r) + 2l(y)$

Theorem 4.0.68 ***(B.H.Neumann)*** *: A group G cannot be the union of finitely many cosets of subgroups of the infinite index.*

Proof: Let $H_1, H_2, ..., H_k$ be the subgroups of infinite index. Let $g_1, g_2, ..., g_k \in G$ such that $\{G : H_i\} = \infty$ and $G = H_1g_1 \cup H_2g_2 \cup ... \cup H_kg_k$. We use induction on k. If $k = 1$, $G = H_1g_1 = H_1$ which is contradiction since H_1 is a proper subgroup. If $k > 1$. Let H be one of the subgroups involved. Since $\{G : H\} = \infty$, So, some coset Hx does not occur in the union, and since it is disjoint from the cosets of H that do appear, it is contained in the union of the cosets of the other subgroups.i.e. $Hx \subseteq H_2g_2 \cup H_3g_3 \cup ... \cup H_kg_k$ if $H_1 = H$, then any coset Hy can be written as $Hx.x^{-1}y$, and this shows that Hy is also contained in finite union of cosets of other subgroups. This implies that all the cosets of H occuring in the union are contained in the finite unions of cosets of other subgroups, and thus G is the union of finitely many cosets of $k - 1$ subgroups, and this contradicts the inductive hypothesis. □

4.0.6 Gromov's theorem

In this section, we will prove Gromov's theorem 4.0.85. In order to prove it, we need some results, which we are stating without proof..

Theorem 4.0.69 ***(Gleason-Montgomery-Zippin: solution of Hilbert's Fifth Problem)****: Let T be a finite dimensional, locally compact, connected and locally connected, homogeneous metric space. Then the group of isomteries of T can be given the structure of a Lie group with finitely many components.*

■

Theorem 4.0.70 *Let G be a Lie group with finitely many components with center of group denoted by Z.*

a). G has a normal abelian subgroup Z, such that G/Z is isomorphic to a subgroup of $GL(k, \mathbb{C}$ for some k.

b). For each natural number n, there exist an open neighbourhood of the identity in G which does not contain any non-identity element of finite order less than n.

$\blacksquare$

We also recall the definition of the topology that makes the isometry group a Lie group. Fix some base point $e \in T$. For any two positive number A and e, let $O(A, e)$ be the set of all isometries σ such that $d(\sigma(x), x) < \epsilon$, for all x such that $d(x, e) \leq A$. The sets $O(A, \epsilon)$ are taken to be a basis for the neighbourhood of the identity in $Isom(T)$.

Theorem 4.0.71 *Let G be a finitely generated infinite group, let K be an asymptotic cone of G and $I =$ Isom(K). Then there exists a homomorphism $\Phi : G \to I$ with kernel N such that one of the following holds:*

i). G/N is infinite.

ii). N is abelian-by-finite

iii). For each neighbourhood O of the identity in I there exists a homomorphism $\phi_O : N \to I$, such that Im(ϕ_O) $\cap\, O$ contains non-identity elements.

Proof: Since we have an isometric action of G on K, it gives a homomorphism $\Phi : G \to I$ given by $\Phi(x) = \sigma_x$, where $\sigma_x : K \to K$ is an isometry given by $\sigma_x(\alpha) = x\alpha$. Let N be the kernel of this homomorphism. If $\mid G : N \mid$ is infinite, then we are done. So assume that $\mid G : N \mid$ is finite.

Then by 2.3.16, N is a finitely generated group, say generated by $y_1, y_2, ..., y_d$ i.e. $N =< y_1, y_2, ..., y_d >$. If $D(y_j, r)$ is bounded for each j, then y_j has only finitely many conjugates for each j. Hence, the centralizer of each y_j is of finite index, i.e. $\mid N : C_G(y_j) \mid < \infty\ \forall 1 \leq j \leq r \Rightarrow \mid N : \bigcap_{j=1}^{r} C_G(y_j) \mid$ is finite. Since y_j are generators, $\bigcap_{j=1}^{r} C_G(y_j) = Z(N)$, where $Z(N)$ is the center of group N, hence $\mid N : Z(N) \mid < \infty$. Hence N is abelian by finite. So case (ii) holds.

So assume that $D(y_j, r)$ is not bounded for some j i.e. there exist some non FC element say y_{j_0}. Then we may assume that none of the generators is an FC element (if some generator y_i is an FC element , then $y_{j_0}y_i$ is a non FC element). Since FC elements form a subgroup, we can always do that. Fix some integer r and some ϵ. For each t between 1 and d, the set of elements y of N such that $D(y^{-1}y_t y) \leq \epsilon r$ is equal to the set of elements such that $l(a^{-1}y^{-1}y_t ya) \leq \epsilon r$ for all $a \in G$ such that $l(a) \leq r$. It means that the conjugate of y_t^{ya} of y_t is one of the finitely many elements and therefore the elements ya lies in one of the finitely many cosets of $C_G(y_t)$, in particular taking $a = 1$, we see that y itself lies in one of the finitley many cosets. Since each of $y_1, ..., y_d$ has infinitely many conjugates in N, i.e. its centralizer has infinite index, the last proposition shows that N is not the union of finitely many cosets of the centralizers of the generators and so there exists some $z_r \in \mathbb{N}$ such that $D(z_r^{-1}y_t z_r, r) > \epsilon r$ for all t.
We write z_r as a word in y_t, and choose the first initial subword x_r of z_r for which $D(x_r^{-1}y_t x_r, r) > \epsilon r$ for some t. We choose for each r one such index $t = t(r)$ and for each $i \leq d$, we write $S(i) = \{r \mid t(r) = i\}$. There finitely many sets $S(i)$ partition $\mathbb{N}$, therefore one of them, say $S(i_0)$, lies in $\mathcal{F}$. Let l be the maximum length ofy_t in the generators of G. We may take r to be large enough, and then $D(y_t, r) \leq \epsilon r$, by Proposition we have $x_r \neq 1$, and we can write $x_r = w_r y$, where w_r is the initial subword of z_r preceding x_r and y in some generator. Then by 4.0.67, we have $D(x_r^{-1}y_t x_r, r) \leq D(w_r^{-1}y_t w_r, r) + 2l \leq \epsilon r + 2l$. This holds for each t, but for i_0 we also have $D(x_r^{-1}y_{i_0}x_r, r) > \epsilon r$. It follows that $\mathcal{F}$ lim $\frac{D(x_r^{-1}y_{i_0}x_r, r)}{r} = \epsilon$. We always have $l(x) \leq D(x, r)$, for every r and thus the previous inequality shows that $l(x_r^{-1}y_t x_r) \leq \epsilon r + 2l$ for each t, and so if $y \in N$ has length m in the y_i. We have $l(x_r^{-1}yx_r) \leq m\epsilon r + 2ml$. Therefore left multipication by the sequence $\{x_r^{-1}yx_r\}$ preservesthe moderate sequence and induce an isometry on K. We define $\phi(y)$ as the isometry. Then ϕ is a homomorphism $N \to I$. Then by 4.0.63 to this homomorphism shows that $\phi(y_{i_0}) \neq 1$, because $\mathcal{F}\lim\frac{D(x_r^{-1}y_{i_0}x_r, r)}{r} \neq 0$. On the other hand $d(\phi(y_{i_0}(\alpha).\alpha) \leq \epsilon$ for all $\alpha \in K$, which shows that $\phi(y_{i_0})$ can be made to lie in any given neighbourhood of the identity in I, by taking a small enough ϵ.

Proposition 4.0.72 *Let G have polynomial growth of degree d. Then there exist* *infinitely many n such that for all $i < n$, we have log $s(2^n)$ $\leq$log$s(2^{n-1}) + i(d+1)$, where logarithm are to the base 2.*

Proof: By the definition of d, we have $s(n) \leq C_1 n^d$. So for large enough n, log$s_n \leq d$log(n), $\frac{logs(n)}{log(n)} \leq d + 1/2$. In particular if we write $l(n)$ =log$s(2^n)$, i.e. $\frac{l(n)}{log(2^n} = \frac{l(n)}{n} < d + 1/2$

$\Rightarrow l(n) < nd + n/2 \Rightarrow l(n) - nd - n/2 < 0$

$\Rightarrow l(n) - n(d+1) < -n/2$ and thus, $lim_{n\to\infty}(l(n) - n(d+1)) = -\infty$. For each negative integer k, let $n(k)$ be the first integer n such that $l(n) - n(d+1) < k$. Then for each $n = n(k)$ and $i < n$, we have $l(n) - n(d+1) < k \leq l(n-i) - (n-i)(d+1)$. Therefore, we have

$$l(n) \leq l(n-i) + i(d+1)$$
$$\therefore log\ s(2^n) \leq log\ s(2^{n-i}) + i(d+1)$$

Since the $n(k)$ takes on infintely many value, the proposition is proved.

We write S for the set of all integers n satisfying the inequality of the log $s(2^n) \leq$ log $s(2^{n-i}) + i(d+1)$ and $T = \{2^n \mid n+1 \in S\}$. We choose our ultrafilter $\mathcal{F}$ to contain T.

Lemma 4.0.73 *Let G be of polynomial growth, let $\mathcal{F}$ be chosen as described, and let ϵ be small enough and K be the asymptotic cone of G. Then the following are equivalent*
1). If a closed ball of radius 1 in K contains k distinct points, such that the closed ball of radius ϵ around them are disjoint, then $k \leq (\frac{1}{\epsilon})^{2(d+1)}$.
2). If a closed ball of radius 1 in K contains k distinct points, such that the distance between any two points are bigger than 2ϵ, then $k \leq (\frac{1}{\epsilon})^{2(d+1)}$.

Proof: We prove that the two properties are indeed equivalent. Suppose (1) holds. Let k be as in (2) such that distance between any two points are bigger than 2ϵ So, balls of radius ϵ around any two points are disjoints (because they are separated by at least 2ϵ distance) So by (1), $k \leq (\frac{1}{\epsilon})^{2(d+1)}$ which proves (2). assume if (2) holds, given any k points as in (1), suppose that two of them are at least a distance of $\delta \leq 2\epsilon$. Then by the Prop(7.4) there exist a continous path $f(\alpha)$ between these two points such that $d(f(\alpha), f(\beta)) \leq (\beta - \alpha)\delta$.

Then $d(f(0), f(1/2) \leq 1/2\delta < \epsilon$ and $d(f(1/2), f(1)) \leq 1/2.2\epsilon < \epsilon$. So $f(1/2)$ lies in the ball of radius ϵ around both points, a contradiction, which proves (1).

Lemma 4.0.74 *For any $\alpha, \beta \in [0,1]$ with $\alpha \leq \beta$ and any $n \in \mathbb{N}$, we have $[n\alpha] - [n\beta] \leq n(\beta - \alpha) + 1$.*

Proof: Suppose $\alpha, \beta \in [0,1]$ are not zero and $\alpha \leq \beta$. Let n be any natural number. If suppose $\alpha < \frac{1}{n}$ and $\beta < \frac{1}{n}$. Then $[n\alpha] = [n\beta] = 1$ so L.H.S. is 0 and R.H.S. is a positive number, and in that case we are done. Suppose if $\alpha < \frac{1}{n}$ and $\beta \geq \frac{1}{n}$, then $n_0 < n\beta \leq n_0 + 1$, therefore $[n\beta] = n_0$ so L.H.S. $= n_0 + 1 - 1 = n_0$ and R.H.S. $= \beta n - \alpha n + 1 = \beta n + (1 - \alpha n) > n_0 =$ L.H.S. Now suppose that $\alpha \geq \frac{1}{n}$ and $\beta \geq \frac{1}{n}$ so $n_0 < n\alpha \leq n_0 + 1$ and $m_0 < n\beta \leq m_0 + 1$, so L.H.S. $= m_0 - n_0$ and R.H.S. $= n\beta - n\alpha + 1$ since $n\alpha < n_0 + 1$ and $n\beta < m_0 + 1 \Rightarrow n\beta - n\alpha \geq m_0 - n_0 - 1 > m_0 - n_0$ $=$ L.H.S. Hence we have $[n\alpha] - [n\beta] \leq n(\beta - \alpha) + 1$. □

Proposition 4.0.75 *The Asymptotic cone of a finitely generated group G is pathwise connected and locally connected.*

Proof: Let a represent a sequence $\{x_n\}$, and for each n, length of x_n is denoted by $l(x_n)$. Let $0 \leq \alpha \leq 1$, and for each word w of length k in generator X, write $w(\alpha)$ for the word consisting of the first $k\alpha$ letters in w. Now, define $f : [0,1] \to K$ given by $f(\alpha) = \{x_n(\alpha)\}$, $f(0) = [e] = e$ and $f(1) = \{x_n\} = a$ Moreover, if $0 \leq \alpha, \beta \leq 1$, By the previous lemma, we have $(\beta - \alpha)l(x_n) - 1 \leq d(w(\alpha), w(\beta)) \leq (\beta - \alpha)l(x_n) + 1$. Since $l(x_n) \leq An$, this implies that $d(f(\alpha), f(\beta)) \leq A(\beta - \alpha)$, and therefore f is continuous. This shows that K is pathwise connected. Moreover, $d(e, f(\beta)) \leq \beta d(e, a)$, and thus the path from e to a is contained in the ball of radius $l(a)$ around e. This shows that each ball around e is pathwise connected. By homogeneity, this holds for all balls, hence K is locally connected. □

Proposition 4.0.76 *the Asymptotic cone of a finitely generated group G complete metric space.*

Proof: The proof refers to [1] ■

Definition 4.0.77 *A group G is said to be linear if G is isomorphic to a subgroup of the general linear group $GL(n, F)$, for some natural number n and some field F.*

Now we will state some theorems without proof.

Theorem 4.0.78 ***(Tit's Alternative)*** *[15] Let G be a finitely generated linear group. Then either G contains a non-abelian free subgroup, or G contains a soluble subgroup of finite index.*

■

Theorem 4.0.79 ***(Jordan's theorem)*** *[20] A finite subgroup of $Gl(n, \mathbb{F})$, where $\mathbb{F}$ is a field of char($\mathbb{F}$) = 0 has an abelian sugroup of index bounded in terms of n only.*

■

Definition 4.0.80 *A topological space has dimension* 0*, if each point has an open neighbourhood with empty boundary. It has dimension at most n, if each point has an open neighbourhood with boundary of dimension at most $n-1$. The dimension equals n, if it is at most n, but it is not at most $n-1$.*

Theorem 4.0.81 *If G is of polynomial growth, the asymptotic cone K is finite dimensional.*

Proof: The proof refers to [1]

■

Proposition 4.0.82 *If G is of polynomial growth, the asymptotic cone K is locally compact.*

Proof: In order to show that K is locally compact, it suffices to show that K is compact. Since K is a metric space, in order to show the compactness of K, it is enough to show that K is sequentially compact. Let x_n be any sequence in B, where B is a closed unit ball. Lets cover B, for each i, by k_i balls of radius $1/2^i$. Take $i = 1$, let's cover by k_1 balls of radius $1/2$, then one of the balls contains infinitely many points of the sequence, say a subsequence x_{n_k} of sequence x_n. Now consider the sequence $x_{n_{k_1}}$, and for $i = 2$, cover the ball B by k_2 balls of radius $1/2^2$, then one of the balls among k_2 contains infinitely many points of the sequence $x_{n_{k_1}}$ say $x_{n_{k_1,k_2}}$ and continue like that. At the mth stage, cover the ball B by k_m points of radius $1/2^m$, then one of the balls contains infinitely many points of the sequence $x_{n_{k_1,k_2,\ldots,k_{m-1}}}$ and so on. Now choose one point from the sequence $x_{n_{k_1}}$ say y_1, and second point from $x_{n_{k_1},n_{k_2}}$ say y_2,..., m^{th} point from the sequence $x_{n_{k_1,k_2,\ldots,k_m}}$ say y_m, then the sequence y_n is a Cauchy sequence, because tail of this sequence belongs to balls of small radius $1/2^m$ as $m \to \infty$. Since K is a complete metric space4.0.76, so y_n is convergent. Since y_n is a subsequence of x_n, K is sequentially compact. Therefore, K is compact and therefore K is locally compact. ☐

Theorem 4.0.83 *Let G be an infinite group of polynomial growth. Then there exists a Lie group Γ with finitely many components, and a natural number k, such that G contains a normal subgroup C of finite index, for which one of the following holds:*
i). C has an infinite abelian factor group.
ii). C has an infinite factor group in $GL(k, \mathbb{C})$.
iii).There exists homomorphisms $\phi_n : C \to \Gamma$, for all natural number n, such that $\mid \frac{C}{Ker(\phi_n)} \mid \geq n$.

Proof: Let G be a finitely generated infinite group. So the asymptotic cone K of G is connected, locally connected4.0.75, homogeneous4.0.61. Since G is of polynomial growth so K is also locally compact4.0.82 and has finite dimensional4.0.81. So, by 4.0.69, the isometry group $I = \mathrm{Isom}(K)$ of K has the structure of a Lie group with finitely many components. Since we have an isometric action of G on K, it gives a homomorphism $\Phi : G \to I$ given by $\Phi(x) = \sigma_x$ where $\sigma_x : K \to K$ is an isometry given by $\sigma_x(\alpha) = x\alpha$. Let N be the kernel of this homomorphism. So, $\Psi : G/N \to I$ be a monomorphism defined as $\Psi(gN) = \Phi(g)$. Since I is a Lie group with finitely many components, by 4.0.70, I has a normal abelian subgroup Z, such that I/Z is isomorphic to a subgroup of $GL(k, \mathbb{C})$ for some k. Now consider the subgroup $L = \Psi^{-1}(Z)$ which contains N. We have $G/N \xrightarrow{\Phi} I \xrightarrow{\eta} I/Z$, hence we got a map $\eta \circ \Phi : G/N \to I/Z$ and the kernel of this map $\eta \circ \Phi$ is L/N, so $\frac{G/N}{L/N}$ is isomorphic to a subgroup of I/Z, since $G/L \cong \frac{G/N}{L/N} \hookrightarrow I/Z \hookrightarrow Gl(k, \mathbb{C})$.

1). If G/L is infinite, then take $C = G$, $|G : C| = 1$ and $G/L \hookrightarrow GL(k, \mathbb{C})$, So C has an infinite factor in $GL(k, \mathbb{C})$, which says that (ii) holds.

2). If G/L is finite, then there are two possibility of G/N, either G/N is finite or infinite

Case(a): If G/N is infinite, and since $G/L \cong \frac{G/N}{L/N}$. In this case take $C = L$. So $|G/N| = |G/L||L/N|$, so L/N is an infinite group. Since we have a monomorphism $\Psi : G/N \to I$ so if we restrict to L/N, it would stil be a monomorphism $\Psi_{L/N} : L/N \to I$ and the image of $\Psi_{L/N}(lN) = \phi(l)Z \in Z$. So $\Psi_{L/N}(L/N) \subseteq Z$, since Z is an abelian group and L/N is an infinite group, so $C = L$ has an infinite abelian factor, which proves that (i) holds.

Case(b): If G/N is finite so G/L is finite and $N \subseteq L$. Now apply [Them 7.5], then (i) and (ii) can not hold, (iii) must holds, then N is virtually abelian say C i.e. $\mid N : C \mid < \infty$ and since $|G : N| < \infty \Rightarrow |G : C| < \infty$, if we take the conjugate of C, then it becomes the characteristics subgroup of N, So C char N and $N \lhd G \Rightarrow C \lhd G$ and $|G : C| < \infty$
$\therefore$ $C/(e) \cong C$ is an infinite abelian group. So we are done. Now, suppose (iii) of 4.0.71 holds, i.e. for each neighbourhood O of the identity in I, $\exists$ a homomorphism $\phi_O : N \to I$, such that $Im(\phi_O) \cap O$ contains a non-identity elements. Now, take $C = N$, I is a Lie group with finitely many components. so for each $n \in \mathbb{N}$, $\exists$ an open neighbourhood of the identity in I which does not contain any non-identity element of finite order less than n. So $n \in \mathbb{N}$, we have $O_n($ neighbourhood of id in I, so if $g \in O_n \Rightarrow o(g) \geq n)$. So $\phi_{O_n} : N \to I$ such that $Im(\phi_O) \cap O_n$ contains a non-identity elements, but we know that, if suppose x be a such that $x \in O_n$ be a non-identity element, then $O(x) \geq n \Rightarrow \{1, x, x^2, ..., x^{n-1}, ..\} \subseteq Im(\phi_{O_n}) \cong \frac{C}{ker\phi_n}$
and it follows that

$$|C : Ker(\phi_n)| \geq n.$$

□

Theorem 4.0.84 *Let G be an infinite group of polynomial growth. Then G contains a subgroup of finite index which has infinite cyclic homomorphic image.*

Proof: Let G be an infinite group of polynomial growth and the isometry group $I = \text{Isom}(K)$ of K has the structure of Lie group with finitely many components4.0.69. So, by previous theorem, we have an isometric action of G on K, that gives a homomorphism $\Phi : G \to I$ given by $\Phi(x) = \sigma_x$ where $\sigma_x : K \to K$ is an isometry given by $\sigma_x(\alpha) = x\alpha$. Let N be the kernel of this homomorphism. So, $\Psi : G/N \to I$ be a monomorphism defined as $\Psi(gN) = \Phi(g)$. Since I is a Lie group with finitely many components, by 4.0.70, I has a normal abelian subgroup Z, such that I/Z is isomorphic to a subgroup of $GL(k, \mathbb{C})$ for some k. Now consider the subgroup $L = \Psi^{-1}(Z)$ which contains N. Now by the above theorem, G contains a normal subgroup C of finite index which satisfies one of three conditions of previous theorem.

Case I: If suppose C satisfies (i) of 4.0.83, i.e. C has an infinite abelian factor group. Let's say that C contains a normal subgroup T, such that $C/T \cong \mathbb{Z} \oplus F$, where F is an abelian group. Hence, we have a natural map $\eta : C \to C/T$ and an epimorphism $f : C/T \to \mathbb{Z}$. Since $|G : C| < \infty$, we have an epimorphism from finite index subgroup C, $f \circ \eta : C \to \mathbb{Z}$. Hence we are done.

Case II: Suppose C satisfies (ii) of 4.0.83, C contain an infinite factor in $G(k, \mathbb{C})$ for some $k \in \mathbb{N}$. From case(ii) of the above theorem, our $C = G$ and C has a subgroup L such that G/L is isomorphic to a subgroup of $G(k, \mathbb{C})$. So G/L is an infinite subgroup of $Gl(k, \mathbb{C})$, Then by the Tit's alternative, either G/L contains $\mathbb{F}_2$ or it is virtually solvable. If it is the former case, then G/L has exponential growth and so G has exponential growth, which is a contradiction. Hence, G/L must be virtually solvable and since G/L has polynomial growth so by 3.0.19,G/L must contain a nilpotent subgroup of finite index say H/L.

$$|\frac{G/L}{H/L}| = |G/H| < \infty.$$

Now, since H/L is nilpotent, H/L is solvable. Consider the derived series of H/L say

$$L \lhd H^{(1)}/L \lhd H^{(2)}/L \lhd \ldots \lhd H^{(i)}/L \lhd H^{(i+1)}/L.. \lhd H/L$$

such that $\frac{H^{(i+1)/L}}{H^{(i)}/L}$ is abelian. If suppose H/L is a finite group, then since $|G/L : H/L| < \infty$, G/L is finite, a contradiction to the fact that G/L is infinite group. So H/L is an infinite group and therefore some quotient in the derived series of H/L

contains a copy of infinite cyclic group $\mathbb{Z}$. Let j be the maximum natural number such that the quotient $\frac{H^{(j+1)}/L}{H^{(j)}/L}$ contains a copy of $\mathbb{Z}$. Since

$$\frac{H^{(j+1)}}{H^{(j)}} \cong \frac{H^{(j+1)}/L}{H^{(j)}/L} \cong \mathbb{Z} \oplus T.$$

where T is an abelian group and $|H/L : H^{(j+1)}/L| = |H : H^{(j+1)}| < \infty$ and Therefore,

$$|G/L : H^{(j+1)}/L = |G/L : H/L|.|H/L : H^{(j+1)}/L| < \infty.$$

So, $H^{(j+1)}/L$ is a finite index subgroup of G/L, which implies that $H^{(j+1)}$ is a finite index subgroup of G and since $\frac{H^{(j+1)}}{H^{(j)}} \cong \mathbb{Z} \oplus T$, $H^{(j+1)}$ has $\mathbb{Z}$ as an epimorphic image. Hence, we are done in this case.

Case III: If case (iii) of the previous theorem holds and take C to as of case(iii). Let $\phi_n : C \to I$ be a homomorphism for each $n \in \mathbb{N}$ and let K_n denote the kernel of the map ϕ_n for each $n \in \mathbb{N}$. Since By 4.0.70 I contains a normal abelian subgroup Z such that I/Z is isomorphic to a subgroup of $Gl(k, \mathbb{C})$ for some k. Let $L_n = \phi_n^{-1}(Z)$, it is clear that $L_n \supseteq K_n$. Since we have a homomorphism $\phi_n : C \to I$ and k_n is the kernel of this map, it implies that, we have a monomorphism $\tilde{\phi} : C/K_n \to I$ and $\tilde{\phi}_n(L_n/K_n) \subseteq Z$, so L_n/K_n is an abelian group. Since $\tilde{\phi}_n(Z) \subseteq Z$, which induces another map

$$\tilde{\phi'}_n : C/K_n \to I/Z$$

and if we restrict this map to subgroup L_n/K_n, then it becomes injective and since I/Z is a subgroup of $GL(k, \mathbb{C})$. Therefore, we get that, $\frac{C/K_n}{L_n/K_n}$ is a linear group. Since we have

$$\frac{C/K_n}{L_n/K_n} \cong C/L_n$$

it follows that C/L_n is linear. Since, in case(iii) of the previous theorem, $G/Ker(\phi)$ is finite, it also follows that G/K_n is finite.

$$|G : L_n| = |G : K_n|.|K_n : L_n|$$

and since G/K_n is finite, $|G : L_n|$ is finite for each n. Also, we have

$$|G : L_n| = |G : C|.|C : L_n|$$

and since G/L_n is finite, $|C : L_n|$ is finite for each n. Now applying theorem(6.5), C/L_n contains a subgroup H_n/L_n such that $|\frac{C/L_n}{H_n/L_n}| = |C : H_n|$ is bounded say $|C : H_n| \leq M_k$, where M_k is a real constant which depends upon on k not on n. Since by prop, for infinitely many n, $H_n's$ are isomorphic, say $H_n \cong H$ for infinitely many n. Then we have H/L_n is abelian for infinitely many n. Then
the order of $|H : L_n|$ tends to infinity as $n \to \infty$. Since, we have a natural map $\eta : H \to H/L_n$ and since H/L_n is abelian, η factors through H/H', i.e. we have

$$\tilde{\eta} : H/H' \to H/L_n$$

and if $|H/L_n|$ tends to infinity as $n \to \infty$, H/H' must be infinite, and therefore H has $\mathbb{Z}$ as an epimorphic image and since $|G : C| < \infty$ and $|C : H| < \infty$ and G has finite index subgroup H which has $\mathbb{Z}$ as an epimorphic image.
If the size of H/L_n is bounded, then again by the 2.3.14, for infinitely many n, L_n coincides with a subgroup equal to R(say). Since we have

$$|G : K_n| = |G : C|.|C : K_n|$$

and since by case(iii) of previous theorem, $|G : K_n|$ tends to infinity as $n \to \infty$ and $|C : R|$ is fixed number, $|C : K_n|$ tends to infinity as $n \to \infty$. Now we have

$$|C : K_n| = |C : R||R : K_n|$$

and since $|C : R|$ is a fixed number, therefore $|R : K_n|$ tends to infinity as $n \to \infty$. Now we have natural map $\theta : R \to R/K_n$ and since $L_n/K_n = R/K_n$ for infinitely many n and since L_n/K_n is abelian for all n. Therefore, the map θ factors through R/R', i.e. we have $\tilde{\theta} : R/R' \to R/K_n$ and since $|R : K_n|$ tends to infinity as $n \to \infty$, R/R' must be infinite group. Hence, R has $\mathbb{Z}$ as an epimorphic image. Since $|H : R|$ is bounded and $|G : H|$ is finite, it follows that R has finite index in G and R has $\mathbb{Z}$ as an epimorphic image, which completes the proof

□

Theorem 4.0.85 *A group of polynomial growth is nilpotent-by-finite.*

Proof: Let G be a finitely generated group of polynomial growth say of degree d. We will use induction on d to prove that G has a nilpotent subgroup of finite index. If $d = 0$, then by2.1.8 G is a finite group and it is clear that finite groups are virtually nilpotent. Suppose if $d > 0$, then G is infinite group. Therefore by the previous theorem, G contains a finite index subgroup H such that H has $\mathbb{Z}$ as an epimorphic image, i.e. there is normal subgroup N of H such that $H/N \cong \mathbb{Z}$. Since H is of finite index in G, H is finitely generated and also H has polynomial growth and $H/N \cong \mathbb{Z}$, so by 2.3.18 N is finitely generated and N has degree of growth $d-1$ or less, so by induction N contains a nilpotent subgroup K of finite index. By2.3.15 , we may assume that K is characteristic subgroup in N and hence normal in H. Then H/K contains the finite normal subgroup N/K, with infinite cyclic factor. Let $H/N =< xN >$. Write $C =< K, x >$. Then $H/K = C/K.N/K$, hence, $|H : C|$ is finite. Since C/K is infinite cyclic, C is soluble. Then by 3.0.20 and 3.0.21 We get C is virtually nilpotent. Therefore, G is virtually nilpotent group, which completes the proof. $\square$

Therefore, Gromov's theorem completely characterized the groups of polynomial growth: In the view of theorems 3.0.27 and 4.0.85, a finitely generated group has polynomial group if and only if it has nilpotent subgroup of finite index.

Chapter 5

Groups of Intermediate growth

So far, we have seen that virtually nilpotent groups have polynomial growth and non-abelian free groups have exponential growth and we have only dealt with those finitely generated groups which have either polynomial or exponential growth. In 1968, Milnor asked that *Is it true that the growth function of every finitely generated group is necessarily equivalent to a polynomial or to the function* 2^n*"?*. This was answered in the negative by R. Grigorchuk in 1983, who constructed a $3-$ generated group, whose growth is neither polynomial nor exponential but lies somewhere in between polynomial and exponential. This group not only gives the answer to Milnor's question but it also gives the answer to Burnside problem: *Can we have a finitely generated infinite group in which every element has finite order.* The Grigorchuk group is 3- generated infinite torsion group.

Apart from Grigorchuk group, we will also see another family of groups of intermediate groups namely Gupta-Sidki groups. These are the finitely generated infinite torsion p-groups for each odd prime p. This family also gives the answer to the Burnside problem.

5.1 Grigorchuk Group

First, we will define the Grigorchuk group. Then we will see its various interesting properties. This group was defined as the subset of the set of Lebesgue preserving transformations of the collection of the open unit interval $(0,1)$. Consider the unit interval $I = (0,1)$ and remove the set of all rational points $\{\frac{1}{2}, \frac{3}{4}, \frac{7}{8}, ..\}$ in $(0,1)$, call this set S. So

$$S = \bigcup_{i=1}^{\infty}(1 - \frac{1}{2^{n-1}}, 1 - \frac{1}{2^n}) = (0,1/2) \cup (1/2,3/4) \cup (3/4,7/8) \cup ....$$

Let E denote the identity transformation on each subinterval i.e. this transformation fixes each point of the interval and let P denote the transformation which interchanges the two halves $(0,1/2)$ and $(1/2,1)$ i.e. a point x is mapped either to $x + 1/2$ if $x \in (0,1/2)$ or to $x - 1/2$ if $x \in (1/2,1)$. Let E_I denote the identity transformation on I and P_I denote the interchange of two halves of I.

Now we will define four transformations a, b, c, d:

- a denotes the transformation P on S as just the interchange the two halves of S

- b denotes the transformation $PPEPPEPPE...$ on S i.e. b acts on S like P on first interval, P on second interval, E on third interval and P on fourth interval so on.

- c denotes the transformation $PEPPEPPEP...$ i.e. c acts on S like P on first interval, E on second interval, P on third interval P on fourth interval and so on.

- d denotes the transformation $EPPEPPEPP..$ on S i.e. like E on first interval, P on second interval, P on third interval, P on fourth interval and so on.

Here, the first interval means first half of S i.e. $(0,1/2)$, second interval means next half of the remaining i.e. $(1/2,3/4)$, third interval means that next half of the remaining i.e.$(3/4,7/8)$ and so on.

In particular, suppose $S = (0, 1/4) \cup (1/4, 1/2) \cup (1/2, 3/4) \cup (3/4, 1)$. Name the subinterval $(0, 1/4)$ as 1, $(1/4, 1/2)$ as 2, $(1/2, 3/4)$ as 3 and $(3/4, 1)$ as 4. Then the action of a on S as P, i.e. interchange of the two halves of $(0, 1)$ i.e. $(0, 1/2) \leftrightarrow (1/2, 1)$ acts like the permutation $(1, 3)(2, 4)$ b acts on S like P on first half $(0, 1/2)$, P on next half $(1/2, 3/4)$ and E on $(3/4, 1)$ i.e. b acts like permuatation $(1, 2)(3)(4)$ c acts on S like P on first half $(0, 1/2)$, E on next half $(1/2, 3/4)$ and P on $(3/4, 1)$ c acts like permuatation $(1, 2)(3)(4)$, d acts on S like E on first half $(0, 1/2)$, P on next half $(1/2, 3/4)$ and P on $(3/4, 1)$ i.e. d acts like permuatation $(1)(2)(3)(4)$.

Definition 5.1.1 *Consider the group Γ generated by the transformations a, b, c, d of S. We call this group Γ, the Grigorchuk group*

Since a is the transformation that interchange the two halves, a^2 is the identity transformation E. Similarly, b acts on S like $PPEPPEPPE..$, so b^2 acts on S like P^2 on first halves, P^2 on remaining next half, E^2 on remaining half and so on, but P^2 is the identity transformation, and so is E^2 is. So b^2 is the identity transformation. Similarly c^2, d^2 represent identity transformation. Hence, we have $a^2 = b^2 = c^2 = d^2 = 1$.

Now consider the transformation bc, first take the action of c then of b, i.e. c acts on S like $PEPPEPPEP...$ and then apply b, which acts like $PPEPPEPPE....$ So the transformation bc acts on S like $P.P = P^2 = E$ on first half, $E.P = P$ on remaining next half, $P.E = P$ on remaining next half, $P.P = P^2 = E$ on remaining next half and so on. Then the complete action of bc on S would be like $EPPEPPEPP...$ which is the same action as of d, hence $bc = d$, similarly if we consider the transformation cb, cb acts on S like $P.P = P^2 = E$ on first half, $P.E = P$ on remaining next half, $E.P = P$ on the third half, $P.P = P^2 = E$ on remaining next half and so on. So the complete action of cb would be like $EPPEPPEPP...$, which is again of d. Hence $bc = cb = d$. Similarly we can get $dc = cd = b$ and $bd = db = c$.

Now we have a group Γ which is generated by 4 elements, say a, b, c and d, and each generator has order 2, and we have the relations $a^2 = b^2 = c^2 = d^2 = 1$, $bc = cb = d$,$db = bd = c$ and $cd = dc = b$. Any arbitrary element of Γ can be written in the terms of a, b, c and d, because of the relations $a^2 = b^2 = c^2 = d^2 = 1$, each generator would have exponent at most 1 in the expression of any arbitrary element. Also, due to the relations $bc = cb = d$, $dc = cd = b$ and $bd = db = c$, if any two of b, c, d come together, we can replace it by new generator. So an arbitrary element of Γ can be written as a occurring between b, c and d.

Since a interchanges the two halves of $(0, 1/2)$ and $(1/2, 1)$ and b, c, d fix both intervals, so it follows that each element of Γ either fixes both of them or interchanges, then so consider the set of all elements of Γ which fixes the both intervals, they form a subgroup, say H. Also it is clear that this subgroup H has index 2 in Γ. Hence, H is a normal subgroup of Γ.

Lemma 5.1.2 *The subgroup H defined above is generated by the elements b, c, d, aba, aca, ada.*

Proof: We know that b, c, d fixes the two subinterval, so $b, c, d \in H$ and since a interchanges the two halves, even occurrence of a fix the two subintervals. Therefore the elements $b, c, d, aba, aca, ada \in H$. Now let $g \in H$, then g can be expressed in terms of b, c, d, aba, aca, ada. □

Since $(0, 1/2)$ and $(1/2, 1)$ are both bijective with $(0, 1)$, we can also define the same kind of group using similar transformations of these subintervals. Suppose Γ_l and Γ_r denote the Grigorchuk groups on intervals $(0, 1/2)$ and $(1/2, 1)$ respectively. The elements of subgroup H fix the interval $(0, 1/2)$ and $(1/2, 1)$. So if we restrict the action of H on $(0, 1/2)$, it will give a subgroup of Γ_l, and similarly the action of H on $(1/2, 1)$ will give a subgroup of Γ_r.
First, we will see how this restriction is gives a subgroup of Grigorchuk group.

Lemma 5.1.3 *Elements b, c, d, aba, aca, ada of H induce transformations $a_l, a_l, 1_l, c_l, d_l, b_l$ on $(0, 1/2)$ respectively and the transformations $c_r, d_r, b_r, a_r, a_r, 1_r$ on $(1/2, 1)$ respectively(where suffix l, r just emphasising that they are the transformation of the interval $(0, 1/2)$ and the interval $(1/2, 1)$).*

Proof: As we know that b acts like $PPEPPEPPE...$ on S, i.e. acts like P on first half $(0, 1/2)$ and acts like $PEPPEP...$ on remaining half and if we restrict the action of b on $(0, 1/2)$ i.e. it will induce the transformation a on $(0, 1/2)$ i.e. we write a_l, and the restriction of b on $(1/2, 1)$ will induce the transformation c and write c_r. Now consider the transformation c, it acts like $PEPPEPPEP...$ on S i.e. acts like P on first half $(0, 1/2)$ and $EPPEPPEPP...$ on second half $(1/2, 1)$, so the restriction of c induce the transformation a on $(0, 1/2)$ say a_l and d on $(1/2, 1)$ say d_r. Similarly the restriction of d on $(0, 1/2)$ and $(1/2, 1)$ induce the transformation 1_l and b_r respectively. Consider the transformation aba, since a acts like interchange the two intervals and b acts like $PPEPPEPPE...$, so aba, first swap the two halves, and then acts like b, and then again swap, so the resultant action would be like c on first half $(0, 1/2)$ and a on second half $(1/2, 1)$. Similarly, the transformation aca induce the transformation d on $(0, 1/2)$ and a on $(1/2, 1)$ write d_l and a_r respectively. Also the transformation ada induce the transformation b on $(0, 1/2)$ and a on $(1/2, 1)$ write b_l and 1_r respectively. □

Proposition 5.1.4 Γ *is an infinite group.*

Proof: We have noticed that H induces the transformations $a_l, a_l, 1_l, c_l, d_l, b_l$ on $(0, 1/2)$. The subgroup generated by $a_l, a_l, 1_l, c_l, d_l, b_l$ in Γ_l is equal to Γ_l, the Grigorchuk group on $(0, 1/2)$, and $\Gamma \cong \Gamma_l$ (just renaming of the elements). Hence, we have a map $\phi : H \to \Gamma_l$ defined as $\phi_l(g) = g_l$(the restriction of g on $(0, 1/2)$. By previous lemma, this map is an epimorphism. Since $H \leq \Gamma$ and $\Gamma \cong \Gamma_l$, hence we have an epimorphism from a proper subgroup of Γ to Γ. Therefore, we conclude that Γ is an infinite group. □

Similarly, we also have a map $\phi_r : \Gamma \to \Gamma_r$, defined as $\phi_r(g) = g_r$(just the restriction of g on $(1/2, 1)$), which is also an epimorphism.

So Now we have a map $\phi : H \to \Gamma_l \times \Gamma_r$ given by $\phi(x) = (x_l, x_r)$. Clearly, this map is injective, if some element acts like identity on $(0, 1/2)$ and $(1/2, 1)$, it must acts like identity transformation on S. So the kernel is trivial. Hence, ϕ is embedding of H in $\Gamma_l \times \Gamma_r$.

Since $a^2 = d^2 = 1$ and $\phi(adad) = \phi(ada)\phi(d) = (b, 1)(b, 1) = (b, b)$, so $\phi((ad)^4) =$

1, since ϕ is injective, So ad has order 4. It is clear that the subgroup $D =< a, d >$, is the dihedral group of order 8

Lemma 5.1.5 *Let $B =< b >^{\Gamma}$ be the normal closure of $< b >$ in Γ. Then $\mid \Gamma : B \mid \leq$ 8.*

Proof: Since we have $bc = cb = d$ and $\Gamma =< a, b, d >$. Since B is normal subgroup of Γ, so the quotient group Γ/B is generated by the images of a, d, and since by the previous lemma, we know that the subgroup generated by $< a, d >$ is of order 8. Therefore, B is normal subgroup of Γ of at most index 8. $\square$

Theorem 5.1.6 *Γ is 2- group i.e. for $x \in G$, $\exists n \in \mathbb{N}$ such that $x^{2^n} = 1$.*

Proof: We know that, Γ is generated by 4 elements a, b, c and d. Let $x \in \Gamma$, then $x \in \Gamma$ can be expressed as a product of a, b, c, d with alternate occurrences of a.
We will use induction on length $l(x)$ of x to prove that x is an element of order 2^s for some $s \in \mathbb{N}$. If $l(x) = 1$, then $x \in \{a, b, c, d\}$, then we have $a^2 = b^2 = c^2 = d^2 = 1$, we are done. Now assume that $l(x) > 1$. If the first generator in the expression of x is u(say), where $u \in \{b, c, d\}$, then $x = uw$, where w is a word in $\{a, b, c, d\}$. Then the conjugate uxu of x is of either same length (if last letter in x is a) or has shorter length(if last letter in x is not a). Since the conjugate elements have same order, so if uxu has shorter length, then by induction, it has order power of 2, then x also has order power of 2, and if uxu has same length, then the word uxu starts with an element different from the initial one and if a is not present in the expression, then $x^2 = 1$, Since, $< b, c, d > \cong V_4$, the non-cyclic group of order 4. In that case we are done.
So we can assume that number of occurrence of a in x is non-zero, and hence by the above argument, we can assume that x starts with the element a. Now suppose $l(x) =$ 2, then $x \in \{ab, ac, ad\}$. If $x = ad$, then by lemma 4.5, we know $(ad)^4 = 1$, if $x = ac$, then $\phi((ac)^2) = (da, ad), \Rightarrow \phi(ac)^8 = ((da)^4, (ad)^4) = (1, 1)$, since ϕ is injective, so $(ad)^8 = 1$ and if $x = ac$, then $\phi((ab)^2) = (ca, ac), \Rightarrow \phi(ac)^{16} = ((ca)^8, (ac)^8) = (1, 1)$, since ϕ is injective, so $(ad)^{16} = 1$. Hence if $l(x) = 2$, then x has order power of 2. Now assume that $l(x) \geq 3$. If x also ends with a, then x is of the form awa for some

word w a, b, c, d. Hence x is conjugate to a shorter word w and by induction, w has order power of 2, so does x. Now assume that x ends with b, c, d, therefore x has even length $2k$, where k is the number of pairs av, where $v \in \{b, c, d\}$.

Case 1: If k is even , then x has even number of $a's$. So $x \in H$. Then, we have a embedding $\phi : H \to \Gamma \times \Gamma$, $\phi(x) = (x_l, x_r)$, where x_l and x_r are have length at most $\frac{1}{2}l(x)$. Hence by induction hypothesis, suppose x_l has order 2^s and x_r has order 2^t, then if suppose $s > t$, then $\phi(x^{2^s}) = (x_l^{2^s}, x_r^{2^s}) = (1, 1)$ and since ϕ is injective. Therefore, $x^{2^s} = 1$, which shows that order of x is a power of 2.

Case 2: If k is odd, i.e. x has odd number of occurrence of a, then x^2 has even number of occurrence of a i.e. $x^2 \in H$, so $\phi(x^2) = (y_l, y_r)$, each of y_l, y_r has length at most $l(x)$.

Case 2.a Suppose first that, x involves the letter d. Since x^2 has length $2l(x)$ and is periodic with period $l(x)$, occurrence of d will be at least twice, at position that differ by $l(x) = 4r + 2$, one in the form d, and the other in form of ada. That means that when we write x^2 as product of generators of H, i.e. b, c, d, aba, aca, ada, then both d and ada will occur. Then in y_l, the generators d becomes 1, and in y_r, the generator ada becomes 1, and so both y_l and y_r have shorter length than x, and by induction hypothesis, x^2 has order power of 2, and order of x^2 is twice that of x, so x has order power of 2.

Case 2.b Suppose x does not involve d but involves c. As before, c will appear either in the form of c or in the form of aca, in any case either y_l or y_r involves d or d will disappear by cancellation. Now suppose without loss of generality, y_l contains d, then either y_l belongs H or not. If $y_l \in H$, then by Case 1, we get y_l has order power of 2 and if $y_l \notin H$, then y_l^2 belongs H. Then again we can write $\phi(y_l^2) = (z_l, z_r)$ and where $l(z_l), l(z_r) \leq l(y_l)$, since y_l^2 involves d, so by case 1 and induction y_l^2 has order power of 2 ad hence y_l has order power of 2. Similarly, we will have y_r of order power of 2. Therefore x^2 has order power of 2 so x has order power of 2.

Case c: If x does not involves d, c, then $x = (ab)^k$ for some $k \in \mathbb{N}$, and since

$(ac)^{16} = 1$, so x has order power of 2. $\square$

Definition 5.1.7 *A group G is said to be residually finite, if for any $g \in G$, there exist a finite group H and an epimorphism $\phi : G \to H$ such that $g \notin ker(\phi)$.*

More generally, If X is a certain family of groups, then a group G is termed as Residually-X if for any distinct elements $g, h \in G$ such that there exist a surjective group homomorphism $\phi : G \to H$ such that $\phi(g) \neq \phi(h)$ for some $H \in X$.

The above condition is equivalent to showing that for any $g \neq 1 \in G$, there exist a surjective group homomorphism $\phi : G \to H$, such that $\phi(g) \neq 1$ for some $H \in X$.

Proposition 5.1.8 *Let X be a certain class of groups. Then the following conditions are equivalent:*
1. A group G is Residually-X
2. For any $g \neq 1 \in G$, there exist a surjective group homomorphism $\phi : G \to H$ such that $\phi(g) \neq 1$ for some $H \in X$.

Proof: If (1) holds, then for $g \neq 1 \in G$, we will have a surjective homomorphism ϕ : $G \to H$ such that $\phi(g) \neq \phi(e) = e'$ for some $H \in X$ which proves (2). Conversely if (2) holds and suppose $g, h \in G$ are two distinct elements of G i.e. $g \neq h$ i.e. $gh^{-1} \neq 1$, and hence by (2)'1', there exist a surjective homomorphism $\phi : G \to H$ such that $\phi(gh^{-1}) \neq 1$ for some $H \in X$, hence $\phi(g) \neq \phi(h)$ which proves (1). $\square$

Definition 5.1.9 *Let G be a Residually-X group. Then we say that*

1. *G is Residually finite if X is the class of finite groups.*

2. *G is Residually nilpotent if X is the class of nilpotent groups.*

3. *G is Residually solvable if X is the class of solvable groups.*

4. *G is Residually-p if X is the class of finite-p groups.*

Similarly, we can define any Residual class, but the above four residually properties are very important.

If X is a certain class of groups, then any group $G \in X$ is Residually-X, because in that we can take H to be G and ϕ to be the identity map. In particular, every finite group is Residually finite, every nilpotent group is Residually nilpotent etc.

Proposition 5.1.10 *If X and Y are two classes of groups such that $X \subseteq Y$, then any group G which is Residually-X must also Residually-Y.*

Proof: Suppose G is Residually-X and $g \in G$ be any non identity element of G. Then there exist a surjective group homomorphism $\phi : G \to H$ such that $\phi(g) \neq 1$ for some $H \in X$ but $X \subseteq Y$, so $H \in Y$ and hence, G is Residually-Y. □

Corollary 5.1.11 *Every Residually nilpotent group is Residually solvable because every nilpotent groups is solvable.*

Corollary 5.1.12 *Every Residually-p group is Residually nilpotent because every finite p group is nilpotent.*

But the converse of any of the two is not true in general. We will see some examples but before that we need to prove a small proposition:

Proposition 5.1.13 *The following two conditions are equivalent:*
1. A group G is Residually finite
2. If $C = \{N | N \triangleleft G$ and $| G/N | < \infty\}$ then $\bigcap_{N \in C} N = \{e\}$.

Proof: Assume (1) holds, Let suppose $g \in \bigcap_{N \in C} N$, if $g \neq e$ then there exist a homomorphism $\phi : G \to H$ such that $\phi(g) \neq e$ for some finite group H. Then $g \in Ker(\phi)$ and since Ker$(\phi) \triangleleft G$ and Ker(ϕ) is of finite index. Therefore $Ker(\phi) \in C$ and hence $g \in Ker(\phi)$ which is a contradiction. Conversely assume (2) holds, and suppose that G is not Residually finite i.e. $\exists\, g \neq e$ such that for any surjective group homomorphism $\phi : G \to H$ for any finite group H, we have $\phi(g) = e$ i.e. $g \in Ker(\phi)$. In particular, if we take natural projection $\pi : G \to G/N$ for any $N \in C$. Then $g \in N$ for all $N \in C$. Hence, $g \in \bigcap_{N \in C} N = \{1\}$, gives a contradiction, which proves (1). □

Theorem 5.1.14 *Let Γ be the Grigorchuk group, then Γ is a residually finite group.*

Proof: Let $\{(0,1/2),(1/2,3/4),(3/4,7/8),...,(\frac{2^{k-1}-1}{2^{k-1}},\frac{2^k-1}{2^k})\}$ be a partition of the interval $(0,1)$ into 2^k subintervals. Elements of the group Γ permute these subintervals, and so we will have a homomorphism $\psi:\Gamma\to S_{2^k}$, the symmetric group on 2^k letters. Let H_k be the kernel of this homomorphism. Let $g\in Ker(\psi)$, this g fixes each 2^k subintervals, if suppose $g\in\bigcap_{k=1}^{\infty}Ker(\phi_k)$, i.e. g fixes each point of the interval, because any point lies in one the subintervals, so g must be the identity.
Therefore $\bigcap_{k=1}^{\infty}Ker(\phi_k)=1$. Thus by the above proposition, we conclude that, Γ is a residually finite group. $\square$

Theorem 5.1.15 *Let Γ be the Grigorchuk group, then Γ has solvable word problem.*

Proof: Let g be any word of Γ. If $l(g)=1$, then $g\in\{a,b,c,d\}$, then we can decide easily whether g is 1 or not. Suppose if $l(g)>1$, then write g in terms of a,b,c,d. Let $n(a)$ be the number of occurrence of a in the expression of g, If $n(a)$ is odd then $g\notin H$. Therefore g can not be the identity. Suppose if $n(a)$ is even, then $g\in H$, and by the previous embedding, write $\phi(g)=(g_l,g_r)$, where g_l and g_r have shorter length than of g. Therefore by induction , we can decide whether g_l or g_r represent the identity or not, and g represent the identity if and only if $g_l=1$ and $g_r=1$. $\square$

Proposition 5.1.16 *The Grigorchuk group Γ is commensurable with $\Gamma\times\Gamma$.*

Proof: We have the embedding $\phi:H\to\Gamma_l\times\Gamma_r$ given by $\phi(x)=(x_l,x_r)$. Since the elements of B can be generated by the conjugates of b i.e. aba,cbc,dbd, but

$$\phi(badab)=\phi(b)\phi(ada)\phi(b)=(a,c)(b,1)(a,c)=(aba,cc)=(aba,1)$$
$$\phi(abadaba)=\phi(aba)\phi(d)\phi(aba)=(c,a)(1,b)(c,a)=(cc,aba)=(1,aba)$$

Also, we have

$$\phi(abaadaaba)=\phi(aba)\phi(ada)\phi(aba)=(c,a)(b,1)(c,a)=(cbc,1)$$
$$\phi(bdb)=\phi(b)\phi(d)\phi(b)=(a,c)(1,b)(a,c)=(1,cbc)$$

Similarly,
$\phi(acaadaaca)=\phi(ada)\phi(aca)\phi(ada)=(d,a)(b,1)(d,a)=(bdb,1)$ and $\phi(cdc)=$

$\phi(c)\phi(d)\phi(c) = (a,d)(1,b)(a,d) = (1,dbd)$ and so the image of ϕ contains $(1,B)$ and $(B,1)$ and therefore contains all the generators of $B \times B$. Hence, $\phi(H)$ contains $B \times B$. Since $|\Gamma : B| \leq 8$, so $|\Gamma \times \Gamma : B \times B| \leq 8.8 = 64$. So $\phi(H)$ is of finite index in $\Gamma \times \Gamma$ and $\phi : H \to \phi(H)$ is an isomorphism. Therefore, Γ is commensurable with $\Gamma \times \Gamma$. □

Lemma 5.1.17 *Let $x \in H$, and write $\phi(x) = (x_l, x_r)$. Then $l(x_l)$ and $l(x_r)$ are at most $\frac{1}{2}(l(x)+1)$.*

Proof: We know that H is generated by the transformation b, c, d, aba, aca, ada, and also any element of Γ can be expressed in a, b, c, d with alternate occurrence of a, So any element $x \in H$ can be written as the product of the form u and ava, with $u, v \in \{b, c, d\}$. Let the length of x in Γ be $4k + r$, where k is the number of pairs (u, ava), present in the expression of $x \in H$, and $r \in \{0, 1\}$ and each pair contributes 4 to length of x $(l(x))$.

Now consider the map $\phi : H \to \Gamma_l \times \Gamma_r$ defined as $\phi(x) = (x_l, x_r)$. Since any generator of H map to elements x_l or x_r at most length 1, so each pair, which has length 4, map to elements x_l or x_r of at most length 2. If $r = 0$, then $l(x_l), l(x_r) \leq \frac{1}{2}l(x) \leq \frac{1}{2}(l(x)+1)$. If $r = 1$, then the remaining factor has length 1 or 3 and is mapped to single generator a or 1 □

5.1.1 Growth of Grigorchuk group

Now, we will show that the Grigorchuk group Γ has neither polynomial growth nor exponential growth, i.e. the growth function of Γ dominates every polynomial function and is strictly dominated by functions $f(n) = a^n$ for any real number $a > 1$. Let's first prove that Γ does not have polynomial growth with the help of Gromov's theorem.

Theorem 5.1.18 *Let Γ be the Grigorchuk group, then Γ does not have polynomial growth.*

Proof: We have seen that Γ is 3-generated infinite torsion group. Suppose Γ has polynomial growth, then by Gromov's theorem Γ must have nilpotent subgroup of finite index. Let N be a nilpotent subgroup of finite index in Γ. i.e. $|\Gamma : N| < \infty$.

Then since by 2.3.16, N is finitely generated group. Since by 2.3.2, N is finitely generated nilpotent group. So consider the lower central series of N

$$N = \gamma_1(N) \supseteq \gamma_2(N) \supseteq ... \supseteq \gamma_n(N) \supseteq \gamma_{n+1}(N) = 1 \tag{5.1}$$

where $\gamma_{i+1}(N) = [N, \gamma_i(N)]$ and $\gamma_i(N)/\gamma_{i+1}(G)$ is finitely generated abelian group. Also N is torsion group as Γ is torsion group. Therefore each successive quotient of lower central series is a finite abelian group, since the extension of finite group by finite group is finite group, i.e. if $\gamma_i(N)/\gamma_{i+1}(N)$ is finite and $\gamma_{i+1}(N)$ is finite then $\gamma_i(N)$ is finite. Now apply this, since $\gamma_n(N)/\gamma_{n+1}(N)$ is finite, and $\gamma_{n+1}(N)$ is finite, so $\gamma_n(N)$ is finite, Repeating this argument n times, we get that N is finite group. Using $|\Gamma : N| < \infty$, Γ is finite group, which is a contradiction. Hence, Γ does not have polynomial growth. □

Now it remains to show that growth Γ is subexponential (less than exponential). We have an index 2 subgroup H of Γ generated by b, c, d, aba, aca, ada and we have an embedding $\phi : H \to \Gamma \times \Gamma$ given by $\phi(x) = (x_l, x_r)$. Since $\mid \Gamma : H \mid= 2$, so $\mid \Gamma \times \Gamma : H \times H \mid= 2.2 = 4$. Now consider the set $K = \{x \in H : \phi(x) \in (H \times H)\}$. Since ϕ is injective, then $|H : K| = |\phi(H) : \phi(H) \cap (H \times H)| \leq 4$. Now K is a subgroup of H of index at most 4.
Therefore, $|\Gamma : K| = |\Gamma : H||H : K| \leq 2.|H : K| = 2.4 = 8$, which shows that K is subgroup of Γ of index at most 8. Now consider a new set $L = \{x \in K : \phi(x) \in K \times K\}$. Then L is a subgroup of K, hence a subgroup of H. Now $|K : L| = |\phi(K) : \phi(K) \cap (K \times K)| \leq 4.4 = 16.$, Therefore, we have $|\Gamma : L| = |\Gamma : K||K : L| \leq 8.16 = 128$.

If $x \in L$, then $\phi(x) \in K \times K$, i.e. $\phi(x) = (x_0, x_1)$, where $x_0, x_1 \in K$, By the definition of K, we have $\phi(x_0) = (x_{00}, x_{01})$ where $x_{00}, x_{01} \in H$. Now we have a map $\phi : H \to \Gamma \times \Gamma$, then $\phi(x_{00}) = (x_{000}, x_{001})$, where $x_{000}, x_{001} \in \Gamma$. Similarly, we can apply ϕ three times on x_1.
So if $x \in L$, then we have a map defined as

$$\phi : H \to \Gamma \times \Gamma \times ... \times \Gamma \ \ (8 times)$$

given by

$$\phi^3(x) = (x_{000}, x_{001}, x_{010}, x_{011}, x_{100}, x_{101}, x_{110}, x_{111})$$

where each coordinate in the octet belongs to Γ. For simplicity, we can write if $x \in L$, $\phi^3(x) = (x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8)$, where $x_i \in \Gamma$. $\square$

Lemma 5.1.19 *If $x \in L$, and $\phi^3(x) = (x_1, ..., x_8)$, then we have $\sum_{i=1}^{8} l(x_i) \leq \frac{3}{4}l(x) + 8$.*

Proof: If $x \in L$, then $\phi(x) = (x_l, x_r)$, and $\phi(x_l) = (x_{l_1}, x_{l_2})$, and $\phi(x_r) = (x_{r_1}, x_{r_2})$, and again apply, we get $\phi(x_{l_1}) = (x_{l_{11}}, x_{l_{12}})$, $\phi(x_{l_2}) = (x_{l_{21}}, x_{l_{22}})$, $\phi(x_{r_1}) = (x_{r_{11}}, x_{r_{12}})$ and $\phi(x_{r_2}) = (x_{r_{21}}, x_{r_{22}})$. Therefore, We have

$$\begin{aligned} \phi(x) &= (x_{l_{11}}, x_{l_{12}}, x_{l_{21}}, x_{l_{22}}, x_{r_{11}}, x_{r_{12}}, x_{r_{21}}, x_{r_{22}}) \\ l(x_{l_{11}}), l(x_{l_{12}}) \leq \frac{1}{2}((l(x_{l_1}) + 1), \quad & l(x_{l_{21}}), l(x_{l_{22}}) \leq \frac{1}{2}((l(x_{l_2}) + 1) \\ l(x_{r_{11}}), l(x_{r_{12}}) \leq \frac{1}{2}((l(x_{r_1}) + 1), \quad & l(x_{r_{21}}), l(x_{r_{22}}) \leq \frac{1}{2}((l(x_{r_2}) + 1) \end{aligned}$$

Let $\phi(x) = (x_{l_{11}}, x_{l_{12}}, x_{l_{21}}, x_{l_{22}}, x_{r_{11}}, x_{r_{12}}, x_{r_{21}}, x_{r_{22}}) = (x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8)$(say) then, we have

$$\begin{aligned} \sum_{i=1}^{8} l(x_i) &= l(x_{l_{11}}) + l(x_{l_{12}}) + l(x_{l_{21}}) + l(x_{l_{22}}) + l(x_{r_{11}}) + l(x_{r_{12}}) + l(x_{r_{21}}) + l(x_{r_{22}}) \\ &\leq \frac{1}{2}(l(x_{l_1}) + 1 + l(x_{l_2}) + 1 + l(x_{r_1}) + 1 + l(x_{r_2}) + 1) \\ &\leq l(x_{l_1}) + 1 + l(x_{l_2}) + 1 + l(x_{r_1}) + 1 + l(x_{r_2}) + 1 \\ &\leq l(x_l) + 1 + 2 + l(x_r) + 1 + 2 \\ &\leq l(x) + 1 + 1 + 2 + 1 + 2 \\ &\leq l(x) + 7 \end{aligned}$$

The number of occurrence of either b, c or d in x is between $\frac{1}{2}(l(x) - 1)$ and $\frac{1}{2}(l(x) + 1)$. Let us write $l_b(x), l_c(x)$ and $l_d(x)$ for the number of occurrence of b, c and d respectively. We saw that on applying ϕ, we get

$$l(x_l) + l(x_r) \leq \frac{1}{2}(l(x) + 1) + \frac{1}{2}(l(x) + 1) = l(x) + 1$$

. But each occurrence of d, either as itself or in ada, becomes 1 in either x_l or x_r. Therefore we have to subtract $l_d(x)$ from the sum. Next, each occurrence of c in x

becomes d in either x_l or x_r (but not in both). it is possible that on reducing x_l and x_r this occurrence of d disappears, but if it does not, it becomes 1 on applying ϕ again. Then when applying ϕ^2, we have to subtract also $l_c(x)$ and similarly, on applying ϕ^3, we subtract also $l_b(x)$. But we can not subtract both $l_c(x)$ and $l_b(x)$, because c and b may cancel out together. Therefore we can subtract either $l_c(x)+l_b(x)$ or $l_d(x)+l_b(x)$. Since at least one of these is at least $\frac{1}{2}(l_b(x)+l_c(x)+l_d(x))$ otherwise if

$$\begin{aligned}
&l_d(x)+l_b(x) < \frac{1}{2}(l_b(x)+l_c(x)+l_d(x)) \\
&l_b(x)+l_c(x) < \frac{1}{2}(l_b(x)+l_c(x)+l_d(x)) \\
&\therefore 2l_b(x)+l_c(x)+l_d(x) < l_b(x)+l_c(x)+l_d(x) \\
&l_b(x) < 0
\end{aligned}$$

which is not possible. So either $l_d(x)+l_b(x) \geq \frac{1}{2}(l_b(x)+l_c(x)+l_d(x))$ or $l_b(x)+l_c(x) \geq \frac{1}{2}(l_b(x)+l_c(x)+l_d(x))$. Now, since we have

$$l_b(x), l_c(x), l_d(x) \geq \frac{1}{2}(l(x)-1)$$

and if

$$\begin{aligned}
l_d(x)+l_b(x) &\geq \frac{1}{2}(l_b(x)+l_c(x)+l_d(x)) \\
&\geq \frac{1}{4}(l(x)-1)
\end{aligned}$$

Now,

$$\begin{aligned}
\sum_{i=1}^{8} l(x_i) &\leq (l(x)-7)-(l_b(x)+l_d(x)) \\
&\leq (l(x)+7)-\frac{1}{4}(l(x)-1) \\
&\leq \frac{3}{4}l(x)+8
\end{aligned}$$

Therefore, we have $\sum_{i=1}^{8} l(x_i) \leq \frac{3}{4}l(x)+8$.

□

Theorem 5.1.20 *Let Γ be the Grigorchuk group, then Γ has subexponential growth.*

Proof: Let $s_\Gamma(n)$ be the growth function of Γ and $w(\Gamma) = \lim(s_\Gamma(n))^{1/n}$.
In order to show that Γ has subexponential growth, we need to show that $w(\Gamma) = 1$.

Let L be the subgroup defined above and we also saw that $|\Gamma : L| < \infty$. Let k be an upper bound for the length of a set(T) of representatives of cosets of L, by 2.3.17 we can take $|\Gamma : L| = k$. Two different elements can give rise to the same element y only if they lie in different cosets because if $x_1, x_2 \in \Gamma(\ x_1 \neq x_2)$, then $x_1 = yz_1$ and $x_2 = yz_2$ so if z_1 and z_2 are same that would lead that x_1 and x_2 are same, which is a contradiction. We denote $s_L^\Gamma(n)$ for the number of elements of L of length (in Γ) at most n. Therefore by 2.3.17 we have

$$s_\Gamma(n) \leq s_L^\Gamma(n+k) \mid \Gamma : L \mid .$$

Consider an embedding $\phi^3 : L \to \Gamma \times \Gamma \times ... \times \Gamma$ (8 times) given by

$$\phi^3(x) = (x_1, x_2, ..., x_8),$$

, where $x \in L$. So by this embedding, x can be completely determined by the action of x_i for each $1 \leq i \leq 8$.

Let $l(x_i) = n_i$. Then it is clear that $n_i \leq n$ by lemma. Since the action of some of the x_i could be trivial i.e. x_i could be identity. So $n_i = l(x_i) \in \{0, 1, 2, ..., n\}$. Therefore the number of possibilities for the octet $(n_1, n_2, ..., n_8)$ is at most $(n+1)^8$. For any such octet, the number of possibilities for $(x_1, ..., x_8)$ is $\prod_i s_\Gamma(n_i)$. Write $w = w(\Gamma)$. Since we have $w = (s_\Gamma(n))^{\frac{1}{n}}$,

$$w^n \leq s_\Gamma(n) \leq (w+\epsilon)^n$$

for large n enough.

Then there exists a constant A such that $s_\Gamma(n) \leq A(w+\epsilon)^n$ for all n. Given an octet $(n_1, n_2, ..., n_8)$ as above, this implies that number of possibilities for the octet $(x_1, x_2, ..., x_8)$ is at most $\prod_{i=1}^8 A(w+\epsilon)^{n_i}$.

$$\prod_{i=1}^{8} A(w+\epsilon)^{n_i} = A^8(w+\epsilon)^{n_1+...+n_8} \leq A^8(w+\epsilon)^{\frac{3}{4}n+8} \leq C(w+\epsilon)^{\frac{3}{4}n}$$

where $C = A^8(w+\epsilon)^8$, Now,

$$w^n \leq s_\Gamma(n) \leq s_L^\Gamma(n+k)|\Gamma : L| \leq |\Gamma : L| C(n+k+1)^8(w+\epsilon)^{\frac{3}{4}n+8}$$

taking n^{th} roots and letting n go to infinity and ϵ go to 0, we have $w \leq w^{\frac{3}{4}}$. This implies that $w = 1$, which shows that the Grigorchiuk group has subexponential growth. $\square$

Corollary 5.1.21 *Let Γ be the Grigorchuk group, then Γ has intermediate growth.*

Proof: By the theorem 5.1.18, Γ does not have polynomial growth and by 5.1.20, Γ has subexponential growth. Therefore, Γ has intermediate growth.. $\square$

Theorem 5.1.22 *There exist number $0 < \alpha, \beta < 1$ and $A, B >$ such that $A^{n^\alpha} \leq s_\Gamma(n) \leq B^{n^\beta}$.*

Proof: The proof refers to [1] $\square$

5.2 Gupta-Sidki group

Now, we will define a new family of groups of intermediate growth. These groups were first constructed by Narain Gupta and Said Sidki in 1983. Along with the intermediate nature of these groups, these groups also gives a answer to the Burnside problem. For each odd prime p, Gupta - Sidki groups is a p-generated infinite torsion group and it has intermediate growth. First, we will define it, then we will see some interesting properties. These groups were defined as the subgroup of automorphism group of p - regular rooted tree.

Fix p be an odd prime. A tree is a connected graph which has no circuits. A regular p -rooted tree is a tree $T(0)$, which has one base vertices (say 0), and from the vertex 0 , there are p vertices say $(0,1),(0,2),...,(0,p)$ attached to the vertex 0, and from each p vertices $(0,i)$, where $1 \leq i \leq p$, there are again p vertices say $(0,i,1),(0,i,2),...,(0,i,p)$ vertices attached to it, and so on. In other words, the subtree hanging from any of the vertices of the tree $T(0)$ looks similar to be as their parental tree $T(0)$. Let $T(0)$ be an infinite regular p-rooted tree with initial vertex at 0 (also called as the root of a tree).

Definition 5.2.1 *An automorphism ϕ of a tree T is map $\phi : T \rightarrow T$which is a bijection on the set of vertices, Such ϕ takes the vertices to vertices and if u, v be any two vertices such that $[u,v]$ is the direct edge between u and v, then $[\phi(u), \phi(v)]$ must be the direct edge between $\phi(u)$ and $\phi(v)$. The automorphism group of a tree T is the set of all automorphism of tree T and is denoted by $Aut(T)$.*

Let $T(0)$ be an infinite regular p - rooted tree. Now we will define Gupta - Sidki group as the subgroup generated by two particular type of automorphisms, say $t(0)$ and $a(u)$ inside the group $Aut(T(0))$.

Suppose $T(0)$ is a infinite regular p - tree with initial vertex 0 and if u is any vertex of this infinite tree $T(0)$, we denote $T(u)$ be the tree hanging at the vertex u, which is also a regular p - rooted tree and looks like as of parental tree $T(0)$. So, there are p-regular subtrees say $T(0,1), T(0,2), ..., T(0,p)$ with roots $(0,1),(0,2),...,(0,p)$

respectively, whose initial vertices are direct connected with initial the root 0 of the tree $T(0)$.

In order to define an automorphism ϕ of tree $T(0)$, it is sufficient to know the image of vertices under the action of ϕ. Now we will define an automorphism $t(u)$. For each vertex u of $T(0)$,

we define $t(u) : T(u) \to T(u)$ by

$$t(u)(T(u,j)) = T(u, j+1) for j = 1, 2, ..., p-1, and$$
$$t(u)(T(u,p)) = T(u, 1)$$

The automorphism $t(u)$ fixes the vertices u, and cyclically permutes the vertices $(u, 1), (u, 2), ..., (u, p)$, so after iterating p times, the action of $t(u)$ becomes trivial so $t(u)$ is of order p. Now, we will define the another automorphism

$$a(u) : T(u) \to T(u)$$
$$a(u)(T(u,j)) = t(u,1)t^{-1}(u,2)i(u,3)...i(u,p-1)a(u,p)$$

where $t(u, 1)$ is an automorphism defined above which cyclically permutes the vertices $(u, 1, 1), (u, 1, 2), ..., (u, 1, p)$ and $t^{-1}(u, 2)$ is the inverse of $t(u, 2)$ and $a(u, p)$ is an automorphism,

$a(u,p) : T(u,p) \to T(u,p)$ defined as $a(u)(T(u,p,j)) = t(u,p,1)t^{-1}(u,p,2)i(u,p,3)...i(u,p,p-1)a(u,p,p)$. So the action of $a(u)$ on $T(0)$ acts recursively in terms of the automorphism $t(u)$ and $a(u)$.

Since we have an infinite regular p-rooted tree, and the action of $a(u)$ like $t(0, 1)$ on $(u, 1)$, $t^{-1}(u, 2)$,identity automorphism $i(u, 3)$ on $(u, 3)$,..., and $a(u, p)$ acts on (u, p) as the same way as $a(u)$ on u.

Definition 5.2.2 *Let p be an odd prime. Consider the subgroup generated by two automorphisms $t(0)$ and $a(0)$ in the group $Aut(T(0))$ and denote it by $G_p(0)$. Then $G_p(0)$ is the Gupta - Sidki group.*

Since we have fixed a prime p. So we use the notation $G(0)$ instead of $G_p(0)$. Now we will see some interesting properties of $G(0)$. More generally, for any vertex u of $T(0)$, let $G(u)$ denote the group generated by the automorphism $t(u)$ and $a(u)$.

Theorem 5.2.3 : *The group $G(0)$ generated by $t(0)$ and $a(0)$ is an infinite group.*

Proof: We defined $a(0)$ as

$$a(u) : T(0) \to T(0)$$
$$a(0)(T(0,j)) = t(0,1)t^{-1}(0,2)i(0,3)...i(0,p-1)a(0,p)$$

Since, $t(0,1)$ is an automorphism of tree $T(0,1)$ (rooted at $(0,1)$), $t(0,1) \in G(0,1)$. Similarly $t^{-1}(0,2)$ is an automorphism of tree $T(0,2)$ (rooted at $(0,2)$) and so $t^{-1}(0,2) \in G(0,2)$. In the same way $i(0,3) \in G(0,3), ..., i(0,p-1) \in G(0,p-1)$ and $a(0,p) \in G(0,p)$.

Since $t(0,1)$ is an automorphism of the $T(0,1)$. So, it fixes all other vertices $(0,2),(0,3),...,(0,p)$. Similarly $t^{-1}(0,2)$ is automorphism of the $T(0,2)$ and it acts as the identity transformation on the tree $T(0,1), T(0,3), ..., T(0,p)$. The identity automorphisms $i(0,3), ..., i(0,p-1)$ acts trivially on each subtree and the automorphism $a(0,p)$ acts as the identity transformation on $T(0,1), T(0,2), ..., T(0,p-1)$.

Therefore,

$$\begin{aligned} a(0) &= t(0,1)t^{-1}(0,2)i(0,3)...i(0,p-1)a(0,p) \\ &\in G(0,1) \times G(0,2) \times G(0,3) \times ... \times G(0,p-1) \times G(0,p) \end{aligned}$$

where, $G(u)$ is the group generated by $t(u)$ and $a(u)$. Let's denote the automorphism

$$a(0) = t(0,1)t^{-1}(0,2)i(0,3)...i(0,p-1)a(0,p)$$

by $a = (t, t^{-1}, i, ..., a)$. Also, let's denote $t^{-j}(0)a(0)t^{j}(0) = a_j$ for each $j = 0, 1, ..., p-1$, then $a_0 = t^{-0}a(0)t^0 = a(0) = (t, t^{-1}, i, i, ..., a)$

Since, $t^{-0}(0)a(0)t^{0}(0) = a(0) = (t, t^{-1}, i, ..., a)$, Now consider the action of $t^{-1}a(0)t^1$, on the following:

on T(0,1): The automorphism $t^{-1}(0)a(0)t^1(0)(T(0,1)) = t^{-1}(0)a(0)(T(0,2))$, since $a(0)$ acts like the automorphism $t(0)$ on $T(0,2)$ and since $t^{-1}(0)$ is the inverse of $t^1(0)$, so $t^{-1}(T(0,2) = T(0,1)$. Hence the automorphism $t^{-1}(0)a(0)t^1(0)$ on $T(0,1)$ acts like $t^{-1}(0)$, denote by t^{-1}.

on T(0,2): The automorphism $t^{-1}(0)a(0)t^1(0)(T(0,2)) = t^{-1}(0)a(0)(T(0,3))$, since $a(0)$ acts like the automorphism $i(0)$ on $T(0,2)$ and since $t^{-1}(T(0,3)) = T(0,2)$, hence the automorphism $t^{-1}(0)a(0)t^1(0)$ on $T(0,2)$ acts like $i(0)$, denote by i.

on T(0,3): The automorphism $t^{-1}(0)a(0)t^1(0)(T(0,3)) = t^{-1}(0)a(0)(T(0,4))$, since $a(0)$ acts like the identity automorphism $i(0)$ on $T(0,4)$ and since $t^{-1}(T(0,4)) = T(0,3)$, hence the automorphism $t^{-1}(0)a(0)t^1(0)$ on $T(0,3)$ acts like $i(0)$, denote by i.

.....

on T(0,p-1): The automorphism $t^{-1}(0)a(0)t^1(0)(T(0,p-1)) = t^{-1}(0)a(0)(T(0,p))$, since $a(0)$ acts like the automorphism a on $T(0,p)$ and since $t^{-1}(T(0,p)) = T(0,p-1)$, hence the automorphism $t^{-1}(0)a(0)t^1(0)$ on $T(0,p-1)$ acts like a_0, denote by a_0.

on T(0,p): The automorphism $t^{-1}(0)a(0)t^1(0)(T(0,p) = t^{-1}(0)a(0)(T(0,1))$, since $a(0)$ acts like the automorphism $t(0)$ on $T(0,1)$ and since $t^{-1}(T(0,1)) = T(0,p)$, hence the automorphism $t^{-1}(0)a(0)t^1(0)$ on $T(0,p)$ acts like $t(0)$, denote by t.

Therefore, we have

$$a_1 = t^{-1}(0)a(0)t^1(0) = (t^{-1}, i, i, ..., a_0, t)$$

Similarly, we can have

$$a_2 = t^{-2}(0)a(0)t^2(0) \qquad = (i, i, ..., a_0, t, t^{-1})$$

$$a_3 = t^{-3}(0)a(0)t^3(0) \qquad = (i, i, ..., a_0, t, t^{-1}, i)$$

$$...$$

$$a_{p-1} = t^{-(p-1)}(0)a(0)t^{(p-1)}(0) \qquad = (a_0, t, t^{-1}, ..., i, i)$$

Since by definition of $a_0, a_1, ..., a_{p-1}$, these p elements of $Aut(T(0))$ belongs to $G(0)$. Consider the subgroup generated by these p elements, call it $H(0)$, say $H(0) = < a_0, a_1, ..., a_{p-1} >$. □

Proposition 5.2.4 *The subgroup $H(0)$ generated by $a_0, a_1, ..., a_{p-1}$ forms a normal subgroup of index p in $G(0)$.*

Proof: Clearly, the generators $H(0)$ is closed under the conjugation action of $t(0)$. So, $H(0)$ is a normal subgroup. Now we will show that $|G(0) : H(0)| = p$, Since $H(0)$ is a normal subgroup of $G(0)$, $G(0)/H(0)$ has natural group structure. Therefore we have natural map $\eta : G(0) \to G(0)/H(0)$ given by $\eta(a(0)) = 1$ and $\eta(t(0)) = t(0)H(0)$, where 1 represent the identity element of $G(0)/H(0)$. Since $G(0) =< a(0), t(0) >$, $G(0)/H(0)$ is generated by $t(0)H(0)$ order p in $G(0)$. Certainly, $(t(0)H(0))^p = t^p(0)H(0) = H(0)$ and also no power less than p (say i), exist for which $t^i \in H(0)$, because t^i just the permutation of first level, and since elements of $H(0)$ permutes at least one branches at each level. So $t^i \notin H(0)\ \forall\ 0 < i < p$. Hence, $t(0)H(0)$ has order p. So $\{G(0) : H(0)\} = p$. Therefore, $H(0)$ is normal subgroup of $G(0)$ of index p. □

Definition 5.2.5 *Let G and H be two groups. A subdirect product of G and H is a subgroup K of the external direct product $G \times H$ such that the natural projections $\pi_G : K \to G$ and $\pi_H : K \to H$ is surjective homomorphisms.*

Lemma 5.2.6 *If H is the subdirect product of $G_1, G_2, ..., G_p$, where each $G_i \cong G$ for some group G and H is a proper subgroup of G, then G is an infinite group.*

Proof: Here, $G_1, G_2, ..., G_p$ be the isomorphic copies of a group G. Since H is the subdirect product of $G_1, G_2, ..., G_p$ i.e. H is a subgroup of $G_1 \times G_2 \times ... \times G_p$ and the projections map $\pi_i : H \to G_i$ given by $\pi_i(g_1, g_2, ..., g_p) = g_i$ is onto. Since $G_i \cong G$ and $H \leq G_i \cong G$. Hence, We have an epimorphism from a proper subgroup H of G to G. Therefore, G is infinite group. □

Proposition 5.2.7 *The group $H(0)$ is the subdirect product of $G(0,1), G(0,2), ..., G(0,p)$.*

Proof: We know the subgroup $H(0)$ generated by $a_0, a_1, ..., a_p$ is a normal subgroup of index p in $G(0)$ and each $a_j \in G(0,1) \times G(0,2) \times G(0,3) \times ... \times G(0,p)$. Therefore $H(0)$ is a subgroup of $\in G(0,1) \times G(0,2) \times G(0,3) \times ... \times G(0,p)$. We have a natural projection $\pi_1 : H(0) \to G(0,1)$ given by $\pi_1(h_1, h_2, ..., h_p) = h_1$. Since

$$\pi_1(a_0) = \pi_1(t, t^{-1}, i, ..., a_0) = t$$
$$\pi_1(a_{p-1}) = \pi_1(a_0, t, t^{-1}, ..., i, i) = a_0$$

Since $G(0,i) \cong G(0)$ for each $1 \leq i \leq p$, and image of π_1 contains the generating set. Hence ,π_1 is surjective map. Similarly each π_j is surjective. So $H(0)$ is the subdirect product of $\in G(0,1) \times G(0,2) \times G(0,3) \times ... \times G(0,p)$, each $G(0,j) \cong G(0)$ and $H(0)$ is a proper subgroup of $G(0)$.
Hence, by previous lemma, $G(0)$ is an infinite group.

Now we will prove that every element in $G(0)$ is of finite order. First we will see that any arbitrary element $g \in G(0)$ must be of the form $g = ht^j$, where $h = h(a_0, a_1, ..., a_{p-1})$ is a word in $a_0, a_1, ..., a_{p-1}$. Since, we have the relation

$$t^{-j}(0)a(0)t^j(0) = a_j \Rightarrow t^j(0)a(0) = a_{-j}t^j(0) \tag{5.2}$$

Using induction, suppose $t^j(0)a^n(0) = h(a_0, a_1, ..., a_p)t^r(0)$, Now consider

$$t^j(0)a^{n+1}(0) = t^j(0).a^n(0).a(0) = h(a_0, a_1, ..., a_p)t^r(0)a(0) = h(a_0, a_1, .., a_p)a_{-r}t^r(0)$$

Hence, using the equation number (9), we can write arbitrary elements g of $G(0)$ as $g = ht^j$, where $h = h(a_0, a_1, ..., a_{p-1})$ is a word in $a_0, a_1, ..., a_{p-1}$.

Thus we may consider $g \in G(0)$ as an element of $(< a_0 > * < a_1 > *...* < a_{p-1} >) \rtimes < t >$. $\square$

Theorem 5.2.8 $G(0)$ *is a torsion group.*

Proof: We will prove that any element $g \in G(0)$ has order power of p. Let $g \in \{t(0), a(0)\}$. We have seen that the automorphism $t(0)$ has order p. Since we know that $a(0) = t(0,1)t^{-1}(0,2)i(0,3)...i(0,p-1)a(0,p)$, iterating p times of $a(0)$, action on the subtree $T(0,1)$ becomes trivial, similarly on $T(0,2),...,T(0,p-1)$ and on the last subtree on the first level i.e. $T(0,p)$, it acts like $a(0,p)$. Since we apply it recursively, we get that $a(0)$ has order p.

Let $\lambda(k)$ be the length contributed by a_k, and then the syllable length of word $h(a_0, a_1, ..., a_{p-1})$ is $\lambda(0) + \lambda(1) + ... + \lambda(p-1)$.
Now we will use induction on the syllable length of g to prove that g has order power of p

Suppose our claim holds for all the words upto syllable length m i.e. all the elements of syllable length at most m have elements of order power of p and suppose g is an element of syllable length $m + 1 \geq 2$.

Case I : If $g = h(a_0, a_1, ..., a_{p-1})t^{p-j}, j \in \{1, 2, ..., p-1\}$. . Since we have

$$\begin{aligned}
g &= ht^{p-j} \\
g^p &= ht^{p-j}.ht^{p-j}...ht^{p-j} \\
&= h.(t^{p-j}ht^{p-j}).ht^{p-j}...ht^{p-j}. \\
&= h.(t^{-j}ht^{j}).(t^{p-2j}ht^{p-j})....ht^{p-j} \\
&= h.h^{t^j}.h^{t^{2j}}.(t^{p-3j}ht^{p-j})...ht^{p-j} \\
&= h.h^{t^j}.h^{t^{2j}}...h^{t^{(p-2)j}} \\
(\because t^{p-(p-1)j}.ht^{p-j} &= t^{-(p-1)j}ht^{(p-1)j}.t^{-(p-1)j+p-j} \\
&= h^{t^{(p-1)j}}.t^{-pj+j+p-j} = ht^{(p-1)j})
\end{aligned}$$

Therefore, we have

$$g^p = h.h^{t^j}.h^{t^{2j}}...h^{t^{(p-2)j}}.h^{t^{(p-1)j}}$$

is an element of $H(0)$ (since generator of $H(0)$ remains in $H(0)$ after taking the conjugation by t). Therefore the syllable length of each the conjugate $t^{-kj}ht^{kj}$ for $j \in \{0, 1, ..., p-1\}$ is same as the syllable length of h i.e. the syllable length of $g^p = m + m + ... + m = mp$. Also, a_k takes the all values a_i for $i \in \{0, 1, ..., k\}$ after conjugating all the $p-1$ powers of t and therefore has the property that the length contribution due to each a_k is $\lambda(0) + \lambda(1) + ... + \lambda(p-1) = m$. Since, we can write each $h^{t^{rj}}$ in p tuple, so expressing g^p as a p-tuple, shows that for each j, the $G(0, j)$-component of g^p is an element of $H(0, j)$ of syllable length at most m and if the component has syllable length $\lambda(p-j)$, then by induction hypothesis, it has order power of p. If the component has $\lambda(p-j) + 1 = m + 1$, then $m = 1$. Now consider the following cases:

Case a: If $\lambda(p-j) + 1 \leq m$
$\lambda(p-j) \leq m - 1 \leq m$. So each component has order power of p
Case b: If $\lambda(p-j) + 1 > m$
$\therefore \lambda(p-j) + 1 \geq m$
but, since $\lambda(0) + \lambda(1) + ... + \lambda(p-j) + ... + \lambda(p-1) = m + 1$
if $\lambda(p-j) + 1 > m + 1$, which implies that $\lambda(p-j) > m$ (not possible) (at least some $\lambda(k) \neq 0$ for $k \in \{1, 2, .., p-1\}$). So, $\lambda(p-j) + 1 = m + 1 \Rightarrow \lambda(p-j) = m$

Therefore, this component has length m so it has order power of p.

Case II: Let $g = h(a_0, ..., a_{p-1}) \in H(0)$. Suppose h has syllable length $m + 1 = \lambda(0) + ... + \lambda(p-1)$. Now express h as in the form p tuple, which shows that $G(0, j)$-component has syllable length $\lambda(p-j)$, then by induction hypothesis, it is a p element (since $\lambda(p-j) \leq m$). if the component has length $\lambda(p-j)+1$ and $\lambda(p-j)+1 \leq m$, then again by the induction hypothesis it is a p element. If the component has length $\lambda(p-j) + 1 = m + 1$, then $m = 1$ and it is a p element by Case I and the induction hypothesis. Thus, g is a p element. Therefore, in any case g is an p element. Hence, $G(0)$ is a torsion group. □

So we have seen so far, for each odd prime p, the Gupta-Sidki Group is finitely generated infinite torsion group.

5.2.1 Growth of Gupta Sidki Group

Now we will prove that the Gupta Sidki group has intermediate growth. We will prove it in two steps first by showing that this group does not have polynomial growth and in the next step we will show that this group has subexponential growth.

Theorem 5.2.9 *For each odd prime p. Let $G(0)$ be the Gupta Sidki group, then $G(0)$ does not have polynomial growth.*

Proof: We have seen that $G(0)$ is finitely generated infinite torsion group. Suppose $G(0)$ has polynomial growth, then by Gromov's theorem, $G(0)$ must have nilpotent subgroup of finite index. Suppose N be a nilpotent subgroup of finite index in $G(0)$. i.e. $|G(0) : N| < \infty$. Then since by 2.3.16 N is finitely generated group. Since by 2.3.2, N is finitely generated nilpotent group, also N is torsion group because $G(0)$ is torsion. So consider the lower central series of N

$$N = \gamma_1(N) \supseteq \gamma_2(N) \supseteq ...\gamma_n(N) \supseteq \gamma_{n+1}(N) = 1 \tag{5.3}$$

where $\gamma_{i+1}(N) = [N, \gamma_i(N)]$, since $\gamma_i(N)/\gamma_{i+1}(G)$ is finitely generated abelian group. Since N is torsion group. Therefore each successive quotient of lower central series is finite abelian group, since the extension of finite group by finite group is finite group, i.e. if $\gamma_i(N)/\gamma_{i+1}(N)$ is finite and $\gamma_{i+1}(N)$ is finite then $\gamma_i(N)$ is finite. Now apply this, since $\gamma_n(N)/\gamma_{n+1}(N)$ is finite, and $\gamma_{n+1}(N)$ is finite, so $\gamma_n(N)$ is finite, Repeating this argument n times, we get N is finite group. Since $|G(0) : N| < \infty$, $\therefore$ $G(0)$ is finite group, which is a contradiction. Hence, $G(0)$ does not have polynomial growth. □

Here we will prove that the Gupta - Sidki group has subexponential growth. In order to prove it, we will use some result regarding Splitter Mixer Group[14]. So Let's define the splitter mixer group.

Let $\omega = \{1, ..., d\}$ be a finite set; the set $\omega*$ of finite sequences over ω is naturally (the vertex set of) a d-regular rooted tree, rooted at the empty sequence, if one connects for all $\sigma_i \in \omega$ the vertices $\sigma_1...\sigma_n$ and $\sigma_1...\sigma_n.\sigma_{n+1}$. Let A be a subgroup of the symmetric group of $\omega \cong S_d$; let B be a finite group, and let $\tilde{B} = B_1 \times B_2 \times ...$ be the direct product of countably many copies of B; let $\phi_1, \phi_2, ..., \phi_{d-1}$ be homomorphism $\tilde{B} \to A$, and let $\phi_d : \tilde{B} \to B$ be the one-sided shift $(b_1, b_2, ...) \to (1, b_1, b_2, ...)$. Write ϕ_i^n for the restriction of ϕ_i to B_n. Now we define a action of A and $\tilde{B}$ on $\omega*$ as follows: the action of $a \in A$ is

$$(\sigma_1\sigma_2...\sigma_n)^a = (\sigma_1)^a\sigma_2...\sigma_n$$

and the action of $\tilde{b} \in \tilde{B}$ is defined inductively by

$$(\sigma_1\sigma_2...\sigma_n)^{\tilde{b}} = \sigma_1(\sigma_1\sigma_2...\sigma_n)^{\phi_{\sigma_1}(\tilde{b})}.$$

Let G be the subgroup of $Aut(\omega*)$ generated by A and B_1, i.e. the largest quotient of $A * B_1$ that acts faithfully on $\omega*$. Such a group G is called a *splitter-mixer group.*

Theorem 5.2.10 *[14] Let G be a splitter-mixer group as defined above, then G has subexponential growth.*

■

Proof: Proof refers to [14]

Theorem 5.2.11 *Let $G(0)$ be the Gupta-Sidki group, then $G(0)$ has subexponential growth.*

Proof: We will use the theorem 5.2.10 to prove that the Gupta-Sidki group has subexponential growth. Since the Gupta Sidki group $G(0)$ can be obtained in above setting by taking $\omega = \{1, 2, .., p\}$ for $p \geq 3$, $A = < x = (1, 2, ..., p) >$ and $B = A$, and $\phi_1^n = \phi_2^n(x^{-1}) = x, \phi_3^n = ... = \phi_{p-1}^n$, which implies that $G(0)$ is a splitter-mixer group and hence by 5.2.10, $G(0)$ has subexponential growth.

Corollary 5.2.12 *Let $G(0)$ be the Gupta-Sidki group, then $G(0)$ has intermediate growth.*

Proof: Since by 5.2.9, $G(0)$ does not have exponential growth and by 5.2.11 $G(0)$ have subexponential growth. Hence, G has intermediate growth. □

Bibliography

[1] Avinoav Mann, *How Groups Grow*, *Lecture Series Notes*, London Mathematical Society,(2002).

[2] Hymann Bass, *The degree of polynomial growth of finitely generated nilpotent group*, *Proc of London Mathematical Society* **25**(1972),603 - 614.

[3] John Milnor, *Growth of finitely generated solvable groups*, *J. Differential Geom.* **2**(1968), 447–449.

[4] M. Gromov, *Groups of polynomial growth and expanding maps*, *Publ. Math. IHES* **53**(1981), 53-73

[5] Martin Issac, *Finite Group Theory*, *American Mathematical Society*

[6] Pierre de la Harpe, *Topics in geometric group theory*, University of Chicago Press, 2000

[7] R.I.Grigorchuk, *Burnside's problem on periodic groups*, *Func. Anal.App,* **14**(1980),41-43

[8] R.I.Grigorchuk, *Degrees of growth of finitely generated groups, and theory of invariants means*, *Izv. Akad. Nauk SSSR Ser. Mat.* **48**(939-985)

[9] J.A.Wolf, *Growth of finitely generated solvable groups and curvature of Riemannian manifolds*, *J. Diff. Geo* **2**(1968), 421-446.

[10] I. Kaplansky, *Lie Algebras and Locally Compact Groups*, 2nd edn., University of Chicago Press, Chicago 1995.

[11] D. Montgomery and L.Zippin, *Topological Transformation Groups*, *Interscience, New York* 1955.

[12] R.I.Grigorchuk, Igor Pak, *Groups of intermediate growth, an introduction*, 2008.

[13] L.Bartholdi, *Lower bounds on the growth of a group acting on the binary rooted tree*, *Int. J. Alg. Comp* **11** (2001),73-88

[14] L.Bartholdi, *Groups of Intermediate Growth*, *arXiv:math/0201293.*

[15] J.Tit's, *Free subgroups in linear groups*, *J. Alg* **20**(1972), 250-270.

[16] V. Nekrashevych, *Self-similar groups*, Mathematical Surveys and Monographs, Volume 117, American Mathematical Society, 2005.

[17] D.S.Dummit and Richard M.Foote, *Abstract Algebra*, *Wiley Student Edition*,2013

[18] Philip Hall, *Notes on Nilpotent groups*, *Lectures Notes at Canadian Mathematical Congress*, University of Alberta, 1957

[19] Clara Loh, *Geometric Group Theory an introduction*,2011

[20] I.M. Issac, *Character theory of Finite Groups*, *Academican Press*, San Diego 1976

[21] R. Grigorchuk, *Milnor's Problem on the Growth of Groups and its consequences*, Frontiers in Complex Dynamics, *51 Princeton and Oxford*, 2014, 705-773.