On the minimal number of generators of a finite group

Diogo Santos
Mestrado em Matemática
Departamento de Matemática
2024

Orientador
Prof. Dr. Claude Marion, Faculdade de Ciências

U.PORTO

FACULDADE DE CIÊNCIAS
UNIVERSIDADE DO PORTO

Todas as correções determinadas
pelo júri, e só essas, foram efetuadas.

O Presidente do Júri,

Porto, ______/______/________

MSc

UNIVERSIDADE DO PORTO

MASTERS THESIS

On the minimal number of generators of a finite group

Author:
Diogo SANTOS

Supervisor:
Claude MARION

A thesis submitted in fulfilment of the requirements
for the degree of MSc. Mathematics

at the

Faculdade de Ciências da Universidade do Porto
Departamento de Matemática

December 19, 2024

Acknowledgements

I would like to express my gratitude to my supervisor, Professor Claude Marion, for his valuable guidance and expertise, as well as for sparking my interest in this fascinating subject.

UNIVERSIDADE DO PORTO

Abstract

Faculdade de Ciências da Universidade do Porto

Departamento de Matemática

MSc. Mathematics

On the minimal number of generators of a finite group

by Diogo SANTOS

A characterization of finite groups whose proper quotients are m-generated, but not themselves, is provided via a structure theorem first established in [1].

Contents

Introduction

One of the questions in finite group theory is to determine the minimal number of generators of a finite group.

For a finite group H, the minimal number of generators $d(H) = min\left\{|X| | \langle X \rangle = H\right\}$ always exists. This is so because H is always generated by itself, a finite set. On the other hand there are infinite groups that do not have a minimal number of generators. One such example is $\mathbb{Z}^{\mathbb{N}}$, the infinite direct product of copies of $\mathbb{Z}$.

It is not generally true that given a group H and a subgroup $K \leq H$, $d(K) \leq d(H)$. In fact, the evidence suggests that there is very little we can say in general about the relationship between $d(H)$ and $d(K)$ for some subgroup K of H. By Cayley's Theorem [2, Theorem 3.12], every finite group can be embedded in a symmetric group S_n, given a large enough integer n. It is also well known that $d(S_n) = 2$ [2, Exercise 2.9 (iii)]. In addition there are finite groups with any minimal number of generators. The group $(\mathbb{Z}_2)^d$, the direct product of d copies of the additive group of integers modulo 2, is generated by d elements for any positive integer d. Thus, any result about the minimal number of generators of subgroups has to account for the fact that any finite group can be embedded in a finite group generated by two elements.

On the other hand, it is easily verifiable that for any $N \lhd H$, $d(H/N) \leq d(H)$. This is so as the generators $h_1, \ldots, h_n$ of H, induce generators of H/N, namely $h_1N, \ldots, h_nN$.

It has been shown [3] that two generators are sufficient to generate any finite simple group. With our current understanding, we can already break down the problem and make meaningful progress in addressing the issue for generic finite groups.

In fact for a generic finite group H, either $d(H) > d(H/K)$ for all non-trivial subgroups $K \lhd H$ or there is some non-trivial $K \lhd H$ such that $d(H) = d(H/K)$. In the second case the problem is reduced to that of determining the minimal number of generators of H/K, usually an easier task since H/K has a smaller order than that of H. Now the group H/K can again have a non-trivial normal subgroup L/K such that $d(H/K) = d((H/K)/(L/K))$

and if that is the case the problem can again be simplified. Proceeding in this manner, the problem of determining the minimal number of generators of a generic finite group H can be reduced to the problem of finding the minimal number of generators of finite groups K which are generated by more elements than any of its proper non-trivial quotients i.e the first case.

Spectacular results regarding this problem were presented in [1]. These results rely on advanced group theory concepts and, although extremely valuable, have some omissions in their explanation, which this dissertation aims to fill.

Chapter 1

Preliminaries

This section aims at laying out the necessary prerequisites for the results that follow in this dissertation. Basic group theory concepts such as the notions of group, subgroup, normal subgroup, group action and Sylow subgroups are assumed.

1.1 Normal closure

Similar to what is done for subgroups (for example in [2]) it is possible to define normal subgroups generated by a set.

Definition 1.1. Let G be a group. If $x, y \in G$ we will denote the conjugate of x by y, namely yxy^{-1} by x^y.

Theorem 1.2. *The intersection of any family of normal subgroups of a group G is again a normal subgroup of G.*

Proof. Let $\{S_i | i \in I\}$ be a family of subgroups of G. It is well known that $\bigcap_{i \in I} S_i$ is a subgroup. Furthermore for any $i \in I$ and $g \in G$, we have $gS_ig^{-1} = S_i$ and thus $g(\bigcap_{i \in I} S_i)g^{-1} = \bigcap_{i \in I} gS_ig^{-1} = \bigcap_{i \in I} S_i$. □

Theorem 1.3. *If X is a subset of a group G, then there is a* ***smallest*** *normal subgroup H of G containing X; that is if $X \subseteq S$ and $S \triangleleft G$, then $H \triangleleft S$.*

Proof. There are normal subgroups of G containing X; for example, G itself is normal and contains X; let us define H as the intersection of all the normal subgroups of G which contain X. Also let us note that H is a normal subgroup, by Theorem 1.2, and $X \subseteq H$. If $S \triangleleft G$ and $X \subseteq S$, then S is one of the subgroups of G being intersected to form H; hence, $H \leq S$, and so H is the smallest such subgroup. □

Definition 1.4. If X is a subset of a group G, then the smallest normal subgroup of G containing X, denoted by $\langle X\rangle_G$, is called the **normal closure of** X in G. If X is a finite set, say $X = \{a_1, \dots, a_n\}$ then we write $\langle X\rangle_G = \langle a_1, \dots, a_n\rangle_G$ instead of $\langle X\rangle_G = \langle\{a_1, \dots, a_n\}\rangle_G$.

Theorem 1.5. *Let G be a group and X a subset of G. The normal closure of X is the group $W = \langle\left\{gxg^{-1}|g \in G, x \in X\right\}\rangle$.*

Proof. If $y \in W$ then y is a word on elements of $\left\{gxg^{-1}|g \in G, x \in X\right\}$, say $y = w_1 \dots w_n$. Obviously for any $g \in G$, $gyg^{-1} = gw_1g^{-1} \dots gw_ng^{-1}$ is also a word on elements of $\left\{gxg^{-1}|g \in G, x \in X\right\}$. We have thus proved that W is a normal subgroup of G and since $\langle X\rangle_G$ is the smallest normal subgroup that contains X, we have that $\langle X\rangle_G \subseteq W$.

On the other hand since $\langle X\rangle_G$ is a normal subgroup of G that contains X, it obviously contains gxg^{-1} for any $x \in X, g \in G$. Thus $W \subseteq \langle X\rangle_G$. □

1.2 Semidirect Products

Definition 1.6. Let K be a subgroup of a group G. A subgroup $Q \subseteq G$ is a **complement** of K in G if $K \cap Q = \{1\}$ and $KQ = G$.

Definition 1.7. A group G is a **semidirect product** of K by Q, denoted by $G = K \rtimes Q$, if $K \lhd G$ and K has a complement $Q' \cong Q$.

The next theorem can be considered as transitivity for semidirect products.

Theorem 1.8. *Let $G \leq H \leq K$ be groups. Suppose that G is complemented in H, its complement is normal in K and H is complemented in K then G is complemented in K.*

Proof. Let H' be the complement of H in K and G' the complement of G in H. Since by hypothesis G' is normal in K we have that $H'G'$ is a group. Also by hypothesis we have that: $K = H'H = H'(G'G) = (H'G')G$. Furthermore $H'G' \cap G = 1$ because if $g \in G \cap H'G'$ then $g = h'g'$ for some $h' \in H'$ and $g' \in G'$. We have that $gg'^{-1} = h' \in H' \cap GG' = H' \cap H = 1$ and so it follows that $h' = 1$ and that $g = g' \in G \cap G' = 1$. □

Theorem 1.9. *Let G be a group, $C_1, \dots, C_n$ be a finite sequence of subgroups of G and $A \leq G$ any subgroup. If $C_1 \dots C_n \cap A = 1$*

$$\bigcap_{l=1}^{n}(AC_l) = A(\bigcap_{l=1}^{n} C_l).$$

Proof. We will do this proof by induction on n. Let $n = 2$.

We will start by proving $AC_1 \cap AC_2 \subseteq A(C_1 \cap C_2)$. We have that $x \in AC_1 \cap AC_2 \iff a_1c_1 = x = a_2c_2$ for some $a_1, a_2 \in A$, $c_1 \in C_1$ and $c_2 \in C_2$. From this follows that $a_2^{-1}a_1 = c_2c_1^{-1} \in A \cap C_1C_2 = 1$. Thus we conclude that $a_1 = a_2$ and $c_1 = c_2 \in C_1 \cap C_2$, that is $x = ac_1 \in A(C_1 \cap C_2)$ and the first inclusion is thus proved.

The other inclusion is trivial.

Let us assume now that the result holds for n. Then by the induction hypothesis,

$$\bigcap_{i=1}^{n}(AC_i) \cap AC_{n+1} = A(\bigcap_{i=1}^{n} C_i) \cap AC_{n+1}.$$

The rest of the proof is now analogous to the case $n = 2$ with $C_1 = \bigcap_{i=1}^{n} C_i$ and $C_2 = C_{n+1}$. □

1.3 Minimal Normal Subgroups

Definition 1.10. A normal subgroup M of a group G is said to be a **minimal normal subgroup** if it is non-trivial and it does not contain any proper non-trivial normal subgroup. That is M is a **minimal normal subgroup** if $M \neq 1$ and there is no normal subgroup K of G such that $1 < K < M$.

There are groups without minimal normal subgroups. One example is the additive group $\mathbb{Z}$. Any subgroup of $\mathbb{Z}$ (all subgroups of $\mathbb{Z}$ are normal) is of the form $m\mathbb{Z}$ for some positive integer m. Taking the subgroup $2m\mathbb{Z}$ we get a non-trivial normal subgroup contained in $m\mathbb{Z}$.

On the other hand minimal normal subgroups always exist for non-trivial finite groups. Let us suppose there is a non-trivial finite group H without a minimal normal subgroup. Then we can construct the following chain of normal subgroups of H,

$$H > M_1 > M_2 > \dots$$

were each subgroup M is strictly contained in the one before. Since none of this groups by assumption can be a minimal normal subgroup we can prolong this chain forever and thus arise at a contradiction on the finiteness of H.

Theorem 1.11. *Let G and H be groups. Given a surjective homomorphism $\alpha\colon G \to H$ and M a minimal normal subgroup of G, $\alpha(M)$ is either a minimal normal subgroup of H or* 1.

Proof. Let us assume that $\alpha(M)$ is neither a minimal normal subgroup of H neither 1.

Since α is surjective, we have that $\alpha(M)$ is normal in H, and by assumption there is a normal subgroup N strictly contained in $\alpha(M)$.

Obviously $\alpha^{-1}(N)$ is normal in G. Considering now the normal subgroup $\alpha^{-1}(N) \cap M$ we see that it is non-trivial and strictly contained in M, contradicting the minimality of M. □

Definition 1.12. Let x and y be elements of a group G. We define the **commutator of** x **and** y as

$$[x, y] = xyx^{-1}y^{-1}.$$

Let us notice that the commutator of two elements is the identity if and only if they commute.

Similarly we can define the commutator of two subgroups.

Definition 1.13. Let G be a group. If $H, K \leq G$, then

$$[H,K] = \langle \left\{ hkh^{-1}k^{-1} | h \in H \text{ and } k \in K \right\} \rangle.$$

Likewise if $H, K \leq G$, $[H,K] = 1$ if and only if all the elements of H commute with all the elements of K. The set $\left\{ hkh^{-1}k^{-1} | h \in H \text{ and } k \in K \right\}$ is not necessarily a subgroup, an example is provided in [4], hence we take the smallest subgroup generated by the commutators in the definition.

Theorem 1.14. *If M_1 and M_2 are distinct minimal normal subgroups of a group then they centralize each other.*

Proof. We have that $[M_1, M_2] \leq M_1 \cap M_2$ and as $M_1 \neq M_2$, $M_1 \cap M_2 = 1$. □

1.4 Socle of a Group

Definition 1.15. The **socle** of a group G, henceforth denoted by $\mathbf{soc}(\mathbf{G})$, is the subgroup generated by all its minimal subgroups.

If G has no minimal normal subgroups, then $soc(G) = 1$. This is so because the group generated by the empty set is the trivial group.

The next Theorem is well-known and an alternative proof can be found in [5, p. 87].

Theorem 1.16. *The socle of a finite group H is a direct product of minimal normal subgroups.*

Proof. Let $M_1, \ldots, M_k$ be the minimal normal subgroups of H. We know that $soc(H)$ is the product of its minimal normal subgroups, that is $soc(H) = M_1 \ldots M_k$.

Now we will construct the following subsequence

$$M_{i_1} = M_1, M_{i_2} = M_2, \ldots, M_{i_j}$$

where $M_{i_l} \cap (M_1 \ldots M_{i_{l-1}}) = 1$ for $1 \leq l \leq j$ and $M_i \leq (M_1 \ldots M_l)$ for all $1 \leq i \leq i_l$.

Assuming we have M_{i_l} we can choose $M_{i_{l+1}}$ in the following way: i_{l+1} is the smallest number such that $i_{l+1} > i_l$ and $M_{i_{l+1}} \cap M_1 \ldots M_l = 1$; if no such number exists the subsequence is completed.

We claim that a subsequence constructed in this way satisfies our conditions.

Obviously if $i \leq i_l$ we have by hypothesis

$$M_i \leq M_{i_1} \ldots M_{i_l} \leq M_{i_1} \ldots M_{i_l} M_{i_{l+1}}.$$

If $i_l < i < i_{l+1}$ we have by the construction of $M_{i_{l+1}}$ that $M_i \cap M_{i_1} \dots M_{i_l} \neq 1$ and since $M_i \cap M_{i_1} \dots M_{i_l}$ is normal in H it must be M_i. Hence $M_i \leq M_{i_1} \dots M_{i_l} \leq M_{i_1} \dots M_{i_{l+1}}$.

It is thus clear that $soc(H) = M_{i_1} \dots M_{i_j}$ and since $M_{i_l} \cap (M_1 \dots M_{i_{l-1}}) = 1$ for $1 \leq l \leq j$ we have $soc(H) = M_{i_1} \times \dots \times M_{i_j}$. □

Our choice of the minimal normal subgroup M_1 in the last theorem was completely arbitrary, whence we can easily see that any minimal normal subgroup is complemented in $soc(H)$.

Theorem 1.17. *Let H be a finite group. Suppose that all its minimal normal subgroups are abelian and complemented. Then $soc(H)$ is complemented.*

Proof. Let $N_1, \dots, N_r$ be the minimal normal subgroups of H and $C_1, \dots, C_r$ be its complements respectively. We are going to construct a complement for $soc(H)$ starting from C_1.

Let K_1 be a subgroup of H such that $(soc(H))K_1 = H$, say for example $K_1 = C_1$ since $H = N_1C_1 = (soc(H))C_1$. We have that $soc(H)$ is abelian as the minimal normal subgroups are abelian and $soc(H)$ is the direct product of some of them. Due to $K_1 \cap soc(H) \lhd K_1$ and $K_1 \cap soc(H) \lhd soc(H)$, as $soc(H)$ is abelian, $K_1 \cap soc(H) \lhd H = (soc(H))K_1$.

If $K_1 \cap soc(H) \neq 1$, since $K_1 \cap soc(H)$ is normal it contains a minimal normal subgroup, N_i say. We assert that $K_1 = N_i(C_i \cap K_1)$. The first inclusion follows as for any $k_1 \in K_1 \subseteq N_iC_i$, $k_1 = n_ic_i$ for some $n_i \in N_i$, $c_i \in C_i$ and hence $c_i = n_i^{-1}k_1 \in K_1 \implies c_i \in K_1 \cap C_i$. The other inclusion is trivial. Hence we have

$$H = (soc(H))K_1 = (soc(H))N_i(K_1 \cap C_i) = (soc(H))(K_1 \cap C_i)$$

We thus proved that if there exists a group K_1 such that $(soc(H))K_1 = H$ and the intersection $soc(H) \cap K_1$ is nontrivial then there exists another group $K_2 = K_1 \cap C_i$ such that $(soc(H))K_2 = H$ and $soc(H) \cap K_2$ is strictly contained in $soc(H) \cap K_1$. The inclusion of $soc(H) \cap K_2$ in $soc(H) \cap K_1$ is strict since the latter contains N_i but by construction of K_2 the former does not. Proceeding in this manner we can construct a K_j that complements $soc(H)$.

□

1.5 Nilpotent Groups

We enumerate here some well known results about nilpotent groups that will be used throughout. The proofs of these results can be found in [2], and are omitted here since the exposition of this subject benefits immensely from a more comprehensive treatment.

Definition 1.18. Let G be a group. The groups $\gamma_i(G)$ are defined by induction as:

$$\gamma_1(G) = G; \quad \gamma_{i+1} = \left[\gamma_i(G), G\right].$$

Definition 1.19. A group G is **nilpotent** if there is an integer c such that $\gamma_{c+1}(G) = 1$.

Theorem 1.20. *[2, Theorem 5.39] A finite group H is nilpotent if and only if it is the direct product of its Sylow subgroups.*

Definition 1.21. Let G be a group. A subgroup K is said to be a maximal subgroup of G if $K < G$ and there is no subgroup M with $K < M < G$.

Theorem 1.22. *[2, Theorem 5.40] If H is a finite p-group, then every maximal subgroup of H is normal and has index p.*

1.6 The Frattini Subgroup

Throughout this section, unless explicitly said otherwise H will always denote a finite group.

For non-trivial finite groups, maximal subgroups always exist. Assuming otherwise, let H be a non-trivial finite group without maximal subgroups. Then we can construct the sequence $1 < K_1 < K_2 \ldots$ where each group K is strictly contained in the one before. Since none of this groups by assumption can be a maximal subgroup of H we can can prolong this sequence forever and thus arise at a contradiction on the finiteness of H.

On the contrary maximal subgroups might not exist for infinite groups and an example is provided in [2, p. 123].

Definition 1.23. The **Frattini subgroup of** H, denoted by $\Phi(H)$, is the intersection of all maximal subgroups of H if H has a maximal subgroup, otherwise $\Phi(H)$ is set to be H.

Theorem 1.24. *[2, Theorem 5.47] The Frattini subgroup of a nontrivial finite group H is the set of all nongenerators, that is the set of those elements $h \in H$ such that if $H = \langle Y, h\rangle$ then $H = \langle Y\rangle$ for any set $Y \subseteq H$.*

Proof. Let $h \in \Phi(H)$ and let $Y \subseteq H$ be such that $\langle Y, h \rangle = H$. If $\langle Y \rangle \neq H$, we have that $\langle Y \rangle \leq M$ for some maximal subgroup M of H. Since $h \in \Phi(H)$, in particular $h \in M$. But this implies that $\langle Y, h \rangle \leq M \neq H$, a contradiction.

Conversely let z be a nongenerator and M a maximal subgroup of H. If $z \notin M$ then $H = \langle z, M \rangle = \langle M \rangle = M$, which is a contradiction. □

Theorem 1.25. *[2, Theorem 5.48] Let H be a finite p-group. Then:*

1. *$\Phi(H) = H'H^p$ where H^p is the subgroup of H generated by all p-th powers,*

2. *$H/\Phi(H) \cong (\mathbb{Z}_p)^q$ for some positive integer q.*

Proof.

1. Let M be a maximal subgroup of H. According to Theorem 1.22, M is a normal subgroup of H with index p. Hence, the quotient group H/M is abelian, implying that the commutator subgroup H' is contained in M. Furthermore, H/M has exponent p, meaning every element of H raised to the p-th power lies in M. Thus $H'H^p \leq \Phi(H)$.

   To show the reverse inclusion, consider the quotient group $H/H'H^p$. It is an abelian group of exponent p, hence isomorphic to $(\mathbb{Z}_p)^q$ for some positive integer q and thus can be regarded as a vector space over the field $\mathbb{F}_p$. It is evident that its Frattini subgroup is trivial. Now, if we have $N \triangleleft H$ such that $N \leq \Phi(H)$, it can be verified easily that $\Phi(H)$ is in the preimage (under the natural quotient map π) of $\Phi(H/N)$, as maximal subgroups correspond. Thus $\Phi(H) \subseteq \pi^{-1}(\Phi(H/(H'H^p))) = \pi^{-1}(1) \subseteq H'H^p$ and we conclude that $\Phi(H) = H'H^p$.

2. Since $H' \leq H'H^p = \Phi(H)$, $H/\Phi(H)$ is abelian. Furthermore since $H^p \leq \Phi(H)$, $H/\Phi(H)$ has exponent p. Thus $H \cong (\mathbb{Z}_p)^q$ for some positive integer q.

□

Theorem 1.26. *Let H be a finite group. Then $d(H) = d(H/\Phi(H))$.*

Proof. Let $d = d(H/\Phi(H))$ and suppose $H/\Phi(H) = \langle g_1\Phi(H), \ldots, g_d\Phi(H) \rangle$. Then $H = \langle g_1, \ldots, g_d, \Phi(H) \rangle$ and since $\Phi(H)$ is the set of non-generators of H, that is the set of those elements $h \in H$ such that if $H = \langle Y, h \rangle$ then $H = \langle Y \rangle$ for any set $Y \subseteq H$, the result follows. □

1.7 Gaschütz's Lemma

Definition 1.27. For any finite group H, $\phi_H(m)$ will denote the number of ordered m-tuples $(x_1, \dots, x_m)$ of elements of H that generate H.

The last Theorem of this section was first proved by Gaschütz in [6]. We present here an alternative proof from Roquette adapted from [7, Lemma 17.7.2].

Theorem 1.28. *Let $\theta : G \to H$ be a surjective homomorphism of finite groups with $d(G) \leq m$. Let $\mathbf{h} = (h_1, \dots, h_m)$ be a tuple that generates H. Then there exists a tuple of generators $\mathbf{g} = (g_1, \dots, g_m)$ of G such that $\theta(g_i) = h_i$, $i = 1, \dots, m$. Moreover the cardinality of the set*

$$\{(g_1, \dots, g_m) \in G^m | \langle g_1, \dots, g_m \rangle = G \text{ and } \theta(g_i) = h_i\}$$

is independent of the choice of $h_1, \dots, h_m$.

Proof. For each subgroup C of G satisfying $\theta(C) = H$ and all tuples $\mathbf{a} = (a_1, \dots, a_m)$ that generate H denote the number of m-tuples $\mathbf{c} \in C^m$ that generate C and satisfy $\theta(\mathbf{c}) = \mathbf{a}$ by $\varphi_C(\mathbf{a})$.

Let $\mathbf{a} = (a_1, \dots, a_m) \in H^m$ be such that $H = \langle a_1, \dots, a_m \rangle$ and C a subgroup of G satisfying $\theta(C) = H$. We prove by induction on $|C|$ that $\varphi_C(\mathbf{a})$ is independent of $\mathbf{a}$.

Let $e = \frac{|C|}{|H|}$. We first claim that if for every subgroup B of C, $\theta(B) \neq H$ we have $\varphi_C(\mathbf{a}) = e^m$. Since $|\theta|_C^{-1}(\{a_i\})| = |\ker \theta|_C| = |C|/|H| = e$ for all i there are e^m $\mathbf{c} = (c_1, \dots, c_m) \in C^m$ tuples that satisfy $\theta(\mathbf{c}) = \mathbf{a}$. In particular since the subgroup $\langle c_1, \dots, c_m \rangle$ generated by any such tuple is a subgroup that satisfies $\theta(\langle c_1, \dots, c_m \rangle) = H$, by the hypothesis on C, it must be C.

Assume now that $\varphi_B(\mathbf{a})$ is independent of $\mathbf{a}$ for every proper subgroup B of C satisfying $\theta(B) = H$. Then there are exactly e^m elements $\mathbf{b} \in C^m$ with $\theta(\mathbf{b}) = \mathbf{a}$. Each such $\mathbf{b}$ generates a subgroup B of C satisfying $\theta(B) = H$. Hence,

$$e^m = \varphi_C(\mathbf{a}) + \sum\nolimits'_{B<C} \varphi_B(\mathbf{a})$$

where $\sum'$ indicates a sum over groups with $\theta(B) = H$. By assumption, the $\sum'$ is independent of $\mathbf{a}$. Therefore, so is $\varphi_C(\mathbf{a})$.

Now choose a tuple of generators $\mathbf{g}' = (g'_1, \dots, g'_m)$ for G. Then $\theta(\mathbf{g}') = \mathbf{h}'$ generates H. By the preceding paragraph, $\varphi_G(\mathbf{h}) = \varphi_G(\mathbf{h}') \geq 1$. Consequently, G has a tuple of generators $\mathbf{g} = (g_1, \ldots, g_m)$ such that $\theta(\mathbf{g}) = \mathbf{h}$. The cardinality of

$$\{(g_1, \ldots, g_m) \in G^m | \langle g_1, \ldots, g_m \rangle = G \text{ and } \theta(g_i) = h_i\}$$

is precisely $\varphi_G(\mathbf{h})$ which is independent of the choice of $\mathbf{h}$. □

Theorem 1.29. *Let N be a normal subgroup of a finite group G and let $g_1, \ldots g_m \in G$ be such that $G = \langle g_1, \ldots, g_m, N \rangle$. If $d(G) \leq m$, then there exists elements $u_1, \ldots, u_m$ of N such that $G = \langle g_1 u_1, \ldots, g_m u_m \rangle$. Moreover the cardinality of the set*

$$\{(u_1, \ldots, u_m) \in N^m | G = \langle g_1 u_1, \ldots, g_m u_m \rangle\}$$

is independent of the choice of $g_1, \ldots, g_m$.

Proof. By applying Theorem 1.28, where H is taken to be the quotient group G/N, $\theta \colon G \to G/N$ is the natural projection, and $h_i = g_i N$, we can find elements $z_1, \ldots, z_m \in G$ such that $\theta(z_i) = z_i N = g_i N$ and $\langle z_1, \ldots, z_m \rangle = G$. Since $z_i N = g_i N$, we have $z_i = g_i u_i$ for a unique $u_i \in N$ for all i, which leads to the desired conclusion. □

1.8 G-homomorphisms

As a reminder we enunciate here the definition of a G-set.

Definition 1.30. [2] If X is a set and G is a group, then X is a G**-set** if there is a function $\alpha : G \times X \to X$ (called an **action**), denoted by $\alpha(g, x) \mapsto gx$, such that:

1. $\alpha(e, x) = x$ for all $x \in X$;
2. $\alpha(g, \alpha(h, x)) = \alpha(gh, x)$ for all $g, h \in G$ and $x \in X$.

One also says that G **acts on** X. If $|X| = n$, then n is called the **degree** of the G-set X.

It is easy to check that the function

$$\begin{aligned} \alpha \colon G \times G &\to G \\ (g, h) &\mapsto ghg^{-1} \end{aligned}$$

is an action, and thus G is a G-set under conjugation.

Definition 1.31. Let G be a group and X a subgroup of G. The centralizer of X is the subgroup

$$C_G(X) = \{g \in G | \forall x \in X, xg = gx\}.$$

We claim that if $X \triangleleft G$ then $C_G(X) \triangleleft G$. For all $g \in G$, $c \in C_G(x)$ and $x \in X$,

$$gcg^{-1}x = gc(g^{-1}xg)g^{-1} = g(g^{-1}xg)cg^{-1} = xgcg^{-1}$$

where the second equality follows from $g^{-1}xg \in g^{-1}Xg = X$ and the fact that $c \in C_G(x)$.

Definition 1.32. Let G be a group and X a subgroup of G. The normalizer of X is the subgroup

$$N_G(X) = \{g \in G | gXg = X\}.$$

A more profound exposition of G-homomorphisms is available on [2, Chapter 9], but for our purposes just the definition suffices.

Definition 1.33. If X and Y are G-sets, a function $f : X \to Y$ is a G**-homomorphism** if $f(g \cdot x) = g \cdot f(x)$ for all $x \in X$ and $g \in G$. If f is also a bijection, then f is called a G**-isomorphism**.

1.9 Free Groups

This section offers a concise overview of fundamental properties of free groups, focusing on the essential information required for our specific objectives. Once again the proofs can be found in the cited references.

Definition 1.34. Let X be a subset of a group F. We say that F is a **free group with basis** X if, for every group G and every function $f \colon X \to G$, there exists a unique homomorphism $\varphi \colon F \to G$ extending f ($\varphi|_X = f$).

Let us note that if F is a **free group with basis** X and denoting by $i \colon X \to F$ the inclusion, then the following diagram commutes

$$\begin{tikzcd} X \arrow[r, "f"] \arrow[d, "i"'] & G \\ F \arrow[ur, "\varphi"'] & \end{tikzcd}.$$

Theorem 1.35. *[2, Theorem 11.1] Given a set X, there exists a free group with basis X.*

Theorem 1.36. *[2, Theorem 11.4] Let F and G be free groups with bases X and Y, respectively. Then $F \cong G$ if and only if $|X| = |Y|$.*

Taking G as F it easily follows from the last theorem that any basis X of a free group F has the same number of elements.

Definition 1.37. The **rank** of a free group F, denoted by $\mathbf{rank}(\mathbf{F})$, is the number of elements in a basis of F.

1.10 Primitive Groups

An extensive exposition of primitive groups is available on [8].

Definition 1.38. Let G be a group and L a subgroup of G. The **core** of L, is the group $core_G(L) = \bigcap_{g \in G} gLg^{-1}$. When the ambient group G is clear from the context, we may drop the subscript and simply write $core(L)$.

Theorem 1.39. *Let G be a group and L a subgroup of G. The group $core(L)$ is the biggest normal subgroup of G contained in L, i.e if $N \triangleleft G$ and $N \subseteq L$ then $N \subseteq core(L)$.*

Proof. That $core(L) \subseteq L$ is obvious since $\bigcap_{g \in G} gLg^{-1} \subseteq 1L1^{-1} = L$. Now let $N \triangleleft G$ and $N \subseteq L$. We have that for all $g \in G$, $N = gNg^{-1} \subseteq gLg^{-1}$ and thus it follows that

$$N = \bigcap_{g \in G} gNg^{-1} \subseteq \bigcap_{g \in G} gLg^{-1} = core(L).$$

□

Definition 1.40. A group G is **primitive** if it has a maximal subgroup with trivial core.

Chapter 2

The groups L_k

In this section L will always denote a finite group with a unique minimal normal subgroup M. Furthermore if M is abelian, we also assume that M is complemented in L.

Given a positive integer k we will denote by L^k the k-fold direct power of L and by $diag(L^k)$ the subgroup $\{(l_1, \ldots, l_k) \in L^k | l_1 = l_2 = \ldots = l_k\}$. If not explicitly said otherwise, we will assume throughout this section that k is a positive integer.

Also π_i will denote the projection of the i-th coordinate from L^k onto L and $M_i = 1 \times \ldots \times M \times \ldots \times 1$ the subgroup of L^k whose elements have some $m \in M$ for the i-th coordinate and 1 for the rest.

Definition 2.1. Given a positive integer k, the group L_k is a subgroup of L^k defined by:

$$L_k = \{(l_1, \ldots, l_k) \in L^k | l_1 M = \ldots = l_k M\}.$$

Let k be a positive integer. We will often simply write π_i to denote $\pi_i|_{L_k}$, the restriction of π_i to L_k. One property of the functions $\pi_i|_{L_k}$ is that given $S \subseteq L$,

$$\pi_i|_{L_k}^{-1}(S) = \pi_i^{-1}(S) \cap L_k.$$

Thus it follows that $\pi_i|_{L_k}^{-1}(M) = \pi_i^{-1}(M) \cap L_k = (L \times \ldots L \times M \times L \ldots . \times L) \cap L_k = M^k$.

2.1 Some basic properties

The properties of the groups L_k will be referenced implicitly throughout.

Theorem 2.2. *The group L_k can be described as $diag(L^k)M^k$.*

Proof. For any $(l_1, \dots, l_k) \in L_k$, we have that for any $1 \leq i \leq k$, $l_1 M = l_i M$. Hence it follows $l_i = l_1 m_i$ for some $m_i \in M$. We thus have $(l_1, \dots, l_k) = (l_1, l_1, \dots, l_1)(1, m_2, \dots, m_k)$ as pretended.

For the other inclusion it suffices to notice that $M^k, diag(L^k) \subseteq L_k$, hence $diag(L^k)M^k \subseteq L_k$. □

Theorem 2.3. *The socle of L_k is M^k.*

Proof. We have by Theorem 1.11 that: if N is a minimal normal subgroup of L_k then for all $1 \leq i \leq k$, $\pi_i(N)$ is either equal to 1 or a minimal normal subgroup of L. Since L has a unique minimal normal subgroup $\pi_i(N) = 1$ or $\pi_i(N) = M$.

We thus have $N \subseteq \bigcap_{i=1}^k \pi_i|_{L_k}^{-1}(M) = M^k$. Since the last inclusion holds for any minimal normal subgroup N, it easily follows that $soc(L_k) \subseteq M^k$.

Since the groups M_i are minimal normal subgroups of L_k, we obviously have $M^k = M_1 \dots M_k \subseteq soc(L_k)$. □

Theorem 2.4. *The group L_k/M^k is isomorphic to L/M.*

Proof. We have that:

$$\frac{L_k}{M^k} = \frac{diag(L^k)M^k}{M^k} \cong \frac{diag(L^k)}{diag(L^k) \cap M^k}$$

by the Second Isomorphism Theorem and by Theorem 2.2.

Evidently, $diag(L^k) \cap M^k = diag(M^k)$ and thus is easy to verify that $diag(L^k)/diag(M^k) \cong L/M$. □

Theorem 2.5. *If M is abelian and complemented by C in L, then M^k is complemented by $diag(C^k)$ in L_k.*

Proof. We have that $diag(L^k) = diag((CM)^k) = diag(C^k)diag(M^k)$. Then by Theorem 2.2, $L_k = diag(L^k)M^k = diag(C^k)diag(M^k)M^k = diag(C^k)M^k$. Furthermore for all $x \in diag(C^k) \cap M^k$ and all $1 \leq i \leq k$, $\pi_i(x) \in \pi_i(diag(C^k)) \cap \pi_i(M^k) = C \cap M = 1$. This means that all the coordinates of x are 1 and consequently that $x = 1$. The proof is thus complete. □

2.2 The minimal normal subgroups of L_k

Theorem 2.6. *If M is not abelian, any minimal normal subgroup of L_k is of the form M_i for some i.*

Proof. Let N be a minimal normal subgroup of L_k. Once again by Theorem 1.11, for each $1 \leq i \leq k$, $\pi_i(N)$ is either 1 or M. We also have that $\pi_j(N) = M$ for some j otherwise N would be the trivial subgroup which is a contradiction.

Let j be such that $\pi_j(N) = M$. Now we will prove that for any $1 \leq i \leq k$ different from j, $\pi_i(N) = 1$ which gives us the result.

Suppose on the contrary that exists some $1 \leq i \leq k$ different from j such that $\pi_i(N) = M$. By Theorem 1.14 we obtain $[N, M_i] = 1$. Since M is not abelian we can choose elements $m_1, m_2 \in M$ such that $m_1 m_2 \neq m_2 m_1$. Besides we have by hypothesis that $m_1 = \pi_i(n_1)$ and $m_2 = \pi_i(n_2)$ for some $n_1 \in N$ and some $n_2 \in M_i$. It thus follows that:

$$\begin{aligned} m_1 m_2 &= \pi_i(n_1)\pi_i(n_2) \\ &= \pi_i(n_1 n_2) \\ &= \pi_i(n_2 n_1), \text{by } [N, M_i] = 1 \\ &= \pi_i(n_2)\pi_i(n_1) = m_2 m_1, \text{ a contradiction.} \end{aligned}$$

□

With the previous theorem, the minimal normal subgroups in the case where M is non abelian are fully characterized. What can we say about the minimal normal subgroups of L_k in general? The next theorems provide some nice properties.

Theorem 2.7. *Let N be a minimal normal subgroup of L_k. Then N has order $|M|$.*

Proof. We have once more that $\pi_i(N) = M$ for some $1 \leq i \leq k$. Considering the appropriate restriction of π_i, by the First Isomorphism Theorem we get that $|N| = |M| \cdot |\ker \pi_i|_N|$ which implies $|N| \geq |M|$.

Let us assume that $|N| > |M|$. Then there is some $n \in \ker \pi_i|_N$ with not all coordinates 1 (obviously the i-th coordinate must be 1).

Consider $\langle n \rangle_{L_k}$ contained in $\ker \pi_i|_N$. Since $n \in N$, and $\langle n \rangle_{L_k}$ is the smallest normal subgroup generated by n we must have $\langle n \rangle_{L_k} \subseteq N$. Since $\pi_i(\langle n \rangle_{L_k}) = \langle \pi_i(n) \rangle_L = 1$ and not all elements of N are in $\ker \pi_i|_N$ we obtain that $\langle n \rangle_{L_k}$ is a non-trivial group strictly contained in N. This is a contradiction since N is a minimal normal subgroup. □

Definition 2.8. Given $l \in L$ and a positive integer q, let $\dot{l}$ denote the element of $diag(L^q)$ with all coordinates equal to l.

The previous definition depends on which power of the group L we are considering, and often the only way to decide the ambient group is through context, but what we lose in formal rigor we gain in readability. Such an example of improved readability is the statement of the next theorem.

Theorem 2.9. *Let N be a minimal normal subgroup of L_k. Then there exists a complement $C \lhd L_k$ of N in $soc(L_k)$ and an isomorphism $\phi\colon C \to M^{k-1}$ that satisfies $\phi(c^l) = \phi(c)^l$ for any $c \in C$ and $l \in L$.*

Proof. We have once more that $\pi_i(N) = M$ for some $1 \leq i \leq k$.

Let $C = M_1 \dots M_{i-1} M_{i+1} \dots M_k$. We claim that $N \cap C = 1$. Let us note first that any element of $N \cap C \subseteq C$ has i-th coordinate 1. Thus $N \cap C \lhd L_k$ is strictly contained in the minimal normal subgroup N. So it must be 1.

From the Second Isomorphism Theorem we get that $|NC|/|N| = |C|/|N \cap C|$. We obtain $|NC| = |N||C| \cdot 1$ and since $|N| = |M|$ by Theorem 2.7, $|NC| = |M||C| = |M|^k = |soc(L_k)|$. Obviously $NC \subseteq soc(L_k)$ as $N, C \subseteq soc(L_k)$. We thus conclude that $NC = soc(L_k)$.

The expected isomorphism

$$\begin{aligned}\phi\colon C = M \times \dots \times M \times 1 \times M \times \dots \times M &\longrightarrow M^{k-1}\\ (m_1, \dots, m_i, 1, m_{i+1}, \dots, m_k) &\mapsto (m_1, \dots, m_i, m_{i+1}, \dots, m_k)\end{aligned}$$

works.

The property is easily verified since for any $l \in L$, $(m_1, \dots, m_i, 1, m_{i+1}, \dots, m_k) \in C$:

$$\begin{aligned}
&\phi(lm_1l^{-1}, \dots, lm_il^{-1}, l1l^{-1}, lm_{i+1}l^{-1}, \dots, lm_kl^{-1}) &&=\\
&(lm_1l^{-1}, \dots, lm_il^{-1}, lm_{i+1}l^{-1}, \dots, lm_kl^{-1}) &&=\\
&(l, \dots, l)(m_1, \dots, m_i, m_{i+1}, \dots, m_k)(l^{-1}, \dots, l^{-1}) &&=\\
&(l, \dots, l)\phi(m_1, \dots, m_i, 1, m_{i+1}, \dots, m_k)(l, \dots, l)^{-1}
\end{aligned}$$

□

2.3 Normal subgroups and quotients of L_k

Theorem 2.10. *The quotient of L_{k+1} by any of its minimal normal subgroups is isomorphic to L_k.*

Proof. Let N be a minimal normal subgroup of L_{k+1}.

If M is not abelian, by Theorem 2.6, $N = M_i$ for some $1 \leq i \leq k+1$. It is trivial to verify that

$$\psi\colon L_{k+1} \longrightarrow L_k$$
$$(l_1, ..., l_{k+1}) \mapsto (l_1, \ldots, l_{i-1}, l_{i+1}, \ldots, l_{k+1})$$

is a surjective homomorphism. We will now verify that $\ker \psi = M_i = N$. Obviously $M_i \subseteq \ker \psi$ as the i-th coordinate is "forgotten" and that is the only non 1 coordinate in M_i. For the other inclusion, we first have by Theorem 2.4 that $|L_k| = |L/M||M|^k$. By the First Isomorphism Theorem, $|L_{k+1}|/|\ker \psi| = |L_k|$. From this two equalities, it follows that $|\ker \psi| = |M_i| = |N|$. Therefore $\ker \psi = M_i = N$ and consequently $L_{k+1}/N = L_{k+1}/\ker \psi \cong L_k$ by the First Isomorphism Theorem.

If M is abelian, by hypothesis we have that M is complemented in L say by C_L. By Theorem 2.5, $diag(C_L^q)$ is a complement of M^q in L_q.

By Theorem 2.9, we have that N is complemented in M^{k+1} and that its complement, say $C_{soc(L_{k+1})}$, is normal in L_{k+1} and isomorphic to M^k. As $diag(C_L^{k+1})$ complements M^{k+1}, by Theorem 1.8 we have that N is complemented in L_{k+1} by $C = diag(C_L^{k+1})C_{soc(L_{k+1})}$.

Then we obtain:

$$L_{k+1}/N = CN/N \cong C/(C \cap N) = C/1 \cong C,$$

using the Second Isomorphism Theorem.

Now we need to show that $C = diag(C_L^{k+1})C_{soc(L_{k+1})} \cong L_k$. Let ψ be the function defined by

$$\psi\colon C \to L_k = diag(C_L^k)M^k$$
$$\dot{l}s \mapsto \dot{l}\phi(s)$$

where $l \in C_L$ and $s \in C_{soc(L_{k+1})}$ and $\phi\colon C_{soc(L_{k+1})} \to M^k$ is the isomorphism from Theorem 2.9.

Let $l_1, l_2 \in C_L$ and $s_1, s_2 \in C_{soc(L_{k+1})}$. To see that ψ is well defined it suffices to notice that if $\dot{l}_1 s_1 = \dot{l}_2 s_2$ then:

$$\dot{l}_2^{-1}\dot{l}_1 = s_2 s_1^{-1} \in C_L^{k+1} \cap C_{soc(L_{k+1})} = 1$$
$$\implies \dot{l}_2 = \dot{l}_1, s_1 = s_2$$
$$\implies \dot{l}_1\phi(s_1) = \dot{l}_2\phi(s_2)$$

Knowing that ϕ is an isomorphism, is easy to see that ψ is surjective since every element $\dot{l}m \in L_k$ (where $\dot{l} \in diag(C_L^k)$ and $m \in M^k$) is the image by ψ of $\dot{l}\phi^{-1}(m)$.

Injectivity follows comparing the orders of C and L_k. We have

$$|C| = |L_{k+1}|/|N| = |L_k|$$

remembering that C complements N in L_{k+1} and that $|N| = |M|$. We thus conclude that ψ is a bijection, since it is a surjection between finite groups of equal orders.

Now we need only to check that ψ is a homomorphism, which follows from:

$$\begin{aligned}
\psi(\dot{l}_1 s_1 \dot{l}_2 s_2) &= \psi(\dot{l}_1 \dot{l}_2 s_1^{\dot{l}_2^{-1}} s_2) \\
&= \dot{l}_1 \dot{l}_2 \phi(s_1^{\dot{l}_2^{-1}} s_2) \\
&= \dot{l}_1 \dot{l}_2 \phi(s_1^{\dot{l}_2^{-1}}) \phi(s_2) \\
&= \dot{l}_1 \dot{l}_2 \phi(s_1)^{\dot{l}_2^{-1}} \phi(s_2) \\
&= \dot{l}_1 \phi(s_1) \dot{l}_2 \phi(s_2) \\
&= \psi(\dot{l}_1 s_1) \psi(\dot{l}_2 s_2).
\end{aligned}$$

□

Theorem 2.11. *Let N be a normal group of L_k. Then either $soc(L_k) \leq N$ or $N \leq soc(L_k)$.*

Proof. The proof will be done by induction on k.

Since L has a unique minimal normal subgroup the proposition is easily seen to be true for $k = 1$.

Suppose now that the result holds for k and that N is not a subgroup of $soc(L_{k+1})$. Then there exists a minimal normal subgroup U of L_{k+1} such that $U \subseteq N$. We have that $L_{k+1}/U \cong L_k$ by some isomorphism f. By induction either $soc(L_k) \leq f(N/U)$ or $f(N/U) \leq soc(L_k)$. Since N is not a subgroup of $soc(L_{k+1})$ we have that $N/U \nleq soc(L_{k+1})/U$ which implies that $soc(L_k) = f(soc(L_{k+1}/U)) \leq f(N/U)$ and thus the first case holds.

Now considering the natural projection $\pi\colon L_{k+1} \longrightarrow L_{k+1}/U$ we obtain, by Theorem 1.11, that $soc(L_{k+1})/N = \pi(soc(L_{k+1})) \subseteq soc(L_{k+1}/N)$.

Applying f^{-1} to $soc(L_k) \leq f(N/U)$ we get $soc(L_{k+1})/U \subseteq soc(L_{k+1}/U) \leq N/U$. Hence as $U \subseteq soc(L_{k+1}), N$ we obtain $soc(L_{k+1}) = \pi^{-1}(soc(L_{k+1}/U)) \leq \pi^{-1}(N/U) = N$. □

2.4 The Sequence $d(L_k)_{k\in\mathbb{N}}$

Throughout we assume that $\mathbb{N}$ is the set of positive integers, i.e does not contain 0. The sequence $d(L^k)_{k\in\mathbb{N}}$ is called the *growth sequence* and has been studied in [9–12]. Here we study the sequence $d(L_k)_{k\in\mathbb{N}}$ given the importance that the groups L_k assume in the study of the minimal number of generators of finite groups.

Theorem 2.12. *The sequence $d(L_k)_{k\in\mathbb{N}}$ is non-decreasing.*

Proof. Let us assume to obtain a contradiction that there is some positive integer k such that $d(L_{k+1}) < d(L_k)$.

Let us consider the function $\rho : L_{k+1} \to L_k$ that drops the last coordinate. That is given $(x_1, \ldots, x_{k+1}) \in L_{k+1}$, $\rho((x_1, \ldots, x_{k+1})) = (x_1, \ldots, x_k)$.

Now let $l_1, \ldots, l_m$ be a minimal generating set of L_{k+1}, that is $\langle l_1, \ldots, l_m\rangle = L_{k+1}$ and $d(L_{k+1}) = m$. Obviously ρ is surjective and thus we obtain that

$$L_k = \rho(L_{k+1}) = \rho(\langle l_1, \ldots, l_m\rangle) = \langle \rho(l_1), \ldots, \rho(l_m)\rangle.$$

This is of course a contradiction since we assumed that $m = d(L_{k+1}) < d(L_k)$. □

Theorem 2.13. *For all positive integers k, $d(L_{k+1}) \leq d(L_k) + 1$.*

Proof. Let $d(L_k) = d$, then there are $l_1, l_2, \ldots l_d \in L_k$ such that $\langle l_1, l_2, \ldots l_d\rangle = L_k$. By abuse of notation, given $l \in L_k$ let $\ell \in L_{k+1}$ be the $k+1$-tuples whose first k coordinates are the coordinates of l and whose last two coordinates are equal, that is $\pi_k(\ell) = \pi_{k+1}(\ell)$.

Let $m \in 1 \times \ldots \times 1 \times M \leq L_{k+1}$ and consider

$$H = \langle m^\ell | l \in L_k\rangle \leq L_{k+1}.$$

For all $i \in \{1, \ldots, k\}$, $\pi_i(H) = 1$, because

$$\pi_i(\langle m^\ell | l \in L_k\rangle) = \langle \pi_i(m)^{\pi_i(\ell)} | l \in L_k\rangle = \langle 1^{\pi_i(\ell)} | l \in L_k\rangle = 1.$$

And $\pi_{k+1}(H) = M$ since

$$\pi_{k+1}(\langle m^\ell | l \in L_k\rangle) = \langle \pi_{k+1}(m)^{\pi_{k+1}(\ell)} | l \in L_k\rangle = \langle \pi_{k+1}(m)\rangle_L.$$

We thus have that $\pi_{k+1}(H)$ is a nontrivial normal subgroup of L that is contained in M, thus $\pi_{k+1}(H) = M$ due to the minimality of M. We thus have that $H = 1 \times \ldots \times 1 \times M$.

Now $L_{k+1} = \{\ell | l \in L_k\} (1 \times \ldots \times 1 \times M) = \{\ell | l \in L_k\} H = \langle \ell_1, \ell_2, \ldots, \ell_d, m \rangle$ and the result is proved.

□

Theorem 2.14. *The sequence $d(L_1), \ldots, d(L_k), \ldots.$ is unlimited.*

Proof. Suppose for the sake of obtaining a contradiction that there exists a natural number m such that $d(L_k) < m$ for all $k \in \mathbb{N}$. Let F be a free group of rank m and K be the set of positive integers k such that there exists a surjective homomorphism from F to L_k. It will be proved that K is a finite set, a contradiction from which the result will follow.

Let $k > 1 \in K$, then there exists a surjective homomorphism $\Psi : F \to L_k$. For $1 \leq i \leq k$, let $\gamma_i = \pi_i \circ \Psi : F \to L_k \to L$ and let $\pi : L \to L/M$ be the natural projection. For all $x \in F$, $\Psi(x) = (l_1, \ldots, l_k)$ for some $(l_1, \ldots, l_k) \in L_k$ thus:

$$\begin{aligned} & Ml_1 = Ml_2 = \ldots = Ml_k \text{ and} \\ & \pi\gamma_1(x) = Ml_1, \ldots, \pi\gamma_k(x) = Ml_k \\ \implies & \pi\gamma_1 = \pi\gamma_2 = \ldots = \pi\gamma_k. \end{aligned}$$

Let $i_1, i_2 \in \{1, \ldots, k\}$ and let $(m_1, \ldots, m_k) \in M_k \leq L_k$ with $m_{i_1} = 1, m_{i_2} \neq 1$. Since $\Psi : F \to L_k$ is surjective there exists an $x \in F$ such that $\Psi(x) = (m_1, \ldots, m_k)$. We then have that $\gamma_{i_1}(x) = m_{i_1} = 1$ and $\gamma_{i_2}(x) = m_{i2} \neq 1$, and thus $x \in \ker \gamma_{i_1}$ and $x \notin \ker \gamma_{i_2}$ and hence $\ker \gamma_{i_1} \neq \ker \gamma_{i_2}$. We thus have that $|\{\ker \gamma_1, \ldots, \ker \gamma_k\}| = k$.

By Theorem 4.12 below, taking β as $\pi\gamma_i$ for any i (it was proved that these functions were all equal) and seeing $\{\ker \gamma_1, \ldots, \ker \gamma_k\}$ as a subset of the appropriate R, the set of normal subgroups N of F arising as kernels of those homomorphisms of F onto L which composed with π yield the given β, we get that $k \leq \phi_L(m)/|\Gamma|\phi_{L/M}(m)$ and thus $|K| \leq \phi_L(m)/|\Gamma|\phi_{L/M}(m)$. In particular K is finite. □

2.5 The function f

We are now in conditions to define the function f. This function will play a key role in finding out the minimal number of generators of a finite group.

Before providing the definition, let us remember that we are assuming L to always denote a finite group with a unique minimal normal subgroup M, complemented if M is abelian. Furthermore we will define L_0 as L/M.

Definition 2.15. Given a group L we define $f(L, m) = k + 1$ if and only if $d(L_k) = m < d(L_{k+1})$. When L can be identified from the context, we denote $f(L, m)$ as $f(m)$.

The function f gives us the integer $k + 1$ for which $d(L_{k+1}) = m + 1$ is bigger than any $d(L_q)$ for $q < k + 1$ (we are implicitly using Theorem 2.13 in this claim).

We claim that any proper quotient of L_{k+1} has a minimal number of generators smaller than or equal to m. Let N be a non-trivial normal subgroup of L_{k+1}. There is a minimal normal subgroup M contained in N and thus by Theorem 2.10 we obtain that $d(L_{k+1}/M) = d(L_k) \leq m$. Now using the Third Isomorphism Theorem and the fact that the minimal number of generators of a quotient is always smaller or equal than the ambient group we obtain

$$d(L_{k+1}/N) = d(\frac{L_{k+1}/M}{N/M}) \leq d(L_{k+1}/M) = d(L_k) = m.$$

Thus the function f gives us *the integer* $k + 1$ *for which any proper quotient of* L_{k+1} *has minimal number of generators smaller or equal to* m *but* $d(L_{k+1}) > m$.

In light of this new characterization of the function f, our reason for our definition of L_0 is now justified, that is $f(m) = 1$ iff $d(L_0) = d(L/M) < d(L)$.

Let us notice that this function of course depends on the group L being considered and that the domain of this function is the positive integers.

Chapter 3

Minimal number of generators of a group

In this section we study the structure of finite groups with the following property: any proper non-trivial group quotient is generated by less elements than the group itself. We will start with the simpler case of when $d(H) > 1$ but $d(H/N) \leq 1$ for every non-trivial normal subgroup N of H. Later we will provide a more detailed account of a Theorem mostly proved in [1], the generalization to the case in which $d(H) > m$ but $d(H/N) \leq m$ for every positive integer m and every non-trivial normal subgroup N.

3.1 The case $m = 1$

Theorem 3.1. *Let H be a finite nilpotent group such that $d(H/N) \leq 1$ for every non-trivial normal subgroup N, but $d(H) > 1$. Then $H \cong \mathbb{Z}_p \times \mathbb{Z}_p$ for some prime p.*

Proof. Since H is nilpotent we have that $H = P_1 \times \ldots \times P_n$ where P_i is a Sylow p_i-subgroup for $1 \leq i \leq n$ and $p_1, \ldots, p_n$ are distinct primes.

Let us remember that for any positive integers a, b if $(a, b) = 1$ then $\mathbb{Z}_a \times \mathbb{Z}_b \cong \mathbb{Z}_{ab}$. If $P_1, \ldots, P_r$ are cyclic, we obtain $H \cong \mathbb{Z}_{p_1 \ldots p_n}$ which contradicts $d(H) > 1$.Without loss of generality we can thus assume that P_1 is not cyclic.

If $n \geq 2$, $P_1 \cong H/(1 \times P_2 \ldots \times P_n)$ and thus $d(P_1) = d(H/(1 \times P_2 \ldots \times P_n)) = 1$, a contradiction. We can then conclude that $H = P_1$.

By Theorem 1.26, $\Phi(H) = 1$ hence $H = (\mathbb{Z}_{p_1})^q$ by Theorem 1.25. In fact $q = 2$ since

$$q - 1 = d((\mathbb{Z}_{p_1})^{q-1}) = d(H/(\mathbb{Z}_{p_1} \times 1 \times \ldots \times 1)) = 1.$$

□

Theorem 3.2. *Let H be a finite group such that $d(H/N) \leq 1$ for every non-trivial normal subgroup N, but $d(H) > 1$. Then either $H \cong \mathbb{Z}_p \times \mathbb{Z}_p$ or H is a primitive monolithic group i.e. primitive and has a unique minimal normal subgroup.*

Proof. If H is nilpotent by Theorem 3.1 we have that $H \cong \mathbb{Z}_p \times \mathbb{Z}_p$. We can thus assume that H is not nilpotent.

Since H is not nilpotent there exists a maximal subgroup L of H such that L is not normal in H. We will prove that $core(L) = 1$, and thus that H is primitive.

Let us suppose to obtain a contradiction that $core(L) \neq 1$. Then by hypothesis $H/core(L)$ is cyclic. Now all subgroups of an abelian group are normal and thus $L/core(L)$ is a normal subgroup of $H/core(L)$. This implies that L is a normal subgroup of H and thus contradicts the assumptions made on L. We have proved that H is primitive.

It remains to show that H is monolithic, i.e. H has a single minimal normal subgroup. To obtain a contradiction, let us suppose H has at least two different minimal normal subgroups (minimal normal subgroups of a non-trivial finite group always exist). We claim that any minimal normal subgroup N of H is abelian; letting J be a minimal normal subgroup different from N we obtain the following isomorphism between N and a subgroup of the cyclic group H/J

$$NJ/J \cong N/(J \cap N) \cong N.$$

Now since $soc(H)$ is the product of abelian minimal normal subgroups, it is itself abelian. We thus obtain that, $L \cap soc(H) \lhd soc(H)$. Also $L \cap soc(H) \lhd L$. Consequently $L \cap soc(H) \lhd soc(H)L = H$, since L is maximal with trivial core. Since $core(L) = 1$ we have that $L \cap soc(H) = 1$. Similarly for any minimal normal subgroup N, $LN = H$ and $L \cap N = 1$. What we obtained was that L is a complement for both any minimal normal subgroup N of H and $soc(H)$ in H.

Now since $N \subseteq soc(H)$ and $|L||soc(H)| = |H| = |L||N| \implies |soc(H)| = |N|$ we obtain that $N = soc(H)$, that is N is the unique minimal normal subgroup of H, a contradiction. □

3.2 An important structural Theorem

Theorem 3.3. *Let H be a finite group and N_1, N_r two different minimal normal subgroups of H complemented by K_r. If the projections $\pi_r : K_r \cap (N_1 \times N_r) \to N_1$, $\rho_r : K_r \cap (N_1 \times N_r) \to N_r$*

are isomorphisms then $K_r \cap (N_1 \times N_r) = \{x\phi_r(x) | x \in N_1\}$ *where* $\phi_r = \rho_r \pi_r^{-1}$.

Proof. For the inclusion $K_r \cap (N_1 \times N_r) \subseteq \{x\phi_r(x) | x \in N_1\}$ let $n_1 n_r \in K_r \cap (N_1 \times N_r)$ where $n_1 \in N_1$ and $n_r \in N_r$. Since π_r is one-to-one, $\pi_r^{-1}(n_1) = n_1 n_r$, and thus $\phi_r(n_1) = \rho_r(\pi_r^{-1}(n_1)) = \rho_r(n_1 n_r) = n_r$. We obtain that $n_1 n_r = n_1 \phi_r(n_1) \in \{x\phi_r(x) | x \in N_1\}$.

For the other inclusion, let $x \in N_1$. Obviously $\pi_r^{-1}(x) \in K_r \cap (N_1 \times N_r)$. We thus have $\pi_r^{-1}(x) = n_1 n_r \in K_r \cap (N_1 \times N_r)$ where $n_1 \in N_1$ and $n_r \in N_r$. Now $x = \pi_r(\pi_r^{-1}(x)) = \pi_r(n_1 n_r) = n_1$. Furthermore $\phi_r(x) = \rho_r(\pi_r^{-1}(x)) = \rho_r(n_1 n_r) = n_r$. Thus we conclude $x\phi_r(x) = n_1 n_r \in K_r \cap (N_1 \times N_r)$. □

Theorem 3.4. *Let* H *be a finite group and* N_1 *be a non-abelian minimal normal subgroup of* H. *Let also* $\alpha_1 : H \to Aut\, N_1$ *be the homomorphism that sends* h *to the function*

$$\begin{aligned} \gamma_h \colon N_1 &\to N_1 \\ x &\mapsto hxh^{-1}, \end{aligned}$$

and L *be the image of* α_1. *Then* L *has a unique minimal normal subgroup, namely* $Inn\, N_1$.

Proof. By Theorem 1.11 we have that $Inn\, N_1 = \{\gamma_x \colon N_1 \to N_1 | x \in N_1\} = \alpha_1(N_1)$ is either a minimal normal subgroup of L or 1.

Since N_1 is non abelian there are $n_1, n_2 \in N_1$ such that $n_1 n_2 \neq n_2 n_1$. Therefore we have that $\alpha_1(n_1) = \gamma_{n_1} \neq 1$ as $1(n_2) = n_2 \neq n_1 n_2 n_1^{-1} = \gamma_{n_1}(n_2)$. Thus $Inn\, N_1$ is not 1, and hence is a minimal normal subgroup of L.

To check that $Inn\, N_1$ is the unique minimal normal subgroup of L we will verify that for every non-trivial normal subgroup N of L, $Inn\, N_1 \subseteq N$.

Let N be a subgroup in the above conditions. Then $\alpha_1^{-1}(N)$ is normal in H. Furthermore since N_1 is a minimal normal subgroup, $\alpha_1^{-1}(N) \cap N_1$ is either 1 or N_1. We will check that $\alpha_1^{-1}(N) \cap N_1$ must be N_1.

If $\alpha_1^{-1}(N) \cap N_1 = 1$ then $[\alpha_1^{-1}(N), N_1] \leq \alpha_1^{-1}(N) \cap N_1 = 1$, that is the elements of N_1 commute with the elements of $\alpha_1^{-1}(N)$. Thus for all $h \in \alpha_1^{-1}(N)$, $\gamma_h(x) = hxh^{-1} = hh^{-1}x = x$. Therefore $N = \alpha_1(\alpha_1^{-1}(N)) = 1$. This is a contradiction, and so $\alpha_1^{-1}(N) \cap N_1 = N_1$. Obviously it now follows from $N_1 \subseteq \alpha_1^{-1}(N)$ that $\alpha_1(N_1) \subseteq \alpha_1(\alpha_1^{-1}(N)) = N$ as we wanted to prove. □

Theorem 3.5. *Let* m *be an integer with* $m \geq 1$ *and* H *a finite group such that* $d(H/N) \leq m$ *for every non-trivial normal subgroup* N, *but* $d(H) > m$. *Then there exists a group* L *which has a* *unique minimal normal subgroup M and is such that M is either non-abelian or complemented in L and $H \cong L_{f(L,m)}$.*

Proof. Since $d(H/N) \leq m$ for every non-trivial normal subgroup N, by Theorem 1.26 we have that $\Phi(H) = 1$.

We are going to consider two cases: first the case where H has only one minimal normal subgroup and later the case where H has more than one minimal normal subgroup. Furthermore each such case will be divided into the case where those minimal subgroups are abelian and the case where they are not abelian (as will be seen these are the only possible cases).

H **has a unique minimal normal subgroup:**

Consider the case in which H has a unique minimal normal subgroup, say M. Taking L as H gives the result for the subcase in which M is non-abelian. If M is abelian since $\Phi(H) = 1$, there exists a maximal subgroup K of H such that K does not contain M. Since K is maximal and does not contain M, $KM = H$. Furthermore by the hypothesis on K, $K \cap M$ is a strictly contained normal subgroup of M (M is abelian). Obviously since M is normal in H, $K \cap M$ is normal in K. We thus have $K \cap M$ is normal in KM and thus in $H = KM$. We have obtained that $K \cap M$ is normal in H and strictly contained in the minimal normal subgroup M, so we conclude that $K \cap M = 1$. It was thus proved that K is the desired complement and we can take L as H.

H **has more than one minimal normal subgroup:**

We can now assume that H contains at least two different minimal normal subgroups. Let us denote these minimal normal subgroups as $N_1, \ldots, N_r, \ldots$. Since $d(H/N_1) \leq m$ by assumption, there exist m elements $h_1, \ldots, h_m$ of H such that $H = \langle h_1, \ldots h_m, N_1 \rangle$. Now consider N_r with $r \neq 1$. Certainly, $H = \langle h_1, \ldots, h_m, N_1 N_r \rangle$. Moreover as $H/N_1 N_r$ is isomorphic to the quotient $(H/N_r)/(N_1 N_r/N_r)$ of H/N_r and H/N_r is generated by at most m elements, by Theorem 1.29 there exists m elements $x_1, \ldots, x_m \in N_1$ such that $\langle h_1 x_1, \ldots, h_m x_m, N_r \rangle = H$.

Consider the subgroup $K_r = \langle h_1 x_1, \ldots, h_m x_m \rangle$. We assert that N_1 and N_r both serve as complements for K_r within H.

Clearly, $H = K_r N_1 = K_r N_r$; hence, we only need to show that $K_r \cap N_1 = K_r \cap N_r = 1$. We claim that the intersection $K_r \cap N_1$ is a normal subgroup of $K_r N_r = H$. In fact as $[N_1, N_r] \leq N_1 \cap N_r = 1$, for any $k_r \in K_r$, $n_r \in N_r$:

$$k_r n_r (K_r \cap N_1) n_r^{-1} k_r^{-1} = k_r n_r n_r^{-1} (K_r \cap N_1) k_r^{-1} = K_r \cap N_1$$

where the first equality follows from the commutativity between the elements of N_1 and N_r and the second from the normality of $K_r \cap N_1$ in K_r. As the normal subgroup $K_r \cap N_1$ is contained in the minimal normal subgroup N_1 of H, if $K_r \cap N_1 \neq 1$ then $N_1 \cap K_r = N_1$. And consequently $H = K_r N_1 = K_r$ is m-generated, which contradicts our hypothesis. The claim $K_r \cap N_r = 1$ is proved similarly.

We can now prove that the projections $\pi_r : K_r \cap (N_1 \times N_r) \to N_1$ and $\rho_r : K_r \cap (N_1 \times N_r) \to N_r$ are isomorphisms. Let us start with π_r: The kernel of π_r is a subgroup of $N_r \cap K_r$, which is trivial since N_r and K_r have trivial intersection. Therefore, π_r is injective. Furthermore, for any $n_1 \in N_1$, there exists $t \in K_r$ and $n_r \in N_r$ such that $n_1 = t n_r$. Thus, $t = n_1 n_r^{-1} \in (N_1 \times N_r) \cap K_r$, and $\pi_r(t) = n_1$. Hence, π_r is also surjective. Similar arguments can be applied to ρ_r.

What we conclude from this is that for each $r > 1$, there exists a subgroup K_r which serves as a complement for both N_1 and N_r, and there exists an isomorphism $\phi_r : N_1 \to N_r$ (specifically, $\phi_r = \rho_r \pi_r^{-1}$) such that $K_r \cap (N_1 \times N_r) = \{x\phi_r(x) | x \in N_1\}$. Furthermore we will define $\phi_1 \colon N_1 \to N_1$ as the identity function. The equality $K_r \cap (N_1 \times N_r) = \{x\phi_r(x) | x \in N_1\}$ follows from Theorem 3.3. Using the fact that this intersection is normal in K_r, we claim that ϕ_r is a K_r-isomorphism, that is for any $k \in K_r$, $k \cdot \phi_r(x) = \phi_r(k \cdot x) \iff k\phi_r(x)k^{-1} = \phi_r(kxk^{-1})$. We have that for any $k \in K_r$, $x \in N_1$, $kx\phi_r(x)k^{-1} = y\phi_r(y)$ for some $y \in N_1$ hence:

$$\begin{aligned} & kxk^{-1}k\phi_r(x)k^{-1} = y\phi_r(y) \\ \iff & y^{-1}kxk^{-1} = \phi_r(y)k\phi_r(x)^{-1}k^{-1} \in N_1 \cap N_r = 1 \\ \implies & y = kxk^{-1} \text{ and } k\phi_r(x)k^{-1} = \phi_r(y) = \phi_r(kxk^{-1}) \end{aligned}$$

Abelian minimal normal subgroups sub-case:

Suppose now that N_1 (and consequently any minimal normal subgroup since they are isomorphic) is abelian. We are now going to construct an isomorphism Ψ from H to a group L_q.

By Theorem 1.17, $soc(H)$ is complemented in H say by K. Knowing also that $soc(H)$ is the direct product of some minimal normal subgroups, say $soc(H) = N_1 \times \ldots \times N_q$, for $1 \leq i \leq q$, N_i is complemented in $soc(H)$ by $C_i = N_1 \times \ldots \times N_{i-1} \times 1 \times N_{i+1} \times \ldots \times N_q$. Consider the functions $\chi_i : soc(H) \to N_i$ that send $n_i c_i$ to n_i for any $n_i \in N_i$, $c_i \in C_i$. It is routine to prove that for any i, χ_i is a surjective H-homomorphism with $\ker \chi_i = C_i$. Also ϕ_i is a H-homomorphism.

We prove only the H-homomorphism claims. For any $h \in H = N_i K_i$, h can be written as $k_i v_i$ where $k_i \in K_i$ and $v_i \in N_i$. Thus for any $n_i c_i \in N_i C_i = soc(H)$

$$\begin{aligned}
\chi_i(h n_i c_i h^{-1}) &= \chi_i(k_i v_i n_i c_i v_i^{-1} k_i^{-1}) \\
&= \chi_i(k_i n_i c_i k_i^{-1}), \text{ since soc}(H) \text{ is abelian and } v_i \in \text{soc}(H) \\
&= \chi_i(k_i n_i k_i^{-1} k_i c_i k_i^{-1}), \text{ let us notice that } k_i c_i k_i^{-1} \in C_i \text{ since } C_i \text{ is normal} \\
&= k_i n_i k_i^{-1} = k_i(v_i v_i^{-1}) n_i k_i^{-1} = k_i v_i n_i v_i^{-1} k_i^{-1} \\
&= h \chi_i(n_i c_i) h^{-1}.
\end{aligned}$$

Similarly for ϕ_i:

$$\begin{aligned}
\phi_i(h n_i h^{-1}) &= \phi_i(k_i v_i n_i v_i^{-1} k_i^{-1}) \\
&= \phi_i(k_i n_i k_i^{-1}) \\
&= k_i \phi_i(n_i) k_i^{-1}, \text{since } \phi_i \text{ is a } K_i\text{-isomorphism} \\
&= k_i(v_i v_i^{-1}) \phi_i(n_i) k_i^{-1} \\
&= k_i v_i \phi_i(n_i) v_i^{-1} k_i^{-1} = h \phi_i(n_i) h^{-1}.
\end{aligned}$$

Obviously the composition $\phi_i^{-1} \circ \chi_i \colon soc(H) \to N_1$ is a surjective H-homomorphism with $\ker \chi_i = C_i$ for any i. Setting $L = KN_1$ we can define the following functions:

$$\begin{aligned}
\Psi_i \colon H &\longrightarrow KN_1 = L \\
ks &\mapsto k\phi_i^{-1} \circ \chi_i(s)
\end{aligned}$$

where $k \in K$ and $s \in soc(H)$. These functions are well defined since for all $k_1, k_2 \in K$ and $s_1, s_2 \in soc(H)$, if $k_1 s_1 = k_2 s_2$ then $k_2^{-1} k_1 = s_2 s_1^{-1} \in K \cap soc(H) = 1$. This implies $k_1 = k_2$ and $s_1 = s_2$. Consequently for any i, $\phi_i^{-1} \circ \chi_i(s_1) = \phi_i^{-1} \circ \chi_i(s_2)$, therefore

$$\Psi_i(k_1 s_1) = k_1 \phi_i^{-1} \circ \chi_i(s_1) = k_2 \phi_i^{-1} \circ \chi_i(s_2) = \Psi_i(k_2 s_2).$$

These functions are homomorphisms since

$$\begin{aligned}
\Psi_i(k_1s_1k_2s_2) &= \Psi_i(k_1(k_2k_2^{-1})s_1k_2s_2) \\
&= \Psi_i(k_1k_2s_1^{k_2^{-1}}s_2) \\
&= k_1k_2\phi_i^{-1}\circ\chi_i(s_1^{k_2^{-1}}s_2) \\
&= k_1k_2\phi_i^{-1}\circ\chi_i(s_1)^{k_2^{-1}}\phi_i^{-1}\circ\chi_i(s_2) \\
&= k_1\phi_i^{-1}\circ\chi_i(s_1)k_2\phi_i^{-1}\circ\chi_i(s_2) \\
&= \Psi_i(k_1s_1)\Psi_i(k_2s_2).
\end{aligned}$$

Since $\phi_i^{-1}\circ\chi_i$ is an isomorphism, Ψ_i is surjective. Furthermore we also easily obtain that $\ker\Psi_i = C_i$, as

$$\Psi_i(k_1s_1) = 1 \iff \phi_i^{-1}\circ\chi_i(s_1) = k^{-1}\in N_1\cap K = 1 \iff k_1 = 1 \text{ and } s_1\in\ker\phi_i^{-1}\circ\chi_i = C_i.$$

Now by Theorem 1.11, $N_1 = \Psi_1(N_1)$ is a minimal normal subgroup of L. We claim it is the only minimal normal subgroup of L.

We will start by proving that $core_L(K) = 1$. To obtain a contradiction, let us assume that $core_L(K)\neq 1$. Then there exists a non-trivial subgroup $A\lhd L$ contained in K. Now it is not difficult to see that $\Psi_i^{-1}(A) = AC_i$ and that these groups are normal subgroups of H. Furthermore $C_1\dots C_q\cap A\subseteq C_1\dots C_q\cap K\subseteq soc(H)\cap K = 1$ and thus by Theorem 1.2, $\bigcap_{i=1}^q AC_i = A(\bigcap_{i=1}^q C_i)$. We thus obtain that

$$A = A(\bigcap_{i=1}^q C_i) = \bigcap_{i=1}^q AC_i = \bigcap_{i=1}^q \Psi_i^{-1}(A)\lhd H.$$

But this is a contradiction since $A\cap soc(H)\subseteq K\cap soc(H) = 1$, that is A is a non-trivial a normal subgroup of H that does not contain any minimal normal subgroup.

Now we claim that $C_L(N_1) = N_1$. To obtain a contradiction let us suppose that there exists elements $k\in K$ and $n_1\in N_1$ such that $kn_1\notin N_1$ (that is $k\neq 1$) and $kn_1\in C_L(N_1)$. Since N_1 is abelian, $n_1^{-1}\in C_L(N_1)$ and thus $k = (kn_1)n_1^{-1}\in C_L(N_1)$. What we proved until now was that $C_L(N_1)\cap K\neq 1$. Now since $C_L(N_1)$ is normal in L, $K\leq N_L(C_L(N_1)\cap K)$ and since N_1 is abelian, $N_1\leq N_L(C_L(N_1)\cap K)$. Thus $L = KN_1\leq N_L(C_L(N_1)\cap K)$. What we conclude is that $C_L(N_1)\cap K$ is a non-trivial normal subgroup of L fully contained in K, but this contradicts the fact that $core_L(K) = 1$.

Now suppose that there exists a minimal normal subgroup $A\neq N_1$ of L. Since A is different from N_1, $[A, N_1] = 1$ and thus $A\leq C_L(N_1) = N_1$, a contradiction. Therefore N_1

is the only minimal normal subgroup of L.

Setting $L = KN_1$ we can define the following function:

$$\begin{aligned} \Psi\colon H &\longrightarrow L_q \\ ks &\mapsto (\Psi_1(ks), \Psi_2(ks), \dots, \Psi_q(ks)) \end{aligned}$$

where $k \in K$ and $s \in soc(H)$. It is obvious that this function is well defined, furthermore it is injective since

$$x \in \ker \Psi \iff x \in \bigcap_{i=1}^{q} \ker \Psi_i \iff x \in \bigcap_{i=1}^{q} C_i = 1.$$

Comparing orders we get surjectivity since

$$|H| = |K||soc(H)| = |K||N_1|^q = |L_q|.$$

The abelian case is thus finished.

Non-abelian minimal normal subgroups sub-case:

We assume that N_1 is non-abelian.

Consider the homomorphism $\alpha_1\colon H \to Aut\, N_1$ that sends each $h \in H$ to

$$\begin{aligned} \alpha_1(h)\colon N_1 &\to N_1 \\ x &\mapsto hxh^{-1}. \end{aligned}$$

We will denote by L the image of α_1. By Theorem 3.4, L has a unique minimal normal subgroup $M = Inn\, N_1$. For $r > 1$, we define $\alpha_r\colon H \to Aut\, N_1$ as the homomorphism that sends $h \in H$ to

$$\begin{aligned} \alpha_r(h)\colon N_1 &\to N_1 \\ x &\mapsto \phi_r^{-1}(h\phi_r(x)h^{-1}). \end{aligned}$$

Given that $H = K_r N_1$, we can represent each $h \in H$ as $h = uv$ where $u \in K_r$ and $v \in N_1$. Consequently,

$$\begin{aligned} \phi_r^{-1}(h\phi_r(x)h^{-1}) &= \phi_r^{-1}(uv\phi_r(x)v^{-1}u^{-1}) = \phi_r^{-1}(uvv^{-1}\phi_r(x)u^{-1}) \\ &= \phi_r^{-1}(\phi_r(x^u)) = x^u = (x^h)^{v^{-1}}. \end{aligned}$$

Here, the second equality holds because N_1 centralizes N_r, and the third equality due to the fact that ϕ_r is a K_r-isomorphism. We thus have that $\alpha_r(h) = \gamma_{v^{-1}}(\alpha_1(h))$ where $\gamma_{v^{-1}}$ is conjugation by v^{-1}.

We obtain that

$$\alpha_1(h)M = \ldots = \alpha_r(h)M.$$

It thus follows that for any $1 \leq i \leq r$, $L = \alpha_1(H) = \alpha_1(H)M = \alpha_i(H)M = \alpha_i(H)$.

Taking q as the number of minimal normal subgroups of H, let us consider now the function

$$\begin{aligned} \Psi \colon H &\to L_q \\ h &\mapsto (\alpha_1(h), \ldots, \alpha_q(h)). \end{aligned}$$

We will prove that this function is an isomorphism. Obviously it is well defined and is an homomorphism since the α_r are homomorphisms. To check injectivity let us first notice that the kernel of Ψ is the intersection of the kernels of the α_r.

If $h \in \ker \alpha_r$ then for all $x \in N_1$, $\phi_r^{-1}(h\phi_r(x)h^{-1}) = x \iff h\phi_r(x) = \phi_r(x)h$. Since ϕ_r is an isomorphism this means that h centralizes N_r. Obviously if h centralizes N_r, $h \in \ker \alpha_r$ and thus we conclude that $\ker \alpha_r$ is the centralizer of N_r.

Since the minimal normal subgroups N_r are not contained in their own centralizers, $\ker \Psi$ is a normal subgroup of H that does not contain any minimal normal subgroup. We obtain that $\ker \Psi = 1$ and injectivity is thus proved.

It is now at last only necessary to prove surjectivity. Given $h \in H$ we will use the auxiliary notation γ_h to denote the function

$$\begin{aligned} \gamma_h \colon N_1 &\to N_1 \\ x &\mapsto hxh^{-1} \end{aligned}$$

and $\phi_1 \colon N_1 \to N_1$ to denote the identity function. Let $(\gamma_{m_1}\gamma_k, \ldots, \gamma_{m_q}\gamma_k) \in L_q$ where $k \in K_r$ and $m_1, \ldots, m_q \in N_1$. Consider the element

$$k\phi_1(m_1)\phi_2(m_2)\ldots\phi_q(m_q) \in H.$$

Now for $1 \leq r \leq q$ and $x \in N_1$

$$\begin{aligned}
\alpha_r(k\phi_1(m_1)\phi_2(m_2)\dots\phi_q(m_q))(x) &= \phi_r^{-1}(\phi_r(x)^{k\phi_1(m_1)\phi_2(m_2)\dots\phi_q(m_q)}) \\
&= \phi_r^{-1}(\phi_r(x)^{k\phi_r(m_r)}) \\
&= \phi_r^{-1}(\phi_r(x^k)^{\phi_r(m_r)}) \\
&= \phi_r^{-1}(\phi_r(x^k))^{\phi_r^{-1}(\phi_r(m_r))} \\
&= m_r k x k^{-1} m_r^{-1} = \gamma_{m_r} \circ \gamma_k(x)
\end{aligned}$$

where the second equality follows from the fact that $N_1, \dots, N_{r-1}, N_{r+1} \dots, N_q$ centralize N_r and the third from ϕ_r being a K_r-isomorphism. We thus conclude that

$$\Psi(k\phi_1(m_1)\phi_2(m_2)\dots\phi_q(m_q)) = (\gamma_{m_1}\gamma_k, \dots, \gamma_{m_q}\gamma_k)$$

and surjectivity is proved.

The non-abelian subcase is thus completed.

Regardless of which case we consider, what was proved was that $H \cong L_q$ for some positive integer q by some isomorphism Ψ. Since the image of a minimal normal subgroup by an isomorphism is again a minimal normal subgroup we obtain that for any minimal normal subgroup N_r of H, $H/N_r \cong L_q/\Psi(N_r)$ and applying Theorem 2.10 $H/N_r \cong L_{q-1}$. Since H/N_r is a proper non-trivial quotient of H we get that

$$d(L_{q-1}) = d(H/N_r) < d(H) = d(L_q).$$

This is precisely the definition of the function f, that is $f(L, m) = q$ and the proof of the theorem is complete.

$\square$

Chapter 4

The Function f

The purpose of this section is to determine a way to calculate $f(L, m)$. Once again, most of the ideas in this section were originally exposed in [1] and more detail is provided here. To aid us in this end, we will denote by π_{L_k} the surjective homomorphism

$$\begin{aligned} \pi_{L_k} \colon L_k &\to L/M \\ x &\mapsto \pi_1(x)M. \end{aligned}$$

It is easy to verify that such a function is well defined and is a surjective homomorphism. Furthermore let us notice that the choice of π_1 in the definition of π_{L_k} is completely arbitrary; any of the π_i functions serve as from the definition of L_k, $\pi_1(x)M = \ldots = \pi_k(x)M$. The following definition will prove to be crucial to the calculation of $f(L, m)$.

Definition 4.1. Given a surjective homomorphism $\beta \colon L_k \to L/M$, we define the set $\mathscr{S}_\beta$ as the set of normal subgroups N of L_k arising as kernels of those homomorphisms of L_k onto L which composed with the natural projection $\pi_L \colon L \to L/M$ yield β.

Theorem 4.2. *Given a surjective homomorphism $\beta \colon L_k \to L/M$, $\ker \beta = M^k$.*

Proof. We have that $|L_k|/|\ker \beta| = |L|/|M| \implies |\ker \beta| = |M^k|$ and hence by Theorem 2.11 we have $\ker \beta = soc(L_k)$. □

Going forwards we are going to divide the study of the function f in two cases: the case where M is abelian and the case where M is not abelian.

4.1 The M abelian case

If M is abelian then it is complemented by C in L. Furthermore it was already proved that $diag(C^k)$ complements M^k in L_k. To simplify notation, given $l \in L$ we will denote by $\dot{l} \in diag(L^k)$ the element with all coordinates equal to l and by $\dot{C} = diag(C^k)$.

Now we can define the following group action:

$$\begin{aligned} \cdot\colon L/M \times M^k &\to M^k \\ (lM, m) &\mapsto \dot{l}^{-1} m \dot{l}. \end{aligned}$$

We claim this action is well defined. Let $(l_1M, m_1) = (l_2M, m_2)$ where $l_1M, l_2M \in L/M$ and $m_1, m_2 \in M^k$. Then $l_1^{-1}M = l_2^{-1}M$ and thus $\dot{l_1}^{-1} = \dot{l_2}^{-1}\dot{x}$ for some $x \in M$. We then obtain

$$\dot{l_1}^{-1} m_1 \dot{l_1} = \dot{l_2}^{-1} \dot{x} m_1 \dot{x}^{-1} \dot{l_2} = \dot{l_2}^{-1} \dot{x}\dot{x}^{-1} m_1 \dot{l_2} = \dot{l_2}^{-1} m_1 \dot{l_2},$$

where the third equality follows since M is abelian.

Now let us consider

$$\begin{aligned} \rho\colon C &\to L/M \\ c &\mapsto cM. \end{aligned}$$

Obviously ρ is well defined and is an homomorphism. It is also injective since for all $c_1, c_2 \in C$, such that $c_1M = c_2M$ then $c_2^{-1}c_1 \in M \cap C = 1$ and consequently $c_1 = c_2$. Furthermore by the First Isomorphism Theorem $|L/M| = |CM/M| = |C||M|/|M| = |C| = |C/\ker\rho| = |\rho(C)|$. Then since $\rho(C) \subseteq L/M$ we conclude that $\rho(C) = L/M$. In other words ρ is a surjective function. We proved that ρ is an isomorphism, and so we can define $\Psi = \rho^{-1}\colon L/M \to C$.

Also, let $\beta\colon L_k \to L/M$ be a surjective homomorphism.

We have now all the necessary conditions to define the group action:

$$\begin{aligned} \cdot\colon L/M \times M &\to M \\ (lM, m) &\mapsto \Psi(\beta(\dot{l}))^{-1} m \Psi(\beta(\dot{l})). \end{aligned}$$

We claim that this function is well defined. Let $(l_1M, m_1) = (l_2M, m_2)$ where $l_1M, l_2M \in L/M$ and $m_1, m_2 \in M$. Then since $l_1M = l_2M \iff l_2^{-1}l_1 \in M$, $\dot{l_2}^{-1}\dot{l_1} \in M^k$ ($= \ker\beta$ by Theorem 4.2), $\beta(\dot{l_2}^{-1}\dot{l_1}) = 1$. This in turn implies $\beta(\dot{l_2})^{-1}\beta(\dot{l_1}) = 1 \implies \beta(\dot{l_1}) = \beta(\dot{l_2})$. Thus

$$l_1M \cdot m_1 = \Psi(\beta(\dot{l_1}))^{-1}m_1\Psi(\beta(\dot{l_1})) = \Psi(\beta(\dot{l_2}))^{-1}m_2\Psi(\beta(\dot{l_2})) = l_2M \cdot m_2.$$

Theorem 4.3. *Let us assume M is abelian. Given a surjective homomorphism $\beta\colon L_k \to L/M$, the set $\mathscr{S}_\beta$ is identical to the set of kernels of surjective L/M-homomorphisms $\nu\colon M^k \to M$ with the above group actions.*

Proof. To prove the first inclusion, let $N \in \mathscr{S}_\beta$. Then there exists a surjective homomorphism φ such that $\ker\varphi = N$ and $\pi_L \circ \varphi = \beta$. We will now prove that the restriction of φ to M^k is a L/M-homomorphism with kernel N.

Since φ is surjective we obtain that $\varphi|_{M^k}(soc(L_k)) \subseteq soc(L) = M$ by Theorem 1.11. Furthermore since $\pi_L \circ \varphi = \beta$, $\ker\varphi$ is contained in $\ker\beta = M^k$. We also claim that this inclusion is strict, since if it were otherwise then $|L| = |L_k|/|\ker\varphi| = |L_k|/|M^k| = |L|/|M|$ but this is a contradiction. Thus $\varphi(M^k)$ is a non-trivial normal subgroup in L. Since M is a minimal normal subgroup we conclude that $\varphi(M^k) = M$.

That $\ker\varphi|_{M^k} = N$ is obvious, since $N = \ker\varphi \subseteq \ker\beta = M^k$.

Now for any $lM \in L/M$ and any $m \in M^k$, we have that $\varphi(\dot{l})M = \pi_L \circ \varphi(\dot{l}) = \beta(\dot{l}) = \rho(\Psi(\beta(\dot{l}))) = \Psi(\beta(\dot{l}))M \implies \varphi(\dot{l})^{-1}M = \Psi(\beta(\dot{l}))^{-1}M$. Thus there exists an $x \in M$ such that $\varphi(\dot{l})^{-1} = \Psi(\beta(\dot{l}))^{-1}x^{-1} \implies \varphi(\dot{l}) = x\Psi(\beta(\dot{l}))$. It then follows that

$$\begin{aligned}
\varphi|_{M^k}(lM \cdot m) &= \varphi(\dot{l}^{-1}m\dot{l}) \\
&= \varphi(\dot{l})^{-1}\varphi(m)\varphi(\dot{l}) \\
&= \Psi(\beta(\dot{l}))^{-1}x^{-1}\varphi(m)x\Psi(\beta(\dot{l})) \\
&= \Psi(\beta(\dot{l}))^{-1}x^{-1}x\varphi(m)\Psi(\beta(\dot{l})), \text{ since } M \text{ is abelian} \\
&= lM \cdot \varphi|_{M^k}(m)
\end{aligned}$$

and the proof of this inclusion is complete.

To prove the other inclusion, let ν be a L/M-homomorphism. Let us first define

$$\begin{aligned}
\psi\colon L_k &\to L \\
\dot{c}m &\mapsto \Psi(\beta(\dot{c}))\nu(m),
\end{aligned}$$

where $\dot{c} \in \dot{C}$ and $m \in M^k$. This function is well-defined since $\dot{C}$ and M^k are complements. It is a homomorphism since for any $\dot{c}_1, \dot{c}_2 \in \dot{C}$ and $m_1, m_2 \in M^k$,

$$\begin{aligned}
\psi(\dot{c}_1 m_1 \dot{c}_2 m_2) &= \psi(\dot{c}_1 \dot{c}_2 m_1^{\dot{c}_2^{-1}} m_2) \\
&= \Psi(\beta(\dot{c}_1 \dot{c}_2)) \nu(m_1^{\dot{c}_2^{-1}}) \nu(m_2) \\
&= \Psi(\beta(\dot{c}_1)) \Psi(\beta(\dot{c}_2)) \nu(\dot{c}_2 M \cdot m_1) \nu(m_2) \\
&= \Psi(\beta(\dot{c}_1)) \Psi(\beta(\dot{c}_2)) (\dot{c}_2 M \cdot \nu(m_1)) \nu(m_2) \\
&= \Psi(\beta(\dot{c}_1)) \Psi(\beta(\dot{c}_2)) \nu(m_1)^{\Psi(\beta(\dot{c}_2))^{-1}} \nu(m_2) \\
&= \Psi(\beta(\dot{c}_1)) \nu(m_1) \Psi(\beta(\dot{c}_2)) \nu(m_2) \\
&= \psi(\dot{c}_1 m_1) \psi(\dot{c}_2 m_2).
\end{aligned}$$

We claim that $\ker \psi = \ker \nu$. Let $\dot{c} \in \dot{C}$ and $m \in M^k$ be such that $\psi(\dot{c}m) = 1$. Then $\Psi(\beta(\dot{c})) = \nu(m)^{-1} \in M \cap C = 1$. Thus $\dot{c} \in \ker \beta \cap \dot{C} = M^k \cap \dot{C} = 1$ and $m \in \ker \nu$. What we conclude from this is that if $\psi(\dot{c}m) = 1$ then $\dot{c} = 1$ and $m \in \ker \psi$, that is $\ker \psi = \ker \nu$.

Since $\psi(L_k) \subseteq L$, applying the First Isomorphism Theorem we obtain

$$|L| = |L_k|/|M|^{k-1} = |L_k|/|\ker \psi| = |\psi(L_k)|$$

and thus surjectivity follows.

We also easily verify that for any $\dot{c} \in \dot{C}$ and $m \in M^k$

$$\begin{aligned}
\pi_L \circ \psi(\dot{c}m) &= \pi_L(\psi(\dot{c})) \pi_L(\psi(m)) \\
&= \pi_L(\Psi(\beta(\dot{c}))) M \\
&= \Psi(\beta(\dot{c})) M \\
&= \beta(\dot{c}) M, \text{ since } \rho(\Psi(\beta(\dot{c}))) = \beta(\dot{c}) \implies \Psi(\beta(\dot{c}))M = \beta(\dot{c}) \\
&= \beta(\dot{c}) \beta(m) \\
&= \beta(\dot{c}m)
\end{aligned}$$

□

Theorem 4.4. *Let us assume that M is abelian. Given a surjective homomorphism $\beta \colon L_k \to L/M$, the cardinality of the set $\mathscr{S}_\beta$ is k when M is non-abelian; it is $(q^k - 1)/(q - 1)$ when M is abelian and q is the number of (L/M)-endomorphisms of M.*

Proof. If M is abelian, by Theorem 4.3 we have to count the kernels of surjective (L/M)-homomorphisms from M^k to M. It is claimed on [1, Lemma 2.5] that this number is $(q^k-1)/(q-1)$ where q is the number of (L/M)-endomorphisms of M. □

4.2 The M not abelian case

Theorem 4.5. *Let us assume that M is not abelian. If $N \triangleleft L_k$ and $N \subseteq soc(L_k)$, then N is a direct product of some $M_1, \ldots, M_k$.*

Proof. Let $N_i = \pi_i(N)$. Since $N_i = \pi_i(N) \subseteq \pi_i(M^k) = M$, M is a minimal normal subgroup of L and $\pi_i(N)$ is normal in L we have that $\pi_i(N)$ is either 1 or M. Furthermore we have that $\pi_i|_{L_k}^{-1}(1) = \pi_i^{-1}(1) \cap L_k = (L \times \ldots \times 1 \times \ldots \times L) \cap L_k = (M \times \ldots \times 1 \times \ldots \times M)$ and that $\pi_i|_{L_k}^{-1}(M) = M^k$ and so $\pi_i^{-1}(N_i)$ is either $\pi_i|_{L_k}^{-1}(1) = (M \times \ldots \times 1 \times \ldots \times M)$ or $\pi_i|_{L_k}^{-1}(M) = M^k$. Thus $N \subseteq \cap_{i=1}^k \pi_i^{-1}(N_i) = \prod_{\{j|N_j=M\}} M_j$, that is N is contained in the set whose coordinate i is M iff $\pi_i(N) = M$ otherwise is 1. The first inclusion is thus complete.

Now we will prove by reduction to absurd that for any $1 \leq i \leq k$, $\pi_i(N) = M$ implies $M_i \subseteq N$. Since M_i is a minimal normal subgroup $N \cap M_i$ is either 1 or M_i. If $N \cap M_i = 1$ then $[N, M_i] \leq N \cap M_i = 1$, that is the elements of N and M_i commute. Furthermore since M is non-abelian there exists $x, y \in M$ such that $xy \neq yx$. Since π_i is a surjective function, there are $m_i \in M_i$ and $n \in N$ such that $y = \pi(m_i)$ and $x = \pi_i(n)$. We thus obtain

$$\begin{aligned} xy &= \pi_i(n)\pi_i(m_i) \\ &= \pi_i(nm_i) \\ &= \pi_i(m_i n) \\ &= \pi_i(m_i)\pi_i(n) \\ &= yx, \end{aligned}$$

a contradiction. From the claim just proven it easily follows that $\prod_{\{j|N_j=M\}} M_j \subseteq N$ and the proof is thus complete.

□

Theorem 4.6. *Let us assume that M is not abelian. If $L_k/N \cong L$ then N is a direct product of $k-1$ factors M_i.*

Proof. Since $|L_k/N| = |L_k|/|N| = |L|$ we obtain that $|N| = |M|^{k-1}$. It thus follows by Theorem 2.11 that $N \subseteq M^k$. Now by Theorem 4.5 N is a direct product of some factors M_i and since it has order $|M|^{k-1}$ it must be of $k-1$ of them. □

Theorem 4.7. *Let us assume that M is not abelian. The cardinality of the set*

$$\mathcal{N} = \{N \triangleleft L_k | N \leq soc(L_k) \text{ and } L_k/N \cong L\}$$

is k.

Proof. By Theorem 4.6, if $N \in \mathcal{N}$ it is a direct product of $k-1$ factors M_i. Since there are exactly k direct products of $k-1$ M_i factors, we obtain that $|\mathcal{N}| = k$. □

Theorem 4.8. *Let us assume that M is not abelian. Given a surjective homomorphism $\beta\colon L_k \to L/M$, the cardinality of the set $\mathscr{S}_\beta$ is k.*

Proof. It is claimed on [1, Lemma 2.5] that the normal subgroups we have to count are precisely the normal subgroups of L_k contained in $soc(L)$ and such that $L_k/N \cong L$. By Theorem 4.7 there are exactly k such subgroups.

□

4.3 Putting It All Together

Definition 4.9. Let F be a free group of rank m. Given a surjective homomorphism $\beta\colon F \to L/M$, we define the set $\mathscr{R}_\beta$ as the set of normal subgroups N of F arising as kernels of those homomorphisms of F onto L which composed with the natural projection $\pi_L\colon L \to L/M$ yield β.

Definition 4.10. Given an automorphism α of L we say that α **acts trivially on** L/M if and only if for all $lM \in L/M$

$$\alpha(lM) = lM.$$

Since L has a unique minimal normal subgroup and minimal normal subgroups are sent into minimal normal subgroups via isomorphisms, we have that

$$\alpha(lM) = lM \iff \alpha(l)\alpha(M) = lM \iff \alpha(l)M = lM.$$

Definition 4.11. We will denote by Γ the set of all automorphisms of L that act trivially on L/M.

Let us remember Definition 1.27, which says that $\phi_L(m)$ is the number of m tuples $(x_1, \dots, x_m)$ of elements of L that generate L.

Theorem 4.12. *Let F be a free group of rank $m \geq d(L)$. Given a surjective homomorphism $\beta\colon F \to L/M$, the cardinality of the set $\mathscr{R}_\beta$ is $\phi_L(m)/|\Gamma|\phi_{L/M}(m)$.*

Proof. Let $x_1, \dots, x_n$ be the canonical basis of F. A surjective homomorphism $\beta : F \longrightarrow L/M$ is uniquely determined by $\beta(x_1) = l_1 M, \dots, \beta(x_m) = x_m M$, where $L = \langle l_1, \dots, l_m, M\rangle$. Now let $\gamma : F \longrightarrow L$ be a surjective homomorphism which composed with the the projection $\pi_L\colon L \longrightarrow L/M$ yields β; we must have $\gamma(x_1) = l_1 z_1, \dots, \gamma(x_m) = l_m z_m$ with $z_1, \dots, z_m \in M$ and $L = \langle l_1 z_1, \dots, l_m z_m\rangle$.

We claim that the number of possible choices for $(z_1, \dots, z_m)$ is $\phi_L(m)/\phi_{L/M}(m)$. To prove so let R be a left transversal of M in L. Also for any $lM \in L/M$ we will denote by r_{lM} the unique element $r \in R$ such that $rM = lM$. For any m-tuple $(t_1 M, \dots, t_m M)$ that generates L/M let us define $Z(t_1 M, \dots, t_m M)$ as

$$\left\{(z_1, \dots, z_m) \in M^m | L = \langle r_{t_1 M} z_1, \dots, r_{t_m M} z_m\rangle\right\}.$$

Let us also denote by T the set

$$\left\{(t_1 M, \dots t_m M) \in (L/M)^m | \langle t_1 M, \dots t_m M\rangle = L/M\right\}.$$

We can now define the function

$$b\colon \bigcup_{(t_1 M, \dots t_m M) \in T} \{(t_1 M, \dots t_m M)\} \times Z(t_1 M, \dots t_m M) \to \left\{(g_1, \dots g_m) \in L^m | \langle g_1, \dots g_m\rangle = L\right\}$$

$$(t_1 M, \dots, t_m M, z_1, \dots, z_m) \mapsto (r_{t_1 M} z_1, \dots, r_{t_m M} z_m).$$

Obviously b is well defined. Also for any $g \in L$, $g \in gM = r_{gM} M$ and thus we have that $g = r_{gM} h$ for some $h \in M$. So for any $(g_1, \dots g_m) \in L^m$ with the property that $\langle g_1, \dots g_m\rangle = L$ we can find $(h_1, \dots, h_m) \in M^m$ such that $(g_1, \dots g_m) = (r_{g_1 M} h_1, \dots, r_{g_m M} h_m)$. Thus $b(r_{g_1 M}, \dots r_{g_m M}, h_1 \dots h_m) = (g_1, \dots g_m)$ and the surjectivity of b is proven. For the injectivity of b it suffices to prove that given $r_1, r_2 \in R$ and $z_1, z_2 \in M$ if $r_1 z_1 = r_2 z_2$ then $r_1 M = r_2 M$ and $z_1 = z_2$, since then it easily follows that for any d_1, d_2 in the domain of b, $b(d_1) = b(d_2) \implies d_1 = d_2$. Let $r_1, r_2 \in R$ and $z_1, z_2 \in M$ if $r_1 z_1 = r_2 z_2$ then $r_2^{-1} r_1 = z_2 z_1 \in M$. That is $r_2 M = r_1 M$ and since r_1, r_2 belong to the left transversal R, $r_1 = r_2$. Thus $z_1 = r_1^{-1} r_2 z_2 = r_2^{-1} r_2 z_2 = z_2$ and injectivity is proven. We just proved that b is a bijection.

By Theorem 1.29, $|Z(t_1M,\dots,t_mM)|$ is independent of the choice of $r_{t_1M},\dots r_{t_mM}$ and thus the sets Z all have the same cardinality.Thus

$$\begin{aligned} &\phi_{L/M}(m)|Z(l_1M,\dots,l_mM)| = |T||Z(l_1M,\dots,l_mM)| \\ =&|\bigcup_{(t_1M,\dots t_mM)\in T}\{(t_1M,\dots t_mM)\}\times Z(t_1M,\dots t_mM)| \\ =&|\left\{(g_1,\dots g_m)\in L^m|\langle g_1,\dots g_m\rangle = L\right\}| = \phi_L(m) \end{aligned}$$

and the proof of the claim that the number of possible choices for $(z_1,\dots,z_m)$ is $\phi_L(m)/\phi_{L/M}(m)$ is complete.

Now let γ_1,γ_2 be two of these homomorphisms; we claim that $\ker\gamma_1 = \ker\gamma_2 = N$ if and only if there exists an automorphism α of L which acts trivially on L/M such that γ_2 is equal to γ_1 composed with α.

If $\ker\gamma_1 = \ker\gamma_2 = N$, then by the First isomorphism Theorem there exist isomorphisms $\bar{\gamma_1}\colon F/N\to L$ and $\bar{\gamma_2}\colon F/N\to L$ such that for all $x\in F$, $\bar{\gamma_1}(xN) = \gamma_1(x)$ and $\bar{\gamma_2}(xN) = \gamma_2(x)$. Now let us consider the isomorphism $\alpha = \bar{\gamma_2}\circ\bar{\gamma_1}^{-1}\colon L\to L$. For all $x\in F$, we have that

$$\begin{aligned} (\alpha\circ\gamma_1)(x) &= \bar{\gamma_2}(\bar{\gamma_1}^{-1}\circ\gamma_1(x)) \\ &= \bar{\gamma_2}(xN) \\ &= \gamma_2(x) \end{aligned}$$

where the second equality follows from applying $\bar{\gamma_1}^{-1}$ to $\bar{\gamma_1}(xN) = \gamma_1(x)$. Furthermore for all $x\in F$, $\pi_L\circ\bar{\gamma_1}(xN) = \pi_L\circ\gamma_1(x) = \beta(x) = \pi_L\circ\gamma_2(x) = \pi_L\circ\bar{\gamma_2}(xN)$. Thus it follows that for all $l\in L$, $(\pi_L\circ\alpha)(l) = \pi_L\circ\bar{\gamma_2}(\bar{\gamma_1}^{-1}(l)) = \pi_L\circ\bar{\gamma_1}(\bar{\gamma}_1^{-1}(l)) = \pi_L(l) = lM$ and hence $\alpha(l)M = (\pi_L\circ\alpha)(l) = lM$.

On the other hand if there exists an automorphism α of L which acts trivially on L/M such that γ_2 is equal to γ_1 composed with α, then $\ker\gamma_2 = \ker\alpha\circ\gamma_1 = \ker\gamma_1$. Furthermore for all $x\in F$, $\pi_L\circ\gamma_2(x) = \pi_L\circ\alpha\circ\gamma_1(x) = \alpha(\gamma_1(x))M = \gamma_1(x)M = \pi_L\circ\gamma_1(x) = \beta(x)$

We conclude that the cardinality of $\mathscr{R}_\beta$ is $\phi_L(m)/|\Gamma|\phi_{L/M}(m)$. □

Theorem 4.13. *Let F be a free group of rank $m\geq d(L)$ and $\beta\colon F\to L/M$ a surjective homomorphism. The group $F/(\bigcap_{N\in\mathscr{R}_\beta}N)$ is isomorphic to L_q for some positive integer q. Furthermore q is* *the biggest integer for which there exists a surjective homomorphism* $\Psi\colon F \to L_q$ *such that*

$$\pi_{L_q} \circ \Psi = \beta.$$

Proof. By Theorem 4.12, $\mathscr{R}_\beta$ is finite so we can assume that $\mathscr{R}_\beta = \{N_1, \ldots, N_r\}$.

Now given $N \in \mathscr{R}_\beta$, let $\gamma_N\colon F \to L$ be such that $\ker \gamma_N = N$ and $\pi_L \circ \gamma_N = \beta$. Let us also consider the subsequence of $N_1, \ldots, N_r$:

$$N_{i_1} = N_1, \ldots, N_{i_q}$$

where $\bigcap_{n=1}^{j} N_{i_n} \nsubseteq N_{i_{j+1}}$ for $1 \leq j \leq q-1$. Assuming we have N_{i_j} we choose $N_{i_{j+1}}$ in the following way: i_{j+1} is the smallest number such that $i_{j+1} > i_j$ and $\bigcap_{n=1}^{j} N_{i_n} \nsubseteq N_{i_{j+1}}$; if no such number exists the subsequence is completed.Let us note that $\bigcap_{n=1}^{q} N_{i_n} = \bigcap_{N \in \mathscr{R}_\beta} N$. Through reindexing we can assume that the sequence just constructed is simply $N_1, \ldots, N_q$.

We will prove by induction that for $1 \leq s \leq q$ the function

$$\begin{aligned} \Psi_s\colon F &\to L_s \\ x &\mapsto (\gamma_{N_1}(x), \ldots, \gamma_{N_s}(x)) \end{aligned}$$

is a surjective homomorphism with kernel $\bigcap_{i=1}^{s} N_i$. After this is proved we can easily conclude that $F/(\bigcap_{N \in \mathscr{R}_\beta} N) \cong L_q$ due to $\bigcap_{N \in \mathscr{R}_\beta} N = \bigcap_{i=1}^{q} N_i$ and the First isomorphism Theorem.

For $s = 1$, $\Psi_s = \gamma_{N_1}$ and thus the hypothesis obviously holds. Let us assume now that it holds for $1 \leq s < q$.

That Ψ_{s+1} maps to L_{s+1} is not obvious. For any $1 \leq i, j \leq q$ we have $\gamma_{N_i}(x)M = \beta(x) = \gamma_{N_j}(x)M$ by the definition of the γ functions. Thus $\gamma_{N_1}(x)M = \ldots = \gamma_{N_{s+1}}(x)M$ and Ψ_{s+1} maps to L_{s+1}.

This function is obviously well defined. We also easily obtain that $\ker \Psi_{s+1} = \bigcap_{i=1}^{s+1} N_i = \bigcap_{N \in \mathscr{R}_\beta} N$ since for any $1 \leq i \leq q$, $\ker \gamma_{N_i} = N_i$.

To check surjectivity let us first notice that,

$$M \subseteq \gamma_{N_{s+1}}(\bigcap_{i=1}^{s} N_i) \text{ and } \gamma_{N_j}(\bigcap_{i=1}^{s} N_i) = 1 \text{ for } 1 \leq j \leq s.$$

This holds because $\bigcap_{i=1}^{s} N_i$ is a normal subgroup in F not contained in $\ker \gamma_{N_{s+1}} = N_{s+1}$ and as $\gamma_{N_{s+1}}$ is surjective the image of $\bigcap_{i=1}^{s} N_i$ is a non-trivial normal group of L. Such a normal subgroup must contain a minimal normal subgroup and M is the unique such subgroup, thus it contains it. Furthermore for $1 \leq j \leq s$, $\gamma_{N_j}(\bigcap_{i=1}^s N_i) = 1$ since $\bigcap_{i=1}^s N_i \subseteq N_j = \ker \gamma_{N_j}$.

Let us also notice that for all $x \in F$, $\Psi_{s+1}(x) = (\Psi_s(x), \gamma_{N_{s+1}}(x))$.

Thus given $(lm_1, \dots, lm_{s+1}) \in L_{s+1}$ by the induction hypothesis there is some $x \in F$ such that $\Psi_s(x) = (lm_1, \dots, lm_s)$. Since $lM = \gamma_{N_1}(x)M = \gamma_{s+1}(x)M$, $\gamma_{s+1}(x) = lm_x$ for some $m_x \in M$. Consider now the element $xy \in F$ where $y \in \bigcap_{i=1}^s N_i$ and $\gamma_{s+1}(y) = m_x^{-1}m_{s+1}$ (such y exists due to $M \subseteq \gamma_{N_{s+1}}(\bigcap_{i=1}^s N_i)$). Then

$$\begin{aligned}
\Psi_{s+1}(xy) &= (\Psi_s(xy), \gamma_{N_{s+1}}(xy)) \\
&= (\gamma_{N_1}(xy), \dots, \gamma_{N_{s+1}}(xy)) \\
&= (\gamma_{N_1}(x)\gamma_{N_1}(y), \dots, \gamma_{N_{s+1}}(x)\gamma_{N_{s+1}}(y)) \\
&= (\gamma_{N_1}(x), \dots, \gamma_{N_s}(x), \gamma_{N_{s+1}}(x)\gamma_{N_{s+1}}(y)) \\
&= (lm_1, \dots, lm_s, lm_x m_x^{-1} m_{s+1}) = (lm_1, \dots, lm_{s+1})
\end{aligned}$$

where the fourth equality follows from $y \in \bigcap_{i=1}^s N_i = \bigcap_{i=1}^s \ker \gamma_{N_i}$. Surjectivity and the first part of the theorem is thus proved. It is now only necessary to prove that there is no quotient of F isomorphic to some L_k for some $k > q$.

Let us suppose to obtain a contradiction that for some $k > q$ there is a surjective homomorphism Ψ between F and L_k such that $\pi_{L_k} \circ \Psi = \beta$. Let us consider the natural projection $\pi_L \colon L \to L/M$.

For $1 \leq i \leq k$ let us also consider the surjective homomorphisms $\gamma_i = \pi_i \circ \Psi \colon F \to L$. The following diagrams help to keep track of the homomorphisms

$$\begin{tikzcd}
F \arrow[r, "\Psi"] \arrow[dr, "\gamma_i"'] & L_k \arrow[r, "\pi_{L_k}"] \arrow[d, "\pi_i"] & L/M \\
& L \arrow[ur, "\pi_L"'] &
\end{tikzcd}
\qquad
\begin{tikzcd}
F \arrow[r, "\alpha"] \arrow[d, "\gamma_i"'] & L/M \\
L \arrow[ur, "\pi_L"] &
\end{tikzcd}.$$

Now obviously $\Psi(x) = (\gamma_1(x), \dots, \gamma_k(x))$ and thus

$$K = \ker \Psi = \bigcap_{i=1}^{q} \ker \gamma_i.$$

Furthermore for all $1 \leq i \leq k$ and all $x \in F$,

$$\begin{aligned}
\beta(x) &= \pi_{L_k} \circ \Psi(x) \\
&= \pi_i(\Psi(x))M \\
&= \pi_L \circ \gamma_i(x)
\end{aligned}$$

and thus $\ker\gamma_i \in \mathscr{R}_\beta$. We obtain that $\bigcap_{N\in\mathscr{R}_\beta} N \subseteq \bigcap_{i=1}^{q} \ker\gamma_i = K$ and consequently $|F/(\bigcap_{N\in\mathscr{R}_\beta} N)| \geq |F/K|$. This is a contradiction since by the First Isomorphism Theorem $|F/(\bigcap_{N\in\mathscr{R}_\beta} N)| = |L_q| < |L_k| = |F/K|$.

□

Theorem 4.14. *Let $m \geq d(L)$ and q be the number of (L/M)-endomorphisms of M when M is abelian. Then*

$$f(m) = 1 + \begin{cases} \phi_L(m)/(|\Gamma|\phi_{L/M}(m)) & \text{if } M \text{ is not abelian,} \\ log_q(1+(q-1)\phi_L(m)/|\Gamma|\phi_{L/M}(m)) & \text{if } M \text{ is abelian.} \end{cases}$$

Proof. Let F denote a free group with rank m. Since an homomorphism from F is totally determined by the images of its canonical base and L/M is a finite group, there are a finite number of surjective homomorphisms from F to L/M. By Theorem 4.13 each such surjective homomorphism α has an associated biggest integer s and surjective homomorphism Ψ such that $\pi_{L_s} \circ \Psi = \alpha$ and thus we can consider the finite set of all such integers s. We can now set k as the maximum of such set, $\beta\colon F \to L/M$ and $\Psi_k\colon F \to L_k$ the associated homomorphisms and $R = \ker\Psi_k = (\bigcap_{N\in\mathscr{R}_\beta} N)$.

Let us note that if for some $K \triangleleft F$, there exists an isomorphism ϕ between F/K and L_i for some i then ϕ induces a surjective homomorphism from F to L/M, namely $\pi_{L_i} \circ \phi \circ \pi$ where $\pi\colon F \to F/K$ is the natural projection. By the remarks above and our choice of k, F/R is the largest quotient of F isomorphic to L_i for some i; since F is a free group of rank m this means that

$$f(m) = 1 + k.$$

Now by the Correspondence Theorem the function $v\colon N \mapsto N/R$ is a bijection from the family of all those subgroups N of F which contain R to the family of all the subgroups of F/R. Furthermore if we denote by ϕ the isomorphism $F/R = F/\ker\Psi_k \cong L_k$ resulting from the First isomorphism Theorem, we can define the induced bijection $\bar{\phi}\colon N \mapsto \phi(N)$ that maps subgroups of F/R to subgroups of L_k. Now consider the bijection $\sigma = \bar{\phi} \circ v$ from the family of all those subgroups N of F which contain R to all subgroups of L_k.

We claim that the restriction of σ to $\mathscr{R}_\beta$ is a bijection between $\mathscr{R}_\beta$ and $\mathscr{S}_{\bar{\beta}\circ\phi^{-1}}$. We need only to prove that if $N \in \mathscr{R}_\beta$ then $\sigma(N) \in \mathscr{S}_{\bar{\beta}\circ\phi^{-1}}$ and if $K \in \mathscr{S}_{\bar{\beta}\circ\phi^{-1}}$ then $\sigma^{-1}(K) \in \mathscr{R}_\beta$. To do so let us first denote by $\pi\colon F \to F/R$ the natural projection and notice that

$$\begin{aligned}\bar{\beta}\colon F/R &\to L/M\\ xN &\mapsto \beta(x)\end{aligned}$$

is a well defined (since $R \subseteq \ker\beta$) surjective homomorphism that satisfies $\bar{\beta}\circ\pi = \beta$. Given a surjective homomorphism such that $\ker\gamma_N = N$ and $\pi_L \circ \gamma_N = \beta$, let us also consider

$$\begin{aligned}\gamma_{N/R}\colon F/R &\to L\\ xN &\mapsto \gamma_N(x);\end{aligned}$$

this is also a well defined (since $R \subseteq \ker\gamma_N$) homomorphism with the property $\gamma_{N/R} \circ \pi = \gamma_N$. Since π is surjective we also obtain

$$\pi_L \circ \gamma_N = \beta \implies \pi_L \circ \gamma_{N/R} \circ \pi = \bar{\beta} \circ \pi \implies \pi_L \circ \gamma_{N/R} = \bar{\beta}.$$

The following diagram helps visualize the homomorphisms:

$$\begin{tikzcd}
 & F \arrow[d, "\pi"] \arrow[dr, "\beta"] & \\
L_k \arrow[dr, "\gamma_K"'] & F/R \arrow[l, "\phi"'] \arrow[r, "\bar{\beta}"] \arrow[d, "\gamma_{N/R}"] & L/M \\
 & L \arrow[ur, "\pi_L"'] &
\end{tikzcd}$$

If $N \in \mathscr{R}_\beta$ then there exists a surjective homomorphism $\gamma_N\colon F \to L$ such that $\ker\gamma_N = N$ and $\pi_L \circ \gamma_N = \beta$. Now $\pi_L \circ \gamma_{N/R} \circ \phi^{-1} = \bar{\beta} \circ \phi^{-1}$ and thus $\ker\gamma_{N/R} \circ \phi^{-1} \in \mathscr{S}_{\bar{\beta}\circ\phi^{-1}}$. Since ϕ is an isomorphism $\ker\gamma_{N/R} \circ \phi^{-1} = \phi(\ker\gamma_{N/R}) = \phi(N/R)$. We thus conclude that

$$\sigma(N) = \phi(N/R) = \ker\gamma_{N/R} \circ \phi^{-1} \in \mathscr{S}_{\bar{\beta}\circ\phi^{-1}}.$$

If $K \in \mathscr{S}_{\bar{\beta}\circ\phi^{-1}}$ then there exists a surjective homomorphism $\gamma_K\colon L_k \to L$ such that $\ker\gamma_K = K$ and $\pi_L \circ \gamma_K = \bar{\beta} \circ \phi^{-1}$. Now $\pi_L \circ \gamma_K \circ \phi \circ \pi = \bar{\beta} \circ \phi^{-1} \circ \phi \circ \pi = \bar{\beta} \circ \pi = \beta$ and thus $\ker\gamma_K \circ \phi \circ \pi \in \mathscr{R}_\beta$. Also $\ker\gamma_K \circ \phi \circ \pi = \pi^{-1}(\phi^{-1}(\ker\gamma_K)) = \pi^{-1}(\phi^{-1}(K))$. We thus conclude that $\sigma^{-1}(K) = \pi^{-1}(\phi^{-1}(K)) = \ker\gamma_K \circ \phi \circ \pi \in \mathscr{R}_\beta$. It is thus proved that there is a bijection between $\mathscr{R}_\beta$ and $\mathscr{S}_{\bar{\beta}\circ\phi^{-1}}$.

Now by Theorems 4.8 and 4.12 we obtain:

$$\frac{\phi_L(m)}{|\Gamma|\phi_{L/M}(m)} = |\mathscr{R}_\beta| = |\mathscr{S}_{\bar{\beta}\circ\phi^{-1}}| = \begin{cases} k & \text{if } M \text{ is not abelian,} \\ (q^k-1)/(q-1) & \text{if } M \text{ is abelian.} \end{cases}$$

Since $k = f(m) - 1$, the proof is complete. $\square$

Bibliography

[1] F. Dalla Volta and A. Lucchini, "Finite groups that need more generators than any proper quotient," *J. Austral. Math. Soc. Ser. A*, vol. 64, no. 1, pp. 82–91, 1998. [Cited on pages v, 2, 25, 35, 39, and 40.]

[2] J. J. Rotman, *An introduction to the theory of groups*, 4th ed., ser. Graduate Texts in Mathematics. Springer-Verlag, New York, 1995, vol. 148. [Online]. Available: https://doi.org/10.1007/978-1-4612-4176-8 [Cited on pages 1, 3, 9, 10, 12, and 13.]

[3] M. Aschbacher and R. Guralnick, "Some applications of the first cohomology group," *Journal of Algebra*, vol. 90, no. 2, pp. 446–460, 1984. [Online]. Available: https://www.sciencedirect.com/science/article/pii/0021869384901832 [Cited on page 1.]

[4] P. J. Cassidy, "Products of commutators are not always commutators: an example," *Amer. Math. Monthly*, vol. 86, no. 9, p. 772, 1979. [Online]. Available: https://doi.org/10.2307/2322031 [Cited on page 7.]

[5] D. J. S. Robinson, *A course in the theory of groups*, 2nd ed., ser. Graduate Texts in Mathematics. Springer-Verlag, New York, 1996, vol. 80. [Online]. Available: https://doi.org/10.1007/978-1-4419-8594-1 [Cited on page 7.]

[6] W. Gaschütz, "Zu einem von B. H. und H. Neumann gestellten Problem," *Math. Nachr.*, vol. 14, pp. 249–252 (1956), 1955. [Online]. Available: https://doi.org/10.1002/mana.19550140406 [Cited on page 11.]

[7] M. D. Fried and M. Jarden, *Field arithmetic*, 2nd ed., ser. Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics]. Springer-Verlag, Berlin, 2005, vol. 11. [Cited on page 11.]

[8] A. Ballester-Bolinches and L. M. Ezquerro, *Classes of finite groups*, ser. Mathematics and Its Applications (Springer). Springer, Dordrecht, 2006, vol. 584. [Cited on page 14.]

[9] J. Wiegold, "Growth sequences of finite groups," *J. Austral. Math. Soc.*, vol. 17, pp. 133–141, 1974. [Cited on page 21.]

[10] ——, "Growth sequences of finite groups. II," *J. Austral. Math. Soc.*, vol. 20, no. part, pp. 225–229, 1975.

[11] ——, "Growth sequences of finite groups. III," *J. Austral. Math. Soc. Ser. A*, vol. 25, no. 2, pp. 142–144, 1978.

[12] ——, "Growth sequences of finite groups. IV," *J. Austral. Math. Soc. Ser. A*, vol. 29, no. 1, pp. 14–16, 1980. [Cited on page 21.]