

On the minimal number of generators of a finite group

Diogo Santos

December 2, 2024

- Finding the minimal number of generators of a finite group H

- Finding the minimal number of generators of a finite group H

Can be reduced to:

- Finding the minimal number of generators of a finite group H such that $d(H/N) \leq m$ for every non-trivial normal subgroup N , but $d(H) > m$

The case $m = 1$

Theorem

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 .

The case $m = 1$

Theorem

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.

- $H = P_1 \times \dots \times P_n$ where P_i is a Sylow p_i -subgroup for $1 \leq i \leq n$ and p_1, \dots, p_n are distinct primes.

The case $m = 1$

Theorem

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.

- $H = P_1 \times \dots \times P_n$ where P_i is a Sylow p_i -subgroup for $1 \leq i \leq n$ and p_1, \dots, p_n are distinct primes.
- If P_1, \dots, P_n are cyclic, we obtain $H \cong \mathbb{Z}_{p_1 \dots p_n}$ which contradicts $d(H) > 1$. Without loss of generality we can thus assume that P_1 is not cyclic.

The case $m = 1$

Theorem

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.

- $H = P_1 \times \dots \times P_n$ where P_i is a Sylow p_i -subgroup for $1 \leq i \leq n$ and p_1, \dots, p_n are distinct primes.
- If P_1, \dots, P_n are cyclic, we obtain $H \cong \mathbb{Z}_{p_1 \dots p_n}$ which contradicts $d(H) > 1$. Without loss of generality we can thus assume that P_1 is not cyclic.
- $n \geq 2 \implies P_1 \cong H/(1 \times P_2 \dots \times P_n)$ and thus $d(P_1) = d(H/(1 \times P_2 \dots \times P_n)) = 1$, contradiction.

The case $m = 1$

Theorem

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.

- $H = P_1 \times \dots \times P_n$ where P_i is a Sylow p_i -subgroup for $1 \leq i \leq n$ and p_1, \dots, p_n are distinct primes.
- If P_1, \dots, P_n are cyclic, we obtain $H \cong \mathbb{Z}_{p_1 \dots p_n}$ which contradicts $d(H) > 1$. Without loss of generality we can thus assume that P_1 is not cyclic.
- $n \geq 2 \implies P_1 \cong H/(1 \times P_2 \dots \times P_n)$ and thus $d(P_1) = d(H/(1 \times P_2 \dots \times P_n)) = 1$, contradiction.
- Since $d(H) = d(H/\Phi(H))$, $\Phi(H) = 1$.

The case $m = 1$

Proof.

- $H \cong H/\Phi(H)$ is a \mathbb{Z}_{p_1} -vector space and thus $H = (\mathbb{Z}_{p_1})^q$



The case $m = 1$

Proof.

- $H \cong H/\Phi(H)$ is a \mathbb{Z}_{p_1} -vector space and thus $H = (\mathbb{Z}_{p_1})^q$
- $q = 2$ since

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



The groups L_k

Throughout 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 .

The groups L_k

Throughout 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 .

Definition

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

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

The group L_k can be described as $\text{diag}(L^k)M^k$.

Properties of L_k

Properties of L_k

- $\text{soc}(L_k) = M^k$

Properties of L_k

- $\text{soc}(L_k) = M^k$
- $L_k/M^k \cong L/M$

Properties of L_k

- $\text{soc}(L_k) = M^k$
- $L_k/M^k \cong L/M$
- If M is abelian and complemented by C in L , then M^k is complemented by $\text{diag}(C^k)$

Properties of L_k

- $\text{soc}(L_k) = M^k$
- $L_k/M^k \cong L/M$
- If M is abelian and complemented by C in L , then M^k is complemented by $\text{diag}(C^k)$
- The quotient of L_{k+1} by any of its minimal normal subgroups is isomorphic to L_k

Properties of L_k

- $\text{soc}(L_k) = M^k$
- $L_k/M^k \cong L/M$
- If M is abelian and complemented by C in L , then M^k is complemented by $\text{diag}(C^k)$
- The quotient of L_{k+1} by any of its minimal normal subgroups is isomorphic to L_k
- The sequence $d(L_k)_{k \in \mathbb{N}}$ is unlimited and non-decreasing.

Properties of L_k

- $\text{soc}(L_k) = M^k$
- $L_k/M^k \cong L/M$
- If M is abelian and complemented by C in L , then M^k is complemented by $\text{diag}(C^k)$
- The quotient of L_{k+1} by any of its minimal normal subgroups is isomorphic to L_k
- The sequence $d(L_k)_{k \in \mathbb{N}}$ is unlimited and non-decreasing.
- For all $k \in \mathbb{N}$, $d(L_{k+1}) \leq d(L_k) + 1$.

The function f

Definition

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

Definition

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 $f(m)$.

- 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 $d(L_{k+1}) > m$.*

The function f

Definition

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 $f(m)$.

- 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 $d(L_{k+1}) > m$.*
- It follows from the last 2 properties of the groups L_k that this function is non-decreasing and unbounded.

Theorem

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 $H \cong L_{f(L,m)}$.

General Case Proof

The proof is divided in 2 cases:

General Case Proof

The proof is divided in 2 cases:

- H has a unique minimal normal subgroup

General Case Proof

The proof is divided in 2 cases:

- H has a unique minimal normal subgroup
- H has more than one minimal normal subgroup

General Case Proof

The proof is divided in 2 cases:

- H has a unique minimal normal subgroup
- H has more than one minimal normal subgroup
 - Abelian minimal normal subgroups

General Case Proof

The proof is divided in 2 cases:

- H has a unique minimal normal subgroup
- H has more than one minimal normal subgroup
 - Abelian minimal normal subgroups
 - Non-abelian minimal normal subgroups

Proof: H has a unique minimal normal subgroup

Let M denote the unique minimal normal subgroup of H .

Proof: H has a unique minimal normal subgroup

Let M denote the unique minimal normal subgroup of H .

- If M is not abelian there is nothing to prove.

Proof: H has a unique minimal normal subgroup

Let M denote the unique minimal normal subgroup of H .

- If M is not abelian there is nothing to prove.
- If M is abelian then we need to prove that it is complemented. Since $\Phi(H) = 1$, then there exists a maximal subgroup K that does not contain M . We have that $K \cap M \triangleleft K$ and $K \cap M \triangleleft M$ (since M is abelian). Thus $K \cap M \triangleleft KM = H$ and since $K \cap M \subset M$, $K \cap M = 1$.

Sketch of Proof: H has more than one minimal normal subgroup

- Let N_1 be a minimal normal subgroup of H . For any other minimal normal subgroups N_r of H ($N_1 \neq N_r$), there exists a subgroup K_r of H that complements both N_1 and N_r in H .

Sketch of Proof: H has more than one minimal normal subgroup

- Let N_1 be a minimal normal subgroup of H . For any other minimal normal subgroups N_r of H ($N_1 \neq N_r$), there exists a subgroup K_r of H that complements both N_1 and N_r in H .
- The projections $\pi_r : K_r \cap (N_1 \times N_r) \rightarrow N_1$ and $\rho_r : K_r \cap (N_1 \times N_r) \rightarrow N_r$ are isomorphisms. Thus there is an isomorphism $\phi_r : N_1 \rightarrow N_r$, specifically $\phi_r = \rho_r \pi_r^{-1}$.

Sketch of Proof: H has more than one minimal normal subgroup

- Let N_1 be a minimal normal subgroup of H . For any other minimal normal subgroups N_r of H ($N_1 \neq N_r$), there exists a subgroup K_r of H that complements both N_1 and N_r in H .
- The projections $\pi_r : K_r \cap (N_1 \times N_r) \rightarrow N_1$ and $\rho_r : K_r \cap (N_1 \times N_r) \rightarrow N_r$ are isomorphisms. Thus there is an isomorphism $\phi_r : N_1 \rightarrow N_r$, specifically $\phi_r = \rho_r \pi_r^{-1}$.

From this follows that either all the minimal normal subgroups of H are abelian or all of them are non-abelian.

Sketch of Proof: H has abelian normal subgroups

- We have that $\text{soc}(H)$ is complemented in H , say by K .

Sketch of Proof: H has abelian normal subgroups

- We have that $\text{soc}(H)$ is complemented in H , say by K .
- Let $L = N_1 K$. Each minimal normal subgroup N_r of H is complemented in $\text{soc}(H)$, say by C_r and there exists a surjective homomorphism $\Psi_r: H \rightarrow L$ with $\ker \Psi_r = C_r$.

Sketch of Proof: H has abelian normal subgroups

- We have that $\text{soc}(H)$ is complemented in H , say by K .
- Let $L = N_1 K$. Each minimal normal subgroup N_r of H is complemented in $\text{soc}(H)$, say by C_r and there exists a surjective homomorphism $\Psi_r: H \rightarrow L$ with $\ker \Psi_r = C_r$.
- There exists a positive integer q such that the function

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

is an isomorphism.

Sketch of Proof: H has abelian normal subgroups

- We have that $\text{soc}(H)$ is complemented in H , say by K .
- Let $L = N_1 K$. Each minimal normal subgroup N_r of H is complemented in $\text{soc}(H)$, say by C_r and there exists a surjective homomorphism $\Psi_r: H \rightarrow L$ with $\ker \Psi_r = C_r$.
- There exists a positive integer q such that the function

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

is an isomorphism.

- The group L has a unique minimal normal subgroup, namely N_1 , and it is complemented by K .

Sketch of Proof: H has non-abelian normal subgroups

- Let $\alpha_1: H \rightarrow \text{Aut } N_1$ that sends each $h \in H$ to

$$\begin{aligned}\alpha_1(h): N_1 &\rightarrow N_1 \\ x &\mapsto h x h^{-1}.\end{aligned}$$

Let L denote the image of α_1 .

Sketch of Proof: H has non-abelian normal subgroups

- Let $\alpha_1: H \rightarrow \text{Aut } N_1$ that sends each $h \in H$ to

$$\begin{aligned}\alpha_1(h): N_1 &\rightarrow N_1 \\ x &\mapsto h x h^{-1}.\end{aligned}$$

Let L denote the image of α_1 .

- The group L has a unique minimal normal subgroup.

Sketch of Proof: H has non-abelian normal subgroups

- Let $\alpha_1: H \rightarrow \text{Aut } N_1$ that sends each $h \in H$ to

$$\begin{aligned}\alpha_1(h): N_1 &\rightarrow N_1 \\ x &\mapsto h x h^{-1}.\end{aligned}$$

Let L denote the image of α_1 .

- The group L has a unique minimal normal subgroup.
- For $r > 1$, we define $\alpha_r: H \rightarrow \text{Aut } N_1$ as the homomorphism that sends $h \in H$ to

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

Sketch of Proof: H has non-abelian normal subgroups

- Let $\alpha_1: H \rightarrow \text{Aut } N_1$ that sends each $h \in H$ to

$$\begin{aligned}\alpha_1(h): N_1 &\rightarrow N_1 \\ x &\mapsto h x h^{-1}.\end{aligned}$$

Let L denote the image of α_1 .

- The group L has a unique minimal normal subgroup.
- For $r > 1$, we define $\alpha_r: H \rightarrow \text{Aut } N_1$ as the homomorphism that sends $h \in H$ to

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

- Taking q as the number of minimal normal subgroups of H , the function

$$\begin{aligned}\Psi: H &\rightarrow L_q \\ h &\mapsto (\alpha_1(h), \dots, \alpha_q(h))\end{aligned}$$

is an isomorphism.

Sketch of Proof: $q = f(L, m)$

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 $H/N_r \cong L_{q-1}$. 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 . \square

The function f

Definition

Given a surjective homomorphism $\beta: L_k \rightarrow L/M$, we define the set \mathcal{S}_β 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 $\pi_L: L \rightarrow L/M$ yield β .

The function f

Theorem

Let us assume that M is abelian. Given a surjective homomorphism $\beta: L_k \rightarrow L/M$, the cardinality of the set \mathcal{S}_β 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 .

Theorem

Let us assume that M is not abelian. Given a surjective homomorphism $\beta: L_k \rightarrow L/M$, the cardinality of the set \mathcal{S}_β is k .

The function f

Definition

Let F be a free group of rank m . Given a surjective homomorphism $\beta: F \rightarrow L/M$, we define the set \mathcal{R}_β 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 $\pi_L: L \rightarrow L/M$ yield β .

The function f

Definition

Let F be a free group of rank m . Given a surjective homomorphism $\beta: F \rightarrow L/M$, we define the set \mathcal{R}_β 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 $\pi_L: L \rightarrow L/M$ yield β .

Theorem

Let F be a free group of rank $m \geq d(L)$. Given a surjective homomorphism $\beta: F \rightarrow L/M$, the cardinality of the set \mathcal{R}_β is $\phi_L(m)/|\Gamma|\phi_{L/M}(m)$, where Γ denotes the set of all automorphisms of L that act trivially on L/M .

The function f

Theorem

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

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

The function f

Theorem

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

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

Sketch of proof

- Let F denote a free group of rank m . There exists a surjective homomorphism $\beta: F \rightarrow L/M$ such that k is the biggest integer for which there exists a surjective homomorphism $\psi_k: F \rightarrow L_k$.

Sketch of proof

- Let F denote a free group of rank m . There exists a surjective homomorphism $\beta: F \rightarrow L/M$ such that k is the biggest integer for which there exists a surjective homomorphism $\psi_k: F \rightarrow L_k$.
- $F/\ker \psi_k$ 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

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

Sketch of proof

- Let F denote a free group of rank m . There exists a surjective homomorphism $\beta: F \rightarrow L/M$ such that k is the biggest integer for which there exists a surjective homomorphism $\Psi_k: F \rightarrow L_k$.
- $F/\ker \Psi_k$ 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

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

- $N \mapsto N/R \mapsto \phi(N/R)$ is a bijection between \mathcal{R}_β and $\mathcal{S}_{\tilde{\beta} \circ \phi^{-1}}$, where $\phi: F/\ker \Psi_k \rightarrow L_k$ is an isomorphism

- Applying the theorems before we obtain:

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