UNIVERSIDADE FEDERAL DO CEARÁ
CENTRO DE CIÊNCIAS
DEPARTAMENTO DE MATEMÁTICA
CURSO DE PÓS-GRADUAÇÃO EM MATEMÁTICA
MESTRADO EM MATEMÁTICA

GRUPOS NOS QUAIS O CONJUNTO DOS COMUTADORES POSSUI COBERTURA FINITA POR SUBGRUPOS CÍCLICOS

Ana Shirley Monteiro da Silva

Fortaleza
2010.1

ANA SHIRLEY MONTEIRO DA SILVA

GRUPOS NOS QUAIS O CONJUNTO DOS COMUTADORES POSSUI COBERTURA FINITA POR SUBGRUPOS CÍCLICOS

Dissertação submetida à Coordenação do Curso de Pós-Graduação em Matemática, da Universidade Federal do Ceará, para a obtenção do grau de Mestre em Matemática.

Orientador: Prof. Dr. José Robério Rogério.

Fortaleza
2010.1

Silva, Ana Shirley Monteiro da
S578g Grupos nos quais o conjunto dos comutadores possui cobertura finita por subgrupos cíclicos / Ana Shirley Monteiro da Silva - Fortaleza: 2010.
110f.

Orientador: Prof. Dr. José Robério Rogério
Área de Concentração : Álgebra
Dissertação (Mestrado) - Universidade Federal do Ceará, Departamento de Matemática, 2010.
1-Teoria dos Grupos
CDD 512.2

À minha vó Raimunda,
que do céu intercedeu por mim
pra que eu alcançasse essa vitória.

Agradecimentos

À Deus, minha força, meu refúgio, meu alento, minha segurança, meu alimento..., meu TUDO. Ao espírito santo que deu-me o dom da fé e capacidade de enxergar além do que os meus olhos podiam ver nos momentos em que tudo parecia desmoronar. À minha mãe do céu, Maria santíssima, que sempre esteve comigo, intercedendo por mim, segurando minha mão.

Ao meu pai, Antônio e minha mãe Euriza, por todos os sacrifícios que fizeram pra que eu pudesse estudar. Obrigada pela fé nos momentos difíceis, pelas palavras que me motivavam. Obrigada mãe por me ensinar os primeiros passos na matemática e o gosto pelo estudo; Às minhas irmãs, Sabrina e Priscila, que foram meu apoio em todas as horas. Obrigada por suportarem com paciência minhas limitações e pelas boas risadas quando estamos juntas.

Ao professor Robério, por sempre me fazer acreditar que eu era capaz. Pra mim, o senhor foi muito mais que um orientador, foi um segundo pai, um amigo, um cuidado de Deus comigo.Obrigada pela paciência, pela humildade, pelos conselhos, por tudo; Ao professor Orlando Juriaans, pelas valiosas sugestões; Aos professores Alexandre e Afonso, que desde a graduação, dedicaram parte do seu precioso tempo a solucionar os problemas matemáticos que eu lhes levava; Sem vocês nada disso seria possível.

Aos meus colegas de mestrado: Vania, Davi, Valéria, Tiagão, Priscila, Joserlan, Kiara, e todos os outros que tanto me ajudaram durante esse tempo. Obrigada pelos grupos de estudos e pelas brincadeiras que me faziam esquecer o cansaço. Agradeço em especial à Vania, Kiara e Davi, que estão comigo desde a graduação e com os quais aprendi muito mais que matemática. Obrigada por tudo o que vivemos juntos, pela amizade dentro e fora da universidade.

Aos meus amigos irmãos: Manu, Deigiane(pequena), Germano, Vanessinha, Francimar, Héricles e Paulo Victor. Obrigada pela amizade verdadeira, pelas *orações, pela compreensão, pela presença constante, pelo carinho; À comunidade católica Canção Nova, minha segunda família, que tanto me apoiou. Obrigada pelas orações, pelo direcionamento, pelo ânimo, pelas lições de fé.*

À Andréia, pela SEMPRE boa disposição e o sorriso nos lábios com que atende a todos os que vão à secretaria da PGMAT; Ao Erivan, à Fernanda, à Rocilda e ao Júnior da biblioteca da matemática, pela solicitude comigo e meus colegas desde a graduação.

Agradeço por fim, à CAPES pelo apoio financeiro.

"Uns põem sua força nos carros, outros, nos cavalos.
Nós, porém, a temos no nome do Senhor, nosso Deus.
Eles fraquejaram e foram vencidos;
mas nós, de pé, continuamos firmes."
Sl 19,8-9

Resumo

Dada uma palavra w e um grupo G, suponha que o conjunto G_w pode ser coberto por finitos subgrupos cíclicos. É verdade que $w(G)$ também pode ser coberto por finitos subgrupos cíclicos? Nesta dissertação mostraremos que a resposta é positiva para a palavra comutador.

Abstract

Given a word w and a group G, suppose that the set can be G_w covered by finite cyclic subgroups. It is true that $w(G)$ can also be covered by finite cyclic subgroups? This dissertation will show that the answer is positive for the word switch.

Sumário

Introdução 10

1 Preliminares 14
1.1 Classes Laterais 14
1.2 Subgrupos Clássicos 18
1.3 Séries Normais e Nilpotência 20
1.4 Séries Centrais 22
1.5 Representação de Permutações 27

2 O Teorema de Schur e FC-Grupos 31
2.1 O Homomorfismo Transfer 31
2.2 O Teorema de Schur 36
2.3 FC-Grupos 39

3 Coberturas de Grupos 44

4 Coberturas do conjunto dos comutadores de um grupo 51
4.1 Grupos sem comutadores não triviais de ordem finita 53
4.2 O Caso Geral 77

Apêndice 95

Referências Bibliográficas 110

Introdução

Dada uma cobertura $\{H_i\}_{i \in I}$ de um grupo G por subgrupos é natural perguntarmos que informações podem ser extraídas a cerca de G a partir das propriedades desses subgrupos. Como qualquer grupo pode ser coberto pelos subgrupos cíclicos gerados por seus elementos, não temos qualquer resposta satisfatória no caso geral. No entanto, a situação muda dramaticamente se pedirmos que a cobertura seja finita. O primeiro resultado nessa direção é devido a Baer, o qual provou que G admite uma cobertura finita por subgrupos abelianos se, e somente se, este é central-por-finito. A parte não trivial desta afirmação é uma consequência imediata de um resultado posterior de B.H.Neumann

Teorema 0.1.(*Neumann*) *Se* $\{S_i\}$ *é uma cobertura de G por classes laterais de subgrupos, então G também pode ser coberto pelas classes* S_i*'s correspondentes aos subgrupos de índice finito em G.*

Em outras palavras, se um grupo G possui uma cobertura finita por classes laterais de subgrupos, podemos nos desfazer das classes de subgrupos de índices infinitos, sem perdermos a propriedade de cobertura.

A motivação para o nosso trabalho é um famoso problema de P. Hall sobre subgrupos verbais. Seja w uma palavra, digamos em n variáveis. Se G é um grupo, seja G_w o conjunto de todos os valores $w(g_1, ..., g_n)$ com $g_1, ..., g_n \in G$, e seja $w(G)$ o subgrupo verbal correspondente a w, i.e.,o subgrupo gerado por G_w. A palavra w é dita ser concisa se $w(G)$ é finito sempre que G_w for finito. P.Hall levantou a seguinte questão:

"Toda palavra é concisa?"

Tempos depois Ivanov[3] mostrou que isto não ocorre. Entretanto, provou-se também que várias palavras relevantes são concisas. Por exemplo, Turner-Smith[7] mostrou que palavras centrais inferiores e palavras derivadas são concisas.

Podemos adotar uma abordagem mais geral para a questão de Hall:

Se assumirmos certas restrições sobre o conjunto G_w, no que isto influencia a estrutura de $w(G)$?

Gustavo A. Fernández e Pavel Schumyasky[2] propuseram o seguinte problema:

"Dada uma palavra w e um grupo G, suponha que o conjunto G_w pode ser coberto por finitos subgrupos cíclicos. É verdade que $w(G)$ também pode ser coberto por finitos subgrupos cíclicos?"

Usando o teorema de Neumann podemos caracterizar grupos que podem ser cobertos por uma quantidade finita de subgrupos cíclicos como grupos que são finitos ou cíclicos. Assim, podemos reescrever nosso questionamento da seguinte maneira:

Dada uma palavra w e um grupo G, suponhamos que G_w possua cobertura finita por subgrupos cíclicos . É verdade que $w(G)$ é finito ou cíclico?

Nosso Teorema Principal mostra que a resposta é positiva para a palavra comutador.

Teorema 0.2. *Seja G um grupo no qual o conjunto de todos os comutadores pode ser coberto por um número finito de subgrupos cíclicos. Então, G' é finito ou cíclico.*

Vamos falar um pouco agora de como o texto está organizado.

No capítulo 1(Premilinares), desenvolvemos alguns tópicos elementares de teoria dos grupos que serão necessários no decorrer da dissertação. A seção 1.1 traz a noção de classe lateral de um subgrupo e apresenta o Teorema de Poincaré que é de simples demonstração mas largamente utilizado neste trabalho. A seção 1.2 define os principais subgrupos que aparecem no texto. A seção 1.3 trata da representação de permutações ou ação de um grupo G sobre um conjunto X. Nas seções 1.4 e 1.5, fazemos um pequeno estudo dos Grupos Nilpotentes, no qual definimos as séries centrais(superior e inferior), demonstrando alguns resultados básicos que nos serão necessários no capítulo 4.

No capítulo 2, trabalhamos o Homomorfismo transfer(seção 2.1), obtendo alguns lemas e em seguida(seção 2.2), usamos os mesmos para a demonstração do principal resultado do capítulo, o Teorema de Schur.

Teorema 0.3.(*Schur*) *Se* $\dfrac{G}{Z(G)} \in \mathcal{F}$ *então* $G' \in \mathcal{F}$, *onde* $\mathcal{F}$ *representa a família dos grupos finitos.*

Para a demonstração desse teorema(assim como em muitas outras demonstrações ao longo do texto), fazemos uso, sem prova, do Teorema Fundamental dos Grupos Abelianos Finitamente Gerados que citamos apenas como T.F.G.A.F.G.

Teorema 0.4.(*T.F.G.A.F.G*) *Seja G um grupo abeliano finitamente gerado. Então, G pode ser decomposto como produto direto de um número finito de grupos cíclicos C_i's. Mais precisamente:*

$$G = C_1 \ldots\ldots\ldots C_k,$$

tal que ou $C_1, \ldots\ldots, C_k$ são todos infinitos, ou para algum $1 \leq j \leq k$, tem-se $C_1, \ldots\ldots, C_j$ finitos, de ordem $m_1, \ldots\ldots, m_j$, respectivamente, com $m_1|m_2|\ldots..|m_j$, e $C_{j+1}, \ldots.., C_k$ infinitos. Em particular, se G for de torção, então ele é finito.

No final do capítulo há ainda uma seção(2.3) dedicada ao estudo dos FC-Grupos, onde fazemos a demonstração do Lema de Dietzmann, o qual usaremos mais tarde, no último capítulo, na prova dos lemas que antecedem o teorema principal.

Lema 0.5.(*Dietzmann*) *Em qualquer grupo G um subconjunto normal finito constituído apenas por elementos de ordem finita, gera um subgrupo normal finito.*

Completamos assim os pré-requisitos essenciais para a compreensão dos resultados de Baer e Neumann que serão vistos no capítulo seguinte.

O capítulo 3 trata de coberturas de grupos. Nele fazemos a demonstração dos Teoremas de Neumann e de Baer, resultados importantes no desenvolvimento do capítulo seguinte. Além disso, no final do capítulo, usamos o resultado de Neumann para caracterizar grupos que podem ser cobertos por uma quantidade finita de subgrupos cíclicos como grupos que são finitos ou cíclicos.

No capítulo 4, estudamos coberturas finitas por subgrupos cíclicos do conjunto dos comutadores de um grupo. Na seção 4.1, provamos uma aproximação do resultado do teorema principal:

Teorema 0.6. *Seja G um grupo no qual todos os comutadores podem ser cobertos por um número finito de subgrupos cíclicos. Se G não possui comutadores de ordem finita, com excessão de 1, então G' é cíclico-por-finito.*

Na seção 4.2, usamos esse resultado para concluir a prova do nosso teorema principal.

Por fim, usamos o apêndice(*Um teste para comutadores*) para a demonstração do teorema 4.13.

Capítulo 1

Preliminares

1.1 Classes Laterais

Em nosso texto, G denotará um grupo multiplicativo com elemento neutro 1.

Se H é um subgrupo de G, podemos definir em G a seguinte relação de equivalência:

$$x \sim y \;\Leftrightarrow\; y^{-1}x \in H$$

Para cada $x \in G$, a classe de equivalência com respeito a essa relação é o subconjunto:

$$xH = \{xh \;;\; h \in H\},$$

o qual chamamos de classe lateral *à* esquerda de H contendo x.

Sendo "$\sim$" relação de equivalência, duas classes laterais *à* esquerda ou são iguais ou são disjuntas.

Além disso,

$$G = \dot{\bigcup_{x \in H}} xH$$

Analogamente, podemos definir em G a relação de equivalência:

$$x \sim y \;\Leftrightarrow\; xy^{-1} \in H$$

na qual a classe de equivalência de cada $x \in G$ é o subconjunto :

$$Hx = \{hx \;;\; h \in H\}$$

o qual chamamos de classe lateral *à* direita de H contendo x.

Um subconjunto $T \subset G$ é dito ser um transversal(*à* esquerda) quando G se escreve como união disjunta:

$$G = \dot{\bigcup_{t \in T}} tH$$

Note que em um transversal T aparece um único representante de cada classe lateral *à* esquerda. Assim, cada elemento de G pode ser escrito de maneira única como th onde $t \in T$ e $h \in H$.

De modo análogo, dizemos que um subconjunto $S \subset G$ é um transversal *à* direita quando podemos escrever:

$$G = \dot{\bigcup_{s \in S}} Hs$$

Proposição 1.1. *Dados G grupo,* $H \leq G$ *e* $x \in G$ *qualquer, temos:*

i) $\mid xH \mid = \mid H \mid$;

ii) $\mid \{xH; x \in G\} \mid = \mid \{Hy; y \in G\} \mid$;

iii) (*Lagrange*)*Se* G *é finito, então* $\mid G \mid = \mid H \mid . \mid G : H \mid$, *onde* $\mid G : H \mid = \mid \{xH \ ; \ x \in G\} \mid$.

Prova: Como $\begin{array}{l} \varphi : H \rightarrow xH \\ \quad\quad h \rightarrow xh \end{array}$ e $\begin{array}{l} \psi : \{xH \ ; \ x \in G\} \rightarrow \{Hx \ ; \ x \in G\} \\ \quad\quad\quad xH \quad\quad \rightarrow \quad\quad Hx^{-1} \end{array}$
são bijeções, i) e ii) seguem.

Para iii) considere $x_1H, ..., x_rH$ as classes laterais(*à* esquerda) distintas.

Então, $\mid G : H \mid = r$.

Sendo $G = x_1H \dot{\cup} ... \dot{\cup} x_rH$, temos:

$\mid G \mid = \mid x_1H \mid + ... + \mid x_rH \mid = \underbrace{\mid H \mid + ... + \mid H \mid}_{r \ vezes} = r \ . \ \mid H \mid$

■

Proposição 1.2(*Teorema do Índice*). *Se $H \leq K \leq G$, então:*

$$| G : H | = | G : K || K : H |$$

Prova: Sejam T um transversal de K em G, e S um transversal de H em K de modo que

$$G = \dot{\bigcup_{t \in T}} tK \quad \text{e} \quad K = \dot{\bigcup_{s \in S}} sH$$

Afirmamos que $G = \dot{\bigcup\limits_{(t,s) \in T \times S}} tsH$.

De fato, tomemos $g \in G$ qualquer.
De $(*)$ temos que $g = tk$ para algum $t \in T$ e $k \in K$.
Mas, sendo $k \in K$, $k = sh$, $\exists s \in S$, $\exists h \in H$.
Daí, $g = tk = tsh \in tsH$ e $G = \bigcup\limits_{(t,s) \in T \times S} tsH$ (ainda não sabemos se disjunta).
Suponha por absurdo, $t_1 s_1 H \cap t_2 s_2 H \neq \emptyset$.
Então, $\exists h_1, h_2 \in H$ tais que $t_1 s_1 h_1 = t_2 s_2 h_2$.
Daí, $t_1 s_1 = t_2 s_2 h_3$ com $h_3 = h_2 h_1^{-1} \in H$.
Segue de $(*)$ que $s_2 h_3 = k \in K$.
$\therefore$ $t_1 s_1 = t_2 k$
$\therefore$ $t_1 = t_2 k s_1^{-1} \in t_2 K$
$\therefore$ $t_1 K = t_2 K$
$\therefore$ $t_1 = t_2$
$\therefore$ $s_1 = s_2 h_3 \in s_2 H$
$\therefore$ $s_1 H = s_2 H$
$\therefore$ $s_1 = s_2$
Portanto, $t_1 s_1 H = t_2 s_2 H$ sempre que $t_1 s_1 H \cap t_2 s_2 H \neq \emptyset$ e nossa afirmação está provada.
Desse modo, $| G | = | TS | \, | H |$.
Afirmo ainda que :

$$| TS | = | T \times S | = | T | \, | S |$$

Considere, $\begin{array}{rcl} \varphi : T \times S & \rightarrow & T\ S \\ (t, s) & \rightarrow & ts \end{array}$

Claramente, φ está bem definida e é sobre.

Além disso,

$$\begin{aligned}\varphi(t_1,s_1)=\varphi(t_2,s_2) &\Rightarrow\ t_1s_1=t_2s_2\ \Rightarrow\ t_2^{-1}t_1=s_2s_1^{-1}\in S\subset K\\ &\Rightarrow\ t_1K=t_2K\ \Rightarrow\ t_1=t_2\ \Rightarrow\ s_1=s_2\\ &\Rightarrow\ (t_1,s_1)=(t_2,s_2)\end{aligned}$$

Logo, φ é bijeção e $|\ T\ S\ | = |\ T\ |\ |\ S\ |$.

Assim,

$$|\ G\ | = |\ T\ | \cdot |\ S\ | \cdot |\ H\ | = |\ G : K\ | \cdot |\ K : H\ | \cdot |\ H\ |$$

O que nos dá:

$$|\ G : H\ | = |\ G : K\ | \cdot |\ K : H\ |$$

$\blacksquare$

Proposição 1.3. *Se $H, K \leq G$, então:*

$$|\ G : H\cap K\ | \leqslant |\ G : H\ | \cdot |\ G : K\ |$$

Prova: Considere $\eta : \{g(H\cap K)\ ;\ g\in G\}\ \rightarrow\ \{aH\ ;\ a\in G\}\times\{bK\ ;\ b\in G\}$ dada por $\eta(\ g(H\cap K)\ ) = (gH, gK)$.
Veja que:

$$\begin{aligned}g_1(H\cap K)=g_2(H\cap K) &\Leftrightarrow\ g_2^{-1}g_1\in H\cap K\\ &\Leftrightarrow\ g_1H=g_2H\ \text{ e }\ g_1K=g_2K\\ &\Leftrightarrow\ (g_1H,g_1K)=(g_2H,g_2K)\\ &\Leftrightarrow\ \eta(g_1(H\cap K))=\eta(g_2(H\cap K))\end{aligned}$$

Logo, η está bem definida e é injetiva.
Daí o resultado segue. $\blacksquare$

Corolário 1.4(*Poincaré*). *Se $H_1, H_2, ..., H_n$ são subgrupos de G com índices fnitos, então $\bigcap_{i=1}^{n} H_i$ tem índice finito em G.*

Prova: Da proposição anterior sabemos que $|\ G : \bigcap_{i=1}^{n} H_i\ | \leq \prod_{i=1}^{n} |\ G : H_i\ |$.

Como $|\ G : H_i\ | <\ \infty$ para cada i, segue que $|\ G : \bigcap_{i=1}^{n} H_i\ | <\ \infty$.

$\blacksquare$

1.2 Subgrupos Clássicos

Nesta seção, introduziremos os principais subgrupos presentes neste trabalho.

Vejamos as definições:

1. Para cada $x \in G$, definimos a ordem de x, e denotamos por $o(x)$ como sendo o menor $n \in \mathbb{N}$ tal que $x^n = 1$. Quando não existe tal n dizemos que $o(x) = \infty$.

2. Dados $x, g \in G$ definimos o conjugado de x por g como $x^g = g^{-1}xg$.
E chamamos de classe de conjugação de x ao subconjunto

$$x^G = \{x^g \ ; \ g \in G\}$$

3. Se $N \leq G$, um subgrupo conjugado N^x é dado por :

$$N^x = x^{-1}Nx = \{x^{-1}nx \ ; \ n \in N\}$$

Se $N^x = N, \ \forall x \in G$, então dizemos que N é normal em G e denotamos isso pondo $N \lhd G$.

4. Dado $x \in G$, chamamos de centralizador de x em G o subgrupo formado por todos os elementos de G que comutam com x. Mais precisamente,

$$C_G(x) = \{g \in G \ ; \ x^g = x\}$$

Agora, se $H \subseteq G$, o centralizador de H em G é o subgrupo:

$$C_G(H) = \{g \in G \ ; \ h^g = h, \ \forall h \in H\} = \bigcap_{h \in H} C_G(h)$$

5. O centro de um grupo G é o subgrupo formado pelos elementos de G que comutam com todos os elementos do grupo, o qual indicamos por:

$$Z(G) = \{g \in G \ ; \ x^g = x, \ \forall x \in G\}$$

Veja que $Z(G) = C_G(G) \trianglelefteq G$.

6. Se $H \leq G$, definimos o normalizador de H em G como sendo o subgrupo

$$N_G(H) = \{g \in G \ ; \ H^g = H\}$$

Note que $H \trianglelefteq N_G(H)$.

7. Se $X \subset G$, definimos o subgrupo gerado por X como sendo

$$\langle X \rangle = \{x_1 ... x_n \ ; \ x_i \in X \cup X^{-1}\}$$

8. Se $x, y \in G$, definimos o comutador de x e y pondo:

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

Definimos ainda o subgrupo derivado de G, o qual denotamos por G' como sendo:

$$G' = \langle [x, y] \ ; \ x, y \in G \rangle$$

Se $H, K \subset G$, definimos $[H, K] = \langle [h, k] \ ; \ h \in H, k \in K \rangle$.

Perceba que $G' = [G, G]$.

9. Sejam G_1, G_2 grupos e $\phi : G_1 \ \rightarrow \ G_2$ um homomorfismo. Chamamos de núcleo de ϕ, ao subgrupo de G_1 dado por:

$$Nuc(\phi) = \{g \in G_1 \ ; \ \phi(g) = 1_{G_2}\}$$

Note que $Nuc(\phi) \triangleleft G_1$.

Se $N \triangleleft G$, o conjunto das classes de N *à* esquerda(ou *à* direita) é um grupo com a operação $xN \cdot yN = xyN$. Chamamos este grupo de grupo quociente de G por N e o denotamos por G/N.

A proposição a seguir caracteriza os grupos quocientes abelianos.

Proposição 1.5. *Se $N \trianglelefteq G$, então:*

$$\frac{G}{N} \ \textit{é abeliano} \ \Leftrightarrow \ G' \leq N$$

Prova: $\Rightarrow$) Sejam $a, b \in G$ quaisquer.

Como $\dfrac{G}{N}$ é abeliano, $aN \cdot bN = bN \cdot aN$.

$$\begin{aligned} aN \cdot bN = bN \cdot aN \ &\Rightarrow \ abN = baN \ \Rightarrow \ (ba)^{-1}ab \in N \\ &\Rightarrow \ a^{-1}b^{-1}a \ b = [a, b] \in N \end{aligned}$$

$\therefore\ G' = \langle [a,b]\ ;\ a,b \in G \rangle \leq N.$

$\Leftarrow$) Suponhamos agora, $G' \leq N$.
Sejam $aN, bN \in G/N$ quaisquer. Como $[a,b] \in N$, temos que $[a,b]N = N$.
Mas, $[a,b]N = a^{-1}N \cdot b^{-1}N \cdot aN \cdot bN$.
Logo, $aN \cdot bN = bN \cdot aN$. ■

Proposição 1.6. *Dado um grupo G e $a,b,c \in G$, temos:*

i) $[a,bc] = [a,c]\ .\ [a,b]^c,\ \forall a,b,c \in G;$

ii) $[ab,c] = [a,c]^b\ .\ [b,c],\ \forall a,b,c \in G.$■

Definição 1.7. *Um grupo é dito cíclico-por-finito se $\exists N \lhd G$ tal que N é cíclico e G/N é finito.*

1.3 Séries Normais e Nilpotência

Definição 1.8. *Uma sequência $(G_0, G_1, ..., G_r)$ de subgrupos normais de um grupo G é chamada uma série normal de G se*

$$1 = G_0 \lhd G_1 \lhd G_2 \lhd ... \lhd G_{r-1} \lhd G_r = G.$$

Chamamos os grupos quocientes G_i/G_{i-1}, $1 \leq i \leq r$, de *fatores* da série normal.
Quando nem todos os subgrupos G_i's são normais em G, dizemos que

$$(S):\ 1 = G_0 \lhd G_1 \lhd G_2 \lhd ... \lhd G_{r-1} \lhd G_r = G,$$

é *série subnormal de G.*

Se em (S) tem-se : $\dfrac{G_{i+1}}{G_i} \leq Z\Big(\dfrac{G}{G_i}\Big)$, $\forall i$, então dizemos que (S) é *série central de G.*

Exemplo 1.9. Seja $V = \{1, (12)(34), (13)(24), (14)(23)\} \lhd S_4$.

Então,

$$(S):\ 1 \overset{4}{\unlhd} V \overset{3}{\unlhd} A_4,$$

é série normal de S_4.

Por outro lado, tomando $H = \langle (12)(34) \rangle$, $H \ntrianglelefteq S_4$, logo,

$$(T): \ 1 \overset{2}{\trianglelefteq} H \overset{2}{\trianglelefteq} V \overset{3}{\trianglelefteq} A_4,$$

é série subnormal de S_4.

Definição 1.10. *Dizemos que um grupo G é nilpotente, se existe uma série normal:*

$$(S): \ 1 = G_0 \trianglelefteq G_1 \trianglelefteq ... \trianglelefteq G_n = G,$$

tal que $\dfrac{G_{i+1}}{G_i} \leq Z\left(\dfrac{G}{G_i}\right)$, $\forall i$ *(Isto é, (S) é série central de G).*

Note que :

$$\frac{G_{i+1}}{G_i} \leq Z\left(\frac{G}{G_i}\right) \ \Leftrightarrow \ [G_{i+1}, G] \leq G_i.$$

De fato, suponhamos $[G_{i+1}, G] \leq G_i$.

Então, dados $g_{i+1}G_i \in G_{i+1}/G_i$ e $gG_i \in G/G_i$ quaisquer, temos:

$(g_{i+1}^{-1}G_i) \ (g^{-1}G_i) \ (g_{i+1}G_i) \ (gG_i) = (g_{i+1}^{-1} \ g^{-1} \ g_{i+1} \ g)G_i = G_i.$

Logo, $(g_{i+1}G_i) \ (gG_i) = (gG_i) \ (g_{i+1}G_i)$ e $g_{i+1}G_i \in Z(G/G_i)$.

Reciprocamente, se $\dfrac{G_{i+1}}{G_i} \leq Z\left(\dfrac{G}{G_i}\right)$, então, tomando $[g_{i+1}, g] \in [G_{i+1}, G]$, temos:

$[g_{i+1}, g]G_i = [g_{i+1}G_i, gG_i] = G_i.$

Daí, $[g_{i+1}, g] \in G_i$ e $[G_{i+1}, G] \leq G_i$.

Teorema 1.11. *Se G é nilpotente e $H \leq G$, então H é nilpotente.*

Prova: Seja

$$\text{(S):} \ \ 1 = G_0 \trianglelefteq G_1 \trianglelefteq ... \trianglelefteq G_n = G,$$

série normal de G com $\dfrac{G_{i+1}}{G_i} \leq Z\left(\dfrac{G}{G_i}\right)$, para cada i.

Consideremos para cada i, $H_i = G_i \cap H$.

Sendo $G_i \trianglelefteq G$, temos $H_i \trianglelefteq H$ $\forall i$.

Além disso, $H_i \leq H_{i+1}$, para cada i.

Veja que

$$[H_{i+1}, H] \;=\; [G_{i+1} \cap H, H] \;\leq\; [G_{i+1}, G] \;\leq\; G_i$$

É claro que:

$$[H_{i+1}, H] \;\leq\; H$$

Logo,

$$[H_{i+1}, H] \;\leq\; H_i, \text{ para cada } i,$$

o que conclui nossa demonstração. ■

1.4 Séries Centrais

Definimos indutivamente o *n-ésimo* centro de um grupo G como a seguir.
Para $n = 0$ e $n = 1$, $Z_0(G) = 1$ e $Z_1 = Z(G)$.
Consideremos o centro do grupo grupo quociente $\dfrac{G}{Z(G)}$.
Como $Z\Big(\dfrac{G}{Z(G)}\Big) \trianglelefteq \dfrac{G}{Z(G)}$, sabemos do Teorema da Correspondência que existe um único subgrupo normal $Z_2(G)$ de G tal que $\dfrac{Z_2(G)}{Z(G)} = Z\Big(\dfrac{G}{Z(G)}\Big)$.
Isto é, $\dfrac{Z_2(G)}{Z_1(G)} = Z\Big(\dfrac{G}{Z(G)}\Big)$.
Analogamente, sendo $Z\Big(\dfrac{Z_2(G)}{Z_1(G)}\Big) \trianglelefteq \dfrac{Z_2(G)}{Z_1}$, existe um único $Z_3(G) \trianglelefteq Z_2(G)$, tal que $\dfrac{Z_3(G)}{Z_2(G)} = Z\Big(\dfrac{Z_2(G)}{Z_1}\Big)$.
Continuando esse raciocínio indutivamente, obtemos, para cada inteiro n maior que 1, um subgrupo normal $Z_n(G)$ de G tal que:

$$\frac{Z_n(G)}{Z_{n-1}(G)} = Z\Big(\frac{G}{Z_{n-1}(G)}\Big)$$

Definição 1.12. *A série normal crescente*

$$1 = Z_0(G) \trianglelefteq Z_1(G) \trianglelefteq Z_2(G) \trianglelefteq \ \dots \ \trianglelefteq Z_n(G) \trianglelefteq \ \dots$$

de subgrupos de um grupo G , é chamada série central superior de G.

Dado um grupo G, definamos

$$\Gamma_1(G) = G \ \text{ e } \ \Gamma_i(G) = [\Gamma_{i-1}(G), G], \text{ se } i > 1.$$

Afirmo que $\Gamma_i(G) \lhd G, \ \forall i.$
De fato, façamos indução sobre i.
Para $i = 1$, ok!
Suponhamos válido para $i = n$ e mostremos para $i = n + 1$.
Seja $g \in G$ qualquer.
Como $\Gamma_n(G) \lhd G$, temos:

$$\Gamma_{n+1}(G)^g = [\Gamma_n(G)^g, G^g] = [\Gamma_n(G), G] = \Gamma_{n+1}(G),$$

o que prova nossa afirmação.
Desse modo,

$$\Gamma_{i+1}(G) \trianglelefteq \Gamma_i(G), \ \forall i \geqslant 1$$

Definição 1.13. *A série normal decrescente*

$$G = \Gamma_1(G) \rhd G' = \Gamma_2(G) \rhd \ \dots \ \Gamma_i(G) \rhd \Gamma_{i+1} \rhd \ \dots$$

de subgrupos de um grupo G é chamada série central inferior de G.

Exemplo 1.14. Seja $G = D_4 = \langle a, b \ ; \ a^4 = 1 = b^2, ab = a^{-1}\rangle = \langle a\rangle \times \langle b\rangle$.
Note que:

$Z_1(G) = Z(D_4) = \langle a^2\rangle$.

$Z\Big(\dfrac{D_4}{\langle a^2\rangle}\Big)$, pois $\dfrac{D_4}{\langle a^2\rangle}$ é abeliano.

$\therefore \ \dfrac{Z_2(D_4)}{\langle a^2\rangle} = \dfrac{D_4}{\langle a^2\rangle}$

$\therefore \ Z_2(D_4) = D_4$

Daí, $Z_i(D_4) = D_4, \ \forall i \geqslant 2$.

Teorema 1.15. *São equivalentes:*

i) *G é nilpotente*;

ii) $\Gamma_n(G) = 1$, *para algum n*;

iii) $Z_n(G) = G$, *para algum n.*

Para demonstração deste Teorema, precisaremos do seguinte

<u>Lema</u>: Se $H, J, K \lhd G$, com $J \lhd H$ e $\dfrac{H}{J} \leq Z\Big(\dfrac{G}{J}\Big)$, então $\dfrac{HK}{JK} \leq Z\Big(\dfrac{G}{JK}\Big)$.

Prova: Como $\dfrac{H}{J} \leq Z\Big(\dfrac{G}{J}\Big)$, temos que $[H, G] \leq J$.

Afirmo que $[HK, G] = [H, G][K, G]$.

Claro que $[H, G][K, G] \leq [HK, G]$.

Para a desigualdade contrária, tomemos $[hk, g] \in [HK, G]$ qualquer.

Sendo $H \lhd G$, temos, em particular, H normal em K.

Assim,

$$\begin{aligned} [hk, g] &= [h, g]^k[k, g] \\ &= [h^k, g^k][k, g] \\ &= [h_1, g_1][k, g], \;\; \text{com } h_1 \in H \text{ e } g_1 \in G \end{aligned}$$

$\therefore \;\; [HK, G] \leq [H, G][K, G]$

$\therefore \;\; [HK, G] = [H, G][K, G]$

Como $K \lhd G$, $[K, G] \leq K$.

Agora,

$$[H, G] \leq J, \;\; [K, G] \leq K \;\Rightarrow\; [HK, G] = [H, G][K, G] \leq JK$$

Logo,

$$\frac{HK}{JK} \leq Z\Big(\frac{G}{JK}\Big)$$

Prova do Teorema:

$i) \Rightarrow ii)$: Seja série normal e central de G.

Afirmo que $G_i \leq Z_i(G),\ \forall i$.

Façamos indução sobre i:

Para $i = 0$: $G_0 = 1 = Z_0(G)$

Suponhamos válido para $i = n$. Isto é, $G_n \leq Z_n(G)$.

Sendo $Z_i(G), G_i, G_{i+1} \lhd G$ e $\dfrac{G_{i+1}}{G_i} \leq Z\Big(\dfrac{G}{G_i}\Big)$, segue do resultado mostrado acima que:

$$\frac{Z_i(G)G_{i+1}}{Z_i(G)G_i} \leq Z\Big(\frac{G}{Z_i(G)G_i}\Big)$$

Mas, $Z_i(G)G_i = Z_i(G)$.

Daí,

$$\frac{Z_i(G)G_{i+1}}{Z_i(G)} \leq Z\Big(\frac{G}{Z_i(G)}\Big) = \frac{Z_{i+1}(G)}{Z_i(G)}$$

$\therefore\ Z_i(G)G_{i+1} \leq Z_{i+1}G$

$\therefore\ G_{i+1} \leq Z_{i+1}(G)$

Isto prova nossa afirmação.

Assim, $G = G_k \leq Z_k(G)$ e temos $Z_k(G) = G$.

$iii) \Rightarrow i)$: Suponhamos $Z(G) = G$.

Então,

$$1 = Z_0(G) \trianglelefteq Z_1(G) \trianglelefteq\ ...\ \trianglelefteq Z_n(G) = G$$

é série normal de G.

Além disso, por definição: $\dfrac{Z_{i+1}(G)}{Z_i(G)} = Z\Big(\dfrac{G}{Z_i(G)}\Big)$.

Logo, G é nilpotente.

$i) \Rightarrow ii)$: Consideremos novamente, $1 = G_0 \trianglelefteq G_1 \trianglelefteq ... \trianglelefteq G_k = G$ série normal de G, com $\dfrac{G_{i+1}}{G_i} \leq Z\Big(\dfrac{G}{G_i}\Big)$, $\forall i$ (o que equivale a $[G_{i+1}, G_i] \leq G_i$, $\forall i$).

Afirmo que $\Gamma_{j+1}(G) \leq G_{k-j}$, $\forall j$

Façamos indução sobre j.

Para $j = 0 : \Gamma_1(G) = G = G_k$.

Suponhamos válido para $j = m$ e mostremos que vale para $j = m + 1$.

Como $\Gamma_{m+1}(G) \leq G_{k-m}$, segue que :

$$\Gamma_{m+2}(G) = [\Gamma_{m+1}(G), G] \leq [G_{k-m}, G] \leq G_{k-m-1} = G_{k-(m+1)}$$

$\therefore$ $\Gamma_{j+1}(G) \leq G_{k-j}$, $\forall j$

Tomando então, $j = k$, temos: $\Gamma_{k+1}(G) \leq G_0 = 1$.

Portanto, $\Gamma_{k+1}(G) = 1$.

$ii) \Rightarrow i)$: Suponha $\Gamma_n(G) = 1$.

Então,

$$\Gamma_1(G) = G \trianglelefteq \Gamma_2(G) \trianglelefteq \ ... \ \trianglelefteq \Gamma_{n-1}(G) \trianglelefteq \Gamma_n(G) = 1$$

é série normal de G.

Além disso,

$$\Gamma_{i+1}(G) = [\Gamma_i(G), G] \ \Rightarrow \ \frac{\Gamma_i(G)}{\Gamma_{i+1}(G)} = Z\Big(\frac{G}{\Gamma_{i+1}(G)}\Big)$$

Logo, G é nilpotente. ∎

Teorema 1.16. *Se G é nilpotente, então, para qualquer série central*

$$(S) : \ 1 = G_0 \trianglelefteq G_1 \trianglelefteq \ ... \ \trianglelefteq G_k = G$$

tem-se $\Gamma_{k-i+1}(G) \leq G_i \leq Z_i(G)$, $\forall i = 0, ..., r$.
Além disso, o menor c tal que $Z_c(G) = G$ *também é o menor tal que* $\Gamma_{c+1}(G) = 1$ (*chamamos c de classe de nilpotência de G*).

Prova: Vimos anteriormente que em qualquer série central de G,

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq ... \trianglelefteq G_k = G$$

temos $G_i \leq Z_i, \ \forall i$ e $\Gamma_{j+1} \leq G_{r-j}, \ \forall j$.

Tomando $j = k - i$, obtemos:

$$\Gamma_{k-i+1}(G) \leq G_i \leq Z_i, \ \forall i = 0, ..., k \qquad (*)$$

Seja c o menor tal que $Z_c(G) = G$ e consideremos a série:

$$1 = Z_0(G) = G_0 \trianglelefteq Z_1(G) = G_1 \trianglelefteq \ ... \ \trianglelefteq Z_c(G) = G = G_c$$

Por $(*)$, temos:

$$\Gamma_{c-i+1}(G) \leq G_i \leq Z_i, \ \forall i = 0, ..., c$$

Em particular, para $i = 0$, temos:

$$\Gamma_{c+1}(G) \leq G_0 = Z_0(G) = 1$$

$\therefore \ \Gamma_{c+1}(G) = 1$

Suponhamos por absurdo que $\exists s < c + 1$ tal que $\Gamma_s(G) = 1$.

Consideremos a série normal central de G:

$$1 = \Gamma_c(G) = G_0 \ \trianglelefteq \ \Gamma_{c-1}(G) = G_1 \ \trianglelefteq \ ... \ \trianglelefteq \ \Gamma_1(G) = G = G_{c-1}$$

Por $(*)$:

$$\Gamma_{c-i}(G) \leq G_i \leq Z_i(G), \ \forall i = 0, ..., c - 1$$

$\therefore \ Z_{c-1}(G) = G$

Absurdo!

Logo, c é o menor tal que $\Gamma_{c+1}(G) = 1$. ■

1.5 Representação de Permutações

Dado X um conjunto qualquer, denotamos por S_X o conjunto de todas as funções $f : X \to X$ bijetoras. É fácil ver que S_X com a operação de composição de funções é um grupo, o qual chamamos de grupo simétrico, ou grupo de permutações de X. Quando $\mid X \mid = n < \infty$, escrevemos $S_X = S_n$ e este será o grupo de permutações de n símbolos, cuja ordem é $n!$.

Definição 1.17. *Uma representação de permutações(ou ação) de um grupo G sobre um conjunto X é um homomorfismo* $\varphi : G \;\rightarrow\; S_X$.

Denotaremos a imagem de cada elemento $g \in G$ pondo $\varphi(g)$ ou φ_g.

Com respeito ao estudo de uma ação φ de um grupo G sobre um conjunto X, definimos os seguintes conjuntos:

- Se $x \in X$, definiremos o estabilizador de x como sendo:

$$G_x = \{g \in G \;;\; \varphi(g)(x) = x\}$$

- Se $x \in X$, definimos a órbita de x por:

$$Gx = \{\varphi(g)(x) \;;\; g \in G\}$$

- Para cada $g \in G$ denotaremos por X_g o conjunto dos pontos fixos de $\varphi(g)$. Isto é,

$$X_g = \{x \in X \;;\; \varphi(g)(x) = x\}$$

- $X_G = \{x \in X \;;\; \varphi(g)(x) = x, \; \forall g \in G\}$

Dada $\varphi : G \;\rightarrow\; S_X$ ação de um grupo G num conjunto X, definamos sobre X a seguinte relação:

$$x \sim y \;\Leftrightarrow\; y = \varphi(g)(x), \text{ para algum } g \in G$$

Veja que:

(i) $x \sim x$, já que $\varphi(1)(x)$.

(ii) Se $x \sim y$, então $y = \varphi(g)(x), \; \exists g \in G$. Daí, $x = \varphi(g^{-1})(y)$ e $y \sim x$.

(iii) Se $x \sim y$ e $y \sim z$, então $\exists g_1, g_2 \in G$ tais que $y = \varphi(g_1)(x)$ e $z = \varphi(g_2)(y)$.

Assim,

$$z = \varphi(g_1)(\varphi(g_2)(x)) = \varphi(g_1 g_2)(x),$$

o que indica $x \sim z$.

Portanto, "$\sim$" é relação de equivalência.

A classe de equivalência de um elemento $x \in X$ é o conjunto:

$$\bar{x} = \{\varphi(g)(x) \ ; \ g \in G\} = Gx \quad \text{(órbita de x)}$$

Teorema 1.18. *Seja $\varphi : G \to S_X$ uma ação de um grupo G em um conjunto X. Então:*

(i) $G_x \leq G$;

(ii) $|\ Gx\ | = |\ G : G_x\ |$.

Prova: (i) Como $\varphi(1)(x) = x$, $\forall x \in X$, temos que $1 \in G_x$. Daí, $G_x \neq \emptyset$.
Dados $g_1, g_2 \in G_x$, temos: $\varphi(g_1)(x) = x$ e $\varphi(g_2)(x) = x$.
Assim,

$$\varphi(g_1 g_2^{-1})(x) = \varphi(g_1)(\varphi(g_2^{-1})(x)) = \varphi(g_1)(x) = x$$

$\therefore \ g_1 g_2^{-1} \in G$

Como g_1 e g_2 foram tomados arbitrariamente em G_x, o resultado segue.
Consideremos a função:

$$\begin{array}{rcl} \phi : \{gG_x \ ; \ g \in G\} & \longrightarrow & Gx \\ gG_x & \longrightarrow & \varphi(g)(x) \end{array}$$

Suponhamos $aG_x = bG_x$. Então, $a = bz$, com $z \in G_x$.
Daí, teremos:

$$\phi(aG_x) = \varphi(a)(x) = \varphi(bz)(x) = \varphi(b)(\varphi(z)(x)) = \varphi(b)(x) = \phi(bG_x)$$

Logo, ϕ está bem definida.
Claramente ϕ é sobre.
Além disso,

$$\begin{array}{rl} \phi(aG_x) = \phi(bG_x) & \Rightarrow \ \varphi(a)(x) = \varphi(b)(x) \\ & \Rightarrow \ \varphi(b^{-1})(\varphi(a)(x)) = x \ \Rightarrow \ \varphi(b^{-1}a)(x) = x \\ & \Rightarrow \ b^{-1}a \in G_x \ \Rightarrow \ aG_x = bG_x \end{array}$$

o que indica ϕ injetiva.
Portanto φ é bijeção e temos: $|\ G : G_x\ | = |\ Gx\ |$. ■

Exemplo 1.19. Seja G um grupo e definamos:

$$\begin{array}{rcl} \varphi : G & \longrightarrow & S_G \\ g & \longrightarrow & \varphi(g) : x \rightarrow gxg^{-1} \end{array}$$

φ é ação de G em si mesmo.

Note que:

$$Gx = \{gxg_{-1} \ ; \ g \in G\} = \{x^{g^{-1}} \ ; \ g \in G\} = x^G$$

Além disso,

$$G_x = \{g \in G \ ; \ x^{g^{-1}} = x, \ \forall x \in G\} = C_G(x)$$

Segue então do teorema anterior que:

$$| \ G : C_G(x) \ | = | \ x^G \ |$$

$\blacksquare$

Capítulo 2

O Teorema de Schur e FC-grupos

2.1 O Homomorfismo Transfer

Seja G um grupo e $H \leq G$ com $\mid G : H \mid = \ n$. Considere ainda A um grupo abeliano e $\theta : H \ \rightarrow \ A$ um homomorfismo. Fixemos um transversal $\{t_1, ..., t_n\}$ de H em G de modo que:

$$G = \bigcup_{1}^{n} Ht_i$$

Para cada $x \in G$ a classe $Ht_i x$ é uma das classes $Ht_j, \ j = 1, 2, ..., n$ (já que $Ht_1, ..., Ht_n$ são todas as classes *à* direita de H).
Denotamos então:

$$Ht_i x = Ht_{(i)x}$$

Note que $i \ \rightarrow \ (i)x$ é uma permutação de $\{1, 2, ..., n\}$.

Vejamos a injetividade:

$$\begin{aligned} (i)x = (j)x \ &\Rightarrow \ Ht_{(i)x = Ht_{(j)x}} \\ &\Rightarrow \ Ht_i x = Ht_j x \\ &\Rightarrow \ Ht_i = Ht_j \\ &\Rightarrow \ i = j \end{aligned}$$

Toda função injetiva de um conjunto finito em si mesmo é sobre.
Logo, $i \ \rightarrow \ (i)x$ é bijeção.
Além disso, sendo $Ht_i x = Ht_{(i)x}$ temos que $t_i x t_{(i)x}^{-1} \in H$ para cada $x \in G$.

Poderíamos perguntar: Dados G grupo e $H \leq G$, podemos sempre exibir um grupo A abeliano e $\theta : H \ \rightarrow \ A$ homomorfismo?

A resposta é sim!

Vimos anteriormente que dados G grupo e $N \lhd G$, tem-se:

$$\frac{G}{N} \text{ abeliano } \Leftrightarrow G' \leq N$$

Logo, $\dfrac{H}{H'}$ é abeliano(Lembre que $H' \lhd H$).

Daí, basta tomarmos $\begin{array}{rcl}\theta : H & \rightarrow & H/H', \\ h & \rightarrow & hH'\end{array}$ o homomorfismo canônico.

Definição 2.1(*Homomorfismo Transfer*). *Definimos* $\theta^* : G \rightarrow A$ *por*

$$\theta^*(x) = \prod_{i=1}^{n} \theta(t_i x t_{(i)x}^{-1})$$

Como A é abeliano, a ordem dos fatores no produto é irrelevante.

Lema 2.2. *Sobre* θ^*, *temos :*

(i) θ^* *é homomorfismo, o qual chamamos de Homomorfismo Transfer;*

(ii) θ^* *independe do transversal.*

Prova:(i) Da definição, temos:

$$Ht_{(i)xy} = Ht_i xy = H(t_i x)y = Ht_{((i)x)y}$$

$$\therefore \; t_{(i)xy} = t_{((i)x)y}, \;\; \forall x, y \in G.$$

Daí,

$$\begin{aligned}
\theta^*(xy) &= \prod_{i=1}^{n} \theta(t_i xy t_{(i)xy}^{-1}) \;=\; \prod_{i=1}^{n} \theta(t_i xy t_{((i)x)y}^{-1}) \\
&= \prod_{i=1}^{n} \theta(t_i x t_{(i)x}^{-1} t_{(i)x} y t_{((i)x)y}^{-1}) \;=\; \prod_{i=1}^{n} \theta(t_i x t_{(i)x}^{-1}) \theta(t_{(i)x} y t_{((i)x)y}) \\
&= \prod_{i=1}^{n} \theta(t_i x t_{(i)x}^{-1}) \prod_{i=1}^{n} \theta(t_{(i)x} y t_{((i)x)y}^{-1}) \quad \text{(já que A é abeliano)} \\
&= \theta^*(x)\theta^*(y)
\end{aligned}$$

(ii) Seja $\{t'_1, t'_2, ..., t'_n\}$ um outro transversal de H em G.

Podemos supor $Ht'_i = Ht_i$, para cada i (caso isso não ocorra, reorganizamos os t_i's).

Daí, $t'_i = h_i t_i$ para algum $h \in H$.

$t'_i = h_i t_i \ \Rightarrow \ t'_i x = h_i t_i x \ \Rightarrow \ Ht'_i x = Ht_i x \ \Rightarrow \ Ht'_{(i)x} = Ht_{(i)x}$

$\therefore \ t'_{(i)x} \in Ht_{(i)x} \in Ht_{(i)x}$
$\therefore \ t'_{(i)x} = h_{(i)x} t_{(i)x} t_{(i)x}$ com $h_{(i)x} \in H$.

Assim,

$$\begin{aligned}
\theta^*(x) &= \prod_{i=1}^{n} \theta(t'_i x t'^{-1}_{(i)x}) = \prod_{i=1}^{n} \theta(h_i t_i x (h_{(i)x} x t_{(i)x})^{-1}) \\
&= \prod_{i=1}^{n} \theta(h_i t_i x t^{-1}_{(i)x} h^{-1}_{(i)x}) \\
&= \prod_{i=1}^{n} \theta(h_i)\ \theta(t_i x t^{-1}_{(i)x})\ \theta(h^{-1}_{(i)x}) \\
&= \prod_{i=1}^{n} \theta(h_i) \prod_{i=1}^{n} \theta(t_i x t^{-1}_{(i)x}) \prod_{i=1}^{n} \theta(h^{-1}_{(i)x}) \\
&= \prod_{i=1}^{n} \theta(h_i) \prod_{i=1}^{n} \theta(h^{-1}_{(i)x}) \prod_{i=1}^{n} \theta(t_i x t^{-1}_{(i)x}) \quad \text{(pois A é abeliano)} \\
&= \prod_{i=1}^{n} \theta(t_i x t^{-1}_{(i)x})
\end{aligned}$$

Observe que nas duas últimas igualdades, usamos o fato de que $i \to (i)x$ é uma permutação de $\{1, ..., n\}$. ■

Lema 2.3(Cálculo de θ^*). *Sejam $H \leq G$ e $\theta : H \to A$, com A grupo abeliano. Se $\mid G : H \mid = n$, para cada $x \in G$ existem $k \in \mathbb{N}$ e $l_1, l_2, ..., l_k \in \mathbb{N}$ tais que:*

$$\theta^*(x) = \prod_{i=1}^{n} (s_i x^{l_i} s_i^{-1})$$

com $s_i \in G$ e $\displaystyle\sum_{i=1}^{k} l_i = n$.

Prova: Fixado $s_1 \in G$, consideremos as classes $Hs_1, Hs_1x, Hs_1x^2...$
Como há somente um número finito de classes laterais, existe $n \in \mathbb{N}$ tal que $Hs_1^n = Hs_1$. Seja l_1 o primeiro natural em que isso ocorre.
Então, temos o ciclo:

$$Hs_1, Hs_1x, Hs_1x^2, ..., Hs_1x^{l_1} = Hs_1$$

Se estas não forem todas as classes laterais de H, tomamos uma nova classe, Hs_2, e procedemos de maneira análoga.
Considerando l_2 o primeiro natural tal que $Hs_2x^{l_2} = Hs_2$, temos as classes:

$$Hs_2,\ Hs_2x,\ Hs_2x^2, ..., Hs_2x^{l_2-1}$$

Se ainda não tivermos todas as classes laterais de H, repetimos esse processo até que isso ocorra. Desse modo, encontramos várias cadeias não intersectantes de classes laterais.

Seja:

$$Hs_k,\ Hs_kx,\ Hs_kx^2, ..., Hs_kx^{l_k-1},$$

a última delas.

Como $Hs_1, ..., Hs_1x^{l_1-1}, Hs_2, ..., Hs_2x_2^{l_2-1}, ..., Hs_k, ..., Hs_kx_k^{l_k-1}$ são todas as classes, temos, $\displaystyle\sum_{i=1}^{k} l_i = n$.

Vimos no Lema anterior que θ^* independe do transversal.

Escolhamos:

$$T = \{s_1, s_1x, ..., s_1x^{l_1-1}, s_2, s_2x, ..., s_2x^{l_2-1}, ..., s_k, s_kx, ..., s_kx^{l_k-1}\},$$

como transversal.

Façamos :

$$\begin{cases} t_1 = s_1,\ t_2 = s_1x,\ ...,\ t_{l_1} = s_1x^{l_1-1} \\ t_{l_1+1} = s_2,\ t_{l_1+2} = s_2x,\ ...,\ t_{l_1+l_2} = s_2x^{l_2-1} \\ . \\ . \\ . \\ t_{l_1+l_2+...+l_{k-1}+1} = s_k,\ t_{l_1+l_2+...+l_{k-1}+2} = s_kx,\ ...,\ t_{\sum l_i} = t_n = s_kx^{l_k-1} \end{cases}$$

Veja que:

$$Ht_{(i)x} = Ht_i x = Hs_1 x = Ht_2$$

$$Ht_{(2)x} = Ht_2 x = Hs_1 x^2 = Ht_3$$

$$\vdots$$

$$Ht_{l_1 x} = Ht_{l_1} x = Hs_1 x^{l_1} = Hs_1 = Ht_1$$

$$- - - - - - - - - - - - - - - - - - - -$$

$$Ht_{(l_1+1)x} = Ht_{l_1+1} x = Hs_2 x = Ht_{l_1+2}$$

$$Ht_{(l_1+2)x} = Ht_{l_1+2} x = Hs_2 x^2 = Ht_{l_1+3}$$

$$\vdots$$

$$Ht_{(l_1+l_2)x} = Ht_{l_1+l_2} x = Hs_2 x^{l_2} = Hs_2 = Ht_{l_1+1}$$

$$- -$$

$$\vdots$$

$$- -$$

$$Ht_{(l_1+\ldots+l_{k-1}+1)x} = Ht_{l_1+\ldots+l_{k-1}+1} x = Hs_2 x = Ht_{l_1+\ldots+l_{k-1}+2}$$

$$\vdots$$

$$Ht_{(\sum l_i)x} = Ht_{\sum l_i} x = Ht_n x = Hs_k x^{t_k} = Hs_k = Ht_{l_1+\ldots+l_{k-1}+1}$$

$$- -$$

Portanto,

$$(i)x = i+1, \ \forall i \neq l_j$$

$$(l_j)x = j, \ \forall j$$

$$(l_1 + \ldots + l_j)x = l_1 + \ldots + l_{j-1} + 1, \ \forall j$$

Daí,

$$\theta^*(x) = \prod_{i=1}^{l_1+\ldots+l_k} \theta(t_i x t_{(i)x}^{-1})$$

$$= \theta(t_i x t_2^{-1})\ \theta(t_2 x t_3^{-1})\ ...\ \theta(t_{l_1-1} x t_{l_1}^{-1})\ \theta(t_{l_1+l_2} x t_{l_1+1}).$$

$$.\theta(t_{l_1+1} x t_{l_1+2}^{-1})\ \theta(t_{l_1+2} x t_{l_1+3}^{-1})\ ...\ \theta(t_{l_1+l_2-1} x t_{l_1+l_2}^{-1})\ \theta(t_{l_1+l_2} x t_{l_1+1}^{-1})$$

$$\vdots$$

$$.\theta(t_{l_1+...+l_{k-1}+1} x t_{l_1+...+l_{k-1}+2})\ .\ .\ .\ .\ \theta(t_{l_1+...+l_k} x t_{l_1+...+l_{k-1}+1}^{-1})$$

$$= \theta(t_1 x^{l_1} t_1^{-1})\ \theta(t_{l_1+1} x^{l_2} t_{l_1+1}^{-1})\ ...\ \theta(t_{l_1+...+l_k} x t_{l_1+...+l_{k-1}+1}^{-1})$$

$$= \theta(s_1 x^{l_1} s_1^{-1})\ \theta(s_2 x^{l_2} s_2^{-1})\ ...\ \theta(s_k x^{l_k} s_k^{-1})$$

$$= \prod_{i=1}^{k} (s_i x^{l_i} s_i^{-1})\ \blacksquare$$

2.2 O Teorema de Schur

O objetivo desta seção é a demonstração do *Teorema de Schur*, o qual usaremos bastante neste trabalho.
Antes, vejamos dois lemas que nos serão necessários.

Lema 2.4. *Seja G um grupo e $H \leq Z(G)$ tal que $\mid G : H \mid = n$. Então, o homomorfismo transfer da função $\theta : H \to H$ com $\theta(h) = h$, $\forall h \in H$ é a função $\theta^*(x) = x^n$.*

Prova: Usando o Lema anterior, temos:

$$\theta^*(x) = \prod_{i=1}^{k} \theta(s_i x^{l_i} s_i^{-1})$$

Agora,

$$\begin{aligned} s_i x^{l_i} s_i^{-1} \in H \leq Z(G) \ &\Rightarrow\ s_i x^{l_i} s_i^{-1} = z \in Z(G) \\ &\Rightarrow\ x^{l_i} = s_i^{-1} z s_i = z \in Z(G) \end{aligned}$$

Assim,

$$\theta^*(x) = \prod_{i=1}^{k} x^{l_i} = x^{l_1+...+l_k} = x^n\ \blacksquare$$

Lema 2.5. *Se G é finitamente gerado e $H \leq G$ com $\mid G : H \mid = n$, então H é finitamente gerado.*

Prova: Seja $T = \{1 = t_1, t_2, ..., t_n\}$ um transversal de H em G.

Definimos para cada $x \in G$, $Ht_i x = Ht_{(i)x}$.
Então, $t_i x = h(i,x)t_{(i)x}$, com $h(i,x) \in H$.
Além disso, como visto anteriormente, $t_{(i)xy} = t_{((i)x)y}$.
Logo,

$$\begin{aligned} t_i xy &= (t_i x)y = (h(i,x)\ t_{(i)x})y = h(i,x)\ (t_{(i)x}y) \\ &= h(i,x)\ h((i)x,y)\ t_{((i)x)y} \\ &= h(i,x)\ h((i)x,y)\ t_{(i)xy} \end{aligned}$$

Analogamente, podemos mostrar que:

$$t_i xyz = h(i,x)\ h((i)x,y)\ h((i)xy,z)\ t_{(i)xyz}$$

Mais geralmente, temos:

$$t_i(x_1...x_s) = h(i,x_1)\ h((i)x_1,x_2)\ ...\ h((i)x_1x_2...x_{s-1},x_s)\ t_{(i)x_1...x_s}$$

Seja $G = \langle X \rangle$ com X finito.

Tomemos $x \in H$ qualquer.

Como $H \leq G$, $x = x_1...x_n$, onde $x_i \in X \cup X^{-1}$.

Sendo $t_1 = 1$ e $x \in H$, temos:

$$\begin{gathered} Ht_1 = H = Hx = Ht_1x = Ht_{(1)x} \\ \therefore\ (1)x = 1 \end{gathered}$$

Daí,

$$\begin{aligned} x &= t_1x = t_1(x_1, ..., x_n) \\ &= h(1,x_1)\ h((1)x_1,x_2)...\ h((1)x_1x_2...x_{s-1},x_s)\ t_{(1)x_1x_2...x_s} \\ &= h(1,x_1)\ h((1)x_1,x_2)\ ...\ h((1)x_1x_2\ ...\ x_{s-1},x_s) \end{aligned}$$

$\therefore\ H\ =\ \langle h(j,x)\ ;\ 1 \leq j \leq n\ \text{ e }\ x \in X \cup X^{-1} \rangle$ ■

Finalmente, podemos provar o

Teorema 2.6(*Schur*). *Se $\dfrac{G}{Z(G)}$ é finito, então G' é finito. Além disso, se $\left| \dfrac{G}{Z(G)} \right| = n$, então $x^n = 1,\ \forall x \in G'$. Isto é, $o(x) \mid n,\ \forall x \in G'$.*

Prova: Do Lema 2.4, sabemos que $\begin{array}{l}\theta^* : G \to Z(G) \\ \quad\; x \to x^n\end{array}$ é o homomorfismo transfer de $\begin{array}{l}\theta : Z(G) \to Z(G). \\ \quad\;\; z \to z\end{array}$

Segue então. do 1° Teorema dos Homomorfismos, que:

$$\frac{G}{Nuc\ \theta} \ \simeq \ \theta^*(G) \ \leq Z(G)$$

Logo, $\dfrac{G}{Nuc\ \theta}$ é abeliano e $G' \leq Nuc\ \theta^*$.

Assim, para qualquer $x \in G'$, tem-se, $x^n = 1$.

Seja $\dfrac{G}{Z(G)} = \{t_1Z(G), t_2Z(G), ..., t_nZ(G)\}$.

Dados $x, y \in G$ quaisquer, $xZ(G), yZ(G) \in \dfrac{G}{Z(G)}$.

Daí, $\exists i, j$ tais que $xZ(G) = t_iZ(G)$ e $yZ(G) = t_jZ(G)$.

Portanto, $x = t_iz_i$ e $y = t_jz_j$ com $z_i, z_j \in Z(G)$.

Desse modo:

$$\begin{aligned}[x, y] = [t_iz_i, t_jz_j] &= (t_iz_i)^{-1}(t_jz_j)^{-1}(t_iz_i)(t_jz_j) \\ &= z_i^{-1}t_i^{-1}z_j^{-1}t_j^{-1}t_i\ z_i\ t_j\ z_j \\ &= t_i^{-1}t_j^{-1}t_i\ t_j \\ &= [t_i, t_j]\end{aligned}$$

e temos:

$$G' = \langle [t_i, t_j]\ ;\ 1 \leq i, j \leq n \rangle,$$

o que implica que G' é finitamente gerado.

Como $Z(G) \lhd G$, segue, do 2° Teorema dos Isomorfismos que:

$$\frac{Z(G)G'}{Z(G)} \simeq \frac{G'}{Z(G)\cap G'}$$

Em diagramas:

$$\begin{tikzcd}
& G \arrow[d, dash] & \\
& Z(G)G' \arrow[dl, equal] \arrow[dr, dash] & \\
Z(G) \arrow[dr, dash] & & G' \arrow[dl, equal] \\
& Z(G)\cap G' &
\end{tikzcd}$$

Por outro lado,

$$\mid Z(G)G' : Z(G) \mid \leq \mid G : Z(G)G' \mid\mid Z(G)G' : Z(G) \mid = \mid G : Z(G) \mid < \infty$$

Logo, $\mid G' : Z(G)\cap G' \mid < \infty$.
Como G' é finitamente gerado, segue do Lema 2.4 que $Z(G)\cap G'$ também o é. Além disso, sendo $Z(G)\cap G'$ subgrupo de $Z(G)$ e de G' este é abeliano e de torção.
Segue então do T.F.G.A.F.G que:

$$Z(G)\cap G' = A_1 \times ... \times A_n,$$

onde os A_i's são subgrupos cíclicos finitos.
Portanto, $Z(G)\cap G'$ é finito.
Finalmente,

$$\mid G' \mid = \mid G' : Z(G)\cap G' \mid \mid Z(G)\cap G' \mid < \infty,$$

o que conclui nossa demonstração. ■

2.3 FC-Grupos

Definição 2.7. Um grupo G é dito um *FC-Grupo*, se para cada $x \in G$ tem-se x^G finito.

Obs.: A sigla FC, vem do inglês : "finite conjugate".

Sobre a classe de conjugação x^G lembramos que: $\mid x^G \mid = \mid G : C_G(x) \mid$.

Proposição 2.8. *Dado G um FC-grupo e $g \in G$, temos:*

(i) $C_G(\langle x^G \rangle) \;=\; C_G(x^G)$;

(ii) $\langle x^G \rangle \lhd G$;

(iii) $C_G(x^G) \lhd G$.

Prova: (i) Seja $x^G = \{x_1, x_2, ..., x_s\}$. Claro que $C_G(\langle x^G \rangle) \leq C_G(x^G)$.
Agora, seja $g \in C_G(x^G)$ qualquer.
Então, $g \in C_G(x_i), \forall i$ e consequentemente, $g \in C_G(x_i^{-1}), \forall i$.
Tomando $y \in \langle x^G \rangle,\ y = y_1, ..., y_n$ com $y_i \in \{x_1, ..., x_s\} \cup \{x_1^{-1}, ..., x_s^{-1}\}$,
temos: $y^g = y_1^g ... y_n^g = y_1 ... y_n = y$
$\therefore\ g \in C_G(y),\ \forall y \in \langle x^G \rangle$
$\therefore\ g \in \langle C_G(x^G) \rangle$
$\therefore\ C_G(x^G) \leq C_G(\langle x^G \rangle)$

Logo, $C_G(x^G) = C_G(\langle x^G \rangle)$.

(ii) $\langle x^G \rangle = \{y_1 ... y_n\ ;\ y_i \in x^G \cup (x^G)^{-1}\}$

Seja $g \in G$ qualquer.

Note que:

$$(y_1 ... y_n)^g = y_1^g ... y_n^g$$

Mas,

$$y_i \in x^G \ \Rightarrow\ y_i^g \in x^G,\ \forall g \in G$$

e

$$y_i \in (x^G)^{-1} \ \Rightarrow\ y_i^g \in (x^G)^{-1},\ \forall g \in G \quad \text{(já que } (x_i^{-1})^g = (x_i^g)^{-1}\text{)}$$

Logo,

$$(y_1 ... y_n)^g \in \langle x^G \rangle$$

$\therefore\ \langle x^G \rangle \lhd G$

(iii) Para esta parte de demonstração usaremos o seguinte:

<u>**Resultado**</u>: Se G é um grupo e $N \lhd G$, então $C_G(N) \lhd G$.

Prova: Seja $g \in G$ qualquer. Mostraremos que $g^{-1} C_G(N) g \leq C_G(N)$.
Tomemos $g^{-1} a g \in g^{-1} C_G(N) g$.
Para cada $n \in N$, temos:

$$n^{g^{-1}ag} = g^{-1}a^{-1}g\ n\ g^{-1}a\ g = g^{-1}(g\ n\ g^{-1})^a g$$

Como $N \lhd G$, $gng^{-1} \in N$. Logo, $(gng^{-1})^a = gng^{-1}$.
Daí,

$$n^{g^{-1}ag} = g^{-1}(gng^{-1})g = n$$

$\therefore\ g^{-1}ag \in C_G(n),\ \forall n \in N$
$\therefore\ g^{-1}ag \in C_G(N)$
$\therefore\ g^{-1}C_G(N)g \leq C_G(N),\ \forall g \in G$

Voltemos agora *à* prova de (iii).
Sendo $\langle x^G \rangle \lhd G$, segue do que mostramos acima que $C_G(\langle x^G \rangle) \lhd G$.
Mas, por (i), $C_G(\langle x^G \rangle) = C_G(x^G)$. ■

A proposição a seguir, é uma caracterização dos FC-Grupos.

Proposição 2.9. *G é FC-Grupo* $\Leftrightarrow$ $\dfrac{G}{C_G(x^G)}$ *é finito para cada* $x \in G$.

Prova: $\Rightarrow$) Suponhamos G um FC-Grupo.
Dado $x \in G$, seja $x^G = \{x_1, ..., x_s\}$.
Então,

$$|\ G : C_G(x_i)\ | = |\ x_i^G\ | = |\ x^G\ | = s$$

E usando o corolário de Poincaré, temos:

$$|\ G : C_G(x^G)\ | = \left|\ G : \bigcap_{i=1}^{s} C_G(x_i) \right| \leq \prod_{i=1}^{s} |\ G : C_G(x_i)\ | < \infty$$

Isto é,

$$\frac{G}{C_G(x^G)} \text{ é finito.}$$

$\Leftarrow$) $\forall x \in G$ temos: $C_G(x^G) \leq C_G(x) \leq G$.

Logo,

$$|\ x^G\ | = |\ G : c_G(x)\ | \leq |\ G : C_G(x^G)\ | < \infty,\ \forall x \in G,$$

o que mostra que G é um FC-Grupo.

■

A seguir, apresentamos um resultado relativos a FC-elementos de um grupo que também nos será bastante útil no desenvolvimento deste trabalho.

Lema 2.10(*Dietzmann*). *Em qualquer grupo G um subconjunto normal finito constituído apenas por elementos de ordem finita, gera um subgrupo normal finito.*

Prova: Sejam $X = x_1, ..., x_n$ subconjunto normal de G e $N = \langle X \rangle$.
Afirmo que $N \lhd G$.
De fato, tomemos $g \in G$ qualquer e $g^{-1}ng \in g^{-1}Ng$.
Como $n \in N,\ n = x_1...x_n$, onde $x_i \in X,\ i = 1, ..., n$(já que $o(x_i) < \infty,\ \forall i$).
Daí,

$$\begin{aligned} g^{-1}n\ g &= g^{-1}\ .\ x_1\ .\ .\ .\ x_n\ .\ g \\ &= x_1^g\ .\ .\ .\ x_n^g \end{aligned}$$

Sendo X normal em G, $x_i \in X$ implica $x_i^g \in X$.
Logo, $g^{-1}n\ g \in N$ e temos $g^{-1}Ng \subset N,\ \forall g \in G$, o que prova nossa afirmação.
Tomemos arbitrariamente, $n \in N$.
Em geral, existem muitas formas de expressar n, entre elas algumas de menor comprimento(no que se refere ao produto de potências com mesma base), diga-
mos r.
Além disso, entre essas expressões de menor comprimento, existe uma que aparece primeiro na ordem lexicográfica(a ordem do dicionário). Esta é a ordem em que $(\alpha_1,\ .\ .\ .\ , \alpha_r)$ precede $(\alpha'_1,\ .\ .\ .\ , \alpha'_r)$ se $\alpha_i = \alpha'_i$ para $i < s$ e $\alpha_s < \alpha'_s$ para algum $s \leq r$.
Denote esta primeira expressão por $n = y_1\ .\ .\ .\ y_r$, onde $y_i = x_{\alpha_i}^{m_i}$.
Afirmo que $\alpha_1 <\ .\ .\ .\ \alpha_r$.

Suponhamos por absurdo que isso não ocorra.
Então, temos dois casos:

1° caso): $\alpha_i = \alpha_j$ para $i < j$.

$$\begin{aligned} n &= x_{\alpha_1^{m_1}}\ .\ .\ .\ x_{\alpha_i}^{m_i}\ .\ .\ .\ x_{\alpha_j}^{m_j}\ .\ .\ .\ x_{\alpha_r}^{m_r}\ =\ x_{\alpha_1^{m_1}}\ .\ .\ .\ x_{\alpha_i}^{m_i}\ .\ .\ .\ x_{\alpha_i}^{m_j}\ .\ .\ .\ x_{\alpha_r}^{m_r} \\ &=\ y_1\ .\ .\ .\ y_i\ .\ .\ .\ y_j\ .\ .\ .\ y_r \end{aligned}$$

Vamos reescrever n de modo a agrupar y_i e y_j :

$$\begin{aligned} n &= y_1\ .\ .\ .\ y_i(y_jy_j^{-1})y_{i+1}(y_jy_j^{-1})\ .\ .\ .\ (y_jy_j^{-1})y_{j-1}(y_jy_j^{-1})y_jy_{j+1}\ .\ .\ .\ y_r \\ &= y_1\ .\ .\ .\ (y_iy_j)\ y_{i+1}^{y_j}\ .\ .\ .\ y_{j-1}^{y_j}y_{j+1}\ .\ .\ .\ y_r \end{aligned}$$

Para j e l quaisquer, temos:

$$y_l^{y_j} = y_j^{-1} y_l y_j = y_j^{-1} x_{\alpha_l}^{m_l} y_j \;=\; y_j^{-1} \underbrace{x_{\alpha_l} \; . \; . \; . \; x_{\alpha_l}}_{m_l \; vezes} \; y_j \;=\; (x_{\alpha_l}^{y_j})^{m_l} \;=\; x_k^{m_l},$$

para algum $k \in \{1, \; . \; . \; . \; n\}$, já que X é normal em G.

Assim, o que vemos acima é uma nova expressão de n, com tamanho menor que r. Absurdo! Portanto, os $\alpha_i' s$ são todos distintos.

2° caso): $\alpha_i > \alpha_{i+1}$

$n = x_{\alpha_1}^{m_1} \; . \; . \; . \; x_{\alpha_i}^{m_i} \; x_{\alpha_{i+1}}^{m_{i+1}} \; . \; . \; . \; x_{\alpha_r}^{m_r} \;=\; y_1 \; . \; . \; . \; y_i \; y_{i+1} \; . \; . \; . \; y_r$

Vamos reescrever n de modo que y_{i+1} passe a ocupar a posição i:

$n = y_1 \; . \; . \; . \; y_{i+1} \; y_{i+1}^{-1} \; y_i \; y_{i+1} \; . \; . \; . \; y_r \;=\; y_1 \; . \; . \; . \; y_{i+1} \; y_i^{y_{i+1} \; . \; . \; . \; y_r}$

Como visto antes, $y_i^{y_{i+1}} = x_k^{m_i}$ para algum k.
Sendo $\alpha_i > \alpha_{i+1}$, esta nova expressão de n precede a anterior na ordem de n-uplas. Absurdo!
Em qualquer caso chegamos a uma contradição. Portanto, devemos ter, necessariamente, $\alpha_1 < \; . \; . \; . \; < \alpha_r$.
Neste caso, na expressão:

$$n = y_1 \; . \; . \; . \; y_r \;=\; x_{\alpha_1}^{m_1} \; . \; . \; . \; x_{\alpha_r}^{m_r},$$

temos $x_{\alpha_i} \in \langle x_i \rangle$, para cada i.

Daí, as possibilidades de expressarmos um elemento $n \in N$, são de, no máximo:

$$\prod_{i=1}^{n} o(x_i)$$

$\blacksquare$

Capítulo 3

Coberturas de Grupos

Uma cobertura de um grupo G é uma família $\{S_i\}_{i\in I}$ de subconjuntos de G tal que $G = \bigcup_{i\in I} S_i$. Se $\{H_i\}_{i\in I}$ é uma cobertura de G por subgrupos é natural perguntarmos que informações podem ser extraídas a cerca de G a partir das propriedades dos subgrupos $H_i's$. No caso geral não temos respostas satisfatórias, já que todo grupo pode ser coberto pelos subgrupos cíclicos gerados por seus elementos. Mas a situação muda se pedirmos que a cobertura seja finita. O primeiro resultado nessa direção é devido a Baer, o qual provou que G admite uma cobertura finita por subgrupos abelianos se, e somente se, este é central-por-finito. A parte não trivial desta afirmação é uma consequência imediata de um resultado posterior de B.H.Neumann. Antes de passarmos á prova destes dois importantes resultados vejamos o seguinte

Lema 3.1.(*Ramsey*) *Seja S um conjunto infinito e suponha que a família $[S]^2$ de subconjuntos de S de 2 elementos é expressa como uma união de n sub-famílias $[S]^2 = \Delta_1 \cup .... \cup \Delta_n$, onde n é finito. Então, existe um subconjunto infinito T de S e um k ($1 \leq k \leq n$) tal que $[T]^2 \subseteq \Delta_k$.*

Prova: Escolha um elemento $x_1 \in S$.
O conjunto $X_1 = \{\ \{x_1, x\}\ ;\ x \in S - \{x_1\}\ \}$ é infinito e está contido em $[S]^2$.
Como existem somente finitos Δ_i's, existe pelo menos um deles que contém uma infinidade de "elementos" de X_1, digamos Δ_{k_1}.
Chamemos de S_1 o subconjunto infinito de $S - \{x_1\}$ formado pelos x tais que

$$\{x_1, x\} \in \Delta_{k_1}$$

Agora escolhamos $x_2 \in S_1$.
Analogamente, $X_2 = \{\ \{x_2, x\}; x \in S_1 - \{x_2\}\ \}$ é subconjunto infinito de

$[S]^2 = \bigcup_{i=1}^{n} \Delta_i$.
Logo, $\exists k_2 \in \{1, ..., n\}$ tal que Δk_2 contém infinitos "elementos" de X_2.
Chamemos de S_2 o subconjunto infinito de $S_1 - \{x_2\}$ formado pelos x tais que:

$$\{x_2, x\} \in \Delta_{k_2}$$

Escolhendo $x_3 \in S_2$, encontramos analogamente, $k_3 \in \{1, ..., n\}$ e $S_3 \subset S_2 - \{x_3\}$ infinito tal que:

$$\{x_3, x\} \in \Delta_{k_3}, \ \forall x \in S_3$$

Continuando a construção obtemos um conjunto infinito de elementos $\{x_1, x_2, ..., ...\}$ e inteiros k_r, $1 \leq k_r \leq n$, tais que $\{x_r, x_s\} \in \Delta_{k_r}$ se $r < s$.
Como há somente um número finito de k_r's, existe um subconjunto infinito $\{x_{r_1}, x_{r_2}, ..., ...\}$ tal que $k_{r_1} = k_{r_2} = ... = k$, digamos. Este é o subconjunto infinito T que procurávamos, já que cada par $\{x_{r_s}, x_{r_t}\} \in \Delta_k$. ■

Agora já podemos provar o

Teorema 3.2(*Neumann*). *Suponha que o grupo G pode ser expresso como união de uma quantidade finita de classes* $G = \bigcup_{i=1}^{n} H_i g_i$. *Se* $H_j g_j \not\subseteq \bigcup_{i \neq j} H_i g_i$, *então* $| G : H_j |$ *é finito.*

Prova: Seja $g \in H_j g_j - \bigcup_{i \neq j} H_i g_i$
Então, $H_j g = H_j g_j$.

Daí, $g_j g^{-1} \in H_j$ e temos

$$\begin{aligned} G = Gg^{-1} &= (\bigcup_{i=1}^{n} H_i g_i) g^{-1} \\ &= H_j(g_j g^{-1}) \ \cup \ (\bigcup_{i \neq j} H_i(g_i g^{-1})) \\ &= H_j \cup (\bigcup_{i \neq j} H_i(g_i g^{-1})) \end{aligned}$$

Suponhamos por absurdo, $| G : H_j |$ infinito.

Seja $S = \{x_1, x_2, ...\}$ um transversal de H_j em G.

Então, $G = \dot{\bigcup\limits_{i}} H_j x_i$

Se $r < s$, então $H_j x_r \neq H_j x_s$ e portanto, $x_r x_s^{-1} \notin H_j$.

Como $G = H_j \cup (\bigcup\limits_{i \neq j} H_i(g_i g^{-1}))$, temos que $x_r x_s^{-1} \in H_l(g_l g^{-1})$ para algum $l \in \{1, ..., n\} \backslash \{j\}$.

Seja m o menor tal que $m \in \{1, ..., n\} \backslash \{j\}$ e $x_r x_s^{-1} \in H_m(g_m g^{-1})$.

Definamos os subconjuntos Δ_m de $[S]^2$ pondo:

$\Delta_m = \{\ \{x_r, x_s\}$; m é o menor com $m \in \{1, ..., n\} \backslash \{j\}$ e $x_r x_s^{-1} \in H_m(g_m g^{-1})\}$

Veja que

$$[S]^2 = \bigcup_{m \neq j} \Delta_m$$

Pelo Lema de Ramsey, existe um subconjunto infinito T de S e um $k \in \{1, ..., n\} \backslash \{j\}$ tal que $[T]^2 \subseteq \Delta_k$.

Sejam x_r, x_s, x_t três elementos de T com $r < s < t$.

$$\begin{aligned} \{\ x_r, x_s\} \in [T]^2 \Longrightarrow \{\ x_r, x_s\} \in \Delta_k &\Longrightarrow x_r x_s^{-1} \in H_k(g_k g^{-1}) \\ &\Longrightarrow H_k(x_r x_s^{-1}) = H_k(g_k g^{-1}) \\ &\Longrightarrow g_k g^{-1} \in H_k(x_r x_s^{-1}) \\ &\Longrightarrow g_k g^{-1}(x_r x_s^{-1})^{-1} \in H_k \\ &\therefore g_k g^{-1}(x_s x_r^{-1}) \in H_k \end{aligned}$$

Analogamente $g_k g^{-1} x_t x_s^{-1} \in H_k$ e $g_k g^{-1} x_t x_r^{-1} \in H_k$.

Note que:

$$(g_k g^{-1} x_s x_r^{-1})(g_k g^{-1} x_t x_r^{-1})^{-1}(g_k g^{-1} x_t x_s^{-1})$$

$$= (g_k g^{-1} x_s x_r^{-1})(x_r x_t^{-1} g g_k^{-1})(g_k g^{-1} x_t x_s^{-1}) \ = \ g_k\ g^{-1}$$

Daí, $g_k g^{-1} \in H_k$ e temos $g \in H_k g_k$.

Absurdo!

Portanto, $\mid G : H_j \mid$ é finito. ∎

Teorema 3.3(*Baer*). *$G = \bigcup_{i=1}^{n} H_i$, H_i's abelianos $\Longleftrightarrow$ $\dfrac{G}{Z(G)}$ é finito.*

Prova:
$\Rightarrow$)Podemos supor $|G : H_i| < \infty$, $\forall i$(por Neumann).
Como $\left| G : \bigcap_{i=1}^{n} H_i \right| \leq \mid G : H_1 \mid \ldots . \mid G : H_n \mid$, segue que $\left| G : \bigcap_{i=1}^{n} H_i \right| < \infty$
Afirmo que $\bigcap_{i=1}^{n} H_i \subset Z(G)$.
De fato, sejam $h \in \bigcap_{i=1}^{n} H_i$ e $g \in G = \bigcup_{i=1}^{n} H_i$ quaisquer.
Como $g \in G$, $\exists j \in \{1, ..., n\}$ tal que $g \in H_j$.
E sendo $h \in \bigcap_{i=1}^{n} H_i$, temos em particular $h \in H_j$.
Como H_j é abeliano, segue que hg = gh.

Logo, $h \in Z(G)$.

$\therefore \bigcap_{i=1}^{n} H_i \subset Z(G)$

Daí temos:

$$\left| G : \bigcap_{i=1}^{n} H_i \right| = \mid G : Z(G)| \left| Z(G) : \bigcap_{i=1}^{n} H_i \right|$$

Como $\left| G : \bigcap_{i=1}^{n} H_i \right| < \infty$, segue que $|G : Z(G)| < \infty$.

$$\begin{array}{c} G \\ | \\ Z(G) \\ | \\ \bigcap_{i=1}^{n} H_i \end{array}$$

$\Leftarrow$) Suponhamos agora $\dfrac{G}{Z(G)}$ finito.

Façamos $Z = Z(G)$ e $\dfrac{G}{Z(G)} = \{Z, t_1 Z, ..., t_n Z\}$, i.e. $\{t_0 = 1, t_1, ..., t_n\}$ é transversal de Z em G.

Então, $G = \dot{\bigcup_i} t_i Z$. Faça $H_i = \langle t_i, Z\rangle = \langle t_i \rangle$Z.

Assim, $t_i Z \subset H_i$ e portanto, $G = \bigcup_{i=0}^{n} H_i$, onde H_i é abeliano. ■

O Teorema de Neumann também pode ser aplicado para caracterizar grupos que podem ser cobertos por uma quantidade finita de subgrupos cíclicos como grupos que são finitos ou cíclicos. É o que mostra nosso próximo resultado.

Proposição 3.4. *Um grupo G possui cobertura finita por subgrupos cíclicos se, e somente se, G é finito ou cíclico.*

Para a demonstração desta proposição precisaremos do

Lema 3.5(*Fedorov*). *Seja G grupo infinito. Então, todo* $1 \neq H \leq G$ *tem índice finito se, e somente se,* $G \simeq C_\infty$*(cíclico infinito)*

Prova: $\Leftarrow$) Segue direto do Teorema dos grupos cíclicos.
$\Rightarrow$) Seja $1 \neq x \in G$. Como $1 \neq \langle x \rangle \leq G$ temos da hipótese que
$\mid G : \langle x \rangle \mid < \infty$.
Digamos que seja $\mid G : \langle x \rangle \mid = n$
Seja $\{ t_1, ..., t_n \}$ um transversal de $\langle x \rangle$ em G, com $t_i \neq 1$, $\forall i$.
Então, $G \ = \ \dot{\bigcup_i} \langle x \rangle t_i \ = \ \langle \ x, t_1, ..., t_n \ \rangle$
Também, $C = C_G(x) \supset \langle x \rangle$.

$\therefore \mid G : C_G(x) \mid \leq \mid G : \langle x \rangle \mid = \ n$

Analogamente, $\forall t_i \in \{ \ t_1, ..., t_n \ \}$, temos $1 \neq \langle t_i \rangle < G$ e $\langle t_i \rangle \subset C_G(t_i)$.

$$\begin{array}{c} G \\ | \\ C_G(t_i) \\ | \\ \langle t_i \rangle \end{array}$$

Logo

$$| G : C_G(t_i) | < | G : \langle t_i \rangle | < \infty, \ \forall i$$

Agora, sendo $Z(G) = \bigcap_{y \in \{x, t_i\}} C_G(y)$, segue de Poincaré que $| G : Z(G) | < \infty$ e portanto, G' é finito.
Afirmo que G é livre de torção(i.e., todo elemento, com exceção da identidade, tem ordem infinita)
De fato, se $\exists 1 \neq g \in G$ com $o(g) < \infty$, então teríamos:

$$| G | = | G : \langle \ g \ \rangle | \, | \langle \ g \ \rangle | < \infty$$

Absurdo !
Logo, devemos ter necessariamente, $G' = 1$.
Então, G é abeliano finitamente gerado e livre de torção.
Daí, $G = H_1 \times ... \times H_n$ com $H_i \simeq C_\infty$.
Afirmo que $n = 1$
De fato, se fosse $n > 1$, tomando $H = H_1 \times ... \times H_{n-1}$, teríamos:

$$\frac{G}{H} \simeq H_n$$

Logo, $| G : H | = | H_n | = \infty$. Absurdo!
Portanto, $n = 1$ e $G \simeq C_\infty$. ■

Prova da Proposição 3.4:

$\Rightarrow$) Seja $\{C_i\}_{i=1}^n$ uma cobertura de G por subgrupos cíclicos.
Suponhamos G infinito.
Pelo Teorema de Neumann podemos considerar $| G : C_i | < \infty$ para cada $i = 1, ..., n$.
Se para algum i tivéssemos $| C_i | < \infty$, então:

$$| G | = | G : C_i | \, | C_i | < \infty$$

Absurdo!
Então, podemos assumir todos os C_i's infinitos.
Afirmo que $\forall H < G \ ; \ H \neq 1$ tem-se $| G : H | < \infty$
De fato, seja $1 \neq g \in H \leq G$.
Como $G = \bigcup_{i=1}^n C_i$, temos que $g \in C_i$ para algum i

$\therefore \ \langle\ g\ \rangle \subset C_i$

$\therefore \mid C_i : \langle\ g\ \rangle \mid < \infty$ (pois cada C_i é cíclico)

Além disso,

$$\mid G : C_i \mid < \infty \quad \text{(por Neumann)}$$

$$\begin{tikzcd} G \arrow[d, dash] \\ C_i \arrow[d, dash] \\ \langle g \rangle \end{tikzcd}$$

Logo,

$$\mid G : \langle g \rangle \mid < \infty$$

Agora, $H \supset \langle g \rangle$.

$$\begin{tikzcd} G \arrow[d, dash] \\ H \arrow[d, dash] \\ \langle g \rangle \end{tikzcd}$$

Daí,

$$\mid G : H \mid \leq \mid G : \langle g \rangle \mid < \infty \ ,$$

como queríamos mostrar.

Sendo G infinito, segue de Fedorov que $G \simeq C_\infty$

$\Leftarrow$) Se G é cíclico tomamos a cobertura como sendo o próprio G.

Agora, se G for finito, digamos $G = \{x_1, ..., x_n\}$, então:

$$G \subset \langle x_1 \rangle \cup .... \cup \langle x_n \rangle \quad ,$$

o que conclui nossa demonstração. ■

Capítulo 4

Coberturas do conjunto dos comutadores de um grupo

Neste capítulo mostraremos nosso teorema principal:

Se G é um grupo no qual o conjunto dos comutadores pode ser coberto por um número finito de subgrupos cíclicos então G' é finito ou cíclico. Ou seja, G' também pode ser coberto por um número finito de subgrupos cíclicos.

No que segue, $\mathcal{C}$ denota a família finita de subgrupos cíclicos de G cobrindo todos os comutadores. Para simplificar a prova do Teorema Principal, fazemos duas suposições.

Suposição 1. Todos os subgrupos em $\mathcal{C}$ são gerados por comutadores, ademais por um número finito deles (não necessariamente por um único comutador). Como consequência, $G' = \langle C; C \in \mathcal{C} \rangle$.

De fato, fazendo X $= \{ \ [\ a, b\ ]\ ;\ a, b \in G\ \}$, temos X $\subset \bigcup_{C \in\ \mathcal{C}} C$.

Daí,

$$X \ = \ X \ \cap \ \left(\ \bigcup_{C\in\mathcal{C}} C \ \right) \ = \bigcup_{C\in\mathcal{C}} (\ X \ \cap \ C \ ) \subset \bigcup_{C\in\mathcal{C}} \langle \ X \ \cap \ C \ \rangle$$

Então, podemos substituir cada $C \in \mathcal{C}$ pelo subgrupo gerado pelos comutadores em C e ainda teremos uma cobertura para X.
Como cada C é cíclico e $\langle\ X \cap C\ \rangle$ é subgrupo de C temos que cada $\langle\ X \cap C\ \rangle$ também é cíclico.
Além disso, se $A = X \cap C$ e $\langle\ X \cap C\ \rangle = \langle\ g_c\ \rangle$, então:

$\langle g_c \rangle = \langle\ X \cap C\ \rangle \ = \ \langle\ A\ \rangle = \{\ a_1^{e_1} ...... a_n^{e_n}\ ;\ a_i \in A\ ,\ e_i = \pm 1\ \}$

$$
\begin{aligned}
g_c \in \langle A \rangle \;\Rightarrow\; & g_c = a_{j_1}^{l_1}......a_{j_n}^{l_n} \;;\; a_{j_i} \in A \;\; e \;\; l_i = \pm 1 \\
& \Rightarrow g_c \in \langle a_{j_1}, ..., a_{j_n} \rangle \\
& \Rightarrow \langle X \cap C \rangle = \langle g_c \rangle \subset \langle a_{j_1}......a_{j_n} \rangle \subset \langle A \rangle = \langle X \cap C \rangle
\end{aligned}
$$

$\therefore \; \langle X \cap C \rangle = \langle a_{j_1}, ..., a_{j_n} \rangle$

Portanto, substituíndo cada $C \in \mathcal{C}$ por $\langle X \cap C \rangle$ temos que $\{\langle X \cap C \rangle\}_{C \in \mathcal{C}}$ é família de subgrupos cíclicos de G cobrindo X, onde cada $\langle X \cap C \rangle$ é gerado por um número finito de comutadores(não necessariamente um único), o que justifica nossa suposição.

Suposição 2. O grupo G é finitamente gerado

Para cada $C \in \mathcal{C}$ seja X_C o conjunto finito de comutadores que gera C.

$$X \subset \bigcup_{C \in \mathcal{C}} C \;\Rightarrow\; G' = \langle X \rangle \;\subset\; \langle \bigcup_{C \in \mathcal{C}} C \rangle = \langle C \;;\; C \in \mathcal{C} \rangle$$

Também,

$$X_C \subset X \;\Rightarrow\; C = \langle X_C \rangle \subset \langle X \rangle = G', \text{ para cada } C \in \mathcal{C}$$

Logo,

$$\langle C \;;\; C \in \mathcal{C} \rangle \;\subset G'$$

Portanto,

$$G' = \langle C \;;\; C \in \mathcal{C} \rangle$$

Agora, sendo $C = \langle X_C \rangle$, segue que:

$$G' = \langle C; C \in \mathcal{C} \rangle = \langle X_C; C \in \mathcal{C} \rangle = \langle \bigcup_{C \in \mathcal{C}} X_C \rangle$$

Consideremos $H = \langle \, a, b \;;\; [\, a, b \,] \in \bigcup_{C \in \mathcal{C}} X_C \, \rangle$.

Como cada X_C é finito, $\bigcup_{C \in \mathcal{C}} X_C$ é finito. Logo, H é finitamente gerado.

Afirmo que $H' = G'$.

De fato,

$$H \subset G \Rightarrow H' \subset G'$$

Além disso,

$$[\ a, b\ ] \in \bigcup_{C \in\ \mathcal{C}} X_C \ \Rightarrow\ a, b \in H\ \Rightarrow\ [\ a, b\ ] \in H'$$

$$\therefore\ \bigcup_{C \in\ \mathcal{C}} X_C \subset H'$$

$$\therefore\ G' = \langle \bigcup_{C \in\ \mathcal{C}} X_C\ \rangle \subset H'$$

$$\therefore\ H' = G'$$

Dados $c, d \in H$ quaisquer, $[\ c, d\ ] \in X$.

Logo,

$$Y = \{\ [\ c, d\ ]\ ;\ c, d \in H\ \}\ \subset\ X\ \subset\ \bigcup_{C\ \in\ \mathcal{C}} C$$

Daí,

$$Y\ \subset\ \bigcup_{C\ \in\ \mathcal{C}} (C \cap Y)\ \subset\ \bigcup_{C\ \in\ \mathcal{C}} \langle\ C \cap Y\ \rangle$$

I.e., o conjunto de todos os comutadores de H pode ser coberto pela família $\{\langle C \cap Y \rangle\}_{C \in\ \mathcal{C}}$ de subgrupos cíclicos de H.
Suponhamos o Teorema provado para grupos finitamente gerados.
Então, se G é um grupo infinitamente gerado, podemos exibir H $\leq$ G como acima e teremos H finitamente gerado e satisfazendo a hipótese do Teorema.
Logo, H' é cíclico ou finito. Mas $H' = G'$.
Daí, G' é cíclico ou finito.

4.1 Grupos sem comutadores não triviais de ordem finita

Em toda esta seção, G denota um grupo no qual o conjunto dos comutadores é coberto por uma família finita $\mathcal{C}$ de subgrupos cíclicos, e na qual todos os comutadores não triviais são de ordem infinita. Como uma consequência, todos os subgrupos em $\mathcal{C}$ são cíclicos infinitos. Nosso objetivo é provar que G' é cíclico-por-finito.

Definimos uma relação "$\sim$" sobre o conjunto $\mathcal{C}$ significando a seguinte regra:

$$C \sim D \text{ se, e somente se } C \cap D \neq 1$$

Veja que

(i) $C \sim C$, pois $C \cap C = C \neq 1$
(ii) $C \sim D \;\Rightarrow\; D \sim C$, já que $C \cap D = D \cap C$
(iii) $C \sim D$, $D \sim E \;\Rightarrow\; C \sim E$

De fato, sejam $C = \langle\ c\ \rangle,\ \ D = \langle\ d\ \rangle$ e $E = \langle\ e\ \rangle$.

$C \sim D \;\Rightarrow\; C \cap D \neq 1 \;\Rightarrow\; \exists\ c^i = d^j \neq 1$
$D \sim E \;\Rightarrow\; D \cap E \neq 1 \;\Rightarrow\; \exists\ d^m = e^n \neq 1$

Seja $k = mmc(j, m)$. Então, $j, m \mid k$ e temos:

$g = (c^i)^{\frac{k}{j}} = (d^j)^{\frac{k}{j}} = d^k = (d^m)^{\frac{k}{m}} = (e^n)^{\frac{k}{m}} \in C \cap D \cap E \subset C \cap E$

Como $c^i, d^m \neq 1$ e os subgrupos $C = \langle c \rangle$ e $D = \langle d \rangle$ são infinitos, segue que $g \neq 1$.

$\therefore C \cap E \neq 1$
$\therefore C \sim E$

Portanto, "$\sim$" é uma relação de equivalência.

Sejam $C_1, ..., C_n$ as classes de equivalência correspondentes.

Defina $R_i = \langle C; C \in C_i \rangle$ e $S_i = \bigcap\limits_{C \in C_i} C$ para cada i.
Sobre R_i e S_i temos:

1. $G' = \langle R_1, ..., R_n \rangle$

De fato,

$$G' = \langle C; C \in \mathcal{C} \rangle = \langle C; C \in \bigcup_{i=1}^{n} C_i \rangle = \langle C_1, ..., C_n \rangle = \langle R_1, ..., R_n \rangle$$

2. $S_i \neq 1, \forall i = 1, ..., n$

Mostraremos por indução que a interseção de quaisquer k "elementos" de C_i é não trivial.

i)Vale para $k = 2$.

$C_{i1}, C_{i2} \in C_i \;\Rightarrow\; C_{i1} \sim C_{i2} \;\Rightarrow\; C_{i1} \cap C_{i2} \neq 1$

ii)Vale para $k \Rightarrow$ Vale para $k+1$

Sejam $C_{i1}, C_{i2}, ..., C_{ik}, C_{i(k+1)} \in C_i$ com $C_{ij} = \langle\, c_j \,\rangle$ para cada $j = 1, ..., k+1$.
Pela hipótese de indução, temos que $C_{i1} \cap C_{i2} \cap ... \cap C_{ik} \neq 1$.
E como $C_{ik} \sim C_{i(k+1)}$, também temos $C_{ik} \cap C_{i(k+1)} \neq 1$
Então, existem inteiros $\alpha_1, ..., \alpha_k, \beta_k, \beta_{k+1}$ tais que:

$$c_1^{\alpha_1} = c_2^{\alpha_2} = ... = c_k^{\alpha_k} \neq 1$$
$$c_k^{\beta_k} = c_{k+1}^{\beta_{k+1}} \neq 1$$

Seja $l = mmc(\alpha_k, \beta_k)$.
Então, $\alpha_k, \beta_k \mid l$ e temos:

$$h = (c_1^{\alpha_1})^{\frac{l}{\alpha_k}} = (c_2^{\alpha_2})^{\frac{l}{\alpha_k}} = ... = (c_k^{\alpha_k})^{\frac{l}{\alpha_k}} = c_k^l = (c_k^{\beta_k})^{\frac{l}{\beta_k}} = (c_{k+1}^{\beta_{k+1}})^{\frac{l}{\beta_k}}$$

Veja que $h \in C_{i1} \cap C_{i2} \cap ... \cap C_{ik} \cap C_{i(k+1)}$
Como $c_i^{\alpha_i}, c_j^{\beta j} \neq 1$ e os C_{ij}'s são infinitos, segue que $h \neq 1$
Logo, $C_{i1} \cap C_{i2} \cap ... \cap C_{ik} \cap C_{i(k+1)} \neq 1$

3. $\mid C : S_i \mid < \infty$, para cada $C \in C_i$ e S_i é cíclico infinito.

Sendo $S_i = \bigcap\limits_{C \in C_i} C, \;\; S_i \leq G \;$ e $\; S_i \subset C, \forall C \in C_i$. Daí, $S_i \leq C, \forall C \in C_i$.
Como $S_i \neq 1$ e cada C é cíclico infinito, S_i é também cíclico infinito.
Além disso, do fato de que $1 \neq S_i \leq C,\; \forall C \in C_i$ temos que $\mid C : S_i \mid < \infty$, $\forall C \in C_i$(Teorema dos grupos cíclicos).

4. $S_i \cap S_j = 1$ para $i \neq j\;$ e $\;S_i$ é central em R_i.

Seja $a \in S_i \cap S_j$ qualquer com $i \neq j$.
Então, $a \in C \cap D, \forall C \in C_i\;$ e $\;\forall D \in C_j$.
Como $i \neq j$, $C \cap D = 1$.
Logo, $a = 1$.
$\therefore S_i \cap S_j = \{1\}$

Veja que

$$S_i \;\subset\; C \;\subset\; \langle\; C \;;\; C \in C_i \;\rangle = R_i,\; \forall i = 1, ..., n$$

Como $S_i \leq C, \forall C \in C_i$ e os C's são cíclicos(portanto abelianos), temos que os elementos de S_i comutam com os elementos de C qualquer que seja $C \in C_i$. Em particular, os elementos de S_i comutam com todos os elementos de R_i.

Denotemos por X_i o conjunto de todos os comutadores não triviais nos subgrupos $C \in C_i$.

Proposição 4.1. *Os conjuntos $X_1, ..., X_n$ são dois a dois disjuntos, e $\{X_1, ..., X_n\}$ é invariante com respeito a conjugação por elementos de G. Além disso,* $X_i^g = X_i$ *para todo* $g \in R_i$.

Prova : Defina sobre o conjunto X^* dos comutadores não triviais de G, a seguinte relação:

$$u \approx v \text{ se, e somente se, } \langle u \rangle \cap \langle v \rangle \neq 1$$

Com um raciocínio análogo ao que fizemos para "$\sim$" podemos mostrar que "$\approx$" é relação de equivalência sobre X^*.

Sejam $u \in C$ e $v \in D$ com $C, D \in \mathcal{C}$.

É claro que

$$u \approx v \;\Leftrightarrow\; \langle u \rangle \cap \langle v \rangle \neq 1 \;\Leftrightarrow\; C \cap D \neq 1$$

Para ver que $C \cap D \neq 1 \Rightarrow \langle u \rangle \cap \langle v \rangle \neq 1$, seja $C = \langle c \rangle$ e $D = \langle d \rangle$.
Como $u \in C$ e $v \in D$, temos que $u = c^m$ e $v = d^n$, com $m, n \in \mathbb{Z}$.

$$\begin{aligned} C \cap D \neq 1 \;\Rightarrow\; \exists\, c^k = d^l \neq 1 \;&\Rightarrow\; (c^k)^{mn} = (d^l)^{mn} \neq 1 \\ &\Rightarrow\; (c^m)^{kn} = (d^n)^{lm} \neq 1 \\ &\Rightarrow\; \langle u \rangle \cap \langle v \rangle \neq 1 \end{aligned}$$

Assim, dado $u \in C$ com $C \in C_i$, temos:

$$\begin{aligned} \overline{u} = \{\; v \in X^* \;;\; v \approx u \;\} &= \{\; v \in X^* \;;\; \langle u \rangle \cap \langle v \rangle \neq 1\} \\ &= \{\; v \in X^* \;;\; v \in D \text{ com } C \cap D \neq 1\} \\ &= \{\; v \in X^* \;;\; v \in D \text{ com } C \sim D\} \\ &= \{\; v \in X^* \;;\; v \in D \text{ com } D \in C_i\} \\ &= X_i \end{aligned}$$

Portanto, as classes de equivalência com respeito a relação "$\approx$" são: $X_1, ..., X_n$ e os X_i's são dois a dois disjuntos.
Fixado $i \in \{1, ..., n\}$ e $g \in G$ qualquer mostraremos que $X_i^g = X_j$ para algum j. O que equivale a mostrar que X_i^g é classe de equivalência com respeito a relação "$\approx$".
Então, dados $u, v \in X_i^g$ devemos provar que $u \approx v$.

$$
\begin{aligned}
u, v \in g^{-1}X_i\ g\ &\Rightarrow\ \exists_{(m)} a, b \in X_i\ ;\ u = g^{-1}a\ g\ ,\ v = g^{-1}b\ g \\
&\Rightarrow\ a \approx b \\
&\Rightarrow \langle a \rangle \cap \langle b \rangle \neq 1 \\
&\Rightarrow\ g^{-1}a^m\ g = g^{-1}b^n\ g \neq 1 \\
&\Rightarrow\ (g^{-1}a\ g)^m = (g^{-1}b\ g)^n \neq 1,\ \ \exists m, n \\
&\Rightarrow\ u^m = v^n \neq 1 \\
&\Rightarrow \langle u \rangle \cap \langle v \rangle \neq 1 \\
&\Rightarrow\ u \approx v
\end{aligned}
$$

$\therefore\ X_i^g = X_j$ para algum $j \in 1, ..., n$

Logo, $\{X_1, ..., X_n\}$ é invariante com respeito a conjugação por elementos de G.
Finalmente, mostraremos que $X_i^g = X_i,\ \forall g \in R_i$.
Como cada $C \in \mathcal{C}$ é gerado pelos comutadores não triviais de G que estão nele, temos para cada i:

$$R_i = \langle C; C \in C_i \rangle = \langle X_i \rangle = \langle x_1...x_m; x_j \in X_i \cup X_i^{-1} \rangle$$

Tomemos $g \in X_i$, com $g \neq 1$. Então, $g \in X_i^g \cap X_i$.
Pelo que vimos acima, $X_i^g = X_j$ para algum j.
Daí, $X_j \cap X_i \neq \emptyset$ e temos $X_i = X_j = X_i^g$.
Agora, se $g \in X_i^{-1}$, então $g^{-1} \in X_i$ e temos $g^{-1} \in X_i^g \cap X_i = X_l \cap X_i$.
$\therefore\ X_l \cap X_i \neq \emptyset$
$\therefore\ X_i = X_l$
$\therefore\ X_i = X_i^g$
Assim,

$$X_i^g = X_i, \forall g \in X_i \cup X_i^{-1}$$

Agora, seja $g \in R_i$ qualquer.
Como $R_i = \langle\ X_i\ \rangle$, $g = x_1....x_m$ com $x_j \in X_i \cup X_i^{-1}$.
Daí,

$$
\begin{aligned}
X_i^g\ &=\ X_i^{x_1....x_m}\ =\ (X_i^{x_1})^{x_2...x_m}\ =\ X_1^{x_2....x_m} \\
&=\ (X_i^{x_2})^{x_3....x_m}\ =\ X_i^{x_3....x_m}\ =\ .\ .\ .\ =\ X_i^{x_m}\ =\ X_i,
\end{aligned}
$$

o que conclui nossa prova. ■

Proposição 4.2. *O conjunto $\{R_1, ..., R_n\}$ é invariante com respeito a conjugação por elementos de G. Desse modo, $\mid G : N_G(R_i) \mid$ é finito para todo $i = 1, ..., n$.*

Prova: $R_i = \langle X_i \rangle = \{x_1 ... x_n; x_j \in X_i \cup X_i^{-1}\}$
Seja $g \in G$ qualquer.
Pela proposição anterior, temos que $X_i^g = X_l$ para algum l.
Afirmo que $(X_i^{-1})^g = X_l^{-1}$.
De fato,

$$\begin{aligned} x_k \in X_i^{-1} &\Leftrightarrow x_k^{-1} \in X_i \Leftrightarrow (x_k^{-1})^g = x_l \text{ para algum } x_l \in X_l \\ &\Leftrightarrow x_k^g = x_l^{-1} \in X_l^{-1} \end{aligned}$$

Daí, temos:

$$\begin{aligned} R_i^g &= \{\ x_1^g ....x_k^g\ ;\ x_j \in X_i \cup X_i^{-1}\} \\ &= \{\ x_{l_1} ....x_{l_n}\ ;\ x_{l_j} \in X_l \cup X_l^{-1}\} \\ &= \langle X_l \rangle \\ &= R_l \end{aligned}$$

Assim, $\{\ g^{-1} R_i\ g\ ;\ g \in G\ \}$ é finito para cada i.
Como $|\ \{R_i^g\ ;\ g \in G\}\ | = |\ G : N_G(R_i)\ |$, o resultado segue. ■

Proposição 4.3. *Cada um dos subgrupos R_i é cíclico-por-finito.*

Prova: Fixemos $i \in \{1, ..., n\}$
Devemos mostrar que $\exists N_i \trianglelefteq R_i$ tal que N_i é cíclico e $\dfrac{R_i}{N_i}$ é finito.
Tome $N_i = S_i$
Como visto antes, S_i é cíclico.
Além disso, do fato de que S_i é central em R_i temos que $S_i \trianglelefteq R_i$.
Então, basta mostrarmos que $\dfrac{R_i}{S_i}$ é finito.
Veja que

(1) $\dfrac{R_i}{S_i} = \langle \overline{X}_i \rangle$, onde $\overline{X}_i = \{xS_i; x \in X_i\}$

De fato,

$$\begin{aligned} \frac{R_i}{S_i} &= \{rS_i\ ;\ r \in R_i\} \\ &= \{rS_i\ ;\ r \in \langle X_i \rangle\} \\ &= \{(x_1 ....x_m)S_i\ ;\ x_j \in X_i \cup X_i^{-1}\} \\ &= \{(x_1 S_i)(x_2 S_i)....(x_m S_i)\ ;\ x_j \in X_i \cup X_i^{-1}\} \\ &= \{y_1 ....y_m\ ;\ y_l \in \overline{X}_i \cup \overline{X}_i^{-1}\} \\ &= \langle\ \overline{X}_i\ \rangle \end{aligned}$$

(2) $\overline{X_i}$ é normal em $\dfrac{R_i}{S_i}$

Dado $g = rS_i \in \dfrac{R_i}{S_i}$ qualquer mostraremos que $\overline{X_i}^{\ g} = \overline{X_i}$.

De fato, seja $xS_i \in \overline{X_i}$ arbitrário.

$(xS_i)^g = g^{-1}(xS_i)\ g = (rS_i)^{-1}(xS_i)(rS_i) = (r^{-1}S_i)(xS_i)(rS_i) = (r^{-1}x\ r)S_i$

Da proposição 4.1 temos que X_i é normal em R_i. Logo, $r^{-1}x\ r = x_i \in X_i$.

Daí, $(xS_i)^g = x_iS_i \in \overline{X_i}$.

Portanto, $\overline{X_i}^{\ g} \subset \overline{X_i}$ e $\overline{X_i}$ é normal em $\dfrac{R_i}{S_i}$.

Por outro lado, $\overline{X_i} \subset \bigcup_{C \in C_i} \left(\dfrac{C}{S_i}\right)$ e como vimos, cada $\dfrac{C}{S_i}$ tem ordem finita.

Como existem somente finitos $C's$ em C_i, $\bigcup_{C \in C_i} \left(\dfrac{C}{S_i}\right)$ é conjunto finito e portanto, $\overline{X_i}$ é conjunto finito consistindo de elementos de ordem finita.

Segue então de Dietzmann que $\langle \overline{X_i} \rangle = R_i/S_i$ é finito e, portanto, R_i é cíclico-por-finito para cada i. ■

Seja $K = \bigcap_{i=1}^{n} N_G(R_i)$

Sabemos da Proposição 4.2 que $\mid G : N_G(R_i) \mid < \infty$ para cada i.

Logo, $\mid G : \bigcap_{i=1}^{n} N_G(R_i) \mid = \mid G : K \mid < \infty$ também.(Poincaré)

Além disso, $K \lhd G$.

De fato, dados $g \in G$ e $k^g \in K^g$ quaisquer, temos:

$$\begin{aligned}
{R_i}^{k^g} &= R_i^{\ g^{-1}k\ g} = (g^{-1}k\ g)^{-1}R_i\ (g^{-1}k\ g)\\
&= g^{-1}k^{-1}\ g\ R_i\ g^{-1}\ k\ g\\
&= g^{-1}k^{-1}(R_i^{g^{-1}})\ k\ g\\
&= g^{-1}k^{-1}R_j\ k\ g\\
&= g^{-1}R_jg\\
&= R_i
\end{aligned}$$

$\therefore k^g \in N_G(R_i)$, $\forall i$
$\therefore k^g \in K$
$\therefore K^g \subset K$, $\forall g \in G$
$\therefore K \lhd G$

Vimos na última proposição que $\mid R_i : S_i \mid < \infty$, $\forall i$.
Seja $\mid R_i : S_i \mid = m_i$ para cada i e $m = mmc(m_1, ..., m_n, \mid G : K \mid)$
Defina $T_i = R_i^m = \langle\ x^m\ ;\ x \in R_i\ \rangle$.

Sobre T_i temos o seguinte:

- T_i é cíclico infinito

Como $m_i \mid m$, $\forall i$ temos que $(r_i S_i)^m = S_i$, $\forall r_i \in R_i$.
Daí, dado r_i^m com $r_i \in R_i$ qualquer, temos:

$$r_i^m S_i = (r_i S_i)^m = S_i$$
$$\therefore r_i^m \in S_i$$
$$\therefore T_i = \langle\ r_i^m\ ;\ r_i \in R_i\ \rangle \leq S_i$$

Como S_i é cíclico, T_i também o é.
Além disso, não podemos ter $T_i = 1$, pois neste caso, teríamos $r_i^m = 1, \forall r_i \in R_i$, o que contradiz o fato de que cada R_i é gerado pelos $C \in C_i$ e $C \simeq C_\infty$.
Logo, T_i é cíclico infinito para cada i.

- $T_i \trianglelefteq K$, $\forall i$

Primeiro vejamos que $T_i \leq K$.
Como $\mid G : K \mid$ divide m, $(gK)^m = K$, $\forall g \in G$.
Em particular,

$$g^m K = K,\ \forall g \in R_i$$
$$\therefore g^m \in K,\ \forall g \in R_i$$
$$\therefore T_i = R_i^m \leq K$$

Como $T_i \leq S_i \leq Z(R_i)$ segue que $T_i \trianglelefteq R_i$.

Além disso, dados $\alpha \in AutR_i$ e $g = x_1^m ... x_k^m \in T_i$ qualquer, temos:

$$\begin{aligned} \alpha(g) \ = \ \alpha(x_1^m ... \ x_k^m) \ &= \ \alpha(x_1)^m ... \ \alpha(x_k)^m \\ &= \ \beta_1^m ... \ \beta_k^m \ , \ \beta_i \in R_i \end{aligned}$$

$\therefore\ \alpha(g) \in T_i$
$\therefore\ \alpha(T_i) \leq T_i$

Agora,

$$\alpha(T_i) \leq T_i \Rightarrow T_i = \alpha^{-1}(\alpha(T_i)) \leq \alpha(T_i) \Rightarrow T_i \leq \alpha(T_i) \leq T_i$$

$\therefore \alpha(T_i) = T_i$

$\therefore\ T_i \ \trianglelefteq_{car} R_i$

É claro da definição de K, que K normaliza cada R_i.

Logo, K normaliza R_i, $\forall i$.
Como já sabemos que $T_i \leq K$, segue que $T_i \trianglelefteq K$.

Agora, seja $T = \langle\ T_1, ..., T_n\ \rangle$

Sobre T assim definido, temos:

- $T_i \trianglelefteq T$, $\forall i$

De fato, $T_i \leq K = \displaystyle\bigcap_{j=1}^{n} N_G(R_j)$.
$\therefore\ T_i \leq N_G(R_j)$, $\forall j$.
$\therefore\ \langle\ T_1, ..., T_n\ \rangle \leq N_G(R_j)$, $\forall j$
$\therefore\ R_j^t = R_j$, $\forall t \in T$ e $j = 1, ..., n$.

Assim, dados $t \in T$ e $g = x_1^m ... x_k^m \in T_i$ quaisquer, temos:

$$\begin{aligned} g^t &= (x_1^m ... x_k^m)^t = (x_1^m)^t ... (x_k^m)^t \\ &= (x_1^t)^m ... (x_k^t)^m \\ &= y_1^m ... y_k^m \ , \text{ com } y_i \in R_i \text{ para cada i} \end{aligned}$$

$\therefore\ g^t \in R_i^m = T_i$
$\therefore\ T_i^t \subset T_i$, $\forall t \in T$
$\therefore T_i \trianglelefteq T$, $\forall i$

- T é grupo abeliano finitamente gerado.

Seja $T_i = \langle a_i \rangle$ para cada i.
Então, $T = \langle\ T_1, ..., T_n\ \rangle = \langle\ a_1, ..., a_n\ \rangle$

Como os T_i's são normais em T, dados $T_i = \langle a_i \rangle$ e $T_j = \langle a_j \rangle$ com $i \neq j$ temos:
$a_i^{-1} a_j a_i a_j^{-1} \in T_i \cap T_j \leq S_i \cap S_j = 1$.
$\therefore a_i^{-1} a_j a_i a_j^{-1} = 1$
$\therefore a_i a_j = a_j a_i$
Portanto, T é abeliano finitamente gerado.

- $T \trianglelefteq G$

Sabemos da Proposição 4.2 que o conjunto $\{R_1, ..., R_n\}$ é invariante com respeito a conjugação por elementos de G.
Assim, para cada $i = 1, ..., n$ e $g \in G$ qualquer, temos:

$$\begin{aligned} T_i^g = (R_i^m)^g &= \langle\ x^m\ ;\ x \in R_i\ \rangle^g \\ &= \langle\ (x^g)^m\ ;\ x \in R_i\ \rangle \\ &= \langle\ y^m\ ;\ y \in R_i^g\ \rangle \\ &= \langle\ y^m\ ;\ y \in R_j\ \rangle \text{ (para algum } j = 1, ..., n) \\ &= R_j^m \\ &= T_j \end{aligned}$$

Logo, o conjunto $\{T_1, ..., T_n\}$ é invariante por conjugação sobre G.
Daí, $\forall g \in G$, temos:

$$T^g = \langle\ T_1^g, ..., T_n^g\ \rangle\ \subset\ \langle\ T_1, ..., T_n\ \rangle = T$$

$$\therefore T \trianglelefteq G$$

Suponha que u é um elemento em um dos subgrupos $R_i = \langle\ X_i\ \rangle$, por exemplo, um comutador em X_i. Se acontecer que $u \in T = T_1\ ...\ T_n$, podemos esperar que $u \in T_i$. Mas não é claro que vale esta propriedade, pois a princípio é possível que $T_1 ... T_{i-1} T_{i+1} ... T_n$ possua algum elemento em comum com $R_i \backslash T_i$. Na proposição a seguir mostramos de que forma isto pode ser fixado.

Proposição 4.4. *Existe um inteiro $l \geqslant 1$ com a seguinte propriedade: Se $u \in T^l$ é um elemento em R_i, então $u \in T_i$, qualquer que seja i.*

Para a prova desta proposição usaremos o seguinte

Resultado: *Se G é grupo abeliano finitamente gerado, então* $\bigcap\limits_{l \geqslant 1} G^l = 1$.

Prova: Segue do Teorema Fundamental dos G.A.F.G que

$$G \;=\; C_1 \times ... \times C_n \times C_{n+1} \times ... \times C_m$$

onde $C_i = \langle \alpha_i \rangle$, $o(\alpha_i) = k_i$ para $i = 1, ..., n$ e $C_j \simeq C_\infty$ para $j = n+1, ..., m$.

Tomando $k = k_1 ... \, k_n$ e $g \in G$ qualquer, temos:

$$G^k \;\; = \langle \; g^k \; ; \; g \in G \; \rangle \;=\; \langle \; (\alpha_1^{l_1} ... \alpha_n^{l_n} ... \alpha_m^{l_m})^k \; ; \; l_i \in \mathbf{Z}_+ \; \rangle$$

$$= \langle \; \alpha_{n+1}^{l_{n+1}k} ... \alpha_m^{l_m k} \; ; \; l_i \in \mathbf{Z}_+ \; \rangle$$

$$G^{2k} = \langle \; \alpha_{n+1}^{2l_{n+1}k} ... \alpha_m^{2l_m k} \; ; \; l_i \in \mathbf{Z}_+ \; \rangle$$

Dado $g \in \bigcap\limits_{l \geqslant 1} G^l$ temos que $g \in G^k \cap G^{2k}$.
Daí, se $g \neq 1$ podemos escrever:

$$g \;=\; \alpha_{n+1}^{r_1} ... \alpha_m^{r_m} \;=\; \alpha_{n+1}^{s_1} ... \alpha_m^{s_m} \quad ,$$

com $r_i > s_i$ para algum i(se não for $r_i > s_i$ para todo i, para os demais índices tem-se $r_j = s_j = 0$)

Isto nos dá:

$$\alpha_i^{r_i - s_i} \in C_i \;\cap\; C_1 \; ... \; C_{i-1} \; \widehat{C_i} \; C_{i+1} \; ... \; C_m \;=\; 1 \quad ,$$

com $i \in \{n+1, ... \; m\}$.

$\therefore \;\; \alpha_i^{r_i - s_i} = 1$

$o(\alpha_i) < \infty$

Mas isto contradiz o fato de que $C_i = \langle \; \alpha_i \; \rangle$ é infinito para cada
$i = n+1, ..., m$.

$\therefore \;\; \nexists g \in \bigcap\limits_{l \geq 1} G^l$ com $g \neq 1$

$\therefore \;\; \bigcap\limits_{l \geq 1} G^l \;=\; 1$

$\blacksquare$

Prova da Proposição :

É suficiente mostrarmos que existe tal l para cada i.
De fato, se para cada i exibirmos $l_i \geq 1$ inteiro satisfazendo a propriedade desejada, então tomando $l = mmc(l_1, ..., l_n)$ teremos:

$$\begin{aligned} u \in T^l \ , \ u \in R_i \ &\Rightarrow \ u \in (T^{l_i})^{\frac{l}{l_i}} \leq T^{l_i} \ , \ u \in R_i \\ &\Rightarrow \ u \in T_i \end{aligned}$$

Seja Y_i um transversal *à* esquerda de T_i em R_i, e suponha $1 \in Y_i$.
Então, $R_i = \dot{\bigcup\limits_{y \in Y_i}} yT_i$ e $\nexists y_i \in Y_i\{1\}$ com $y \in T_i$.
Como $T_i \leq S_i$ o qual é cíclico e $T_i \neq 1$ temos que $\mid S_i : T_i \mid < \infty$.

Logo,

$$\mid Y_i \mid = \mid R_i : T_i \mid = \mid R_i : S_i \ \mid \mid S_i : T_i \mid < \infty$$

Note que que $R_i = Y_i T_i$.
Sendo T abeliano finitamente gerado, temos que para cada i, $\dfrac{T}{T_i}$ também é abeliano finitamente gerado.
Assim, segue do resultado mostrado acima que $\bigcap\limits_{k \geq 1} \left(\dfrac{T}{T_i} \right)^k = T_i$.

Mas , $$\bigcap_{k \geq 1} \left(\frac{T}{T_i} \right)^k = \bigcap_{k \geq 1} \left(\frac{T^k T_i}{T_i} \right) = \frac{\bigcap\limits_{k \geq 1} (T^k T_i)}{T_i} \ .$$

$$\therefore \ \frac{\bigcap\limits_{k \geq 1} (T^k T_i)}{T_i} \ = \ T_i$$

$$\therefore \ \bigcap_{k \geq 1} T^k T_i \ = \ T_i$$

Vimos acima que dado $y \in Y_i \backslash \{1\}$, $y \notin T_i$.
Logo,

$$\exists l \geq 1 \text{ tal que } y \notin T^l T_i \quad , \quad \forall y \in Y_i \backslash \{1\} \qquad (*)$$

Afirmo que l satisfaz a propriedade desejada.
De fato, suponha que não.
Isto é, suponha que $\exists u \in T^l$ tal que $u \in R_i$ mas $u \notin T_i$.

Como $u \in R_i = \dot{\bigcup_{y \in Y_i}} yT_i$, $\exists y \in Y_i$ tal que $u \in yT_i$.

Já que $u \notin T_i$ não podemos ter $y = 1$. Daí, $u = yg$ com $y \in Y_i \setminus \{1\}$ e $g \in T_i$. Logo, $y = ug^{-1} \in T^l T_i$, contradizendo $(*)$. Portanto, l é o inteiro que procurávamos. ■

Proposição 4.5. *O subgrupo $C_G(G')$ possui índice finito em G, e G' é abeliano.*

Prova: Como $G' = \langle\ R_1, ..., R_n\ \rangle$, temos que $C_G(G') = \bigcap_{i=1}^{n} C_G(R_i)$.

Daí, se mostrarmos que $|\ G : C_G(R_i)\ |$ é finito para cada i, teremos $|\ G : C_G(G')\ | <\ \infty$.

Defina $\varphi : K \to S_{R_i/S_i}$, pondo $\varphi(k) = \varphi_k$, onde $\varphi_k(r/T_i) = r^{k^{-1}}T_i$ e $K = \bigcap_{i=1}^{n} N_G(R_i)$.

Como K normaliza R_i, para cada $rT_i \in R_i/T_i$ tem-se
$\varphi_k(rT_i) = r^{k^{-1}}T_i \in R_i/T_i$.

$\therefore\ \varphi_k(R_i/T_i) \subset R_i/T_i$

Veja que:

- φ_k está bem definida e é injetiva, para cada $k \in K$ fixado

De fato,

$$
\begin{aligned}
\varphi_k(r_1T_i) = \varphi_k(r_2T_i) &\Leftrightarrow r_1^{k^{-1}}T_i = r_2^{k^{-1}}T_i \\
&\Leftrightarrow (r_1k^{-1})T_i = (r_2k^{-1})T_i \\
&\Leftrightarrow (r_2k^{-1})^{-1}(r_1k^{-1}) \in T_i \\
&\Leftrightarrow kr_2^{-1}r_1k^{-1} \in T_i \\
&\Leftrightarrow r_2^{-1}r_1 \in T_i^k = T_i \quad (\text{já que } T_i \trianglelefteq K\ ) \\
&\Leftrightarrow r_1T_i = r_2T_i
\end{aligned}
$$

- φ_k é sobre

Dado $rT_i \in R_i/T_i$ qualquer seja $\alpha = r^k T_i$.
Como $R_i \trianglelefteq K$, $r^k \in R_i$.
Logo, $\alpha \in R_i/T_i$ e temos:

$$\varphi_k(\alpha) \;=\; \varphi_k(r^k T_i) \;=\; r^{kk^{-1}} T_i \;\;,$$

o que mostra a sobrejetividade de φ_k.

$\therefore\;\; \varphi_k \in S_{R_i/T_i} \;=\; \{\psi : R_i/T_i \to R_i/T_i \;;\; \psi \text{ é bijeção}\}$

Além disso,

- φ está, claramente, bem definida

- φ é homomorfismo

$$\varphi(ab)(rT_i) \;=\; \varphi_{ab}(rT_i) \;=\; r^{(ab)^{-1}} T_i \;=\; r^{b^{-1}a^{-1}} T_i \;=\; \varphi_a(r^{b^{-1}} T_i)$$

$$= \; \varphi_a \; \varphi_b(rT_i) \;=\; \varphi(a)\; \varphi(b)(rT_i)$$

Portanto, φ é a ação de K sobre R_i/T_i, o qual é finito(como vimos na proposição 4.4.)

Daí, chamando $N_i = Nuc\; \varphi$, temos:

$$\frac{K}{N_i} \;\simeq\; \varphi_K \;\leq\; S_{R_i/S_i}$$

$\therefore\;\; |\; K : N_i \;| \;|\; |\; R_i : T_i \;| \;! < \infty$

$\therefore |\; K : N_i \;| < \;\infty \;\;,\;\; \forall i$

$$\begin{array}{c} G \\ | \\ K \\ | \\ N_i \end{array}$$

Como já tinhamos $|\; G : K \;| < \;\infty$, segue que $|\; G : N_i \;| < \;\infty$.

Sendo G finitamente gerado, pela suposição 2, temos que N_i também é finitamente gerado.

Como $N_i^2 \trianglelefteq N_i$, N_i/N_i^2 é grupo.

Dado $gN_i^2 \in N_i/N_i^2$ qualquer, temos:

$(gN_i^2)^2 \;=\; g^2N_i^2 \;=\; N_i^2.$

$\therefore\ \dfrac{N_i}{N_i^2}$ é abeliano e todo elemento diferente de 1 tem ordem 2.

Como N_i é finitamente gerado, $\dfrac{N_i}{N_i^2}$ também o é.

Daí, sendo $\dfrac{N_i}{N_i^2}$ abeliano finitamente gerado e de torção segue que $\dfrac{N_i}{N_i^2}$ é finito.

$$\begin{array}{c} K \\ | \\ N_i \\ | \\ N_i^2 \end{array}$$

Como já tinhamos $\dfrac{K}{N_i} \;<\; \infty$ conclui-se que $\dfrac{K}{N_i^2} \;<\; \infty$.

Daí, é suficiente mostrarmos que $N_i^2 \leq C_G(R_i)$.

Sendo $R_i \;=\; \langle C\ ;\ C \in C_i \rangle$, temos $C_G(R_i) = \displaystyle\bigcap_{C \in C_i} C_G(C)$.

Daí, precisamos mostrar que $K_i \leq C_G(C)\ ,\ \forall C \in C_i$.

Afirmação 1 : Dado $C \in C_i$ temos : $[C, N_i] \leq [R_i, N_i] \leq T_i \leq C$.

Do fato de que $C \leq R_i$ segue que $[C, N_i] \leq [R_i, N_i]$

Seja $[r, N_i] \in [R_i, N_i]$. Como $k_i \in N_i$, $\ n_i^{-1} \in N_i$ também.

Logo, $\varphi(n_i^{-1}) = Id$

$\therefore\ \varphi(n_i^{-1})(rT_i) = rT_i$

$\therefore\ r^{n_i}T_i = rT_i$

$\therefore\ r^{-1}r^{n_i} \in T_i$

$\therefore\ \underbrace{r^{-1}n_i^{-1}rn_i}_{} \in T_i$

$[r, n_i]$

Portanto,

$$[R_i, N_i] \ = \ \langle \ [r, n_i] \ ; \ r \in R_i, n_i \in N_i \ \rangle \ \leq \ T_i$$

Além disso,

$$T_i \leq S_i = \bigcap_{C \in C_i} C \leq C$$

$\therefore \ T_i \leq C$

Afirmação 2 : Ni normaliza C , $\forall C \in C_i$.

Dado $c \in C$ e $n_i \in N_i$, temos:

$c^{-1} n_i^{-1} c \ n_i = [c, n_i] \in [C, N_i] \leq C$

$\therefore c^{-1} n_i^{-1} c \ n_i \in C$

$\therefore n_i^{-1} c \ n_i \in C$

$\therefore N_i$ normaliza C

Sendo cada $C \ = \ \langle c \rangle \in C_i$ cíclico infinito, Aut $C = \{Id, \alpha\}$ onde $\alpha(c) = c^{-1}$.

I.e. , Aut $C \simeq C_2$.

Como N_i normaliza C,

$$\begin{aligned} \psi : N_i &\to \text{Aut } C \\ n_i &\to \quad \psi_{n_i} : c \to n_i \ c n_i^{-1} \end{aligned}$$

é uma ação de N_i sobre C.

Dado $n_i \in N_i$ qualquer, temos : $\psi_{n_i} \psi_{n_i} = Id$ (pois $| \ Aut \ C \ |= 2$).

$\psi_{k_i} \psi_{n_i} = \psi_{n_i^2} = Id \Rightarrow \psi_{n_i^2}(c) = c, \ \forall c \in C$

$$\Rightarrow (n_i^2)^{-1} c \ n_i^2 = c, \ \forall c \in C$$

$\therefore \ n_i^2 \in C_G(c), \ \forall c \in C$

$\therefore \; n_i^2 \in C_G(C)$

$\therefore \; N_i^2 \leq C_G(C), \; \forall C \in C_i$

Finalmente, provaremos que G' é abeliano.

Primeiro, veja que $C_G(G') \cap G' = Z(G')$.

Sendo $G' \trianglelefteq G$ temos, pelo 2° Teorema dos Isomorfismos:

$\mid G' : Z(G') \mid = \mid C_G(G')G' : C_G(G') \mid \leq \mid G : C_G(G') \mid < \infty$

$$\begin{tikzcd}
 & G \arrow[d, dash] & \\
 & C_G(G')G' \arrow[dl, equal] \arrow[dr, dash] & \\
C_G(G') \arrow[dr, dash] & & G' \arrow[dl, equal] \\
 & C_G(G') \cap G' = Z(G') &
\end{tikzcd}$$

Segue então de Schur que $\mid G'' \mid < \; \infty$.

Mas $G'' < G'$ e todos os comutadores não triviais de G têm ordem infinita.

Logo, $G'' = 1$.

$\therefore \; G'$ é abeliano ■

Seja L o subgrupo de G definido pela condição $Z\left(\dfrac{G}{T^l}\right) = \dfrac{L}{T^l}$, onde l é como na proposição 4.4.

Defina $H = L \cap C_G(G')$.

Proposição 4.6. *O subgrupo H possui índice finito em G, e todo comutador $[h, g]$ com $h \in H$ e $g \in G$ pertence a um dos subgrupos T_i's.*

Prova: Já sabemos da Proposição 4.5, que $\mid G : C_G(G') \mid$ é finito.

Portanto, para mostrar a primeira parte desta proposição é suficiente provarmos que $| G : L |$ também é finito, pois neste caso, teremos:

$$| G : H | \leq | G : C_G(G') | \, | G : L | < \infty$$

Seja $\overline{G} = \dfrac{G}{T^l}$.

Como $T \trianglelefteq G$, $T^l \trianglelefteq G$. Logo, $\dfrac{G}{T^l} = \{gT^l \ ; \ g \in G\}$ é grupo.

Consideremos ainda, para cada $C \in \mathcal{C}$, $\overline{C} = \{ \ cT^l \ ; \ c \in C \ \}$.

Veja que:

• O conjunto dos comutadores em $\overline{G}$ está contido na união de todos os $\overline{C}$.

De fato, $[g_1T^l, g_2T^l] = [g_1, g_2]T^l, \ \forall g_1, g_2 \in G$.

Daí,

$$\{ \ [g_1T^l, g_2T^l] \ ; \ g_1, g_2 \in G \ \} = \{ \ [g_1, g_2]T^l \ ; \ g_1, g_2 \in G \ \} \subset \bigcup_{C \in \mathcal{C}} \overline{C}$$

• $| \overline{C} | < \infty, \ \forall C \in \mathcal{C}$

Mostraremos que $\forall C \in C_i$, tem-se :

$$| \overline{C} | = | C : T^l \cap C | \leq | C : T_i^l \cap C | \leq | C : T_i^l |$$

Primeiro, note que $\overline{C} = \{cT^l \ ; \ c \in C\} \simeq \dfrac{CT^l}{T^l}$.

Do 2° Teorema dos Isomorfismos, temos:

$$\frac{T^lC}{T^l} \simeq \frac{C}{T^l \cap C}$$

Em diagramas,

$$\begin{tikzcd}
 & T^lC \arrow[dl, equal] \arrow[dr, dash] & \\
T^l \arrow[dr, dash] & & C \arrow[dl, equal] \\
 & T^l \cap C &
\end{tikzcd}$$

Daí,

$$|\ \overline{C}\ | = \left|\frac{CT^l}{T^l}\right| = |\ C : T^l \cap C\ |$$

Também,

$$T_i \leq T \ \Rightarrow\ T_i^l \leq T^l$$
$$\Rightarrow\ T_i^l \cap C \leq T^l \cap C$$

$$\begin{array}{c} C \\ | \\ T^l \cap C \\ | \\ T_i^l \cap C \\ | \\ 1 \end{array}$$

$\therefore\ |\ C : T^l \cap C\ | \leq |\ C : T_i^l \cap C\ |$

Vimos na demonstração da Proposição 4.5, que $T_i \leq C,\ \forall C \in C_i$.

Logo, $T_i^l \leq C$ e temos ${T_i}^l \cap C = {T_i}^l$.

Assim,

$$|\ \overline{C}\ | \leq |\ C : T^l \cap C\ | \leq |\ C : T_i^l\ |$$

Como $T_i^l\ \leq\ C$ o qual é cíclico e $T_i^l \neq 1$(pois T_i é infinito) temos que T_i^l

também é cíclico infinito e $|\ C : T_i^l\ | <\ \infty$.

Logo, $|\ \overline{C}\ | < \infty$.

Portanto, $\overline{G}$ possui um número finito de comutadores.

Fixado $\overline{x} \in \overline{G}$ qualquer seja $\alpha : \begin{array}{lcl} \overline{x}^{\overline{G}} & \rightarrow & \{\text{comutadores de } \overline{G}\} \\ \overline{x}^{\overline{g}} & \rightarrow & [\overline{x}, \overline{g}] \end{array}$.

α está bem definida e é injetiva.

Logo, $\mid \overline{x}^{\overline{G}} \mid \leq \mid \{$comutadores de $\overline{G}\} \mid < \infty$.

$\therefore$ $\overline{G}$ é FC-grupo.

Sendo G finitamente gerado (suposição 2) temos que $\overline{G}$ também o é.

Digamos que seja $\overline{G} = \langle\, \overline{x_1}, ..., \overline{x_k}\, \rangle$.

Então, $Z(\overline{G}) = \displaystyle\bigcap_{i=1}^{k} C_{\overline{G}}(\overline{x}_i)$.

Como $\mid \overline{G} : C_G(\overline{x}_i) \mid = \mid \overline{x}_i^{\overline{G}} \mid < \infty$, segue que $\mid G : L \mid < \infty$, como desejado.

Sendo $\dfrac{L}{T^l} = Z\left(\dfrac{G}{T^l}\right)$, temos que $[L, G] \leq T^l$.

Assim, para cada $h \in H \leq L$ e $g \in G$, temos $[h, g] \in [L, G] \leq T^l$

Como $[h, g] \in R_i$ para algum i, segue da proposição 4.4. que $[h, g] \in T_i$,

o que completa a prova. ■

Para a próxima proposição precisaremos do lema a seguir.

Lema 4.7. *Seja $\langle x\rangle \times \langle y\rangle$ o produto direto de dois grupos cíclicos infinitos. Então, os subgrupos $\langle x^i y\rangle$ e $\langle x^j y\rangle$ têm interseção trivial para todo $i \neq j$.*

Prova: Seja $g \in \langle x^i y\rangle \cap \langle x^j y\rangle$ com $i \neq j$.
Então, $g = (x^i y)^k = (x^j y)^l$ com $k, l \in \mathbf{Z}$.
$\therefore$ $x^{ik} y^k = x^{jl} y^l$
$\therefore$ $x^{ik-jl} = y^{l-k} \in \langle x\rangle \cap \langle y\rangle = 1$.
$\therefore$ $l = k$ e $ik = jl$ (pois x e y têm ordem infinita)
Se for $l = k \neq 0$, então $i = j$. Absurdo!
Portanto, $l = k = 0$ e $g = 1$. ■

Proposição 4.8. *Se $h \in H$, então $[h, G]$ está contido em um dos subgrupos T_i's e, em particular, $[h, G]$ é cíclico.*

Prova: Já sabemos que cada comutador $[h, g]$ pertence a algum dos subgrupos T_i's. Suponhamos, por absurdo, que existam $[h, a]$ e $[h, b]$ comutadores

não triviais pertencentes a dois subgrupos diferentes T_i e T_j.
Note que $\langle [h,a] \rangle \times \langle [h,b] \rangle$ é produto direto.
Além disso, $\langle [h,a] \rangle \times \langle [h,b] \rangle \simeq C_\infty \times C_\infty \simeq \mathbf{Z^2}$.
Para quaisquer inteiros r e s, consideremos o comutador $u_{r,s} = [ah^r, bh^{-s}]$.
Como $G' \lhd G$, $C_G(G') \lhd G$.
Daí, se $h \in H \subset C_G(G')$, $[h,G] \leq C_G(G')$.
Portanto,

$$[a,b]\ .\ [h,a] \ = \ [h,a]\ .\ [a,b]$$

e

$$[a,b]\ .\ [h,b] \ = \ [h,b]\ .\ [a,b],$$

$\forall a, b \in G$
.

<u>Afirmação</u>: $\forall k \in \mathbf{Z}$ temos $[a,h]^k = [a,h^k]$ e $[h,b]^k = [h^k, b]$.

Prova por Indução:

Primeiro mostraremos para $k \in \mathbb{N}$.

(i) Para $k = 1$, ok!

(ii) vale para $k \quad \Rightarrow \quad$ vale para $k+1$

Com efeito,

$$\begin{aligned}
[a,h]^{k+1} &= [a,h]^k\ .\ [a,h] \\
&= [a,h^k]\ .\ [a,h] \\
&= a^{-1}(h^{-k}a\ h^k a^{-1})h^{-1}a\ h \\
&= a^{-1}h^{-1}(h^{-k}a\ h^k a^{-1})a\ h \\
&= a^{-1}h^{-(k+1)}a\ h^{k+1} \\
&= [a,h^{k+1}]
\end{aligned}$$

Portanto, $[a,h]^k = [a,h^k], \forall k \in \mathbb{N}$.

Se $k < 0$, então $-k < 0$ e temos:

$[a,h]^k = ([a,h]^{-k})^{-1} = ([a,h^{-k}])^{-1} = [h^{-k}, a]$

Mas, sendo $H \subset C_G(G')$, segue que $[h^{-k}, a] = [a, h^k]$.

Logo, $[a,h]^k = [a,h^k], \forall k < 0$.

$\therefore\ [a,h]^k = [a,h^k], \forall k \in \mathbb{Z}$

Analogamente, tem-se $[h,b]^k = [h^k,b], \forall k \in \mathbb{Z}$.

Assim,

$$\begin{aligned} u_{r,s} &= [ah^r, bh^{-s}] \\ &= [ah^r, h^{-s}]\ [ah^r, b]^{h^{-s}} \\ &= [ah^r, h^{-s}]\ [ah^r, b] \\ &= [a, h^{-s}]^{h^r}[h^r, h^{-s}][a,b]^{h^r}[h^r, b] \\ &= [a, h^{-s}][a,b][h^r, b] \\ &= [a,h]^{-s}[a,b][h,b]^r \\ &= [h,a]^s[a,b][h,b]^r \\ &= [a,b][h,a]^s[h,b]^r \end{aligned}$$

Dado $I \subset \mathbb{Z}^2$ infinito, seja $U = \{u_{r,s}\ ;\ (r,s) \in I\}$.

Sendo $T_i \cap T_j = 1$, para $i \neq j$ e $T_i \simeq C_\infty$, para $r \neq r'$ ou $s \neq s'$, temos $u_{r,s} \neq u_{r',s'}$.

Logo, U é subconjunto infinito de $X = \{[a,b]\ ;\ a,b \in G\}$.

Como $U \subset X \subset \bigcup\limits_{C \in \mathcal{C}} C$ e $\mathcal{C}$ é família finita, existe pelo menos um $C \in \mathcal{C}$ contendo os comutadores $u_{r,s}$ para uma infinidade de pares $(r,s) \in I$.

Se escolhermos $I = \{(r,r^2)\ ;\ r \in \mathbb{N}\}$, então existe $J \subset \mathbb{N}$ infinito tal que

$u_{r,r^2} \in C$ para todo $r \in J$.

Daí, fixado $r \in J$ temos:

$$\begin{aligned} u_{r,r^2}u_{s,s^2}^{-1} &= [a,b][h,a]^{r^2}[h,b]^r([a,b][h,a]^{s^2}[h,b]^s)^{-1} \\ &= [a,b][h,a]^{r^2}[h,b]^r[h,b]^{-s}[h,a]^{-s^2}[a,b]^{-1} \\ &= [h,a]^{r^2-s^2}[h,b]^{r-s} \quad (G' \text{ é abeliano}) \\ &= ([h,a]^{r+s}[h,b])^{r-s} \in C,\ \ \forall s \in J \end{aligned}$$

Do fato de $\langle [h,a] \rangle \times \langle [h,b] \rangle$ ser produto direto e $[h,a]$ e $[h,b]$ terem ordem infinita temos que $[h,a]^{r+s}[h,b]$ também tem ordem infinita.
Então, se $r \neq s$, temos

$$\langle [h,a]^{r+s}[h,b]\rangle \ \cap \ C \neq 1.$$

Tomando agora um terceiro elemento, $t \in J$ com $t \neq r, s$ temos também:

$$1 \neq u_{r,r^2}u_{t,t^2}^{-1} \ = \ \langle [h,a]^{r+t}[h,b]\rangle^{r-t} \in C$$

$$\therefore \ \langle [h,a]^{r+t}[h,b]\rangle \ \cap \ C \neq 1$$

Sendo C cíclico infinito, $\begin{cases} \langle\ [h,a]^{r+s}\ [h,b]\ \rangle \cap \ C \neq 1 \\ \langle\ [h,a]^{r+t}\ [h,b]\ \rangle \cap \ C \neq 1 \end{cases}$ implica,

$$\langle\ [h,a]^{r+s}\ [h,b]\ \rangle \ \cap \ \langle\ [h,a]^{r+t}\ [h,b]\ \rangle \neq 1.$$

Mas isto contradiz o Lema 4.7, já que $\langle\ [h,a]\ \rangle \times \langle\ [h,b]\ \rangle$ é produto direto de cíclicos infinitos e $r+s \neq r+t$.

Logo, $[h,G] \subset T_i$ para algum i. ■

Teorema 4.9. *Seja G um grupo no qual todos os comutadores podem ser cobertos por uma quantidade finita de subgrupos cíclicos. Se G não possui comutadores de ordem finita, exceto 1, então G' é cíclico-por-finito*

Prova: Mostraremos que $\exists N \lhd G'$ tal que N é cíclico e $\dfrac{G'}{N}$ é finito.

Para cada $i = 1, ..., n$, definamos $H_i = \{h \in H \ ; \ [h,G] \subseteq T_i\}$.

Sejam $h_1, h_2 \in H_i$ quaisquer.

Então, $[h_1,G],[h_2,G] \subseteq T_i$.

Como $H \leq C_G(G')$, temos:

$$[h_1h_2,g] \ = \ [h_1,g]^{h_2}[h_2,g] \ = \ [h_1,g][h_2,g] \in T_i, \ \forall g \in G$$

$\therefore \ [h_1h_2,G] \subseteq T_i$.
$\therefore \ a \cdot b \in H_i, \ \forall a,b \in H_i$

Além disso, dado $h \in H_i$ qualquer, temos:

$$
\begin{aligned}
[h^{-1}, g] &= hg^{-1}h^{-1}g \\
&= h(g^{-1}h^{-1}g\ h)h^{-1} \\
&= h\ [g, h]\ h^{-1} \\
&= h\ h^{-1}[g, h] \\
&= [g, h] \\
&= [h, g]^{-1}, \forall g \in G
\end{aligned}
$$

$\therefore\ [h^{-1}, G] = [h, G]$
$\therefore\ H_i \leq G$

Como $H_i \subset H$ para cada i, temos que $H_1 \cup ... \cup H_n \subset H$.

E da proposição 4.8 sabemos que para cada $h \in H$, $[h, G] \subset T_i$ para algum i.

Isto é, $h \in H_i$ para algum i.

Logo, $H = H_1 \cup ... \cup H_n$.

Por Neumann temos que $\mid H : H_i \mid < \infty$ para algum i.

Como já tinhamos $\mid G : H \mid < \infty$ segue que $\mid G : H_i \mid < \infty$.

Seja $N = [H_i, G]$.

Dado $h \in H_i$ e $g_1, g_2 \in G$ quaisquer, temos:

$$[h, g_1g_2] = [h, g_2][h, g_1]^{g_2}$$

$$\therefore\ [h, g_1]^{g_2} = [h, g_2]^{-1}[h, g_1g^2] \in [H_i, G]$$

Assim, dado $g \in G$ qualquer, $N^g = [H_i, G]^g \subset [H_i, G]$

$\therefore\ N \lhd G$

Pela definição de H_i temos $[H_i, G] \subseteq T_i$ o qual é cíclico.

Logo, N é cíclico.

Seja $\overline{G} = \dfrac{G}{N}$ e $\overline{H_i} = \{hN\ ;\ h \in H_i\}$.

Sendo $N = [H_i, G]$ temos que $\overline{H_i} \subseteq Z(\overline{G})$.

$$\begin{array}{c} \overline{G} \\ | \\ Z(\overline{G}) \\ | \\ \overline{H_i} \end{array}$$

Por outro lado, $\mid G : H_i \mid < \infty$ implica $\mid \overline{G} : \overline{H_i} \mid < \infty$.

Logo, $\mid \overline{G} : Z(\overline{G}) \mid < \infty$.

Segue então, do Teorema de Schur, que $\overline{G}' = \dfrac{G'}{N}$ é finito.

$\therefore$ G' é cíclico-por-finito.

$\blacksquare$

4.2 O caso geral

Nesta seção completamos a prova do Teorema Principal. Precisaremos de três lemas elementares.

Lema 4.10. *Seja H um grupo no qual o subgrupo derivado é cíclico infinito. Se H não é nilpotente de classe menor ou igual a 2, então H possui um subgrupo abeliano A de índice 2 tal que $Z(H) \leq A$ e $\dfrac{A}{Z(H)}$ é cíclico.*

Prova: Seja $A = C_H(H')$. Claro que $Z(H) \leq A$. Daí, $Z(H) \lhd A$.

Pelo NC-Lema temos :

$$\frac{N_H(H')}{C_H(H')} \leq \text{ Aut } H' \simeq \mathbb{Z}_2 \text{ (já que } H' \simeq C_\infty)$$

Mas $H' \lhd H$. Logo, $N_H(H') = H$.

Daí, $\left| \dfrac{H}{A} \right| \Big| \, 2$, o que nos dá $\mid H : A \mid = 1$ ou $\mid H : A \mid = 2$.

Se fosse $\mid H : A \mid = 1$, então teríamos $H = A = C_H(H')$.

$\therefore\ H' \ \leq\ Z(H)$

$\therefore\ \Gamma_3(H) = [H', H] = 1$

$\therefore$ H é nilpotente de classe ≤ 2.

Absurdo!

Portanto, $\mid H : A \mid = 2$.

Escolhamos $h \in H \backslash A$ qualquer.

Como $H' \lhd H$, $\begin{array}{rcl} \varphi : H' & \rightarrow & H' \\ u & \rightarrow & u^h \end{array}$ é automorfismo de H'.

E pela escolha de h, este é um automorfismo não trivial.

Sendo $H' \simeq C_\infty$, temos Aut $H' = \{\ I,\ \theta : u \rightarrow u^{-1}\ \}$.

Daí, devemos ter $\varphi \equiv \theta$.

$\therefore\ \varphi(u) = \theta(u),\ \forall u \in H'$

$\therefore\ u^h = u^{-1},\ \forall u \in H'$

Desse modo,

$$\begin{aligned} C_{H'}(h) &= \{u \in H'\ ;\ h^u = h\} \\ &= \{u \in H'\ ;\ u^{-1}h\ u = h\} \\ &= \{u \in H'\ ;\ u^{-1}h^{-1}u = h^{-1}\} \\ &= \{u \in H'\ ;\ h^{-1}u\ h = u\} \\ &= \{u \in H'\ ;\ u^{-1} = u\} \\ &= \{u \in H'\ ;\ u^2 = 1\} \\ &= 1 \end{aligned}$$

Consideremos $\begin{array}{rcl} \nu : A & \rightarrow & H'. \\ a & \rightarrow & [h, a] \end{array}$

$$\begin{aligned} \nu(a_1a_2) &= [h, a_1a_2] = [h, a_2][h, a_1]^{a_2} = [h, a_2][h, a_1] = [h, a_1][h, a_2] \\ &= \nu(a_1)\nu(a_2) \ \ \text{(pois } A = C_H(H') \text{ e } H' \text{ é abeliano)} \end{aligned}$$

Portanto, ν é homomorfismo.

$$\begin{aligned}\mathrm{Nuc}(\nu) &= \{a \in A \ ; \ \nu(a) = 1\} \\ &= \{a \in A \ ; \ [h,a] = 1\} \\ &= \{a \in A \ ; \ h^{-1}a^{-1}h\ a = 1\} \\ &= \{a \in A \ ; \ ha = ah\} \\ &= C_A(h)\end{aligned}$$

Segue então do 1° Teorema dos Isomorfismos que:

$$\frac{A}{C_A(h)} \ \simeq \ \nu(A) \ \leq \ H'$$

Assim, $\dfrac{A}{C_A(h)}$ é cíclico e portanto, abeliano.

$\therefore \ A' \leq C_A(h)$

Mas, $A' \leq H'$. Logo, $A' \leq C_{H'}(h) = 1$ e A é abeliano.

Como $\mid H : A \mid = 2$, temos $H = A \,\dot\cup\, hA$.

Claro que $H = A \,\dot\cup\, hA \ \leq \ \langle h, A \rangle$.

Também,

$$h \in H \text{ e } A \leq H \ \Rightarrow \ \langle h, A \rangle \leq H.$$

$$\therefore \ H = \langle h, A \rangle$$

Daí, $Z(H) = C_H(h) \cap C_H(A)$.

Afirmo que $Z(H) = C_A(h)$.

De fato,

$$\begin{aligned} x \in C_A(h) \ &\Rightarrow \ x \in A \ \text{ e } \ h^x = h \\ &\Rightarrow \ a^x = a, \ \forall a \in A \ \text{ e } \ h^x = h \\ &\Rightarrow \ x \in C_H(A) \cap C_H(h) = Z(H) \\ \therefore \ C_A(h) \leq Z(H) & \end{aligned}$$

Agora, seja $z \in Z(H)$ qualquer.

Então, $z \in H$ e $y^z = y, \ \forall y \in H$.

Em particular, $y'^z = y', \ \forall y' \in H'$.

$\therefore\ z \in C_A(H') = A$

Também, sendo $h \in H$ e $z \in Z(H)$, $h^z = h$.

Logo, $z \in C_A(h)$.

$\therefore\ Z(H) \leq C_A(h)$

$\therefore\ Z(H) = C_A(h)$

Portanto, $\dfrac{A}{Z(H)} = \dfrac{A}{C_A(h)}$ é cíclico. ■

Lema 4.11. *Seja G um grupo e seja A um subgrupo abeliano normal de G tal que o quociente $\dfrac{G}{A}$ é cíclico. Se gA é um gerador de $\dfrac{G}{A}$, então $G' = \{[g,a]\ ;\ a \in A\}$ consiste inteiramente de comutadores.*

Prova: Afirmo que $\forall k \in \mathbb{N}$ e $\forall a \in A$, $[g^k, a] = [g, a']$ para algum $a' \in A$.
Façamos indução sobre k.
Claramente vale para $k = 1$
Suponhamos agora, válido para k.
Então,

$$\begin{aligned}[g^{k+1}, a] &= [g\ .\ g^k a] = [g,a]^{g^k}[g^k, a] \\ &= [g^{g^k}, a^{g^k}]\ [g, a'], \\ &= [g, a_1][g, a'] \quad (\text{como } A \lhd G,\ a_1 = a^{g^k} \in A) \\ &= [g, a''] \quad \text{com } a'' = a_1 a' \in A,\end{aligned}$$

O que prova nossa afirmação.

Agora, sendo A abeliano e normal em G, para cada $k > 0$, temos:

$1 = [g^k g^{-k}, a] = [g^k, a]^{g^{-k}}[g^{-k}, a] = [g^k, a']\ [g^{-k}, a]$.

$\therefore [g^{-k}, a] = [g^k, a']^{-1} = [g^k, a'^{-1}] = [g, a'']$

Daí, $[g^k, a] = [g, a']$ para algum $a' \in A, \forall k \in \mathbb{Z}$ e $\forall a \in A$.

Sejam $x, y \in G$ quaisquer.

Como $G/A = \langle gA \rangle$, $xA = g^n A$ e $yA = g^m A$ com $n, m \in \mathbb{Z}$.

Daí, $\exists_{(m)} a_1, a_2 \in A$ tais que $x = g^n a_1$ e $y = g^m a_2$.

Isso nos dá:

$$
\begin{aligned}
[x,y] &= [g^n a_1, g^m a_2] = [g^n a_1, a_2][g^n a_1, g^m]^{a_2} \\
&= [g^n a_1, a_2][g^n a_1, g^m] \quad \text{(pois } G' \leq A \text{ e A é abeliano)} \\
&= [g^n, a_2]^{a_1}[a_1, a_2][g^n, g^n]^{a_1}[a_1, g^m] \\
&= [g^n, a_2][a_1, g^m] \\
&= [g, a_3][a_4, g], \quad \exists a_3, a_4 \in A \\
&= g^{-1}a_3^{-1}g\ (a_3\ a_4^{-1})(g^{-1}a_4\ g) \\
&= g^{-1}a_3^{-1}g\ g^{-1}a_4\ g\ a_3\ a_4^{-1} \\
&= g^{-1}a_3^{-1}a_4\ g\ a_3\ a_4^{-1} \\
&= g^{-1}(a_3a_4^{-1})^{-1}g\ (a_3a_4^{-1}) \\
&= [g, a_3a_4^{-1}]
\end{aligned}
$$

Portanto, dados $x, y \in G$ quaisquer, $[x, y] = [g, a]$ para algum $a \in A$.

Veja que:

$$
\begin{aligned}
[x_1, y_1][x_2, y_2] &= [g, a_1][g, a_2] \\
&= [g, a_1][g, a_2]^{a_1} \quad \text{(já que } a_1 \in A) \\
&= [g, a_2a_1] \\
&= [g, a_1a_2]
\end{aligned}
$$

Mais geralmente, $[g, a_1]...[g, a_k] = [g, a_1...a_k]$.

Assim,

$$
\begin{aligned}
G' &= \langle [x, y]\ ;\ x, y \in G \rangle \\
&= \{[x_1, y_1]...[x_k, y_k]\ ;\ x_i, y_i \in G\} \\
&= \{[g, a]\ ;\ a \in A\}
\end{aligned}
$$

■

Lema 4.12. *Seja G um gupo no qual o conjunto dos comutadores é coberto por uma quantidade finita de subgrupos cíclicos. Suponha $L = \langle u \rangle \times \langle w \rangle \simeq C_\infty \times C_m$ subgrupo de G', onde $m > 1$ é finito. Então, existem elementos da forma $u^i w$, com $i \in \mathbb{Z}$, os quais não são comutadores em G.*

Prova: Suponha por absurdo que todos os elementos $u^i w$ são comutadores. Faça $u_i = u^{m^i} w$ para cada $i \in \mathbb{N}$.
Como $\forall i,\ u^i w$ é comutador e $o(u) = \infty$, G possui infinitos comutadores.
Mas por hipótese, o conjunto dos comutadores pode ser coberto por um número finito de subgrupos cíclicos. Logo, existem inteiros i,j com $i < j$ tais

que u_i e u_j pertencem a um mesmo subgrupo cíclico da cobertura, digamos C.
Sendo $L = \langle u \rangle \times \langle w \rangle$ produto direto, $uw = wu$.
Como C é cíclico e $C \cap L \leq C$ temos que $C \cap L$ também é cíclico.
Seja $c = u^k w^l$ um gerador de $C \cap L$.
Sendo $u_i, u_j \in C \cap L$. Sendo $u_i, u_j \in C \cap L$, temos $u_i = c^r$ e $u_j = c^s$ para algum r e algum s inteiros.

Daí

$$u^{m^i} w = (u^k w^l)^r = w^{kr} w^{lr}$$
$$u^{m^j} w = (u^k w^l)^s = u^{ks} w^{ls}$$

$\therefore\ m^i = kr$ e $m^j = ks$
$\therefore\ m^{j-i} = s/r$

Portanto, s/r é uma potência de m maior que 1.

Então,

$$u^{m^j} w = u_j = c^s = (c^r)^{s/r} = u_i^{s/r}$$
$$= (u^{m^i} w)^{m^{j-i}} = u^{m^j} w^{m^{j-i}} = u^{m^j} \quad \text{(pois } o(w) = m \text{)}$$

$\therefore\ w = 1$
$\therefore\ m = 1$

Absurdo! ■

Também precisaremos do resultado a seguir, devido a Liebeck, cuja demonstração encontra-se no apêndice.

Teorema 4.13. *Seja G grupo nilpotente de classe 2. Se G' é 2-gerado, então todo elemento de G' é um comutador.*

Agora podemos refinar a conclusão do Teorema 4.9.

Teorema 4.14. *Seja G um grupo no qual o conjunto dos comutadores pode ser coberto por uma quantidade finita de subgrupos cíclicos. Se G não possui qualquer comutador de ordem finita, exceto 1, então G' é cíclico.*

Prova: Podemos supor $G' \neq 1$. Daí, G' é infinito.
Pela proposição 4.5, G' é abeliano.
Seja $P = \{g' \in G' \ ; \ o(g') < \infty\}$, o subgrupo de torção de G'.
Como $P \trianglelefteq_{car} G' \trianglelefteq G$, $P \triangleleft G$.
Do Teorema 4.9, sabemos que G' é cíclico-por-finito.

Daí, $\exists Q \trianglelefteq G'$ tal que Q é cíclico e $\dfrac{G'}{Q}$ é finito.
Sendo G' infinito, devemos ter, necessariamente, $Q \simeq C_\infty$.
Logo, $P \cap Q = 1$.
Segue então do 2° Teorema dos Isomorfismos que: $\dfrac{PQ}{P} \simeq Q \simeq C_\infty$.

Em diagramas:

$$\begin{tikzcd}
& G' \arrow[d, dash] & \\
& PQ \arrow[dl, equal] \arrow[dr, dash] & \\
P \arrow[dr, dash] & & Q \arrow[dl, equal] \\
& Q \cap P = 1 &
\end{tikzcd}$$

Por outro lado, sendo $G' = \langle X_C; C \in \mathcal{C} \rangle$ onde cada X_C é finito, temos que G' é finitamente gerado e segue do T.F.G.A.F.G , que:

$$G' = C_{n_1} \times ... \times C_{n_k} \times C_\infty \times ... \times C_\infty,$$

onde $P = C_{n_1} \times ... \times C_{n_k}$.
Daí, $\dfrac{G'}{P} \simeq C_\infty \times ... \times C_\infty$.

Mas, $\mid G' : PQ \mid \leq \mid G' : Q \mid < \infty$. Logo, devemos ter $\mid G' : PQ \mid = 1$.

Desse modo,

$$G' = P \times C_\infty$$

Então, basta mostrarmos que $P = 1$.

Suponhamos, por absurdo, $P \neq 1$.

<u>Afirmação</u>: Podemos assumir P cíclico.

De fato, tomemos $P = C_{n_1} \times ... \times C_{n_k}$, com $n_i > 1$ para cada i.

Seja $H = C_{n_1} \times ... \times C_{n_k - 1}$.

Sendo $P \lhd G$, $[P, G] \leq P$. Logo, $[P, G] = 1$ e, portanto, $P \leq Z(G)$.

Daí, $H \leq Z(G)$, o que implica $H \lhd G$.

Veja que:

$$\{ \text{ comutadores de } \ G/H \ \} \ \subset \ \bigcup_{C \in \mathcal{C}} \frac{CH}{H},$$

onde para cada $C \in \mathcal{C}$, $\dfrac{CH}{H}$ é cíclico $\Big($já que $\dfrac{CH}{H} \simeq \dfrac{C}{C \cap H}\Big)$.

Além disso, $\dfrac{G}{H}$ não possui qualquer comutador não trivial de ordem finita.

Note que $\Big(\dfrac{G}{H}\Big)' = \dfrac{G'}{H}$.

Denotando por $T\Big(\dfrac{G'}{H}\Big)$ o subgrupo torção de $\dfrac{G'}{H}$, temos:

$$T\Big(\frac{G'}{H}\Big) = \frac{T(G')}{H} = \frac{P}{H} \simeq C_{n_k} \quad (\text{já que } H \leq P)$$

Supondo então nosso Teorema provado para grupos nos quais o derivado possui subgrupo de torção cíclico, segue que $\dfrac{G'}{H} \simeq C_\infty$.

Por outro lado, $\dfrac{G'}{H} \simeq C_{n_k} \times C_\infty$.

Logo, $C_{n_k} = 1$.

Absurdo!

Daí, $P = 1$ e o teorema está provado no caso geral.

Isto mostra nossa afirmação.

Desse modo, G' é 2-gerado.

Consideremos $\overline{G} = \dfrac{G}{P}$. Afirmo que: $Z(\overline{G}) = \overline{Z(G)}$.

De fato, sendo $P \lhd G$, para cada $z \in Z(G)$ e $g \in G$, temos:

$[zP, gP] = [z, g]P = P$ (pois $[z, p] = 1$)

$\therefore \ \Big[\dfrac{Z(G)}{P}, \dfrac{G}{P}\Big] = P = 1_{G/P}$

$\therefore \ \dfrac{Z(G)}{P} \leq Z\Big(\dfrac{G}{P}\Big)$

Agora, sejam $aP \in Z\Big(\dfrac{G}{P}\Big)$ e $gP \in \dfrac{G}{P}$ quaisquer.

$$\begin{aligned} aP \ . \ gP = gP \ . \ aP \ &\Rightarrow \ agP = gaP \\ &\Rightarrow (ga)^{-1}(ag) \in P \\ &\Rightarrow \ [a,g] \in P \\ &\Rightarrow \ [a,g] = 1 \quad (\text{pois } o(p) < \infty, \forall p \in P) \\ &\Rightarrow \ a \in Z(G) \end{aligned}$$

$\therefore \ aP \in \dfrac{Z(G)}{P}.$

$\therefore \ Z\Big(\dfrac{G}{P}\Big) = \dfrac{Z(G)}{P}$

Sobre $\overline{G}$ analisemos dois casos.

Primeiro, suponhamos $\overline{G}$ nilpotente de classe no máximo 2.

Se fosse $\overline{G}$ de classe 0, teríamos $Z_0(\overline{G}) = \overline{G} = \dfrac{G}{P}$.

Mas, $Z_0(\overline{G}) = 1_{\overline{G}} = P$.

Logo, teríamos: $G = P$. Absurdo!

Supondo $\overline{G}$ de classe 1, temos: $Z\Big(\dfrac{G}{P}\Big) = \dfrac{G}{P}$.

Daí, $\dfrac{G}{P}$ seria abeliano e portanto, $G' \leq P$.

Assim, teríamos $G' = P$ o que mais uma vez é uma contradição.

Logo, $\overline{G}$ deve ser nilpotente de classe 2.

Como $\dfrac{G}{Z(G)} \simeq \dfrac{\overline{G}}{\overline{Z(G)}} = \dfrac{\overline{G}}{Z(\overline{G})}$, temos:

$\dfrac{Z_2(G)}{Z(G)} = Z\Big(\dfrac{G}{Z(G)}\Big) \simeq Z\Big(\dfrac{\overline{G}}{\overline{Z(G)}}\Big) = \dfrac{\overline{G}}{Z(\overline{G})} = \dfrac{\overline{G}}{\overline{Z(G)}} \simeq \dfrac{G}{Z(G)}$

$\therefore \ Z_2(G) = G$

Além disso, sendo $G' \neq 1$, não podemos ter $Z_0(G) = G$ ou $Z_1(G) = G$.

Portanto, G é nilpotente de classe 2.

Segue então do Teorema 4.13 que todo elemento de G' é um comutador.

Assim, G' pode ser coberto por uma quantidade finita de subgrupos cíclicos, o que implica G' finito ou cíclico.

$\therefore\ G' \simeq C_\infty$

$\therefore\ P = 1$

Absurdo!

Portanto, $\overline{G}$ não é nilpotente de classe menor ou igual a 2.

Pelo Lema 4.10, existe $\overline{A} \leq \overline{G}$ com $\mid \overline{G} : \overline{A} \mid = 2$ e $\overline{A}$ é abeliano.

Então, A é subgrupo de G com índice 2 tal que $\overline{A}$ é abeliano.

Afirmo que A é abeliano.

De fato, sejam $a_1, a_2 \in A$ quaisquer.

$$\begin{aligned} a_1P, a_2P \in \overline{A} \ &\Rightarrow\ a_1P \,.\, a_2P = a_2P \,.\, a_1P \ \Rightarrow\ a_1a_2P = a_2a_1P \\ &\Rightarrow\ [a_1, a_2] \in P \\ &\Rightarrow\ [a_1, a_2] = 1 \\ &\Rightarrow\ a_1a_2 = a_2a_1 \end{aligned}$$

Além disso, sendo $\mid G : A \mid = 2$, temos que $\dfrac{G}{A}$ é cíclico e $A \lhd G$.

Portanto, segue do Lema 4.11 que todo elemento de G' é um comutador, o que mais uma vez nos leva a uma contradição.

Portanto, $P = 1$ e $G' \simeq C_\infty$.$\blacksquare$

Antes da demonstração do Teorema Principal vejamos três resultados que nos serão necessários.

Resultado 1: Sejam G grupo, $X \subset G$ e $N \leq G$. Então, considerando $\overline{X} = \{xN; x \in X\}$, temos:

$$| X | \leq | \overline{X} | \,.\, | N |$$

Prova: Note que $XN = \dot{\bigcup_{x \in X}} xN$.
Portanto, $| XN | = | \overline{X} || N |$. Mas, $X \subseteq XN$.

Logo, $| X | \leq | XN | = | \overline{X} | \, | N |$. ■

Resultado 2: Se G é um grupo e $H < G$, com $H \neq G$, então $\langle G \backslash H \rangle = G$.

Prova: Tome $g \in G \backslash H$ e $h \in H$.
Veja que $gh \notin H$. Do contrário, teríamos $g \in H$.
Daí, $g^{-1}, gh \in G \backslash H \subset \langle G \backslash H \rangle$.
Em particular, $h = g^{-1}gh \in \langle G \backslash H \rangle$.
Como h foi tomado arbitrariamente em H, segue que $H \leq \langle G \backslash H \rangle$.
E, claro que $G \backslash H \subset \langle G \backslash H \rangle$. Logo, $G = H \cup G \backslash H \subset \langle G \backslash H \rangle$.
Portanto, $G = \langle G \backslash H \rangle$. ■

Finalmente podemos provar o Teorema principal.

Teorema 4.15. *Seja G um grupo no qual o conjunto dos comutadores é coberto por finitos subgrupos cíclicos. Então, G' é finito ou cíclico.*

Prova: Assumindo G' infinito, mostraremos que G' é cíclico.
Sejam X_0 o conjunto de todos os comutadores em G de ordem finita e N o subgrupo gerado por X_0.
Como $X_0 \subseteq X = \{[a, b] \; ; \; a, b \in G\} \subset \bigcup_{C \in \mathcal{C}} C$, temos que, para cada $x_0 \in X_0$, existe C_{x_0} em $\mathcal{C}$ tal que $x_0 \in C_{x_0}$. Em particular, $\langle x_0 \rangle \leq C_{x_0}$.
Como existem somente finitos C's em $\mathcal{C}$, $\{\langle x_0 \rangle\}_{x_0 \in X_0}$ é família finita de subgrupos cíclicos de G cobrindo X_0. E subgrupos finitos, já que $o(x_0) < \infty$ para cada x_0. Logo, X_0 é finito.
Além disso, X_0 é claramente, subconjunto normal de G (o que implica $N \lhd G$).
Segue então do Lema de Dietzmann, que N é finito.
Sendo N finito, todos os seus elementos são de ordem finita.

Afirmação 1: G/N não possui comutadores não-triviais de ordem finita.

De fato, suponha por absurdo que $\exists [aN, bN] \in G/N$ tal que $[aN, bN] \neq N$ e $([aN, bN])^k = N, \ k \in \mathbb{N}$.

$$\begin{aligned} ([aN, bN])^k = N \ &\Rightarrow \ [a,b]^k N = N \ \Rightarrow \ [a,b]^k \in N \\ &\Rightarrow \ [a,b]^{kl} = 1, \text{ para algum } l \in \mathbb{N} \\ &\Rightarrow \ o([a,b]) < \infty \ \Rightarrow \ [a,b] \in N \end{aligned}$$

Absurdo!
Com isso mostramos nossa afirmação.
Note também que:

$$X \subset \bigcup_{C \in \mathcal{C}} C \ \Rightarrow \ \{[\overline{a}, \overline{b}] \ ; \ \overline{a}, \overline{b} \in G/N\} \subset \bigcup_{C \in \mathcal{C}} CN/N,$$

onde para cada $C \in \mathcal{C}$, $\dfrac{CN}{N} \simeq \dfrac{C}{C \cap N}$ o qual é cíclico.

Portanto, pelo Teorema 4.14, $\left(\dfrac{G}{N}\right)' = \dfrac{G'}{N}$ é cíclico infinito.

Seja $B = C_G(G')$.

Afirmamos que $| \ G : B \ |$ é finito.

Lembre que G' é finitamente gerado.

Digamos que seja: $G' = \langle x_1, ..., x_n \rangle$

Assim,

$$B = C_G(G') = \bigcap_{w \in G'} C_G(w) = \bigcap_{i=1}^{n} C_G(x_i)$$

e temos:

$$| \ G : B \ | \leq \prod_{i=1}^{n} | \ G : C_G(x_i) \ |$$

Então, basta mostrarmos que $| \ G : C_G(x_i) \ | = | \ x_i^G \ |$ é finito, para cada i.

Seja $\overline{w} \in \overline{G'}$ qualquer, onde $\overline{G} = \dfrac{G}{N}$.

Sendo $\overline{G'}$ cíclico infinito, $Aut\overline{G'} = \{Id, \theta : x \to x^{-1}\}$.

Daí, $\langle \overline{w} \rangle \lhd_{car} \overline{G'} \lhd \overline{G}$, o que implica $\langle \overline{w} \rangle \lhd \overline{G}$.

Pelo NC-Lema, temos então:

$$\frac{\overline{G}}{C_{\overline{G}}(\langle\overline{w}\rangle)} \lesssim Aut\langle\overline{w}\rangle \simeq \mathbb{Z}_2$$

Como $C_{\overline{G}}(\langle\overline{w}\rangle) = C_{\overline{G}}(\overline{w})$, segue que

$$\mid \overline{w}^{\overline{G}} \mid = \mid \overline{G} : C_{\overline{G}}(\overline{w}) \mid \leq 2$$

Do resultado 1 sabemos que:

$$\mid w^G \mid \leq \mid \overline{w^G} \mid \mid N \mid$$

Agora,

$$\overline{w}^{\overline{G}} = \{wN^{gN} \ ; \ g \in G\} = \overline{w^G}$$

Daí,

$$\mid G : C_G(w) \mid = \mid w^G \mid \leq \mid \overline{w}^{\overline{G}} \mid \mid N \mid \leq 2. \mid N \mid < \infty, \ \forall w \in G'$$

$\therefore \mid G : B \mid < \infty$

Seja $F = \{x \in G \ ; \ x^G$ é finito $\}$, o FC-subgrupo de G.

Se $F = G$, então $\mid G : C_G(x) \mid = \mid x^G \mid < \infty, \ \forall x \in G.$

Por outro lado, sendo G finitamente gerado, digamos, $G = \langle g_1, ..., g_n\rangle$, temos:

$$Z(G) = \bigcap_{i=1}^{n} C_G(g_i)$$

Daí,

$$\mid G : Z(G) \mid \leq \prod_{i=1}^{n} \mid G : C_G(g_i) \mid < \infty$$

Segue então de Schur, que G' é finito, o que é uma contradição.

Portanto, F é subgrupo próprio de G.

Tomemos $g \in G \backslash F$. Então, $\mid g^G \mid = \infty$.

Como $\mid g^G \mid \leq \mid \overline{g^G} \mid \mid N \mid$ e $\mid N \mid < \infty$, devemos ter necessariamente, $\mid \overline{g}^{\overline{G}} \mid = \mid \overline{g^G} \mid = \infty$.

Afirmação 2: $\exists b \in B$ tal que $[\overline{g}, \overline{b}] \neq \overline{1}$

Suponhamos por absurdo, $[\overline{g}, \overline{b}] = \overline{1}, \ \forall b \in B$.

$\overline{g}^{\ -1} \ \overline{g}^{\ \overline{b}} = [\overline{g}, \overline{b}] = \overline{1} \ \Rightarrow \ \overline{g}^{\ \overline{b}} = \overline{g}, \forall b \in B$

Logo, $\overline{B} \leq C_{\overline{G}}(\overline{g})$.

Em diagramas:

$$\begin{array}{c} \overline{G} \\ | \\ C_{\overline{G}}(\overline{g}) \\ | \\ \overline{B} \end{array}$$

Sendo $| \ \overline{G} : \overline{B} \ | = | \ G : B \ | < \infty$, segue que $| \ \overline{g}^{\overline{G}} \ | = \ \overline{G} : C_{\overline{G}}(\overline{g}) < \infty$, o que é uma contradição.

Isso prova nossa afirmação.

Agora,

$$\begin{aligned} [\overline{g}, \overline{b}] \neq \overline{1} \ &\Rightarrow \ [g,b]N \neq N \ \Rightarrow \ [g,b] \notin N \\ &\Rightarrow \ o([g,b]) = \infty \end{aligned}$$

Além disso,

$$[g, b^i] = [g,b]^i, \ \forall i \in \mathbb{N}$$

Para ver isto, façamos indução sobre i.
Para $i = 1$, ok!
Suponhamos válido para $i = n$.

Então,

$$\begin{aligned} [g, b^{n+1}] &= [g, b^n.b] = [g,b] \ [g, b^n]^b \\ &= [g,b] \ [g, b^n] \\ &= [g,b] \ [g,b]^n \\ &= [g,b]^{n+1} \end{aligned}$$

Portanto,

$$[g, b^i] = [g,b]^i, \ \forall i \in \mathbb{N} \qquad (*)$$

Afirmação 3: $N = \langle X_0 \rangle$ não contém comutadores não triviais da forma $[g, x]$, com $x \in G$ qualquer.

Suponhamos ao contrário, que exista $1 \neq [g, x] \in N$ para algum $x \in G$.

Sendo $G' \lhd G$, segue que $C_G(G') = B \lhd G$.

Logo, $[g, b] \in B$ (I.e., $[g, b]$ centraliza G')

Assim, o subgrupo $L = \langle [g, b], [g, x] \rangle$ é abeliano e, consequentemente, $L = \langle [g, b] \rangle \times \langle [g, x] \rangle \simeq C_\infty \times C_m$,para algum $m > 1$ (já que $[g, b]$ tem ordem infinita e $[g, x] \in N$).

Por outro lado, usando $(*)$, temos:

$$\begin{aligned} [g, b]^i [g, x] &= [g, b^i]\ [g, x] \\ &= [g, b^i]\ [g, x]^{b^i} \quad \text{(pois } b^i \in B) \\ &= [g, xb^i],\ \forall i \in \mathbb{N}, \end{aligned}$$

o que contradiz o Lema 4.12.

Fica então provada nossa afirmação.

Sendo $N \lhd G$, temos: $[g, N] \leq N$.

Logo, $[g, N] = 1$ e $N \leq C_G(g),\ \forall g \in G \backslash F$

$$\therefore\ N \leq \bigcap_{g \in G \backslash F} C_G(g) = C_G(G \backslash F)$$

Como F é subgrupo próprio de G, segue do resultado 2, mostrado acima que

$$G = \langle G \backslash F \rangle$$

Assim, $Z(G) = C_G(G \backslash F)$ e $N \leq Z(G)$.

Afirmo que $Z(\overline{G}) = \overline{Z(G)}$.

Claramente, $\overline{Z(G)} \leq Z(\overline{G})$.

Agora, seja $xN \in Z(\overline{G})$ qualquer.

Então,
$$[gN, xN] = N, \ \forall g \in G \backslash F$$

o que implica,
$$[g, x] \in N, \ \forall g \in G \backslash F$$

Daí, pelo que mostramos acima, temos: $[g, x] = 1, \ \forall g \in G \backslash F$.

$\therefore \ x \in C_G(G \backslash F) = Z(G)$

$\therefore \ Z(\overline{G}) \leq \overline{Z(G)}$

$\therefore \ \overline{Z(G)} = Z(\overline{G})$

O restante da prova é praticamente a mesma do Teorema 4.14.

Afirmo que $N = 1$.

Suponhamos $N \neq 1$.

Afirmação 4: Podemos assumir N cíclico

Como $N \leq Z(G)$, N é abeliano.
Além disso, N é gerado por X, que é finito.
Daí, N é abeliano finitamente gerado. E sendo N de torção, temos pelo T.F.G.A.F.G que:

$$N = C_{n_1} \times \ \ldots \ \times C_{n_k}$$

Suponhamos que fosse $n_i > 1, \forall i$.
Seja $H = C_{n_1} \times \ \ldots \ \times C_{n_{k-1}}$.
Como $H < N \leq Z(G), H \lhd G$.
Consideremos o quociente G/H.
Note que:

$$\{[g_1 H, g_2 H]; g_i \in G\} = \{[g_1, g_2]H; g_i \in G\} \subset \bigcup_{C \in \mathcal{C}} \frac{CH}{H}$$

E pelo 2° Teorema dos Isomorfismos, $\dfrac{CH}{H} \simeq \dfrac{C}{C \cap H}$.
Como C é cíclico, $\dfrac{C}{C \cap H}$ é cíclico. Logo, $\dfrac{CH}{H}$ é cíclico para cada $C \in \mathcal{C}$.

Portanto, $\left\{\dfrac{CH}{H}\right\}_{C \in \mathcal{C}}$ é família finita de subgrupos cíclicos cobrindo o conjunto dos comutadores de $\dfrac{G}{H}$.

Seja $\widetilde{X_0}$ o conjunto dos comutadores de $\dfrac{G}{H}$ de ordem finita e $\widetilde{N} = \langle \widetilde{X_0} \rangle$.

Afirmo que $\widetilde{N} = \dfrac{N}{H}$.

De fato,

$$\begin{aligned}
[g_1H, g_2H] \in \widetilde{X_0} \ &\Rightarrow \ o([g_1H, g_2H]) = l, \exists l \in \mathbb{Z}_+ \ \Rightarrow \ [g_1, g_2]^l \in H \leq N \\
&\Rightarrow \ \exists k \in \mathbb{Z}_+; [g_1, g_2]^{lk} = 1 \\
&\Rightarrow \ [g_1, g_2] \in N \\
&\Rightarrow \ [g_1H, g_2H] = [g_1, g_2]H \in N/H
\end{aligned}$$

Portanto, $\widetilde{N} = \langle \widetilde{X_0} \rangle \leq N/H$ e temos $\widetilde{N} = N/H = C_{n_k}$.

Supondo então o teorema provado para grupos cujo N seja cíclico finito temos que $\dfrac{G'}{H} \simeq C_\infty$. Logo, $G' = H \times C_\infty$.

Por outro lado, $G' = N \times C_\infty = H \times C_{n_k} \times C_\infty$.

Daí, $C_{n_k} = 1$. Absurdo!

Portanto, N é cíclico.

Lembre que $\overline{G}' \simeq C_\infty$. Digamos que seja $\overline{G}' = \dfrac{G'}{N} = \langle aN \rangle$.

Então,

$$G' = \langle a, N \rangle = \langle a \rangle N$$

e G' é 2-gerado.

Suponha $\overline{G}$ nilpotente de classe menor ou igual a 2.

Se $\overline{G}$ for nilpotente de classe 0, então $Z_0(\overline{G}) = \overline{G}$. Mas, $Z_0(\overline{G}) = \overline{1} = N$.

Logo, $G = N$, o que contradiz o fato de que G' é infinito.

E se $\overline{G}$ for nilpotente de classe 1, então, $Z_1(\overline{G}) = \overline{G}$ e $\overline{G}$ é abeliano.

Daí, $\overline{G}' = \overline{1}$. Absurdo!

Desse modo, devemos ter $\overline{G}$ nilpotente de classe 2.

Sendo $\dfrac{G}{Z(G)} \simeq \dfrac{\overline{G}}{\overline{Z(G)}} = \dfrac{\overline{G}}{Z(\overline{G})}$, temos que G também é nilpotente de classe 2.

Segue então do Teorema 4.13 que todo elemento de G' é um comutador.

Portanto, $G' = \langle X \rangle$ possui cobertura finita por cíclicos, daí é finito ou cíclico.

Mas, estamos supondo G' infinito.

Logo, teríamos G' cíclico e, portanto, todos os seus elementos não triviais são de ordem infinita, o que contradiz o fato de que $N \neq 1$.

Desse modo, $\overline{G}$ não é nilpotente de classe menor ou igual a 2.

Pelo Lema 4.10, existe um subgrupo A de índice 2 em G o qual contém N, e tal que $\overline{A}$ é abeliano e $\dfrac{\overline{A}}{Z(\overline{G})}$ é cíclico.

Como $\dfrac{\overline{A}}{Z(\overline{G})} = \dfrac{\overline{A}}{\overline{Z(G)}} \simeq \dfrac{A}{Z(G)}$, temos que $\dfrac{A}{Z(G)}$ também é cíclico.

Digamos que seja $\dfrac{A}{Z(G)} = \langle aZ(G) \rangle$.

Sejam $a_1, a_2 \in A$ quaisquer.

Como $a_1Z(G) \in A/Z(G)$ e $a_2Z(G) \in A/Z(G)$, $\exists m, n \in \mathbb{N}$ tais que $a_1Z(G) = a^mZ(G)$ e $a_2Z(G) = a^nZ(G)$.

Daí, $a_1 = a^m z_1$ e $a_2 = a^n z_2$ com $z_1, z_2 \in Z(G)$.

Desse modo,

$$\begin{aligned} a_1\ a_2 = a^m\ z_1\ a^n\ z_2 \ &= \ a^m\ a^n\ z_1\ z_2 \ = \ a^n\ a^m\ z_2\ z_1 \\ = a^n\ z_2\ a^m\ z_1 \ &= \ a_2\ a_1 \end{aligned}$$

Portanto, A é abeliano.

Pelo Lema 4.11, G' consiste inteiramente de comutadores, o que mais uma vez é uma contradição.

Portanto, $N = 1$, e segue do Teorema 4.14 que G' é cíclico. ■

Apêndice : Um teste para comutadores

1. Introdução

No decorrer do estudo de subgrupos comutadores, I.D.Macdonald [1] apresentou um grupo nilpotente livre G_4 de classe 2, gerado por 4 elementos, como exemplo de um grupo nilpotente no qual o subgrupo comutador possui elementos que não são comutadores. Para demonstrar isso, ele procedeu como segue: seja $G_4 = \langle a_1, a_2, a_3, a_4 \rangle$ e faça $c_{ij} = [a_i, a_j]$ para $1 \leq i < j \leq 4$ e $1 \leq k \leq 4$, e suas consequências. Macdonald observou que um comutador arbitrário pode ser escrito como:

$$[a_1^{\alpha_1} \ . \ a_2^{\alpha_2} \ . \ a_3^{\alpha_3} \ . \ a_4^{\alpha_4} \ , \ a_1^{\beta_1} \ . \ a_2^{\beta_2} \ . \ a_3^{\beta_3} \ . \ a_4^{\beta_4}] \quad ,$$

o que simplicado dá:

$$\prod_{1 \leq i < j \leq 4} c_{ij}^{\delta_{ij}}$$

onde $\delta_{ij} = \alpha_i \beta_j - \alpha_j \beta_i$. Os índices δ_{ij} satisfazem a relação:

$$\delta_{12}\delta_{34} - \delta_{13}\delta_{24} + \delta_{14}\delta_{23} = 0$$

(1)

Segue que o elemento $c_{13}c_{24}$ em G_4'(para o qual $\delta_{12} = \delta_{14} = \delta_{23} = \delta_{34} = 0$ e $\delta_{13} = \delta_{24} = 1$) não é um comutador.
A relação (1) não é somente necessária, mas também suficiente para que o elemento $\prod c_{ij}^{\delta_{ij}}$ seja comutador no grupo G_4. Provaremos a generalização para grupos nilpotentes de classe 2 finitamente gerados. Como uma aplicação mostraremos que se o subgrupo comutador G' de um grupo G é central em G e pode ser gerado por um ou por dois elementos, então todo elemento de G' é um comutador.

2. O Teorema Principal

Em toda esta seção, G denota um grupo nilpotente de classe 2 que é gerado pelos elementos $a_1, \ . \ . \ . \ , a_n$.
Seja $c_{ij} = [a_i, a_j]$ para $1 \leq i < j \leq 4$. Então, $c_{ji} = c_{ij}^{-1}$.
Um elemento c do subgrupo comutador G' é expresso da forma:

$$c = \prod_{1\leq i<j\leq n} c_{ij}^{\delta_{ij}} \tag{2}$$

onde $\delta_{ij} \in \mathbb{Z}$, para todos $1 \leq i < j \leq n$.
Associemos a cada $c \in G'$ como acima, a matriz quadrada $\Delta = (\delta_{ij})$ e façamos:

$$\Delta_{qrst} = \delta_{qr}\delta_{st} - \delta_{qs}\delta_{rt} + \delta_{qt}\delta_{rs}$$

quando $1 \leq q, r, s, t \leq n$.

As seguintes regras se verificam:

a) Se τ é uma transposição que permuta dois dos símbolos q, r, s, t, então:

$$\Delta_{\tau(q)\tau(r)\tau(s)\tau(t)} = -\Delta_{qrst}$$

b) Se dois entre q, r, s, t são iguais, então $\Delta_{qrst} = 0$.

Prova: a) Suponhamos, por exemplo, $\tau = (qr)$

Então,

$$\begin{aligned} \Delta_{\tau(q)\tau(r)\tau(s)\tau(t)} = \Delta_{rqst} &= \delta_{rq}\delta_{st} - \delta_{rs}\delta_{qt} + \delta_{rt}\delta_{qs} \\ &= -\ \delta_{qr}\delta_{st} + \delta_{qs}\delta_{rt} - \delta_{qt}\delta_{rs} \\ &= -(\delta_{qr}\delta_{st} - \delta_{qs}\delta_{rt} + \delta_{qt}\delta_{rs}) \\ &= -\Delta_{qrst} \end{aligned}$$

b) Suponhamos, por exemplo, $q = r$.

Então,

$$\Delta_{qrst} = \Delta_{qqst} = \delta_{qq}\delta_{st} - \delta_{qs}\delta_{qt} + \delta_{qt}\delta_{qs} = 0$$

Temos o seguinte resultado:

Teorema 1. *O elemento c de G' dado em (2) é um comutador se a matriz associada Δ satisfaz:*

$$\Delta_{qrst} = 0, \quad \forall\ 1 \leq q, r, s, t \leq n \qquad (4)$$

Observação: Em virtude das propriedades a) e b), a condição (4) é equivalente a

$$\Delta_{qrst} = 0, \quad \forall\ 1 \leq q < r < s < t \leq n$$

(5)

De fato, suponhamos (5) válida e consideremos $1 \leq q, r, s, t \leq n$.
Se existirem dois iguais entre q, r, s, t, então, sabemos de b) que $\Delta_{qrst} = 0$, e a prova estaria concluída.
Então, podemos supor q, r, s, t todos distintos.
Se for $q < r < s < t$, o resultado segue da nossa hipótese.
Agora, se tivermos, por exemplo, $r < q < s < t$, tomando $\tau = (rq)$, temos por a):

$$\Delta_{qrst} \;=\; \Delta_{\tau(r)\tau(q)\tau(s)\tau(t)} \;=\; -\Delta_{rqst} \;=\; 0$$

Analogamente, nos demais casos em que q, r, s, t são distintos, temos:

$$\Delta_{qrst} = 0,$$

bastando tomar a transposição adequada e usar a propriedade a) quantas vezes for necessário. Essas condições valem trivialmente quando $n \leq 3$, daí, um caso especial do Teorema 1 é que G' consiste inteiramente de comutadores quando G pode ser gerado por não mais que três elementos.

Antes da prova do Teorema 1, estabelecemos o lema seguinte, relativo ao efeito de certas mudanças do conjunto gerador de G sobre a representação de c como produto de comutadores.

Lema 1. Considere os seguintes tipos de mudanças "elementares" do conjunto gerador de G:

Tipo I(*Transposição*): $a_i^* = a_{\tau(i)}, \forall i$, onde τ é uma transposição (kl),
$1 \leq k, l \leq n$;
Tipo II(*Inversão*): $a_k^* = a_k^{-1},\ a_i^* = a_i, \forall i \neq k$;
Tipo III(*Combinação*): $a_k^* = a_k.a_l^*(k \neq l,\ \alpha \in \mathbb{Z}),\ a_i^* = a_i,\ \forall i \neq k$.

Faça $c_{ij}^* = [a_i^*, a_j^*]$. Seja o elemento c de G' expresso por:

$$c = \prod_{1 \leq i < j \leq n} c_{ij}^{\delta_{ij}}$$

relativo ao conjunto gerador $\{c_{ij}\ ;\ 1 \leq i < j \leq n\}$ de G'. Então, existe uma expressão para c da forma:

$$c = \prod_{1 \leq i < j \leq n} {c_{ij}^*}^{\delta_{ij}^*}$$

onde as entradas das matrizes correspondentes $\Delta = (\delta_{ij})$ e $\Delta^* = (\delta_{ij}^*)$ estão relacionadas como segue:

Tipo I: $\delta_{ij}^* = \delta_{\tau(i)\tau(j)}$; em particular, $\delta_{kl}^* = -\delta_{kl}$
$\Delta_{qrst}^* = \Delta_{\tau(q)\tau(r)\tau(s)\tau(t)}$

Tipo II: $\delta_{ik}^* = -\delta_{ik}$ e $\delta_{ij}^* = \delta_{ij}$ para $j \neq k$
$$\Delta_{qrst}^* = (-1)^{\lambda}\Delta_{qrst}, \text{ onde } \lambda = \begin{cases} 1, & se\ k \in \{q,r,s,t\} \\ 0, & se\ k \notin \{q,r,s,t\} \end{cases}$$

Tipo III: $\delta_{il}^* = \delta_{il} - \alpha\delta_{ik},\ \forall i$ e $\delta_{ij}^* = \delta_{ij}$ quando $i, j \neq l$
$\Delta_{qrst}^* = \Delta_{qrst}$, se $l \notin q, r, s, t$
$\Delta_{lrst}^* = \Delta_{lrst} - \alpha\Delta_{krst}$

Em particular, se $\Delta_{qrst} = 0$ sempre, então $\Delta_{qrst}^* = 0$ sempre.

Prova: · Tipo I
Note que δ_{ij}^* é o expoente de $c_{ij}^* = [a_i^*, a_j^*] = [a_{\tau(i)}, a_{\tau(j)}]$.
Logo, $\delta_{ij}^* = \delta_{\tau(i)\tau(j)},\ \forall i, j$.
Em particular, $\delta_{kl}^* = \delta_{\tau(k)\tau(l)} = \delta_{lk} = -\delta_{kl}$.

Daí,
$$\begin{aligned}\Delta_{qrst}^* &= \delta_{qr}^*\delta_{st}^* - \delta_{qs}^*\delta_{rt}^* + \delta_{qt}^*\delta_{rs}^* \\ &= \delta_{\tau(q)\tau(r)}\delta_{\tau(s)\tau(t)} - \delta_{\tau(q)\tau(s)}\delta_{\tau(r)\tau(t)} + \delta_{\tau(q)\tau(t)}\delta_{\tau(r)\tau(s)} \\ &= \Delta_{\tau(q)\tau(r)\tau(s)\tau(t)}\end{aligned}$$

· Tipo II
Sendo G nilpotente de classe 2, temos:
$1 = [a_i, a_k^{-1}a_k] = [a_i, a_k]\ [a_i, a_k^{-1}]^{a_k} = [a_i, a_k]\ [a_i, a_k^{-1}]$
$\therefore [a_i, a_k^{-1}] = [a_i, a_k]^{-1}$
Daí, $\forall i \neq k$, temos: $c_{ik}^* = [a_i^*, a_k^*] = [a_i, a_k^{-1}] = c_{ik}^{-1}$, o que implica, $\delta_{ik}^* = -\delta_{ik}$.
Para $i, j \neq k$, temos: $c_{ij}^* = c_{ij}$ e consequentemente, $\delta_{ij}^* = \delta_{ij}$.
Desse modo, se $k \in \{q, r, s, t\}$, por exemplo, $k = r$, então:

$$\begin{aligned}\Delta_{qrst}^* &= \delta_{qr}^*\delta_{st}^* - \delta_{qs}^*\delta_{rt}^* + \delta_{qt}^*\delta_{rs}^* \\ &= \delta_{qk}^*\delta_{st}^* - \delta_{qs}^*\delta_{kt}^* + \delta_{qt}^*\delta_{ks}^* \\ &= -\delta_{qk}\delta_{st} + \delta_{qs}\delta_{kt} - \delta_{qt}\delta_{ks} \\ &= -\delta_{qk}\delta_{st} - \delta_{qs}\delta_{kt} + \delta_{qt}\delta_{ks}\end{aligned}$$

$$\begin{aligned} &= -\Delta_{qkst} \\ &= -\Delta_{qrst} \end{aligned}$$

Agora, se $k \notin \{q, r, s, t\}$, como $\delta^*_{ij} = \delta_{ij},\ \forall i, j \neq k$, temos $\Delta^*_{qrst} = \Delta_{qrst}$.
Assim,

$$\Delta^*_{qrst} = (-1)^{\lambda}\Delta_{qrst}, \text{ onde } \lambda = \begin{cases} 1, & se\ k \in \{q, r, s, t\} \\ 0, & se\ k \notin \{q, r, s, t\} \end{cases}$$

$\cdot$ Tipo III
Suponhamos $k < l$.

Veja que

$$\begin{aligned} c^*_{ik} = [a^*_i, a^*_k] &= [a_i, a_k a^{\alpha}_l] \\ &= [a_i, a^{\alpha}_l]\ [a_i, a_k] \\ &= [a_i, a_k]\ [a_i, a_l]^{\alpha} \\ &= c_{ik}\ .\ c^{\alpha}_{il} \end{aligned}$$

$\therefore\ c_{ik} = c^*_{ik}\ .\ c^{-\alpha}_{il}$
$\therefore\ c^{\delta_{ik}}_{ik} = c^*_{ik}\ .\ c^{-\alpha\delta_{ik}}_{il}$ e $c^{\delta_{ij}}_{ij} = c^*_{ij},\quad \forall i, j \neq k$

Daí,

$$c = \prod_{1 \leq < j \leq n} c^{\delta_{ij}}_{ij} = c^{\delta_{12}}_{12} \ldots c^{\delta_{1n}}_{1n} \ldots c^{\delta_{i1}}_{i1} \ldots c^{\delta_{ik}}_{ik} \ldots c^{\delta_{il}}_{il} \ldots c^{\delta_{in}}_{in} \ldots c^{\delta_{n-1,n}}_{n-1,n}$$

$$= c^{\delta_{12}}_{12} \ldots c^{\delta_{1n}}_{1n} \ldots c^{\delta_{i1}}_{i1} \ldots \left(c^{*\ \delta_{ik}}_{ik} c^{-\alpha\delta_{ik}}_{il}\right) \ldots c^{\delta_{il}}_{il} \ldots c^{\delta_{in}}_{in} \ldots c^{\delta_{n-1,n}}_{n-1,n}$$

$$= c^{*\ \delta_{12}}_{12} \ldots c^{*\ \delta_{1n}}_{1n} \ldots c^{*\ \delta_{i1}}_{i1} \ldots c^{*\ \delta_{ik}}_{ik} \ldots c^{*\ \delta_{il} - \alpha\delta_{ik}}_{il} \ldots c^{*\ \delta_{in}}_{in} \ldots c^{*\ \ \delta_{n-1,n}}_{n-1,n}$$

Portanto, $\delta^*_{il} = \delta_{il} - \alpha\delta_{ik},\ \forall i$ e $\delta^*_{ij} = \delta_{ij},\ \forall i, j \neq l$.

Isso nos dá:

$$\begin{aligned} \Delta^*_{lrst} &= \delta^*_{lr}\delta^*_{st} - \delta^*_{ls}\delta^*_{rt} + \delta^*_{lt}\delta^*_{rs} \\ &= -\delta^*_{rl}\delta^*_{st} + \delta^*_{sl}\delta^*_{rt} - \delta^*_{tl}\delta^*_{rs} \\ &= -(\delta_{rl} - \alpha\delta_{rk})\delta_{st} + (\delta_{sl} - \alpha\delta_{sk})\delta_{rt} - (\delta_{tl} - \alpha\delta_{tk})\delta_{rs} \\ &= \delta_{rl}\delta_{st} - \delta_{ls}\delta_{rt} - \delta_{lt}\delta_{rs} - \alpha(\delta_{kr}\delta_{st} - \delta_{ks}\delta_{rt} + \delta_{kt}\delta_{rs}) \\ &= \Delta_{lrst} - \alpha\Delta_{krst} \end{aligned}$$

e

$$\Delta^*_{qrst} = \Delta_{qrst}, \quad \text{se} \quad l \notin \{q, r, s, t\}$$

$\blacksquare$

Dizemos que a matriz $\overline{\Delta}$ é equivalente a Δ se $\overline{\Delta}$ está relacionada a Δ por uma sequência finita de transformações dos tipos I, II e III. Essas transformações são claramente invertíveis, o que condiz com o fato de que esta relação é de equivalência.

Prova do Teorema 1: A prova é por indução sobre n, o número de elementos no conjunto gerador $a_1, ..., a_n$ de G.
Quando $n = 1$, G é cíclico e portanto, abeliano. Daí, $G' = 1$ e o resultado segue.
Para $n = 2$, $G = \langle a_1, a_2 \rangle = \{x_1 \ . \ . \ . \ x_n \ ; \ x_i \in \{a_1, a_2, a_1^{-1}, a_2^{-1}\}\}$
É fácil ver que, $G' = \langle [a_1, a_2] \rangle$.
Sendo G nilpotente de classe 2, temos que:

$$[a_1, a_2]^k = [a_1^k, a_2], \ \forall k \in \mathbb{Z}$$

Logo, todo elemento de G' é um comutador.
Agora, analisemos o caso em que $n \geq 3$.
Suponhamos o Teorema válido para todos os grupos nilpotentes de classe 2 definidos sobre menos que n geradores. Seja c um elemento de G' dado como em (2) e tal que $\Delta_{qrst} = 0$ para todos $1 \leq q, r, s, t \leq n$. Mostraremos que c é um comutador.
Sendo G nilpotente de classe 2, temos que $G' \leq Z(G)$.
Daí, G' é abeliano e podemos escrever:

$$c = \prod_{1 \leq k \leq n-1} c_{kn}^{\delta_{kn}} \prod_{1 \leq i < j \leq n-1} c_{ij}^{\delta_{ij}}$$

Da nossa hipótese de indução, segue que $\displaystyle\prod_{1 \leq i < j \leq n-1} c_{ij}^{\delta_{ij}}$ é comutador do grupo $G_1 = \langle a_1, ..., a_{n-1} \rangle \subset G$.
Se fosse $\delta_{kn} = 0, \ \forall k = \{1, ..., n-1\}$, já teríamos c comutador. Então, podemos supor $\delta_{kn} \neq 0$ para algum k. Seja d o MDC de $\delta_{1n}, \delta_{2n}, ..., \delta_{n-1,n}$.
Note que $d \neq 0$.
Faça $\delta_{kn} = d\alpha_k$, para cada $k = 1, ..., n-1$.
Consideremos o conjunto gerador $\{\overline{a}_1, ..., \overline{a}_n\}$ de G_n, onde

$$\overline{a}_1 = a_1^{\alpha_1} ... a_n^{\alpha_n} \ \text{ e } \ \overline{a}_i = a_i, \ \forall i \neq 1$$

o qual é obtido de $\{a_1, ..., a_n\}$ por uma sequencia de mudanças elementares . Então, existe uma matriz $\overline{\Delta} = (\overline{\delta}_{ij})$ equivalente a Δ e uma expressão correspondente para c da forma:

$$c = \prod_{1 \leq i < j \leq n-1} \overline{c}_{ij}^{\ \overline{\delta}_{ij}}$$

Veja que: $\begin{cases} \overline{c}_{1n} \;=\; [\overline{a}_1, \overline{a}_n] \;=\; [a_1^{\alpha_1} \ldots\, a_{n-1}^{\alpha_{n-1}}, a_n] \;=\; c_{1n}^{\alpha_1} \ldots\, c_{n-1,n}^{\alpha_{n-1,n}} \\ \overline{c}_{in} \;=\; c_{in},\ \forall i \neq 1 \end{cases}$

Daí, $\overline{c}_{1n}^{d} = c_{1n}^{\delta_{1n}} \ldots\, c_{n-1,n}^{\delta_{n-1,n}}$ e temos:

$$c = \overline{c}_{1n}^{d} . \prod_{1 \leq i < j \leq n-1} c_{ij}^{\delta_{ij}} \;=\; \overline{c}_{1n}^{d} . \prod_{1 \leq i < j \leq n-1} \overline{c}_{ij}^{\overline{\delta}_{ij}}$$

Isto indica que $\overline{\delta}_{1n} = d$ e $\overline{\delta}_{in} = 0$ para $i = 2, ..., n-1$.

Para o caso $n = 3$, temos:

$$\begin{aligned} c \;&=\; \overline{c}_{13}{}^{d}\, \overline{c}_{12}{}^{\overline{\delta}_{12}} \;=\; [\overline{a}_1, \overline{a}_3]^d\, [\overline{a}_1, \overline{a}_2]^{\overline{\delta}_{12}} \\ &=\; [\overline{a}_1, \overline{a}_3^{d}]\, [\overline{a}_1, \overline{a}_2^{\overline{\delta}_{12}}] \\ &=\; [\overline{a}_1, \overline{a}_2^{\overline{\delta}_{12}} \overline{a}_3^{d}] \end{aligned}$$

provando que c é um comutador.

Suponhamos então, $n \geq 4$. Pelo Lema 1, $\overline{\Delta}_{qrst} = 0,\ \forall 1 \leq q, r, s, t \leq n$. Em particular, escolhamos q, r, s e t tais que $q = 1 < r < s < n = t$. Sendo $\overline{\delta}_{kn} = 0$ para $1 < k < n$ temos que $\overline{\delta}_{rn} = 0 = \overline{\delta}_{sn}$.

Daí,

$$\begin{aligned} 0 = \overline{\Delta}_{qrst} &= \overline{\delta}_{qr}\overline{\delta}_{st} - \overline{\delta}_{qs}\overline{\delta}_{rt} + \overline{\delta}_{qt}\overline{\delta}_{rs} \\ &= \overline{\delta}_{1r}\overline{\delta}_{sn} - \overline{\delta}_{1s}\overline{\delta}_{rn} + \overline{\delta}_{1n}\overline{\delta}_{rs} \\ &= \overline{\delta}_{1n}\overline{\delta}_{rs} \\ &= d\ \overline{\delta}_{rs} \end{aligned}$$

Como $d \neq 0$, segue que $\overline{\delta}_{rs} = 0$

$\therefore\ \overline{\delta}_{rs} = 0,\ \forall 1 < r < s < n$

Assim,

$$\begin{aligned} c = \;& \overline{c}_{1n}^{d} \prod_{j=2}^{n-1} \overline{c}_{1j}^{\overline{\delta}_{1j}} \\ &= [\overline{a}_1, \overline{a}_n]^d\ [\overline{a}_1, \overline{a}_2]^{\overline{\delta}_{12}}\ .\ .\ .\ [\overline{a}_1, \overline{a}_{n-1}]^{\overline{\delta}_{1,n-1}} \\ &= [\overline{a}_1, \overline{a}_{n-1}^{\overline{\delta}_{1,n-1}} \ldots\, \overline{a}_{12}^{\overline{\delta}_{12}} \overline{a}_n^{d}] \end{aligned}$$

o que conclui nossa prova.

■

3. Aplicações

Aplicamos nosso teste para comutadores para provar o seguinte resultado:

Teorema 2. *Suponha o subgrupo comutador G' de um grupo G central em G e gerado por não mais que dois geradores. Então, todo elemento de G' é um comutador.*

Prova: Analisemos o caso em que G' é um grupo cíclico.
Suponhamos primeiro G' finito.
Se G é finito, então este é produto direto de finitos p_i-grupos G_i para primos distintos $p_1 \; . \; . \; . \; p_n$.
I.e.,

$$G = G_1 \times \; . \; . \; . \; \times G_n$$

onde $\mid G_i \mid = \; p_i^{e_i}$ para cada i e $G_i \lhd G, \; \forall i$.
Agora, sendo G' cíclico e G_i p_i-grupo, G_i' é um p_i-grupo cíclico.
Digamos que seja $G_i' = \langle x_i \rangle$ com $o(x_i) = p_i^{m_i}, \; m_i \leq e_i$.
Para que um subgrupo de G_i' seja maximal este deve ter ordem p.
Sendo G_i' cíclico sabemos que seu único subgrupo de ordem p é $M = \langle x_i^{p_i^{m_i-1}} \rangle$.
Assim, $\phi(G_i') = \langle x_i^{p_i^{m_i-1}} \rangle$ e $\mid G_i' : \phi(G_i') \mid = \; p$.

Seja $c_i = [a_i, b_i] \in G_i' \backslash \phi(G_i')$ e considere $H = \langle c_i, \phi(G_i) \rangle$.
Como $\phi(G_i') \lneqq H < G_i'$ e $\phi(G_i')$ tem índice primo em G_i', segue que $H = G_i'$.
I.e.,

$$G_i' = \langle \; c, \; \phi(G_i') \; \rangle$$

Afirmo que $G_i' = \langle c_i \rangle$.
De fato, suponhamos $G_i' \neq \langle c_i \rangle$.
Então, $\exists M \lessdot G_i'$ tal que $c_i \in M$.
Claro que também, $\phi(G_i') \leq M$. Daí, $G_i' = \langle \; c, \; \phi(G_i') \; \rangle \leq M$. Absurdo!
Logo, $G_i' = \langle c_i \rangle, \; \forall i = 1, ..., n$.
Sendo $G = G_1 \times \; . \; . \; . \; \times G_n$, temos que:

$$\begin{aligned} G' &= G_1' \times \; . \; . \; . \; \times G_n' \\ &= \langle \; [a_1, b_1] \; \rangle \times \; . \; . \; . \; \times \langle \; [a_n, b_n] \; \rangle \\ &= \langle \; [a_1, b_1] \; . \; . \; . \; [a_n, b_n] \; \rangle && \text{(pois } G' \leq Z(G)\text{)} \\ &= \langle \; [a_1 a_2 \; . \; . \; . \; a_n \; , \; b_1 b_2 \; . \; . \; . \; b_n] \; \rangle && \text{(pois os } H_i\text{'s comutam)} \end{aligned}$$

Quando G é infinito, G' ainda é gerado por um número finito de comutadores.
Digamos que seja $G' = \langle g_1', \; . \; . \; . \; g_r' \rangle$, onde $g_i' = [c_i, d_i] \in G$.

Podemos supor, nesse caso, G finitamente gerado.
De fato, suponhamos o resultado válido para grupos finitamente gerados.
Então, se G é um grupo o qual não é finitamente gerado, tomando
$H = \langle c_i, d_i \ ; \ i = 1, ..., n\rangle$ temos que $H' = G'$ e daí o resultado segue também para G.
Façamos $G = \langle g_1, ..., g_r\rangle$.

Fixado $x \in G$ consideremos a aplicação $\begin{array}{l} \varphi : x^G \rightarrow G' \\ \quad\ x^g \rightarrow [x, g] \end{array}$

É fácil ver que φ é injetiva. Daí, $\mid G : C_G(x) \mid = \mid x^G \mid \leq \mid G' \mid < \infty, \ \forall x \in G$.
Em particular,

$$\mid G : C_G(g_i) \mid < \infty, \ \forall i = 1, ..., r$$

Assim,

$$\mid G : Z(G) \mid = \mid G : \bigcap_{i=1}^{r} C_G(g_i) \mid < \infty$$

e $Z(G)$ também é finitamente gerado.

<u>*Afirmação*</u>: $\exists N \lhd G$ tal que $\dfrac{G}{N}$ é finito e $N \cap G' = 1$.

De fato, basta tomar N como sendo qualquer subgrupo maximal livre de torção do centro de G.
Considere o conjunto

$$\mathcal{A} = \{L \leq Z(G) \ ; \ L \text{ é livre de torção}\}$$

Se $\forall x \in Z(G)$ tivéssemos $o(x) < \infty$, então, como $Z(G)$ é abeliano finitamente gerado, teríamos $Z(G)$ finito e, consequentemente, G seria finito. Absurdo!
Daí, existe $x \in Z(G)$ de ordem infinita e $\mathcal{A} \neq \emptyset$.
Seja $\mathcal{A}'$ uma cadeia qualquer em $\mathcal{A}$.
Façamos $L_0 = \bigcup_{L \in \mathcal{A}} L$.
O fato de que dados $L_1, L_2 \in \mathcal{A}'$ ou $L_1 \leq L_2$ ou $L_2 \leq L_1$ nos garante que L_0 é subgrupo. Além disso, sendo cada $L \in \mathcal{A}$ livre de torção, L_0 também o é.
Assim, $L_0 \in \mathcal{A}$.
Claro que $\forall L \in \mathcal{A}$ temos $L \leq L_0$.
Segue então, do Lema de Zorn que $\mathcal{A}$ possui um elemento maximal.
I.e., $\exists N \leq Z(G)$ maximal, entre os que são livres de torção.

Sobre N temos:

- $N \cap G' = 1$, pois N é livre de torção
- $\dfrac{G}{N}$ é finito

A maximalidade livre de torção de N garante que $\dfrac{Z(G)}{N}$ é de torção.

De fato, se $\exists xN \in Z(G)/N$ com $o(xN) = \infty$ também.

Daí, tomando $M = N\langle x\rangle$, temos que M é livre de torção, pois N e $\langle x\rangle$ o são, e

$$N \lneqq M < Z(G) \quad ,$$

contrariando a maximalidade de M entre os subgrupos de $Z(G)$ livres de torção.
Portanto, $\dfrac{Z(G)}{N}$ é livre de torção.
Sendo $\dfrac{Z(G)}{N}$ também abeliano finitamente gerado, temos que este é finito.
Como já tínhamos $\dfrac{G}{Z(G)}$ finito, segue que $\dfrac{G}{N}$ é finito.

Isso prova nossa afirmação.
Pelo caso já provado acima, $\left(\dfrac{G}{N}\right)'$ é gerado por um comutador.
Agora,

$$\left(\frac{G}{N}\right)' = \frac{G'N}{N} \simeq \frac{G'}{G' \cap N} \simeq G'$$

Logo, G' também é gerado por um comutador e consequentemente é constituído somente de comutadores. Assim, concluímos o caso em que G' 'e finito.
Suponhamos agora, G' infinito e gerado por um elemento c de ordem infinita.
Como $c^k \in G'$ implica $c^{-k} \in G'$, existe $l > 0$ tal que $c^l \in G'$.
Tome γ como sendo o menor inteiro positivo tal que $c^\gamma \in G'$. Podemos supor $\gamma > 1$, pois do contrário, nosso resultado estaria provado.
Considere $\dfrac{G}{\langle c^\gamma\rangle}$, para o qual $\left(\dfrac{G}{\langle c^\gamma\rangle}\right)' = \dfrac{G'}{\langle c^\gamma\rangle}$.
Como este grupo possui subgrupo comutador finito central, segue do que provamos acima, que seu subgrupo derivado é gerado por um comutador.
Desse modo,

$$\left(\frac{G}{\langle c^\gamma\rangle}\right)' = \langle\ c^\delta\langle c^\gamma\rangle\ \rangle, \text{ onde } c^\delta \text{ é comutador de G e } \delta > \gamma$$

Note que também

$$\left(\frac{G}{\langle c^\gamma\rangle}\right)' = \langle\ c\langle c^\gamma\rangle\ \rangle$$

Logo, $\left|\dfrac{G'}{\langle c^\gamma\rangle}\right| = \ o(\ c\langle c^\gamma\rangle\ ) = \gamma.$

Seja d um divisor de γ e δ.
Veja que

$$(c^\delta\langle c^\gamma\rangle)^{\gamma/d} = c^{\delta\ \gamma/d}\langle c^\gamma\rangle = (c^\gamma)^{\delta/d}\langle c^\gamma\rangle = \overline{1}$$

Daí, $\gamma|\gamma/d$, o que implica $d = 1$.

Assim, $(\delta, \gamma) = 1$.

Sendo $\dfrac{G'}{\langle c^\gamma\rangle} = \langle\ c^\delta\langle c^\gamma\rangle\ \rangle$ segue que $G' = \langle c^\delta, c^\gamma\rangle$.

Sejam a_1, a_2, a_3, a_4 em G tais que:

$$c^\gamma = [a_1, a_2] \ \text{ e } \ c^\delta = [a_3, a_4]$$

Faça $c_{ij} = [a_i, a_j]$, para $1 \leq i, j \leq 4$.

Sendo G' cíclico, existem relações:

$$c_{ij} = c^{\gamma_{ij}}\ , \quad ij = 13, 14, 23, 24 \tag{1}$$

Além disso, da minimalidade de γ segue que γ divide cada γ_{ij}.
De fato, supondo por exemplo, $\gamma_{13} = q\gamma + r$ com $0 < r < \gamma$, temos:

$$\begin{aligned} c^r &= c^{\gamma_{13}-q\gamma} = c_{13}(c^\gamma)^{-q} \\ &= c_{13}c_{12}^{-q} \\ &= [a_1, a_3]\ [a_1, a_2^{-q}] \\ &= [a_1, a_2^{-q}a_3] \end{aligned}$$

o que contradiz a escolha de γ.
Logo, $r = 0$ e γ divide γ_{13}.
Analogamente se mostra que γ divide todo γ_{ij}.
Sejam $\alpha_1 = \dfrac{\gamma_{13}}{\gamma}$, $\ \alpha_2 = \dfrac{\gamma_{14}}{\gamma}$ $\ \alpha_3 = \dfrac{\gamma_{23}}{\gamma}$ $\ $ e $\ \alpha_4 = \dfrac{\gamma_{24}}{\gamma}$.
Então, podemos reescrever as relações em (1) na forma:

$$c_{13} = c_{12}^{\alpha_1}, \quad c_{14} = c_{12}^{\alpha_2}, \quad c_{23} = c_{12}^{\alpha_3}, \quad c_{24} = c_{12}^{\alpha_4}$$

Seja $H = \langle a_1, a_2, a_3, a_4 \rangle$.
Claro que $H' < G'$.
Agora, como $c^\gamma, c^\delta \in H'$, também temos $G' = \langle c^\gamma, c^\delta \rangle < H'$.
Logo, $G' = H'$.
Considere a mudança de geradores de H dada por:

$$a_1^* = a_1, \quad a_2^* = a_2, \quad a_3^* = a_3 a_2^{-\alpha_1} \quad \text{e} \quad a_4^* = a_4 a_2^{-\alpha_2}$$

Fazendo $c_{ij}^* = [a_i^*, a_j^*]$, temos:

$$c_{12}^* = c^\gamma; \quad c_{13}^* = 1 = c_{14}^*; \quad c_{23}^* = c_{23} = c_{12}^{\alpha_3}; \quad c_{24}^* = c_{24} = c_{12}^{\alpha_4}; \quad c_{34}^* = c^{\delta^*}, \tag{2}$$

onde $\delta^* = \delta + \gamma(\alpha_2\alpha_3 - \alpha_1\alpha_4)$.
Sendo $(\delta, \gamma) = 1$, segue que $(\delta^*, \gamma) = 1$.
Sejam h e k inteiros tais que $h\gamma + k\delta^* = 1$.
Desse modo,

$$c = c^{h\gamma + k\delta^*} = c_{12}^h \; {c_{34}^*}^k \; (c_{13}^*)^\lambda \; (c_{24}^* {c_{12}^*}^{-\alpha_4})^\mu \tag{3}$$

e em virtude das relações em (2), a expressão (3) de c é verdadeira para quaisquer inteiros λ e μ. Note que $c \in H' = G'$. Para completar a prova demonstraremos a existência de inteiros λ e μ tais que o lado direito de (3) seja um comutador. Observamos que a matriz Δ^* associada a expressão (3) para c é tal que:

$$\Delta_{1234}^* = (h - \alpha_4\mu)k - \lambda\mu$$

Fazendo $\mu = 1$ e $\lambda = (h - \alpha_4)k$, obtemos $\Delta_{1234}^* = 0$.
Do Lema 1 temos que $\Delta_{1234} = 0$ também, e consequentemente(teorema 1), c é um comutador.
De fato,

$$\begin{aligned} c &= {c_{12}^*}^h \; {c_{34}^*}^k \; {c_{13}^*}^{(h-\alpha_4)k} \; c_{24}^* \; {c_{12}^*}^{-\alpha_4} \\ &= {c_{12}^*}^{h-\alpha_4} \; c_{13}^{(h-\alpha_4)k} \; c_{24}^* \; {c_{34}^*}^k \\ &= [{a_1^*}^{h-\alpha_4} {a_4^*}^{-1}, a_2^* {a_3^*}^k] \end{aligned}$$

Façamos $x = {a_1^*}^{h-\alpha_4} {a_4^*}^{-1}$ e $y = a_2^* {a_3^*}^k$.
Sendo G' central em G, temos:

$$c^m \;=\; [x, y]^m \;=\; [x^m, y], \quad \forall m \in \mathbb{Z}$$

Logo, G' é constituído inteiramente por comutadores.
Analisemos agora, o caso em que G' é 2-gerado. Suponhamos $G' = \langle c, d \rangle$.
Afirmamos que G' é gerado por 2 comutadores.
Seja $D = \langle d \rangle$.
Sendo G' central, este é abeliano. Daí, $D \lhd_{car} G' \lhd G$. O que implica, $D \lhd G$.
Como $D \leq G'$, temos:

$$\left(\frac{G}{D}\right)' = \frac{G'}{D} = \langle cD\rangle$$

Daí, pelo que mostramos acima, segue que $\left(\dfrac{G}{D}\right)'$ é constituído somente por comutadores.
Em particular, cD é um comutador de G/D.
Isto é, $\exists_m a, b \in G$ tais que $cD = [aD, bD]$.
$\therefore\ cD = [a, b]D$
$\therefore\ [a, b]^{-1}c \in D$
$\therefore\ \exists\gamma \in \mathbb{Z};\ [a, b]^{-1}c = d^{-\gamma}$
$\therefore\ cd^{\gamma} = [a, b]$
Agora, considere $N = \langle cd^{\gamma}\rangle$. Sendo $N \lhd_{car} G' \lhd G$, temos $N \lhd G$.
Veja que $G' = \langle d, N\rangle = \langle d, cd^{\gamma}\rangle$.
De fato, como $d \in \langle d, cd^{\gamma}\rangle$, temos que $d^{-\gamma} \in \langle d, cd^{\gamma}\rangle$ também.
Daí, $c = cd^{\gamma}\ .\ c^{-\gamma} \in \langle d, cd^{\gamma}\rangle$.
Agora, $c, d \in \langle d, cd^{\gamma}\rangle$ implica $G' = \langle c, d\rangle \leq \langle d, cd^{\gamma}\rangle$.
E, claramente, $\langle d, cd^{\gamma}\rangle \leq G'$.
Logo, $G' = \langle d, cd^{\gamma}\rangle = \langle d, N\rangle$.
Isto nos dá:

$$\frac{G'}{N} = \langle dN\rangle$$

Desse modo, G'/N é constituído somente de comutadores.
Em particular, $\exists_m u, v \in G$ tais que $dN = [uN, vN]$.
$\therefore\ dN = [u, v]N$
$\therefore\ [u, v]^{-1}d \in N$
$\therefore\ \exists\mu \in \mathbb{Z};\ [u, v]^{-1}d = (cd^{\gamma})^{-\mu}$
$\therefore\ d(cd^{\gamma})^{\mu} = [u, v]$
Portanto, cd^{γ} e $d(cd^{\gamma})^{\mu}$ são comutadores de G.
Façamos $e = cd^{\gamma}$ e $f = d(cd^{\gamma})^{\mu}$.
Note que

$$d = f\ .\ e^{-\mu} \in \langle e, f\rangle$$

Daí,

$$c = e\ .\ d^{-\gamma} \in \langle e, f\rangle$$

e temos,

$$G' = \langle c, d\rangle \leq \langle e, f\rangle$$

Logo,

$$G' = \langle e, f\rangle$$

provando nossa afirmação.

Façamos $e = [a_1, a_2] = c_{12}$ e $f = [a_3, a_4] = c_{34}$.

Consideremos $H = \langle a_1, a_2, a_3, a_4 \rangle$.
Mostraremos que todo elemento de G' é um comutador no subgrupo H e como $H' = G'$, o resultado segue.
Seja, como antes, $c_{ij} = [a_i, a_j]$, para cada ij.
Existem relações:

$$c_{13} = c_{12}^{\alpha_1} c_{34}^{\beta_1}, \quad c_{14} = c_{12}^{\alpha_2} c_{34}^{\beta_2}, \quad c_{23} = c_{12}^{\alpha_3} c_{34}^{\beta_3}, \quad c_{24} = c_{12}^{\alpha_4} c_{34}^{\beta_4} \tag{4}$$

Suponha os β_i's nem todos nulos. Suponhamos também que todas as representações de H sobre quatro geradores sujeitos as relações em (4) tenham índices de c_{34} nem todos nulos. A menos de uma reordenação dos a_i's, podemos supor β_1 o menor índice de c_{34} não nulo, em módulo.
Além disso, podemos supor $\beta_2 = 0 = \beta_3$.
De fato, a minimalidade de β_1 nos garante que $\beta_1 \mid \beta_2$ e $\beta_1 \mid \beta_3$.

Digamos que seja $\beta_2 = k\beta_1$ e $\beta_3 = l\beta_2$, com $k, l \in \mathbb{Z}$.

Considerando a mudança do Tipo III

$$\begin{cases} a_4^* = a_4 a_3^{-k} \\ a_i^* = a_i, \quad i = 1, 2, 3 \end{cases}$$

obtemos $c_{14}^* = {c_{12}^*}^{\alpha_2 - k\alpha_1} {c_{34}^*}^{\beta_2 - k\beta_1} = {c_{12}^*}^{\alpha_2 - k\alpha_1}$.

Logo, $\beta_2^* = 0$.

Analogamente, considerando a mudança

$$\begin{cases} \overline{a}_2 = a_2 a_1^{-q} \\ \overline{a}_i = a_i, \quad i = 1, 3, 4 \end{cases}$$

obtemos $\overline{c}_{23} = \overline{c}_{12}^{\alpha_3 - l\alpha_1} \,.\, \overline{c}_{34}^{\beta_3 - l\beta_1} = \overline{c}_{12}^{\alpha_3 - l\alpha_1}$.

I.e., $\beta_3 = 0$. Isto prova nossa afirmação.

Desse modo, as relações em (4) podem ser reescritas da forma:

$$c_{13} = c_{12}^{\alpha_1} c_{34}^{\beta_1}, \quad c_{14} = c_{12}^{\alpha_2}, \quad c_{23} = c_{12}^{\alpha_3}, \quad c_{34} = c_{12}^{\alpha_4} c_{34}^{\beta_4} \tag{5}$$

Desta forma, para analisarmos o caso em que em (4) todos os β_i's são nulos basta fazer $\beta_1 = 0 = \beta_4$.
Agora, seja c um elemento arbitrário de G'. Então, existem inteiros δ e ε tais que, para quaisquer inteiros λ e μ, tem-se:

$$c \;=\; c_{12}^{\delta}\, c_{34}^{\varepsilon}\, (c_{14}\, c_{12}^{-\alpha_2})^{\lambda}\, (c_{23} c_{12}^{-\alpha_3})^{\mu} \tag{6}$$

Seja Δ a matriz $4x4$ associada com a expressão (6) de c.
Então,

$$\Delta_{1234} \;=\; (\delta - \alpha_2\lambda - \alpha_3\mu)\varepsilon \;+\; \lambda\mu \;=\; \mu(\lambda - \alpha_3\varepsilon) - \varepsilon(\alpha_2\lambda - \delta)$$

e este pode ser zerado escolhendo:

$$\lambda = \alpha_3\varepsilon + 1 \;\text{ e }\; \mu = \varepsilon(\alpha_2\lambda - \delta)$$

Portanto, o elemento c de G' é um comutador.

$\blacksquare$

Referências Bibliográficas

[**1**] BHATTACHARYA, P.B.; JAIN,S.K. ; NAGPAUL,S.R. *Basic abstract algebra.* 2^{nd} ed. New York : Cambridge University Press,1995. 487 p.

[**2**] GUSTAVO, A.F. ; SHUMYATSKY,P. On groups in which commutators are covered by finitely many cyclic subgroups. *Journal of Algebra*, v. 319, p. 4844-4851, 2008.

[**3**] IVANOV, S.V. Hall's conjecture on the finiteness of verbal subgroups. *Soviet Math.*, v. 33, n. 6, p. 59-70. 1989

[**4**] LIEBECK, Hans. A test for commutators. *Glasgow Math.J.*, v. 17, n. 1, p. 31-36. 1976.

[**5**] ROBINSON ,D.J.S. *A course in the theory of groups.* 2^{nd} ed. Berlim : Springer-Verlag, 1996. 499 p.

[**6**] TOMKINSON, M.J. *FC-groups.* Londres :University of Glasgow,1983.

[**7**] TURNER-SMITH, R.F. Finiteness conditions for verbal subgroups. *J. London Math. Soc.*, v. 41, p.166-176, 1966.