Universidade de Brasília

Propriedades Estruturais do Subgrupo Comutador de um Grupo

Tharles Araújo de Souza

Orientador: Dr. Raimundo de Araújo Bastos Júnior

Departamento de Matemática
Universidade de Brasília

Dissertação apresentada como requisito parcial para obtenção do grau de
Mestre(a) em Matemática

Brasília, 16 de julho de 2021

Universidade de Brasília

Instituto de Ciências Exatas

Departamento de Matemática

Propriedades estruturais do subgrupo comutador de um grupo

por

Tharles Araujo de Souza*

Dissertação apresentada ao Departamento de Matemática da Universidade de Brasília, como parte dos requisitos para obtenção do grau de

MESTRE EM MATEMÁTICA

Brasília, 16 de julho de 2021.

Comissão Examinadora:

Prof. Dr. Raimundo de Araujo Bastos Junior - MAT/UnB (Orientador)

Prof. Dr. Noraí Romeu Rocco – MAT/UnB (Membro)

Profa. Dra. Irene Naomi Nakaoka – UEM (Membro)

* O autor foi bolsista da CAPES durante a elaboração desta dissertação.

Ficha catalográfica elaborada automaticamente,
com os dados fornecidos pelo(a) autor(a)

Ap

Araújo de Souza, Tharles
Propriedades Estruturais do Subgrupo Comutador de um Grupo / Tharles Araújo de Souza; orientador Raimundo de Araújo Bastos Júnior. -- Brasília, 2021.
62 p.

Dissertação (Mestrado - Mestrado em Matemática) -- Universidade de Brasília, 2021.

1. Comutadores . 2. Subgrupo Comutador . 3. Condições de finitude. I. de Araújo Bastos Júnior, Raimundo , orient. II. Título.

Dedico este trabalho aos meus familiares, amigos e aos professores José Ivan e Sérgio Brazil.

Agradecimentos

Agradeço primeiramente a Deus por ter me dado coragem de sair do Acre para Brasília.

À minha família, meu pai Teodúlo, minha mãe Maria Aparecida, meus irmãos Tácio, Thalysson, Tharlyane, Thiago e Tales. À minha sobrinha Thayla, meu sobrinho Thaysson, meu vô José Cavalcante (Seu Zeca), minha vó Dona Luzia, meu tio Yledo, minhas tias Virtucia e Elissandra.

À minha namorada Talita pelo carinho e apoio dado durante todos esses anos.

Aos colegas e amigos da UFAC, Renã, Maiara, Pamela, Cristiane, Tauane, Sidney, Keila, Henrylla, Raylane e Carlos. Não posso deixar de citar os meus amigos de "piseiro" William Maia, Douglas, Athyeli, Kennedy e meu conterrâneo Ricardo.

Aos amigos de Brasília, JR e Guir por abrirem as portas de sua casa durante meu primeiro semestre.

Aos meus colegas e amigos que tive a oportunidade de conhecer durante o mestrado, Geovane, Murilo, Maria Edna, Mateus, Junior, Jailson, Adler, Gabriel, Katianny, Vinicius Kobayashi, Rômulo, Joseph Pucllas e Rosalina. Agradeço pelas experiências compartilhadas, conversas e os momentos de descontração no PDS tomando uma cerveja.

Aos professores que contribuíram para a minha formação como mestre, os professores Alexei Krassilnilkov, Martino Garonzi, João Paulo, Luis Miranda e, as professoras, Sheila Campos e Cátia Gonçalves.

Um agradecimento especial ao meu orientador, professor Raimundo Bastos pela dedicação, compromisso, paciência e por suas valiosas orientações que me ajudaram bastante na elaboração desta dissertação. Também quero agradecê-lo pela disposição de continuar trabalhando comigo nas minhas próximas fases como estudante de matemática.

Um outro agradecimento especial aos professores da UFAC, José Ivan e Sérgio Brazil pelo apoio, motivação, ajuda e por terem me incentivado desde o inicio da graduação a vim fazer o mestrado na UnB.

Aos professores Noraí Rocco, Alex Dantas e a professora Irene Naomi por terem aceitado o convite para participar da minha banca, pelas correções e por todas as sugestões que enriqueceram este trabalho.

À CAPES pelo financiamento durante a elaboração desta dissertação.

Resumo

O objetivo desse trabalho é investigar a influência do conjunto dos comutadores na estrutura do subgrupo derivado de um grupo. Os principais resultados abordados estão associados a condições de finitude para dados subgrupos do subgrupo comutador e à questão de quando podemos assegurar que o subgrupo comutador difere do conjunto de todos os comutadores de um grupo.

Palavras-chave: Comutadores. Subgrupo Comutador. Condições de finitude.

Abstract

The aim of this work is to investigate the influence of the set of commutators in the structure of the commutator subgroup. We study two kind of results: finiteness conditions for some subgroup of the commutator subgroup and when we can ensure that the set of all commutators differs from the commutator subgroup.

Keywords: Commutators. Commutator subgroup. Finiteness conditions.

Conteúdo

Introdução

Neste trabalho estudamos duas classes de questões envolvendo comutadores em grupos: condições de finitude para um dado subgrupo do subgrupo comutador e sob que condições podemos assegurar que o subgrupo comutador é diferente do conjunto de todos os comutadores de um grupo.

Por uma questão de completude cabe mencionar os matemáticos, resultados e trabalhos que influenciaram direta ou indiretamente a elaboração desta dissertação: Reinhold Baer (Teorema D, abaixo), John D. Dixon [2, Capítulo 5], Ian D. MacDonald [9], Bernhard H. Neumann (Teorema B, abaixo), Derek J. S. Robinson [10, Capítulos 10 e 14], Maxwell Rosenlicht [11], Issai Schur (Teorema A, abaixo) e James Wiegold [12, Capítulo 4].

Condições de Finitude: Para simplificar a notação, usaremos o termo "$\{m,n,\ldots\}$-limitado” para expressar que uma quantidade é finita e limitada superiormente por uma função que depende somente dos parâmetros $m,n,\ldots$.

Seja G um grupo. Escrevemos G' e $Z(G)$ para denotar o subgrupo comutador e o centro de G, respectivamente. Dizemos que G é central-por-finito, se o índice $|G:Z(G)|$ é finito. Podemos observar que G é abelino se, e somente se $|G:Z(G)|=1$, e isto ocorre se, e somente se, $|G'|=1$. De modo geral, no caso de G não ser abeliano, será que também existe uma relação entre $|G:Z(G)|$ e a ordem de G'? A resposta é sim e a (primeira) conexão vem do famoso Teorema de Issai Schur:

Teorema A: (I. Schur): Seja G um grupo central-por-finito. Suponha que $|G:Z(G)|=n$. Então, o subgrupo comutador G' é finito e tem ordem n-limitada. Além disso, o expoente $\exp(G')$ divide n.

Seja G um grupo. Dado $x\in G$, escrevemos x^G para a classe de conjugação de G contendo x. O grupo G é dito FC-grupo se as classes de conjugação são finitas. Adicionalmente, se existir uma constante (uniforme) $k\in\mathbb{N}$ de tal modo que $|x^G|\leq k$ para todo $x\in G$, então G é dito um BFC-grupo. De certa forma, Bernhard H. Neumann estendeu o Teorema de Schur dando uma caracterização dos grupos nos quais o subgrupo comutador é finito em termos de

BFC-grupos e/ou da finitude do conjunto dos comutadores (veja também Lema 2.2.2 para um resultado de natureza quantitativo):

Teorema B: (B. H. Neumann): Seja G um grupo. As seguintes afirmações são equivalentes:

(a) O conjunto de comutadores $\Gamma(G) = \{[x,y] \mid x,y \in G\}$ é finito;

(b) G é BFC-grupo;

(c) O subgrupo comutador G' é finito.

O Teorema de Maxwell Rosenlicht [11] pode ser visto como uma generalização dos itens (a) e (c) do Teorema B.

Teorema C: (M. Rosenlicht) Sejam H e N subgrupos de um grupo G, com $N \trianglelefteq G$. Suponhamos que o conjunto de comutadores $\{[n,h] \mid n \in N, h \in H\}$ seja finito, com m elementos. Então $[N,H]$ é finito, de ordem m-limitada.

A partir do Teorema C estendemos um resultado devido a Reinhold Baer [10, 14.5.2]. Na referência supracitada é suposto que todos os subgrupos envolvidos são normais; e na demonstração é usado "produtos tensoriais de grupos abelianos" (cf. Lema 2.4.1, abaixo). Além disso, conseguimos "retirar" a normalidade de alguns dos subgrupos envolvidos e em nossa demonstração usamos propriedade de comutadores. Esse resultado será utilizado na demonstração do Teorema D a seguir.

Denotamos por $Z_i(G)$ e por $\gamma_{i+1}(G)$ os termos das séries centrais superior e inferior de um grupo G, respectivamente. O grupo G ser nilpotente de classe i, $|G/Z_i(G)| = 1$ e também equivale à condição de que $|\gamma_{i+1}(G)| = 1$. Dessa forma, também é natural se perguntar qual é a relação entre $G/Z_i(G)$ e $\gamma_{i+1}(G)$ no caso geral em que G não é necessariamente nilpotente. Respondendo a tal questionamento Reinhold Baer generalizou o Teorema de Schur para os demais termos das séries centrais superior e inferior de G.

Teorema D: (R. Baer) Seja G um grupo. Se $|G : Z_i(G)| = n$, com $i \geq 1$, então o $(i+1)$-ésimo termo da série central inferior $\gamma_{i+1}(G)$ é finito, de ordem n-limitada.

Tentamos incluir as condições de finitude envolvendo certos subgrupos e comutadores levando em conta aspectos quantitativos. Entretanto, os limites mencionados no trabalho são de carácter meramente teórico e não buscamos cotas "optimais".

Comutadores e o Subgrupo Comutador: Agora nosso foco será construir exemplos de grupos que possuem elementos no subgrupo derivado que não são comutadores. Mais precisamente, estudamos grupos finitos de matrizes, com estrutura relativamente "fácil" de manusear (p-grupos finitos de classe 2), nos quais o conjunto dos comutadores é diferente do subgrupo comutador (nesse caso dizemos que existem elementos não comutadores). Tais exemplos foram propostos por Ian D. MacDonald [9].

Vale a pena explicar a natureza dos exemplos que apresentamos. A grosso modo, a analogia que usamos para "justificar" o Teorema de Schur também é capaz de sugerir uma maneira de criar grupos com elementos não comutadores. Mais precisamente, se G é um grupo no qual $|G:Z(G)|^2 < |G'|$, então G contém elementos no seu derivado que não são comutadores (veja Lema 3.1.2). Com isso, temos uma critério capaz de assegurar quando um grupo contém elementos não comutadores. Seguindo o trabalho de Ian D. MacDonald [9], temos:

Teorema E: (I. D. MacDonald) Seja p um número primo. Existe um p-grupo 6-gerado G, nilpotente de classe 2 com $|G| = p^{21}$ e $|G'| = |Z(G)| = p^{15}$. Em particular, G contém elementos no subgrupo derivado que não são comutadores.

Para simplificar a escrita dessa Introdução optamos por nomear os resultados principais de forma linear: **Teorema A** – **Teorema E**. Entretanto, ao longo do texto os teoremas aparecem com uma numeração independente.

Este trabalho está dividido em três capítulos:

No Capítulo 1, apresentamos alguns resultados preliminares da Teoria de Grupos, Teorema dos índices, Lema de Poincaré, um caso particular do Teorema dos Grupos Abelianos Finitamente Gerados, propriedades básicas de comutadores, série derivada, série centrais superior e inferior, ação de um grupo, o homomorfismo transfer, propriedades básicas de FC-grupos e BFC-grupos. Trazemos também o Princípio Fundamental de Contagem e o Princípio da Casa dos Pombos que serão aplicados no capítulo seguinte.

No Capítulo 2, inicialmente expomos alguns resultados básicos e demonstramos o Teorema A. Posteriormente, apresentamos alguns resultados sobre FC-grupos e BFC-grupos, bem como o famoso Lema de Dietzmann para, em seguida, demonstrar o Teorema B. A seção seguinte é baseada no artigo do M. Rosenlicht [11] e tem como objetivo demonstrar o Teorema C. Na última seção deste capítulo demonstramos o Teorema D.

O capítulo final é baseado no trabalho do MacDonald [9]. Inicialmente abordamos um resultado que assegura quando um grupo contém elementos não comutadores. Na seção seguinte, apresentamos cálculos envolvendo matrizes, com entradas inteiras $\mathbb{Z}$ (ou, no corpo dos inteiros módulo p, $\mathbb{Z}_p$), que serão usados no decorrer do capítulo. Subsequentemente, construimos exemplos de grupos de matrizes, nilpotentes de classe 2, sendo que alguns desses grupos possuem elementos não comutadores em seu subgrupo comutador. Com isso, demonstraremos o Teorema E. Veremos que os exemplos explicitados nesse teorema nos fornecem uma “máquina”capaz de gerar p-grupos com elementos não comutadores.

Capítulo 1

Preliminares

Assumimos que o leitor tem familiaridade com os conceitos básicos da Teoria de Grupos. Alguns teoremas como o Teorema de Lagrange e os Teoremas de Isomorfismo também são assumidos como conhecidos, podendo serem encontrados em vários referências, em particular em [5]. A construção deste capítulo foi baseada em [10, Capítulos 1,5,10 e 14].

1.1 Grupos e Subgrupos

Definição 1.1.1. *Dado um subconjunto não vazio X de um grupo G, definimos o* ***subgrupo gerado*** *por X, denotado por $\langle X\rangle$, como sendo o menor subgrupo de G contendo X, ou seja, $\langle X\rangle$ é a interseção de todos os subgrupos de G que contém X.*

Proposição 1.1.2. *Seja $X \subseteq G$ não vazio. Então,*

$$\langle X\rangle = \{x_1^{\varepsilon_1}x_2^{\varepsilon_2}\dots x_k^{\varepsilon_k} \mid x_i \in X, \varepsilon_i = \pm 1, k \in \mathbb{N}\}.$$

(quando $k = 0$ podemos interpretar o produto como 1). No caso em que $X = \{x\}$ é um conjunto unitário, temos $\langle X\rangle = \{x^n \mid n \in \mathbb{Z}\}$.

Demonstração. Considere $S = \{x_1^{\varepsilon_1}x_2^{\varepsilon_2}\dots x_k^{\varepsilon_k} \mid x_i \in X, \varepsilon_i = \pm 1, k \in \mathbb{N}\}$. De fato, S é um subgrupo de G, pois: $1 = xx^{-1} \in S$, $x \in X$, e se $x = x_1^{\varepsilon_1}x_2^{\varepsilon_2}\dots x_k^{\varepsilon_k}, y = y_1^{\beta_1}y_2^{\beta_2}\dots y_l^{\beta_l} \in S$, temos

$$\begin{aligned} xy^{-1} &= x_1^{\varepsilon_1}x_2^{\varepsilon_2}\dots x_k^{\varepsilon_k}(y_1^{\beta_1}y_2^{\beta_2}\dots y_l^{\beta_l})^{-1} \\ &= x_1^{\varepsilon_1}x_2^{\varepsilon_2}\dots x_k^{\varepsilon_k}y_l^{-\beta_1}\dots y_2^{-\beta_2}y_l^{-\beta_l} \in S. \end{aligned}$$

Sendo $S \leq G$ e como $X \subseteq S$, tem-se que $\langle X\rangle \leq S$. Por outro lado, $S \leq \langle X\rangle$, caso contrário, existiria um elemento $z \in S$ tal que $z \notin \langle X\rangle$, mas $\langle X\rangle \leq G$ e z é da forma $z = z_1^{\varepsilon_1}z_2^{\varepsilon_2}\dots z_k^{\varepsilon_k}$, onde $z_i \in X$, $1 \leq i \leq k$, ou seja, $z \in \langle X\rangle$ e temos uma contradição. Portanto, $\langle X\rangle = S$. $\square$

Definição 1.1.3. *(Transversal) Seja G um grupo e $H \leq G$. Um subconjunto $T \subseteq G$ é dito ser um **transversal** (à esquerda) de H em G, quando*

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

Proposição 1.1.4. *(Teorema dos índices). Sejam H, K subgrupos de um grupo G. Suponhamos que $H \leq K \leq G$. Então,*

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

A demostração do resultado acima pode ser encontrado em [10, 1.3.5].

Teorema 1.1.5. *(Lema de Poincaré) Sejam H, K subgrupo de um grupo G. Então*

$$|G : H \cap K| \leq |G : H||G : K|.$$

Ademais, se os índices $|G : H|$ e $|G : K|$ são coprimos, então $|G : H \cap K| = |G : H||G : K|$.

O resultado acima pode ser encontrado em [10, 1.3.11].

Definição 1.1.6. *Seja G um grupo. Dados os elementos $g, h \in G$ o **conjugado** de g por h é o elemento*

$$g^h = h^{-1}gh \in G.$$

Definição 1.1.7. *Um subconjunto X de um grupo G é dito **normal** (em G), se $x^g \in X$ para todo $x \in X$ e todo $g \in G$.*

Tal definição nos sugere o seguinte resultado:

Proposição 1.1.8. *Sejam G um grupo e $X \subseteq G$ um conjunto não vazio normal (em G). Então, $\langle X \rangle$ é normal em G.*

Definição 1.1.9. *Um grupo G é dito **finitamente gerado** se existe um subconjunto finito $X \subseteq G$ tal que $G = \langle X \rangle$.*

Proposição 1.1.10. *Seja G um grupo finitamamente gerado. Suponhamos que H é um subgrupo de G com índice $|G : H|$ finito. Então H é finitamente gerado.*

O resultado acima pode ser encontrado em [10, 1.6.11].

Definição 1.1.11. *Seja G um grupo e $X \subseteq G$ não vazio. Definimos por*

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

*o **centralizador** de X em G. Em particular, se $X = \{x\}$, escreveremos apenas $C_G(x)$. E*

$$N_G(X) = \{g \in G \mid x^g \in X, \forall x \in X\}$$

*o **normalizador** de X em G.*

Definição 1.1.12. *O **centro** $Z(G)$ de um grupo G é definido como,*

$$Z(G) := \{z \in G \mid zg = gz, \forall g \in G\}$$

Proposição 1.1.13. *Seja G um grupo finitamente gerado. Suponha que $G = \langle x_1, x_2, \ldots x_n \rangle$. Então*

$$\bigcap_{i=1}^{n} C_G(x_i) = Z(G)$$

Demonstração. Se $y \in \bigcap_{i=1}^{n} C_G(x_i)$, então $yx_i = x_i y$, $1 \leq i \leq n$, logo y comuta com todos os elementos de G. Daí, $y \in Z(G)$, e portanto, $\bigcap_{i=1}^{n} C_G(x_i) \leq Z(G)$. Por outro lado, se $z \in Z(G)$, então $zx_i = x_i z$. Logo $z \in \bigcap_{i=1}^{n} C_G(x_i)$, e assim, $Z(G) \leq \bigcap_{i=1}^{n} C_G(x_i)$. □

Definição 1.1.14. *Seja G um grupo. Definimos o **expoente** de G, como o seguinte número (se existir):*

$$\exp(G) = mmc\{|g| \mid g \in G\}.$$

Assim, dizemos que G tem expoente n, se n é o menor inteiro positivo tal que $g^n = 1$ para todo $g \in G$. Definimos por

$$Tor(G) := \{g \in G \mid |g| < +\infty\},$$

*o conjunto de **torção** de G. Dizemos que um G é de torção se $G = Tor(G)$.*

A seguir temos um caso particular do Teorema dos Grupos Abelianos Finitamente Gerados:

Proposição 1.1.15. *Seja G um grupo abeliano finitamente gerado. Então $Tor(G)$ é finito.*

1.2 Comutadores

Definição 1.2.1. *Seja G um grupo. Dados os elementos x e y em G o* ***comutador*** *de x e y é o elemento*

$$[x,y] = x^{-1}y^{-1}xy \in G.$$

Mas geralmente, um ***comutador de comprimento*** *$n \geq 2$ define-se intuitivamente por*

$$[x_1,x_2,\ldots,x_n] = [[x_1,x_2,\ldots,x_{n-1}],x_n].$$

Proposição 1.2.2. *Sejam x,y e z elementos de um gupo G. Então, valem:*

(a) $[x,y] = 1$ *se, e somente se,* $xy = yx$*;*

(b) $[x,y] = [y,x]^{-1}$*;*

(c) $[x,y]^z = [x^z,y^z]$*;*

(d) $[x,yz] = [x,z][x,y]^z$*;*

(e) $[xy,z] = [x,z]^y[y,z]$*;*

(f) $[x,y^{-1}] = ([x,y]^{y^{-1}})^{-1}$*;*

(g) $[x^{-1},y] = ([x,y]^{x^{-1}})^{-1}$.

Demonstração. A demontração segue da definição de comutadores:

(a)

$$[x,y] = 1 \Longleftrightarrow x^{-1}y^{-1}xy = 1 \Longleftrightarrow xy = yx;$$

(b)

$$[x,y] = x^{-1}y^{-1}xy = (y^{-1}x^{-1}yx)^{-1} = [y,x]^{-1};$$

(c)

$$\begin{aligned}
[x,y]^z &= z^{-1}[x,y]z = z^{-1}x^{-1}y^{-1}xyz \\
&= z^{-1}x^{-1}(zz^{-1})y^{-1}(zz^{-1})x(zz^{-1})yz \\
&= (x^{-1})^z(y^{-1})^z x^z y^z = (x^z)^{-1}(y^z)^{-1}x^z y^z \\
&= [x^z,y^z];
\end{aligned}$$

(d)

$$\begin{aligned}[x,yz] &= x^{-1}z^{-1}y^{-1}xyz = x^{-1}z^{-1}(xzz^{-1}x^{-1})y^{-1}xyz \\ &= [x,z]z^{-1}[x,y]z = [x,z][x,y]^z;\end{aligned}$$

(e)

$$\begin{aligned}[xy,z] &= y^{-1}x^{-1}z^{-1}xyz = y^{-1}x^{-1}z^{-1}x(zyy^{-1}z^{-1})yz \\ &= y^{-1}[x,z]y[y,z] = [x,z]^y[y,z];\end{aligned}$$

(f)

$$\begin{aligned}[x,y^{-1}] &= x^{-1}yxy^{-1} = (yx^{-1}y^{-1}x)^{-1} \\ &= (y(x^{-1}y^{-1}xy)y^{-1})^{-1} = ([x,y]^{y^{-1}})^{-1};\end{aligned}$$

(g)

$$\begin{aligned}[x^{-1},y] &= xy^{-1}x^{-1}y = (y^{-1}xyx^{-1})^{-1} \\ &= (x(x^{-1}y^{-1}xy)x^{-1})^{-1} = ([x,y]^{x^{-1}})^{-1}.\end{aligned}$$

□

Definição 1.2.3. *Dados os subconjunto $X_1, X_2, \ldots, X_n$ não vazios de um grupo G. Definimos, por*

$$[X_1, X_2] := \langle [x_1, x_2] \mid x_1 \in X_1, x_2 \in X_2 \rangle,$$

*o **subgrupo comutador** de X_1 e X_2. Em particular, se $X_1 = X_2 = G$, denotaremos por $\Gamma(G)$, o conjunto de **todos os comutadores** de G, isto é, $\Gamma(G) := \{[x,y] \mid x,y \in G\}$; definimos o **subgrupo comutador** (ou **subgrupo derivado**) de G, denotado por G', como sendo*

$$G' := \langle \Gamma(G) \rangle = \langle [x,y] \mid x,y \in G \rangle;$$

e de modo mais geral

$$[X_1, \ldots, X_n] := [[X_1, \ldots, X_{n-1}], X_n],$$

onde $n \geq 2$.

Observação 1.2.4. *Usando o item (a) da Proposição 1.2.2 podemos mostrar que um grupo G é abeliano se, e somente se, $G' = 1$.*

Proposição 1.2.5. *Sejam H, K e N subgrupos de um grupo G. Então,*

(a) Se $N \trianglelefteq G$, então $[HN/N, KN/N] = [H,K]N/N$;

(b) $H \leq C_G(K)$ se, e somente se, $[H,K] = 1$;

(c) $H \leq N_G(K)$ se, e somente se, $[H,K] \leq K$;

(d) Se $HN \leq G$ e $H \leq N_G(K)$, então $[HN,K] = [H,K][N,K]$;

(e) O subgrupo $[H,K]$ é normal em $\langle H,K \rangle$.

Demonstração. (a) De fato,

$$[HN/N, KN/N] = \langle [hN, kN] \,|\, h \in H, k \in K \rangle \leq G/N$$

e

$$[H,K] = \langle [h,k] \,|\, h \in H, K \in K \rangle.$$

Assim, a imagem $[H,K]N/N$ de $[H,K]$ pelo homomorfismo canônico de G em G/N é gerado pelos elementos do tipo $[h,k]N$, com $h \in H$ e $k \in K$. Por outro lado, $[hN,kN] = [h,k]N$ para todo $h \in H$ e $k \in K$, ou seja, os geradores de $[HN/N, KN/N]$ e de $[H,K]N/N$ coincidem.

(b) De fato,

$$H \leq C_G(K) \Longleftrightarrow [h,k] = 1 \Longleftrightarrow [H,K] = 1$$

para todo $h \in H$ e todo $k \in K$.

(c) De fato, para todo $h \in H$ e todo $k \in K$,

$$H \leq N_G(K) \Longleftrightarrow k^h \in K \Longleftrightarrow [h,k] = h^{-1}k^{-1}hk \in K \Longleftrightarrow [H,K] \leq K$$

(d) Para mostrar que $[H,K][N,K] \leq G$, é suficiente provar que $[H,K] \leq N_G([N,K])$. Como $H \leq N_G(K)$, temos que $[H,K] \leq K$, por (c). Além disso,

$$[n,k]^{k_1} = [n,k_1]^{-1}[n,k_1][n,k]^{k_1} = [n,k_1]^{-1}[n,kk_1] \in [N,K], \forall h \in H \text{ e } \forall k,k_1 \in K,$$

e assim, $K \leq N_G([N,K])$. Portanto, $[H,K] \leq N_G([N,K])$. Agora veja que,

$$\begin{aligned}[hn,k] &= [h,k]^n[n,k] = [h,k]([h,k]^{-1}n^{-1}[h,k]n)[n,k] \\ &= [h,k][[h,k],n][n,k] = [h,k][n,[h,k]]^{-1}[n,k] \in [H,K][N,K],\end{aligned}$$

para todo $h \in H$, $n \in N$ e $k \in K$, pois $[h,k] \in K$. Logo, $[HN,K] \leq [H,K][N,K]$.

Por outro lado, $[H,K] \leq [HN,K]$ e $[N,K] \leq [HN,K]$, e então, $[H,K][N,K] \leq [HN,K]$.

(e) Para mostrar que $[H,K] \trianglelefteq \langle H,K\rangle$ é suficiente mostrar que $H,K \leq N_G([H,K])$. Dados $h,h_1 \in H$ e $k,k_1 \in K$, note que:

$$[hh_1,k] = [h,k]^{h_1}[h_1,k] \Longrightarrow [h,k]^{h_1} = [hh_1,k][h_1,k]^{-1} \in [H,K]$$

e,

$$[h,kk_1] = [h,k_1][h,k]^{k_1} \Longrightarrow [h,k]^{k_1} = [h,k_1]^{-1}[h,kk_1] \in [H,K].$$

Então, pela arbitrariedade dos elementos envolvidos, $H,K \leq N_G([H,K])$ e, consequentemente, $\langle H,K\rangle \leq N_G([H,K])$. □

O seguinte resultado é conhecido como **Lema dos Três Subgrupos**, sua demonstração pode ser encontrada em [10, 5.1.10].

Lema 1.2.6. *Seja N um subgrupo normal de um grupo G. Se dois dos subgrupos $[H,K,L]$, $[L,H,K]$ e $[K,L,H]$ estão contidos em N, então o outro também está contido em N.*

Proposição 1.2.7. *Seja G um grupo. Então, o subgrupo comutador G' é normal em G.*

Demonstração. Dados $g \in G$ e $\alpha = [x_1,y_1][x_2,y_2]\dots[x_k,y_k] \in G'$. Temos que,

$$\begin{aligned}\alpha^g &= ([x_1,y_1][x_2,y_2]\dots[x_k,y_k])^g \\ &= [x_1,y_1]^g[x_2,y_2]^g\dots[x_k,y_k]^g \\ &= [x_1^g,y_1^g][x_2^g,y_2^g]\dots[x_k^g,y_k^g] \in G'.\end{aligned}$$

Como os elementos g e α foram dados arbitrários, segue que G' é normal em G. □

Proposição 1.2.8. *Seja N um subgrupo normal de um grupo G. Então, o grupo quociente G/N é abeliano se, e somente se, $G' \leq N$. Em particular, G/G' é abeliano.*

Demonstração. Dados os elementos $x, y \in G$. Suponha que G/N é abeliano, logo

$$xyN = xNyN = yNxN = yxN,$$

e assim, $[x,y] \in N$. Como x e y foram dados arbitrários, $G' \leq N$. Reciprocamente, se $G' \leq N$, temos

$$xNyN = xyN = yx[x,y]N = yxN = yNxN,$$

isto é, G/N é abeliano. □

Lema 1.2.9. *Seja G um grupo em que $G' \leq Z(G)$. Então,* *(a)* $[xy,z] = [x,z][y,z]$*;*

(b) $[x,yz] = [x,y][x,z]$*;*

(c) $[y^n,x] = [y,x]^n = [y,x^n]$*. Em particular,* $[x^m,y^n] = [x,y]^{mn}$ *;*

(d) $(xy)^n = x^n y^n [y,x]^{\frac{n(n-1)}{2}}$

para todos $x,y,z \in G$ *e todos os inteiros positivos* m,n*.*

Demonstração. Temos que, $G' \leq Z(G)$. Assim, $[x,y]^z = [x,y]$ para todos $x,y,z \in G$. Logo,

$$[xy,z] = [x,z]^y[y,z] = [x,z][y,z]$$

e,

$$[x,yz] = [x,z][x,y]^z = [x,z][x,y]$$

o que demonstra (a) e (b).

Agora, demonstraremos (c) e (d) por indução sobre n: Inicialmente,vamos mostrar que $[y,x]^n = [y^n,x]$. Para $n = 1$ é imediato. Suponha que a identidade vale para algum n. Assim,

$$\begin{aligned} [y,x]^{n+1} &= [y,x][y,x]^n = y^{-1}x^{-1}yx[y^n,x] \\ &= y^{-1}[y^n,x]x^{-1}yx = y^{-1}(y^{-n}x^{-1}y^n x)x^{-1}yx \\ &= y^{-(n+1)}x^{-1}y^{n+1}x = [y^{n+1},x]. \end{aligned}$$

Para mostrar que $[y,x]^n = [y,x^n]$ basta observar que $[y,x^n] = [x^n,y]^{-1} = [x,y]^{-n} = [y,x]^n$.

Do mesmo modo, a identidade (d) é verdadeira para $n = 1$: Prosseguiremos novamente por indução sobre n. Suponha que o resultado seja válido para algum n, lembrando que cada $[x,y] \in Z(G)$ e pelo item anterior, temos que $y^n x = [y,x]^n x y^n$. Logo,

$$\begin{aligned} (xy)^{n+1} = &\ (xy)^n xy = x^n y^n [y,x]^{\frac{n(n-1)}{2}} xy \\ = &\ x^n (y^n x) y [y,x]^{\frac{n(n-1)}{2}} = x^n [y,x]^n x y^n y [y,x]^{\frac{n(n-1)}{2}} \\ = &\ x^n x y^n y [y,x]^n [y,x]^{\frac{n(n-1)}{2}} = x^{n+1} y^{n+1} [y,x]^{n+\frac{n(n-1)}{2}} \\ = &\ x^{n+1} y^{n+1} [y,x]^{\frac{(n+1)n}{2}}, \end{aligned}$$

o que completa a demonstração. □

1.2.1 Séries: Derivada e Centrais

Definição 1.2.10. *Seja G um grupo. Uma sequência finita de subgrupos de G*

$$\mathcal{S} : 1 = G_0 \leq G_1 \leq \ldots \leq G_n = G,$$

*é dita ser **série subnormal** se $G_i \trianglelefteq G_{i+1}$ e **série normal** se $G_i \trianglelefteq G$, $0 \leq i \leq n-1$. Ademais, os subgrupos G_i são chamados de **termos da série** $\mathcal{S}$; os grupos quocientes G_{i+1}/G_i são os **fatores da série** $\mathcal{S}$.*

Definição 1.2.11. *Seja G um grupo. Considere $G^{(0)} = G$, $G^{(1)} = G' = [G,G]$ e definamos:*

$$G^{(n)} = [G^{(n-1)}, G^{(n-1)}], \text{ para } n \geq 1.$$

Tal construção formam um série

$$G \geq G' \geq G'' \geq \cdots,$$

*de tal forma que $G^{(i)} \trianglelefteq G$. Esta série é chamada de **série derivada** de G.*

Definição 1.2.12. *(Série Central Inferior). Seja G um grupo. Considere $\gamma_1(G) = G$ e defininamos:*

$$\gamma_{n+1}(G) = [\gamma_n(G), G],$$

para todo $n \geq 1$. Tais subgrupos forma uma série

$$G = \gamma_1(G) \geq \gamma_2(G) \geq \cdots \geq \gamma_n(G) \geq \cdots,$$

*de tal forma que $\gamma_i(G)/\gamma_{i+1}(G) \leq Z(G/\gamma_{i+1}(G))$. Tal série é chamada de **série central inferior** de G.*

A partir da definição de série central inferior e de uma condicão de finitude sobre ela, definimos uma classe muito importante de grupos: os **grupos nilpotentes**.

Definição 1.2.13. *Dizemos que um grupo G é **nilpotente** de classe c, quando c é o menor número natural tal que $\gamma_{c+1}(G) = 1$.*

Definição 1.2.14. *(Série Central Superior). Seja G um grupo. Consideremos $Z_0(G) = 1$, $Z_1(G) = Z(G)$ e definamos:*

$$Z_i(G)/Z_{i-1}(G) = Z(G/Z_{i-1}(G)),$$

*para todo $i \geq 1$. Assim, definimos a **série central superior** de G:*

$$1 = Z_0(G) \le Z_1(G) = Z(G) \le Z_2(G) \le \cdots \le Z_i(G) \le \cdots.$$

Proposição 1.2.15. *Seja G um grupo. Então,*

$$Z_i(G) = \{x \in G \,|\, [x, g_1, \ldots, g_i] = 1, \forall g_1, \ldots, g_i \in G\},$$

para todo $i \ge 1$.

Demonstração. Demonstraremos por indução sobre i. O caso $i = 1$ é imediato, visto que $Z_1(G) = Z(G) = \{x \in G \mid [x, g_1] = 1, \forall g_1 \in G\}$. Suponha que o resultado seja válido para algum i. Pela definição de $Z_{i+1}(G)$,

$$\begin{aligned} Z_{i+1}(G) &= \{x \in G \mid xZ_i(G) \in Z(G/Z_i(G))\} \\ &= \{x \in G \mid [x, g_1] \in Z_i(G), \forall g_1 \in G\} \\ &= \{x \in G \mid [x, g_1, \ldots, g_{i+1}] = 1, \forall g_1, \ldots, g_{i+1} \in G\}, \end{aligned}$$

onde a última igualdade é consequência da hipótese de indução. E completamos a demonstração. □

Lema 1.2.16. *Sejam G um grupo e $i \le j$ inteiros positivos. Então,*

$$[\gamma_i(G), Z_j(G)] \le Z_{j-i}(G)$$

Em particular, $Z_i(G)$ centraliza $\gamma_i(G)$.

Demonstração. Demontraremos por indução sobre i. Para $i = 1$,

$$[\gamma_i(G), Z_j(G)] = [G, Z_j(G)] \le Z_{j-1}(G).$$

Agora, suponha que o resultado seja válido para algum i. Pelo Lema dos Três Subgrupos,

$$[\gamma_{i+1}(G), Z_j(G)] = [\gamma_i(G), G, Z_j(G)] \le [Z_j(G), \gamma_i(G), G][G, Z_j(G), \gamma_i(G)].$$

Por hipótese de indução,

$$[Z_j(G), \gamma_i(G), G] \le [Z_{j-i}(G), G] \le Z_{j-(i+1)}(G)$$

e

$$[G, Z_j(G), \gamma_i(G)] \le [Z_{j-1}(G), \gamma_i(G)] \le Z_{j-(i+1)}(G).$$

Portanto,

$$[\gamma_{i+1}(G), Z_j(G)] \leq Z_{j-(i+1)}(G).$$

Isto conclui a demonstração. □

Lema 1.2.17. *Seja N um subgrupo normal de um grupo G. Então, $\gamma_i(G/N) = \gamma_i(G)N/N$, para todo $i \geq 1$.*

Demonstração. Vamos demonstrar por indução sobre i. Para $i = 1$, o resultador é verdadeiro, pois $\gamma_1(G/N) = G/N = GN/N = \gamma_1(G)N/N$. Agora, suponhamos que o resultado é válido para algum $i \geq 1$. Assim,

$$\gamma_{i+1}(G/N) = [\gamma_i(G/N), G/N] = [\gamma_i(G)N/N, G/N].$$

Pelo Lema 1.2.5 segue que,

$$[\gamma_i(G)N/N, G/N] = [\gamma_i(G)N/N, GN/N][\gamma_i(G), G]N/N = \gamma_{i+1}(G)N/N.$$

Portanto, $\gamma_i(G/N) = \gamma_i(G)N/N$, para todo $i \geq 1$.

□

Lema 1.2.18. *Seja G um grupo e $i, j \geq 0$. Então, $Z_i(G/Z_j(G)) = Z_{i+j}(G)/Z_j(G)$.*

Demonstração. Pela Proposição 1.2.15, o elemento $xZ_j(G) \in Z_i(G/Z_j(G))$ se, e somente se,

$$Z_j(G) = [xZ_j(G), g_1Z_j(G), \ldots, g_iZ_j(G)] = [x, g_1, \ldots, g_i]Z_j(G),$$

para todo $g_1Z_j(G), \ldots, g_iZ_j(G) \in Z_i(G/Z_j(G)$, ou seja, $xZ_j(G) \in Z_i(G/Z_j(G)$ se, e somente se, $[x, g_1, \ldots, g_i] \in Z_j(G)$, para todo $g_1, \ldots, g_i \in G$. Isso ocorre, se, e somente se,

$$[x, g_1, \ldots, g_i, g_{i+1}, \ldots, g_{i+j}] = [[x, g_1, \ldots, g_i], g_{i+1}, \ldots, g_{i+j}] = 1$$

para todo $g_{i+1}, .., g_{i+j} \in G$. Assim, $xZ_j(G) \in Z_i(G/Z_j(G))$ se, e somente se, $x \in Z_{i+j}(G)$, que é equivalente a $xZ_j(G) \in Z_{i+j}(G)/Z_j(G)$, o que completa a demonstração. □

1.3 Ação de Grupo

Definição 1.3.1. *Seja G um grupo. Dizemos que G* ***age*** *(à esquerda) sobre o conjunto não vazio X se é dada uma função $G \times X \longrightarrow X$, $(g, x) \longmapsto gx$ com as seguintes:*

(a) $1x = x$*, para todo* $\in X$*;*

(b) $g(hx) = (gh)x$*, para todo* $x \in X$ *e para todo* $g,h \in G$*.*

Observação 1.3.2. *Da mesma forma pode-se definir o grupo* G *agindo no conjunto* X *à direita. Toda ação à direita pode ser substituida por uma ação à esquerda via:* $gx := xg^{-1}$*,* $x \in X$ *e* $g \in G$*. Se* $H \leq G$ *e* G *age sobre* X*, então* H *também age sobre* X*, a ação de* H *sobre* X *sendo definida pela mesma regra que define a ação de* G *sobre* X*.*

Definição 1.3.3. *Sejam* X *um conjunto não vazio e* G *um grupo. Suponha que* G *age sobre* X*. Dado* $x \in X$ *defina por*

$$G_x = \{g \in G \mid gx = x\} \leq G$$

o ***estabilizador*** *de* x *e*

$$O_G(x) = \{gx \mid g \in G\} \subseteq X$$

a ***órbita*** *(ou* ***G-órbita****) de* x*. Ação é dita ser* ***transitiva*** *se existe* $x \in X$ *tal que* $O_G(x) = X$*, isto é, se existe apenas uma órbita.*

Proposição 1.3.4. *Suponha que o grupo* G *age sobre o conjunto* X*. Então,* X *é igual a união disjunta das G-órbitas.*

Proposição 1.3.5. *Suponha que o grupo* G *age sobre* X *e* $x \in X$*. Então,*

$$|O_G(x)| = |G : G_x|$$

Em particular, se G *for finito, então* $|O_G(x)| = \dfrac{|G|}{|G_x|}$*.*

O resultado acima pode ser encontrado em [7, 1.2.2 Corollary].

Seja X um conjunto não vazio. Uma **permutação** de X é uma função bijetiva $X \to X$. Denotamos por S_X o conjunto das permutações de X. Além disso, S_X com a operação de composiçao de funções é um grupo, chamado o grupo das permutações de X. Uma ação de G sobre X pode ser vista como um homomorfismo:

Proposição 1.3.6. *Sejam* G *um grupo e* X *um conjunto não vazio.*

(a) *Se* $A : G \times X \longrightarrow X$*,* $(g,x) \longmapsto gx$*, é uma ação de* G *sobre* X*, então o homomorfismo correspondente é* $\psi_A : G \longrightarrow S_X$*,* $\psi_A(g) : X \longrightarrow X$*,* $x \longmapsto gx$*;*

(b) *Se* $\psi : G \longrightarrow S_X$ *é um homomorfismo, então a ação correspondente é* $A_\psi : G \times X \longrightarrow X$*,* $(g,x) \longmapsto \psi(g)(x)$*.*

Seja H um subgrupo de um grupo G e Considere $H_G := \bigcap\limits_{g \in G} gHg^{-1}$. Temos que H_G é um subgrupo normal de G contido em H, e o chamaremos de **coração normal** de H em G. Em particular, $H \trianglelefteq G$ se, e somente se, $H = H_G$.

Lema 1.3.7. *Seja H um subgrupo de um grupo G. Se o índice $|G:H| = n$, então a ordem do grupo quociente G/H_G divide $n!$*

O resultado acima pode ser encontrado em [10, 1.6.9]

1.4 Homomorfismo Transfer

O objetivo dessa seção será desenvolver homomorfismos de grupos a partir de homomorfismos dados em alguns subgrupos de G.

Definição 1.4.1. *Sejam H um subgrupo próprio de um grupo G com $|G:H| = n$, A um grupo abeliano e $\theta : H \longrightarrow A$ um homomorfismo de grupos. Consideramos um transversal $\tau = \{t_1, t_2, \ldots, t_n\}$ de H em G, ou seja,*

$$G = \dot{\bigcup_{i=1,\ldots,n}} Ht_i.$$

E dado qualquer elemento $x \in G$: existe um único par $(h, t_j) \in H \times \tau$ tal que $x = ht_j$. Agora, consideramos a seguinte ação nas classes laterais: $Ht_ix := Ht_{(i)x}$, assim $t_ixt_{(i)x}^{-1} \in H$. Definamos a seguinte aplicação:

$$\begin{array}{rcl} \theta^* : G & \to & A \\ x & \mapsto & \prod\limits_{i=1}^{n} (t_ixt_{(i)x}^{-1})^{\theta}. \end{array}$$

Uma vez que A é abeliano, a ordem dos fatores no produto é irrelevante.

Observação 1.4.2. *Note que a aplicação $i \to (i)x$ é uma permutação de $\{1, 2, \ldots, n\}$. É suficiente observar que a aplicaçao é injetiva. De fato, se $(i)x = (j)x$, então $Ht_{(i)x} = Ht_{(j)x}$. Daí, $Ht_ix = Ht_jx$ implica que $t_it_j^{-1} \in H$, ou seja, $t_i = t_j$ e obtemos $i = j$.*

Lema 1.4.3. *Sejam H um subgrupo próprio de um grupo G com $|G:H| = n$, A um grupo abeliano e $\theta : H \to A$ um homomorfismo de grupos. Consideramos um transversal (à direita) $\tau = \{t_1, t_2, \ldots, t_n\}$ de H em G. Então*

(a) *θ^* é um homomorfismo de grupos;*

(b) O homomorfismo θ^* independe da escolha do transversal τ de H em G

Demonstração. Lembrando que A é abeliano e θ é um homomorfismo. Dados os elementos $x, y \in G$:

(a) Da definição: $Ht_ixy = Ht_{(i)x}y = Ht_{((i)x)y}$. Por outro lado, $Ht_ixy = Ht_{(i)xy}$. Logo, $Ht_{((i)x)y} = Ht_{(i)xy}$, e assim, $t_{(i)xy} = t_{((i)x)y}$. Então,

$$\begin{aligned}(xy)^{\theta^*} &= \prod_{i=1}^{n}(t_ixyt_{(i)xy}^{-1})^{\theta} = \prod_{i=1}^{n}(t_ixyt_{((i)x)y}^{-1})^{\theta} = \prod_{i=1}^{n}(t_ixt_{(i)x}^{-1}t_{(i)x}yt_{((i)x)y}^{-1})^{\theta} \\ &= \prod_{i=1}^{n}(t_ixt_{(i)x}^{-1})^{\theta}(t_{(i)x}yt_{((i)x)y}^{-1})^{\theta} = \prod_{i=1}^{n}(t_ixt_{(i)x}^{-1})^{\theta}\prod_{i=1}^{n}(t_{(i)x}yt_{((i)x)y}^{-1})^{\theta} \\ &= (x)^{\theta^*}(y)^{\theta^*},\end{aligned}$$

Portanto, θ^* é um homomorfismo conforme afirmado.

(b) Tomemos $\tau' = \{t'_1, t'_2, \ldots, t'_n\}$ um outro transversal de H em G. Calcule o homomorfismo associado a τ'. Chamemos tal homomorfismo de $\overline{\theta}^*$.

Sem perda de generalidade podemos supor que $Ht'_i = Ht_i$ (a menos de uma reordenação dentro do transversal). Assim, $t'_i = h_it_i$, com $h_i \in H$. Agora veja que

$$Ht'_{(i)x} = Ht'_ix = Hh_it_ix = Ht_ix = Ht_{(i)x}.$$

E temos que $t'_{(i)x} = h_{(i)x}t_{(i)x}$, com $h_{(i)x} \in H$.Portanto,

$$\begin{aligned}(x)^{\overline{\theta}^*} &= \prod_{i=1}^{n}(t'_ixt'^{-1}_{(i)x})^{\theta} = \prod_{i=1}^{n}(h_it_ix(h_{(i)x}t_{(i)x})^{-1})^{\theta} = \prod_{i=1}^{n}(h_it_ixt_{(i)x}^{-1}h_{(i)x}^{-1})^{\theta} \\ &= \prod_{i=1}^{n}(h_i)^{\theta}(t_ixt_{(i)x}^{-1})^{\theta}(h_{(i)x}^{-1})^{\theta} = \prod_{i=1}^{n}(t_ixt_{(i)x}^{-1})^{\theta} = (x)^{\theta^*}\end{aligned}$$

□

Observação 1.4.4. *O homomorfismo θ^* será chamado de **homomorfismo transfer** associado a θ e tal homomorfismo independe do grupo abeliano A.*

Lema 1.4.5. *(Cálculo do homomorfismo θ^*). Sejam A um grupo abeliano e H um subgrupo de índice finito no grupo G. Suponhamos que existe um homomorfismo $\theta : H \to A$ e $|G : H| = n$. Então, para cada $x \in G$ existem $l_1, l_2, \ldots, l_m \in \mathbb{N}$ e $s_1, s_2, \ldots, s_m \in G$ tais que*

$$(x)^{\theta^*} = \prod_{i=1}^{m}(s_ix^{l_i}s_i^{-1})^{\theta} \quad e \quad \sum_{i=i}^{m} l_i = n$$

Demonstração. Vamos escolher um transversal conveniente e depois efetivaremos o cálculo do homomorfismo transfer.

Primeiro iremos descrever o tal transversal de H em G. Tomemos $s_1 \in G$ (qualquer). Daí, existem exatamente, l_1 classes laterais associadas ao elemento s_1:

$$Hs_1, Hs_1x, \ldots, Hs_1x^{l_1} = Hs_1.$$

De fato existe um número natural l_1 com tal propriedade, pois $|G:H| = n$. Caso $l_1 = n$, temos que $\tau = \{t_1 = s_1, \ldots, t_n = s_1x^{l_1-1}\}$ é um transversal para H em G. Caso contrário $l_1 < n$ e tomemos $s_2 \in G$ tal que

$$s_2 \quad \notin \quad \bigcup_{j_1=0}^{l_1-1} Hs_1x^{j_1}.$$

Da finitude do índice $|G:H| = n$, temos que existem l_2 classes laterais associadas ao elemento s_2:

$$Hs_2, Hs_2x, \ldots, Hs_2x^{l_2} = Hs_2.$$

Caso $l_1 + l_2 = n$, obtemos que $\tau = \{t_1 = s_1, \ldots, t_{l_1} = s_1x^{l_1-1}, t_{l_1+1} = s_2, \ldots, t_n = s_2x^{l_2-1}\}$ é um transversal para H em G. Caso contrário $l_1 + l_2 < n$ e tomemos $s_3 \in G$ tal que

$$s_3 \quad \notin \quad \left(\bigcup_{j_1=0}^{l_1-1} Hs_1x^{j_1} \cup \bigcup_{j_2=0}^{l_2-1} Hs_2x^{j_2} \right).$$

Prosseguindo com o argumento acima e baseado na finitude do índice $|G:H| = n$, obtemos: elementos $s_1, s_2, s_3, \ldots, s_m \in G$ e números naturais $l_1, l_2, l_3, \ldots, l_m$ tais que $l_1 + l_2 + \ldots + l_m = n$ tais que

$$\begin{array}{ccccccccc}
Hs_1 & , & Hs_1x \, , \, Hs_1x^2 \, , \, \ldots \, , \, Hs_1x^{l_1-1} \, , \, Hs_1x^{l_1} & = & Hs_1 \\
Hs_2 & , & Hs_2x \, , \, Hs_2x^2 \, , \, \ldots \, , \, Hs_2x^{l_2-1} \, , \, Hs_2x^{l_2} & = & Hs_2 \\
Hs_3 & , & Hs_3x \, , \, Hs_3x^2 \, , \, \ldots \, , \, Hs_3x^{l_3-1} \, , \, Hs_3x^{l_3} & = & Hs_3 \\
\ldots & , & \ldots \, , \, \ldots \, , \, \ldots \, , \, \ldots \, , \, \ldots \, , \, \ldots \, , \, \ldots \, , \, \ldots & = & \ldots \\
Hs_m & , & Hs_mx \, , \, Hs_mx^2 \, , \, \ldots \, , \, Hs_mx^{l_m-1} \, , \, Hs_mx^{l_m} & = & Hs_m.
\end{array}$$

E, pela construção, obtemos a seguinte decomposição de G em classes laterais de H:

$$G=\left(\bigcup_{j_1=0}^{l_1-1} Hs_1x^{j_1}\right)\cup\left(\bigcup_{j_2=0}^{l_2-1} Hs_2x^{j_2}\right)\cup\ldots\cup\left(\bigcup_{j_m=0}^{l_m-1} Hs_mx^{j_m}\right).$$

Notemos que para o primeiro bloco com l_1 elementos temos:

$$\begin{aligned}
Ht_1x &= Hs_1x = Ht_2 \text{ e, temos } t_{(1)x}=t_2\\
Ht_2x &= Hs_1x^2 = Ht_3 \text{ e, temos } t_{(2)x}=t_3\\
\ldots &= \ldots\\
Ht_{l_1-1}x &= Hs_1x^{l_1-1} = Ht_{l_1} \text{ e, temos } t_{(l_1-1)x}=t_{l_1}\\
Ht_{l_1}x &= Hs_1x^{l_1} = Ht_1 \text{ e, temos } t_{(l_1)x}=t_1
\end{aligned}$$

E, em particular, por um argumento de “série telescópica”:

$$(t_1xt_{(1)x}^{-1})^\theta(t_2xt_{(2)x}^{-1})^\theta\ldots(t_{l_1-1}xt_{(l_1-1)x}^{-1})^\theta(t_{l_1}xt_{(l_1)x}^{-1})^\theta=$$
$$=(t_1xt_2^{-1})^\theta(t_2xt_3^{-1})^\theta\ldots(t_{l_1-1}xt_{l_1}^{-1})^\theta(t_{l_1}xt_1^{-1})^\theta=(t_1x^{l_1}t_1^{-1})^\theta.$$

Façamos o mesmo em cada um dos $m-1$ blocos restantes e obtemos a fórmula desejada:

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

□

Definição 1.4.6. *Dizemos que um grupo G é **central-por-finito** se o índice $|G:Z(G)|$ é finito.*

Lema 1.4.7. *Seja G um grupo central-por-finito. Suponhamos que o índice $|G:Z(G)|=n$ e $\theta:Z(G)\to Z(G)$ é o homomorfismo identidade. Então o homomorfismo transfer θ^* associado θ é dado por $(x)^{\theta^*}=x^n$.*

Demonstração. Dado $x\in G$. Pelo Lema 1.4.5, existem $l_1,l_2,\ldots,l_m\in\mathbb{N}$ e $s_1,s_2,\ldots,s_m\in G$ tais que

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

pois θ é o homomorfismo identidade, $s_ix^{l_i}s_i^{-1}\in Z(G)$, $i\in\{1,2,\ldots,n\}$ e $\sum_{i=1}^m l_i=n$. Essa análise somente dependeu do índice $|G:Z(G)|$ e, consequentemente, $(x)^{\theta^*}=x^n$, para todo $x\in G$. □

1.5 FC-grupo e BFC-grupo

Definição 1.5.1. *Seja G um grupo. Dado $x \in G$ o conjunto*

$$x^G = \{x^g \mid g \in G\},$$

de todos os conjugados de x em G, é chamado de **classe de conjugação** *de x (em G).*

Proposição 1.5.2. *Seja G um grupo. Dado $x \in G$, o número de conjugados de x em G é igual ao índice do seu centralizador em G, isto é,*

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

Demonstração. Dado $x \in G$, considere $C = C_G(x)$ e $K = x^G$. Seja X o conjunto de todos as classes laterais à direta de C. Sabemos que $|X| = |G : C|$, defina $\varphi : X \longrightarrow K$ dada por $(Cg)^\varphi = x^g$. Inicialmente, vamos verificar se φ é bem definida. De fato, se $Cg = Ch$, então $gh^{-1} \in C$, e assim $(gh^{-1})x = x(gh^{-1})$, que pode ser escrito $x^h = x^g$, e isso mostrar que $(Ch)^\varphi = (Cg)^\varphi$.

Agora, vamos mostrar que φ é injetora. Suponha que $(Cg)^\varphi = (Ch)^\varphi$, assim $x^g = x^h$, que pode ser escrito $x(gh^{-1}) = (gh^{-1})x$, mas isso implica que $gh^{-1} \in C$. Portanto, $Cg = Ch$.

Por fim, φ é sobrejetora. Seja $k \in K$ um elemento qualquer, existe $g \in G$ tal que $k = x^{g^{-1}}$. Observe que, $(Hg^{-1})^\varphi = x^{g^{-1}} = k$. E completamos a demostração. □

Se o número de elementos em cada classe de conjugação de um grupo for finito (ou uniformemente limitado), então o grupo recebe um nome especial.

Definição 1.5.3. *Um grupo G é dito um* ***FC-grupo*** *se para todo $x \in G$ temos que a classe de conjugação x^G é finita. Adicionalmente, se existir uma constante (uniforme) $k \in \mathbb{N}$ de tal modo que $|x^G| \leqslant k$ para todo $x \in G$, então G é dito um* ***BFC-grupo****.*

Exemplo 1.5.4. *Os grupos abelianos e os grupos finitos são exemplos de FC-grupos. Nos grupos abelianos cada classe de conjugação possui apenas um único elemento; e, naturalmente, toda classe de conjugação de um grupo finito é finita (e uniformente limitada pela ordem do grupo). Em particular, todo grupo que é BFC-grupo é também um FC-grupo. Além disso, no próximo resultado demostraremos que todo grupo central-por-finito é um exemplo de um BFC-grupo.*

Lema 1.5.5. *Seja G um grupo central-por-finito. Então G é BFC-grupo.*

Demonstração. Suponha que $|G : Z(G)| = n$. Dado qualquer $x \in G$, temos que $Z(G) \leq C_G(x)$. Pela Proposição 1.5.2,

$$|x^G| = |G : C_G(x)| \leq |G : Z(G)| = n,$$

consequentemente $|x^G| \leq n$, para todo $x \in G$. Pontanto, G é um BFC-grupo. $\square$

Lema 1.5.6. *Seja G um FC-grupo finitamente gerado. Então G é central-por-finito.*

Demonstração. Sejam $x_1, x_2, \ldots, x_n \in G$ tais que

$$G = \langle x_1, x_2, \ldots, x_n \rangle.$$

Lembrando que G é FC-grupo, chamemos

$$m_i = |x_i^G| = |G : C_G(x_i)|,\ 1 \leq i \leq n.$$

Sabemos que $Z(G) = \bigcap_{i=1}^{n} C_G(x_i)$, pela Proposição 1.1.13. Daí, pelo Lema de Poincaré,

$$|G : Z(G)| = |G : \bigcap_{i=1}^{r} C_G(x_i)| \leq \prod_{i=1}^{r} |G : C_G(x_i)| \leq m_1 m_2 \ldots m_r < +\infty.$$

Portanto, G é central-por-finito. $\square$

Observação 1.5.7. *Dos Lemas 1.5.5 e 1.5.6, podemos verificar que todo FC-grupo finitamente gerado é um BFC-grupo.*

Na Seção 2.2 veremos que existe uma classificação para BFC-grupos devida a B. H. Neumann em termos da finitude do seu subgrupo derivado (e do conjunto dos comutadores) (cf. [10, 14.5.11]).

1.6 Contagem e o Princípio da Casa dos Pombos

Por uma questão de completude incluímos os enunciados dos Princípio Fundamental da Contagem e o Princípio da Casa dos Pombos. Ambos os resultados são frequentemente abordados em cursos de Matemática Discreta. Seguem os seus enunciados junto com referências nas quais esse tema são trabalhados com mais detalhes.

Lema 1.6.1. *(Princípio Fundamental de Contagem). Se há m modos de tomar a decisão D_1 e, tomada a decisão D_1, há n modos de tomar a decisão D_2, então o número de modos de tomar as decisões D_1 e D_2 (sucessivamente) é mn.*

O resultado acima pode ser encontrado em [8, pág. 81].

Lema 1.6.2. *(Princípio da Casa dos Pombos) Se $n+1$ objetos são colocados em n casas, então, pelo menos uma casa recebe mais de um objeto.*

Para uma demonstração desse fato, veja [8, pág. 134].

Capítulo 2

Condições de Finitude para o Subgrupo Comutador

O objetivo deste capítulo é estudar certos teoremas que envolvem a finitute de um dado subgrupo do subgrupo comutador em termos de seus comutadores. Focaremos nos teoremas de Issai Schur [10], Bernhard Neumman [10, 14.5.11], Reinhold Baer [10, 14.5.1 e 14.5.2] e Maxwell Rosenlicht [11].

Nesse capítulo, para simplificar a notação, usaremos o termo "$\{m,n,\ldots\}$-limitado" para expressar que uma quantidade é finita e limitada superiormente por uma função que depende somente dos parâmetros $m,n,\ldots$.

2.1 Teorema de Schur

O objetivo dessa seção é demonstrar o famoso Teorema de Schur: Se G é um grupo com $|G:Z(G)|$ finito, então podemos concluir que o subgrupo comutador G' é finito. A grosso modo, isso significa que, se o centro de G for grande, então o subgrupo comutador G' será pequeno. Inicialmente mostraremos que G' é finitamente gerado.

Lema 2.1.1. *Seja G um grupo com $|G:Z(G)|=n$. Então o subgrupo comutador G' é finitamente gerado. Mais ainda, G' é gerado por, no máximo, n^2 geradores.*

Demonstração. Seja $\tau=\{t_1,t_2,\ldots,t_n\}$ um transversal de $Z(G)$ em G. Dados $x,\ y\in G$, existem $i,\ j\in I:=\{1,2,\ldots,n\}$ e elementos $z_1,\ z_2\in Z(G)$ tais que $x=z_1t_i,\ y=z_2t_j\in G$. Note que

$$\begin{aligned}[x,y]&=[z_1t_i,z_2t_j]=(z_1t_i)^{-1}(z_2t_j)^{-1}(z_1t_i)(z_2t_j)\\&=t_i^{-1}z_1^{-1}t_j^{-1}z_2^{-1}z_1t_iz_2t_j=t_i^{-1}t_j^{-1}t_it_j=[t_i,t_j],\end{aligned}$$

pois $z_1, z_2 \in Z(G)$. Logo, $G' = \langle [x,y] \,|\, x,y \in G \rangle = \langle [t_i,t_j] \,|\, i,j \in I \rangle$, o que completa a demonstração. $\square$

O próximo resultado mostra que, se o centro de um grupo G tiver índice n, então a $(n+1)$-ésima potência de qualquer comutador (em G) é igual ao produto de n comutadores.

Lema 2.1.2. *Seja um grupo G com $|G : Z(G)| = n$. Então, $[x,y]^{n+1} = [x,y^2][x^y,y]^{n-1}$ para todo $x,y \in G$.*

Demonstração. Como $G/Z(G)$ tem ordem n, segue que $[x,y]^n \in Z(G)$ para todo x, $y \in G$. Então,

$$\begin{aligned}
[x,y]^{n+1} &= [x,y]^n[x,y] = [x,y]^n x^{-1}y^{-1}xy \\
&= x^{-1}y^{-1}x[x,y]^n y = x^{-1}y^{-1}x[x,y][x,y]^{n-1}y \\
&= x^{-1}y^{-2}xy[x,y]^{n-1}y = x^{-1}y^{-2}xy^2y^{-1}[x,y]^{n-1}y \\
&= [x,y^2][x^y,y]^{n-1}.
\end{aligned}$$

$\square$

Lema 2.1.3. *Seja um grupo G com $|G : Z(G)| = n$. Então, todo elemento do subgrupo comutador G' pode ser escrito como um produto de, no máximo, n^3 comutadores.*

Demonstração. Suponhamos que existe $\alpha \in G'$ tal que α pode ser escrito como um produto de n^3+1 comutadores e não menos que n^3+1, isto é,

$$\alpha = c_1c_2\ldots c_{n^3+1},$$

onde $c_i = [x_i,y_i]$. Por outro lado, existem no máximo n^2 comutadores em G, pelo Lema 2.1.1. Assim, pelo Lema 1.6.2, existe pelo menos um comutador, digamos $[x,y]$, que ocorre mais de n vezes nesse produto. Daí, podemos reescrever α da seguinte forma

$$\alpha = [x,y]^{n+1}c'_{n+2}c'_{n+3}\cdots c'_{n^3+1},$$

onde cada c'_j é um comutador conjugado a um dos comutadores c_i sob alguma potência de $[x,y]$. Segue do Lema 2.1.2 que

$$\alpha = [x,y^2][x^y,y]^{n-1}c'_{n+2}c'_{n+3}\cdots c'_{n^3+1},$$

ou seja, α é um produto de n^3 comutadores, uma contradição. $\square$

Agora estamos em condicões de demonstrar o Teorma de Schur.

Teorema 2.1.4. *(Schur) Seja G um grupo central-por-finito. Suponha que $|G : Z(G)| = n$. Então, o subgrupo comutador G' é finito e tem ordem n-limitada. Além disso,* $\exp(G')$ *divide n.*

Demonstração. Sabemos pelo Lema 1.4.7 que a aplicação $\theta^* : G \to Z(G)$ definida por $(x)^{\theta^*} = x^n$, é o homomorfismo transfer associado a identidade $\theta : Z(G) \to Z(G)$, sendo $n = |G : Z(G)|$. Por definição, $\ker(\theta^*) = \{g \in G \mid g^n = 1\}$. Segue do primerio Teorema de Isomorfismo que

$$G/\ker(\theta^*) \cong \mathrm{Im}(\theta^*) \leq Z(G).$$

Logo, $G/\ker(\theta^*)$ é abeliano, donde segue da Proposição 1.2.8 que $G' \leq \ker(\theta^*)$, e portanto, $\exp(G')$ divide n.

Resta mostar que $|G'|$ é n-limitada. Sabemos que existem no máximo n^2 comutadores distintos em G, pelo Lema 2.1.1. Além disso, pelo Lema 2.1.3 cada elemento $\alpha \in G'$ pode ser escrito como um produto de, no máximo, n^3 comutadores, isto é,

$$\alpha = c_1 c_2 \dots c_{n^3},$$

segue do Lema 1.6.1, que existem, no máximo, $(n^2)^{n^3} = n^{2n^3}$ elementos em G'. $\square$

As demonstrações dos resultados apresentados nesta seção foram baseadas no livro do John Dixon [2, Capítulo 5].

2.2 Teorema de Neumann

Essa seção tem por objetivo demonstrar o clássico Teorema de B. Neumann. Para isso, demonstraremos alguns resultados sobre FC-grupos. Mas, inicialmente demonstraremos que se o conjunto de todos comutadores de um grupo G for finito, então G é um BFC-grupo e, nessa mesma hipótese, o subgrupo comutador G' é finito.

Lema 2.2.1. *Sejam G um grupo e $\Gamma(G) = \{[x_1, y_1], [x_2, y_2], \dots, [x_m, y_m]\}$ o conjunto de todos os comutadores de G. Suponhamos que $X = \{x_1, y_1, \dots, x_m, y_m\} \subseteq G$ e $H = \langle X \rangle$. Então,*

(a) $H' = G'$.

(b) *G é um BFC-grupo.*

Demonstração. (a) De fato, $\{[h,k] \mid \mid h,k \in H\} \subseteq G'$, pois todo comutador de H é também um comutador de G. Logo, $H' \leq G'$. Por outro lado, $\Gamma(G) \subseteq H'$, pois cada $[x_i, y_i] \in H'$, $1 \leq i \leq m$, e assim, $G' \leq H'$. Portanto, $H' = G'$.

(b) Para cada $x \in G$ fixo e qualquer $g \in G$, temos que

$$x^g = g^{-1}xg = (xx^{-1})g^{-1}xg = x[x,g].$$

Como G tem m comutadores, segue que $|x^G| = |\{x[x,g] \mid g \in G\}| \leq m$. Portanto, G é um BFC-grupo. □

Lema 2.2.2. *Sejam G um grupo e $\Gamma(G) = \{[x_1,y_1],[x_2,y_2],\dots,[x_m,y_m]\}$ o conjunto de todos os comutadores de G. Suponhamos que $X = \{x_1,y_1,\dots,x_m,y_m\} \subseteq G$ e $H = \langle X\rangle$. Então, $H' = G'$ é finito de ordem m-limitada.*

Demonstração. De fato, para cada $x \in X$ temos que

$$|H : C_H(x)| = |x^H| = |\{x[x,h] \mid h \in H\}| \leq m,$$

pela Proposição 1.5.2. Além disso, $Z(G) = \bigcap_{x\in X} C_H(x)$, pela Proposição 1.1.13. Lembrando que $|X| = 2m$, segue do Lema de Poincaré que

$$|H : \bigcap_{x\in X} C_H(x)| \leq \prod_{x\in X} |H : C_H(x)| \leq m^{2m}.$$

Daí, $|H : Z(H)| \leq m^{2m}$. Pelo Teorema de Schur, H' é finito, mais ainda,

$$|H'| \leq (m^{2m})^{2(m^{2m})^3},$$

o que completa a demonstração. □

A cota para a ordem do Subgrupo comutador obtida no Lema acima não tem a pretenção de ser a melhor possível! A incluímos apenas com o interesse de expressar a m-limitação. Cotas mais razoáveis dependem de técnicas mais avançadas e não serão desenvolvidas nessa dissertação. Para maiores detalhes veja o trabalho de James Wiegold [12, Theorem 4.7].

Agora, vamos incluir alguns resultados sobre FC-grupo, bem como o Lema de Dietzmann, e definir grupo localmente finito. Com isso, teremos condições para demonstrar o Teorema de Neumann.

Lema 2.2.3. *Se G é um FC-grupo, então o grupo quociente $G/Z(G)$ é de torção.*

Demonstração. Dado $x \in G$. Pela Proposição 1.5.2, $|x^G| = |G : C_G(x)|$. Como G é FC-grupo, $|G : C_G(x)| = k < +\infty$, para algum inteiro positivo k. Seja $\tau = \{t_1, t_2, \dots t_k\}$ um transversal de $C_G(x)$ em G. Considere $H = \bigcap_{i=1}^{k} C_G(t_i)$, pelo Lema de Poincaré,

$$|G : H| = |G : \bigcap_{i=1}^{k} C_G(t_i)| \leq \prod_{i=1}^{k} |G : C_G(t_i)| = n < +\infty,$$

para algum inteiro positivo n. Seja H_G o coração normal de H em G. Pelo Lema 1.3.7 $|G/H_G|$ divide $n!$. Daí, $|G/H_G| = m$, para algum inteiro m. Consequentemente $x^m \in H_G \leq H$ e, assim, $x^m t_i = t_i x^m$, $1 \leq i \leq k$. Como τ e $C_G(x)$ geram G, segue que $x^m \in Z(G)$. Logo, $G/Z(G)$ é de torção. $\square$

Teorema 2.2.4. *(Lema de Dietzmann). Seja X um subconjunto finito de um grupo G. Suponhamos que X seja normal (em G) e que $|x|$ seja finita para todo $x \in X$. Então $\langle X \rangle$ é um subgrupo normal finito de G*

Demonstração. Considere $H = \langle X \rangle$. Vamos mostrar que H é finito. Note que,

$$|H : C_H(x)| = |x^H| \leq |x^G| \leq |X| < +\infty, \forall x \in X.$$

Temos que $Z(H) = \bigcap_{x \in X} C_H(x)$, pela Proposição 1.1.13 e, assim, pelo Lema de Poincaré, o índice $|H : Z(H)|$ é finito. Logo, H' é finito, pelo Teorema de Schur. Para finalizar é necessário mostrar que H/H' é finito. De fato, H/H' é um grupo abeliano finitamente gerado e de torção, pois cada gerador de H tem ordem finita. Logo, H/H' é finito e concluímos a demonstração. $\square$

Lema 2.2.5. *Seja G um grupo de torção. Então, G é um FC-grupo se, e somente se, cada subconjunto finito de G está contido em um subgrupo normal finito de G.*

Demonstração. Suponhamos que G seja FC-grupo. Seja X um subconjunto finito de G. Assim, o subconjunto $Y = \{x^g \mid x \in X, g \in G\}$ é normal finito em G. Como G é um grupo de torção, segue pelo Teorema 2.2.4, que $\langle Y \rangle$ é um subgrupo normal finito em G contendo X.

Reciprocamente, suponha que todo subconjuto finito de G esteja contido em um subgrupo normal finito de G. Então, para cada $x \in G$, x pertence a algum subgrupo normal finito N de G e, assim, a classe de conjugação $x^G \subseteq N$ é finita. Logo, G é um FC-grupo. $\square$

Definição 2.2.6. *Um grupo G é considerado* ***localmente finito*** *se cada subgrupo finitamente gerado $H \leq G$ é finito.*

Lema 2.2.7. *Seja G um FC-grupo. Então o subgrupo comutador G' é um grupo de torção. Além disso, $Tor(G)$ é um subgrupo característico de G contendo G'.*

Demonstração. Pelo Lema 2.2.3, $G/Z(G)$ é de torção. Além disso, $G/Z(G)$ é FC-grupo; segue pelo Lema 2.2.5 que cada subconjunto finito de $G/Z(G)$ está contido em um subgrupo normal finito, donde obtemos que $G/Z(G)$ é localmente finito. Agora, dado $\alpha \in G'$, pode-se escrever $\alpha = c_1c_2\ldots c_k$, onde $c_i = [x_i,y_i]$, $1 \leq i \leq k$. Se $H = \langle x_1,y_1,x_2,y_2,\ldots x_k,y_k\rangle$, então temos que $HZ(G)/Z(G)$ é finitamente gerado e, portanto, finito. Assim,

$$H/Z(H) = H/H\cap Z(G) \cong HZ(G)/Z(G)$$

é finito. Logo, pelo Teorema de Schur, H' é finito. Com isso, $\alpha \in H'$ tem ordem finita. Sendo $\alpha \in G$ arbitrário, segue que G' é um grupo de torção. Claramente, $G' \subseteq Tor(G)$.

Agora, vamos demonstrar que o conjunto $Tor(G)$ é um subgrupo característico de G contendo G'. De fato, $1 \in Tor(G)$, pois 1 tem ordem finita. Dados $x,y \in Tor(G)$, existem inteiros positivos m e n tais que $x^m = 1 = y^n$. logo, $(x^{-1})^m = 1$ e

$$(xy)^{mn}G' = x^{mn}y^{mn}G' = (x^m)^n(y^n)^mG' = G',$$

visto que G/G' é abeliano. Daí, $(xy)^{mn} \in G'$; lembrando que G' é de torção, existe um inteiro l tal que $((xy)^{mn})^l = 1$. Logo $Tor(G) \leq G$. Dado quaisquer $\psi \in Aut(G)$, temos que $((x)^{\psi})^m = (x^m)^{\psi} = (1)^{\psi} = 1$, isto é, $(x)^{\psi} \in Tor(G)$, para todo $x \in Tor(G)$ e todo $\psi \in Aut(G)$. Logo, $Tor(G)$ é característico em G. □

Lema 2.2.8. *Seja N um subgrupo de um BFC-grupo G. Então, N é um BFC-grupo.*

Demonstração. Basta observar que $n^N \subseteq n^G$, para todo $n \in N$. Como G é um BFC-grupo, segue que N também o é. □

Lema 2.2.9. *Seja G um FC-grupo finitamente gerado. Então, $Tor(G)$ é finito.*

Demonstração. Combinando o Lema 1.5.6 e o Teorema de Schur, segue que G é central-por-finito e, consequentemente, o subgrupo derivado é finito. Agora, pelo Lema 2.2.7, $Tor(G) \leqslant G$. Pelo Teorema de Lagrange, é suficiente mostrar que $Tor(G)/G'$ é finito. De fato, $Tor(G)/G'$ é um subgrupo de torção do grupo abeliano finitamente gerado G/G'. Pela Proposição 1.1.15, segue que $Tor(G)/G'$ é um grupo finito. □

Agora estamos em condições de demonstrar o Teorema de B. H. Neumann.

Teorema 2.2.10. *(B. H. Neumann) Seja G um grupo. As seguintes afirmações são equivalentes:*

(a) O conjunto de comutadores $\Gamma(G) = \{[x,y] \mid x,y \in G\}$ é finito;

(b) G é BFC-grupo;

(c) O subgrupo comutador G' é finito.

Demonstração. De fato, (a) $\Longrightarrow$ (b) pelo Lema 2.2.1 e, pelo Lema 2.2.2, (a) $\Longleftrightarrow$ (c). Agora vamos mostrar que (b) $\Longrightarrow$(c). Se G é um BFC-grupo tal que $|x^G| \leq m$, para todo $x \in G$, escolhemos $a \in G$ tal que $|a^G| = m$ e, assim, $|G : C_G(a)| = m$. Seja $\{t_1, t_2, \ldots, t_m\}$ um transversal de $C_G(a)$ em G, logo $a^G = \{a^{t_1}, a^{t_2}, \ldots , a^{t_m}\}$. Defina $C = \bigcap_{i=1}^{m} C_G(t_i)$; pelo Lema de Poincaré, $|G : C| = |G : \bigcap_{i=1}^{m} C_G(t_i)| \leq \prod_{i=1}^{m} |G : C_G(t_i)| \leq m^m$. Então, para algum $k \leq m^m$, existe um transversal $\tau = \{s_1, s_2, ..., s_k\}$ de C em G.

Agora, considere

$$N = \langle\, a, s_1, s_2, ..., s_k \rangle^G.$$

Como G é um BFC-grupo, temos que N é um BFC-grupo (Lema 2.2.8). Em particular, N é FC-grupo finitamente gerado, então $|N : Z(N)|$ é finita, pelo Lema 1.5.6. Pelo Lema 2.2.9, $Tor(N)$ é finito. Combinando os Lemas 2.2.7 e 2.2.9 é suficiente provar que $G' \leq N$.

Seja $x \in C$. Então, $(xa)^{t_i} = t_i^{-1} x a t_i = x a^{t_i}$. A partir disso, podemos observar que os m elementos $xa^{t_1}, xa^{t_2}, ..., xa^{t_m}$ são distintos e, assim, representam todos os conjugados de xa em G, pois $|(xa)^G| \leq m$. Consequentemente, se $y \in C$, existe i tal que $(xa)^y = xa^{t_i}$. Daí, $x^y = xa^{t_i}(a^y)^{-1}$. Assim,

$$[x, y] = x^{-1}x^y = x^{-1}xa^{t_i}(a^y)^{-1} = a^{t_i}(a^y)^{-1} \in N.$$

Logo, $C' \leq N$. Observe que $G = CN$, pois G é gerado por $\tau \subseteq N$ e C. Portanto,

$$G' = (NC)' \leq NC' = N.$$

□

2.3 Teorema de Baer-Rosenlicht

O objetivo desta seção é demonstrar o Teorema de Baer-Rosenlicht. Esse resultado consiste em deduzir a finitude de um subgrupo $[N, H]$ de um grupo G em termos da finitude do conjunto gerador $\{[n, h] \mid n \in N, h \in H\}$. Tal resultado foi demonstrado por Rosenlicht em [11] e generaliza o Lema 2.2.2 caso em que $N = H = G$. Colocamos os nomes R. Baer e M. Rosenlicht juntos como homenagem ao trabalho de ambos neste contexto. Na próxima seção ficará claro a inclusão de ambos os nomes.

Lema 2.3.1. *Sejam N e H subgrupos de um grupo G, com $N \trianglelefteq G$. Suponha que o conjunto de comutadores $C = \{[n, h] \mid n \in N,\ h \in H\}$ possui m elementos. Então, o conjunto*

$$X = \{[n, h^{n_1}] \mid n, n_1 \in N, h \in H\}$$

possui, no máximo, m^2 elementos. Em particular, X gera $[H,N]$.

Demonstração. sejam $n, n_1 \in N$ e $h \in H$. Note que

$$\begin{aligned}[n,h^{n_1}] &= [n_1 n n_1^{-1}, h]^{n_1} = ([n_1 n,h]^{n_1^{-1}}[n_1^{-1},h])^{n_1} \\ &= [n_1 n,h][n_1^{-1},h]^{n_1} = [n_1 n,h]n_1^{-1}(n_1 h^{-1} n_1^{-1} h)n_1 \\ &= [n_1 n,h][h,n_1] = [n_1 n,h][n_1,h]^{-1} \in CC^{-1}.\end{aligned}$$

Como C tem m elementos, temos que C^{-1} possui m elementos. Como $n,n_1 \in N$ e $h \in H$ foram dados arbitrários, segue que X possui, no máximo, m^2 elementos. Observe que $C \subseteq X = \{[n,h^{n_1}] \mid n,n_1 \in N, h \in H\}$. Logo, X gera $[N,H]$. □

Lema 2.3.2. *Sejam H e N subgrupos de um grupo G, com $N \trianglelefteq G$. Então, o conjunto*

$$X = \{[n,h^{n_1}] \mid n,n_1 \in N, h \in H\}$$

é um conjunto normal de NH. Em particular, $[N,H] \trianglelefteq NH$.

Demonstração. Dados $n,n_1 \in N$, $h \in H$ e $ab \in NH$. Note que,

$$\begin{aligned}h^{n_1 ab} &= b^{-1}a^{-1}n_1^{-1}hn_1 ab = b^{-1}(n_1 a)^{-1}b(b^{-1}hb)b^{-1}(n_1 a)b \\ &= ((n_1 a)^b)^{-1}(b^{-1}hb)(n_1 a)^b = (b^{-1}hb)^{(n_1 a)^b}.\end{aligned}$$

Assim, $[n,h^{n_1}]^{ab} = [n^{ab}, h^{n_1 ab}] = [n^{ab}, (b^{-1}hb)^{(n_1 a)^b}] \in X$, pois $n^{ab}, (n_1 a)^b \in N$ e $b^{-1}hb \in H$. Como os elementos foram tomados arbitrariamente, segue que X é normal em NH e, portanto, $[N,H] \trianglelefteq NH$. □

Lema 2.3.3. *Sejam H e N subgrupos de um grupo G, com $N \trianglelefteq G$. Suponha que $G = NH$ e que o conjunto de comutadores $\{[n,h] \mid n \in N, h \in H\}$ seja finito, com m elementos. Então existe um subgrupo $M \trianglelefteq G$, com índice $|G:M|$ m-limitado, que centraliza $[N,H]$.*

Demonstração. Consideremos $X = \{[n,h^{n_1}] \mid n,n_1 \in N, h \in H\}$. Pelos Lemas 2.3.1 e 2.3.2, temos que X é um subconjunto normal finito em G que gera $[N,H]$. Agora defina a aplicação

$$\begin{aligned}\psi : G &\longrightarrow S_X \\ g &\longmapsto \psi_g : X \longrightarrow X \\ &\qquad\quad x \longmapsto x^{g^{-1}}\end{aligned}$$

Note que, para cada $g \in G$, temos que ψ_g é uma permutação de X. É suficiente mostrar que ψ_g é injetiva, dados $x,y \in X$ tal que $\psi_g(x) = \psi_g(y)$, temos que, $x^{g^{-1}} = y^{g^{-1}}$, e assim, $x = y$.

Além disso, ψ é uma ação de G sobre o conjunto X. De fato, ψ é um homomorfismos de grupos, veja que,

$$\psi(gh) = \psi_{gh} = \psi_g \psi_h = \psi_(g)\psi(h)$$

pois, $\psi_{gh}(x) = x^{(gh)^{-1}} = x^{h^{-1}g^{-1}} = (\psi_h(x))^{g^{-1}} = \psi_g(\psi_h(x)) = \psi_g\psi_h(x)$ para todo $g,h \in G$ e para todo $x \in X$. Note que,

$$\begin{aligned} \ker(\psi) &= \{g \in G \mid \psi_g = Id_X\} = \{g \in G | x^{g^{-1}} = x, \forall x \in X\} \\ &= \{g \in G | xg = gx, \forall x \in X\} = C_G(X). \end{aligned}$$

Assim, pelo primeiro Teorema Isomorfismo, $G/\ker(\psi) = G/C_G(X) \cong \psi(G) \leq S_X$.

Pelo Lema 2.3.1, temos que $|X| \leq m^2$. Logo, $|G : C_G(X)| \leq |S_X| = |X|! \leq (m^2)!$. Além disso, temos que X gera $[N,H]$, e assim, $C_G(X)$ centraliza $[N,H]$. Basta tomar $M = C_G(X)$ e completamos a demonstração. □

Agora estamos em condições de demonstrar o Teorema de Baer-Rosenlicht. No final da demonstração incluiremos um reticulado no qual aparecem os subgrupos "mais importantes" que surgem ao longo da demonstração do resultado.

Teorema 2.3.4. *(Baer-Rosenlicht) Sejam H e N subgrupos de um grupo G, com $N \trianglelefteq G$. Suponhamos que o conjunto de comutadores $\{[n,h] \mid n \in N, h \in H\}$ seja finito, com m elementos. Então $[N,H]$ é finito, de ordem m-limitada.*

Demonstração. Podemos supor que $G = NH$, pois analisaremos apenas alguns subgrupos de NH. Seja $X = \{[n,h^{n_1}] \mid n,n_1 \in N, h \in H\}$ e considere $E = [N,H]$. Por hipótese o conjunto de comutadores $\{[n,h] | n \in N,\ h \in H\}$ é finito. Então:

- X é um conjunto normal finito de G tal que $\langle X \rangle = E \trianglelefteq G$, pelos Lemas 2.3.1 e 2.3.2;
- Existe um subgrupo $M \trianglelefteq G$, com índice $|G : M|$ m-limitado, que centraliza E, pelo Lema 2.3.3.

Com isso $M \cap E \leq Z(E)$ e, assim, $|ME : M| \leq |G : M|$ é m-limitado. Pelo Segundo Teorema de Isomorfismo, $E/M \cap E \cong ME/M$. Daí, $|E : Z(E)| \leq |E : M \cap E| = |ME : M|$ é m-limitado. Portando, pelo Teorema de Schur temos que $C := E' = [N,H]'$ é finito, de ordem m-limitada.

Afirmamos que o subgrupo $B := [[N,H],H]$ é normal em E. Lembrando que $N \trianglelefteq G$, $[n,h] = n^{-1}n^h \in N$ para todos $n \in N$, $h \in H$; assim $B \leq E$. Veja que

$$\begin{aligned} [e,h]^{e_1} &= e_1^{-1}e^{-1}h^{-1}ehe_1 = (ee_1)^{-1}h^{-1}(ee_1)h(h^{-1}e_1^{-1}he_1) \\ &= [ee_1,h][h,e_1] = [ee_1,h][e_1,h]^{-1} \in B, \end{aligned}$$

para todos $e, e_1 \in E$ e para todo $h \in H$. Logo, B é normal em E. Além disso, $C \trianglelefteq E$, pois $E = [N,H]$ e $C = [N,H]' = E'$. Então o subgrupo $D := BC$ também é normal em E.

Agora, vamos mostrar que

$$E/D = \langle [n,h]D \mid n \in N, h \in H \rangle \text{ e } D/C = \langle [[n,h],h_1]C \mid n \in N, h, h_1 \in H \rangle$$

são finitos. De fato, E/D é abeliano, pois E/C é abeliano e $E/D \cong E/C/D/C$, pelo terceiro Teorema de Isomorfismo. Lembrando que $\{[n,h] \mid n \in N, h \in H\}$ possui m elementos, o conjunto de geradores de E/D tem m elementos. Além disso, cada gerador $[n,h]D$ tem ordem, no máximo, m. Basta verificar que $[n,h^i]D = ([n,h]D)^i = [n,h]^i D$, para todo $i \geq 1$, donde decorre que E/D é finito. Usando indução sobre i, temos que para $i = 1$ é imediato e para $i = 2$,

$$\begin{aligned}
[n,h^2]D &= [n,h][n,h]^h D = [n,h]^2[n,h]^{-1}h^{-1}[n,h]hD \\
&= [n,h]^2[[n,h],h]D = [n,h]^2 D,
\end{aligned}$$

pois $[[n,h],h] \in B \leq D$. Suponha que o resultado seja verdadeiro para algum i. Assim,

$$\begin{aligned}
[n,h^{i+1}]D &= [n,h]h^{-1}[n,h^i]hD = [n,h]^{i+1}[n,h]^{-i}h^{-1}[n,h^i]hD \\
&= [n,h]^{i+1}[n,h^i]^{-1}h^{-1}[n,h^i]hD = [n,h]^{i+1}[[n,h^i],h]D \\
&= [n,h]^{i+1}D,
\end{aligned}$$

pois $[[n,h]^i,h] \in B \leq D$. Note que cada elemento de E/D, que é abeliano, é da forma $c_1c_2...c_mD$, onde $c_j \in \{[n,h] \mid n \in N, h \in H\}$. Logo, E/D possui, no máximo, m^m elementos, pelo Princípio Fundamental de Contagem.

Do mesmo modo, $D/C \leq E/C$ é abeliano, pois E/C é abeliano. Como cada comutador de $[N,H]$ e de H é um comutador de N e de H, respectivamente, $\{[[n,h],h_1]C \mid n \in N, h, h_1 \in H\}$ tem, no máximo, m elementos. Além disso, $[[n,h]^i,h_1]C = [[n,h],h_1]^i C$ para todo $i \geq 1$. De fato, fazendo indução sobre i, temos que o caso $i = 1$ é imediato e, para $i = 2$,

$$\begin{aligned}
[[n,h]^2,h_1]C &= [[n,h],h_1]^{[n,h]}[[n,h],h_1]C \\
&= [[n,h],h_1]([[n,h],h_1]^{-1}[[n,h],h_1]^{[n,h]})[[n,h],h_1]C \\
&= [[n,h],h_1][[n,h],h_1],[n,h]][[n,h],h_1]C = [[n,h],h_1]^2 C,
\end{aligned}$$

pois $[[n,h],h_1],[n,h]] \in C$. Suponha que o resultado seja válido para algum i. Logo,

$$\begin{aligned}
[[n,h]^{i+1},h_1]C &= [[n,h]^i,h_1]^{[n,h]}[[n,h],h_1]C \\
&= [n,h]^{-1}[[n,h],h_1]^i[n,h][[n,h],h_1]C \\
&= [[n,h],h_1]^i[[n,h],h_1]^{-i}[n,h]^{-1}[[n,h],h_1]^i[n,h][[n,h],h_1]C \\
&= [[n,h],h_1]^i[[n,h],h_1]^i,[n,h]][[n,h],h_1]C = [[n,h],h_1]^{i+1}C,
\end{aligned}$$

pois $[[n,h],h_1]^i,[n,h]] \in C$. Logo, D/C tem, no máximo, m^m elementos.

Dessa forma, sendo

$$C = [N,H]',\ E/D = [N,H]/[[N,H],H][N,H]' \text{ e } D/C = [[N,H],H][N,H]'/[N,H]'$$

finitos de ordens m-limitadas, segue do Teorema de Lagrange que $[N,H]$ é finito, de ordem m-limitada. □

Reticulado da demonstração anterior:

$$\begin{tikzcd}
 & E = [N,H] \arrow[d, dash] & \\
 & D \arrow[dl, dash] \arrow[dr, dash] & \\
B = [[N,H],H] \arrow[dr, dash] & & C = [N,H]' \arrow[dl, dash] \\
 & A \arrow[d, dash] & \\
 & 1 &
\end{tikzcd}$$

2.4 Teorema de Baer

O objetivo desta seção é mostrar um resultado de R. Baer que generaliza o Teorema de Schur para os termos das séries centrais superior e inferior, mostrando que se $G/Z_i(G)$ é finito para algum $i \geq 0$, então $\gamma_{i+1}(G)$ é finito.

Inicialmente, a partir do Teorema de Baer-Rosenlicht, vamos generalizar um resultado devido a R. Baer [10, 14.5.2]. Na referência supracitada é suposto que todos os subgrupos envolvidos são normais, e na demonstração é usado "produtos tensoriais de grupos abelianos".

Aqui, conseguimos “retirar” a normalidade de alguns dos subgrupos envolvidos e a demonstração apresentada usamos apenas ideias de comutadores e o Teorema de Baer-Rosenlicht. Mais precisamente:

Lema 2.4.1. *Sejam $M \leq H$ e $K \leq N$ subgrupos de um grupo G, com $N \trianglelefteq G$. Suponha que $|H:M| = r$, $|N:K| = s$ e que $[H,K] = 1 = [M,N]$. Então, $[N,H]$ é finito de ordem $\{r,s\}$-limitada.*

Demonstração. Por hipótese, $|H:M| = r$ e $|N:K| = s$. Sejam $\tau_1 = \{t_1,t_2,\ldots,t_r\}$ um transversal de M em H, e $\tau_2 = \{u_1,u_2,\ldots,u_s\}$ um transversal de K em N. Dados, $h \in H$ e $n \in N$, existem únicos $x \in M$, $y \in K$, $i \in \{1,2,\ldots,r\}$ e $j \in \{1,2,\ldots,s\}$, tais que $h = xt_i$ e $n = yu_j$. Da hipótese $[K,H] = 1 = [N,M]$, temos

$$\begin{aligned}[n,h] &= [n,xt_i] = [n,t_i][n,x]^{t_i} = [yu_j,t_i] \\ &= [y,t_i]^{u_j}[u_j,t_i] = [u_j,t_i] \in \{[u_j,t_i] \mid 1 \leq j \leq s,\ 1 \leq i \leq r\},\end{aligned}$$

pois, $[n,x] = 1 = [y,t_i]$. Logo, $\{[n,h] \mid n \in N, h \in H\}$ possui no máximo sr elementos. Lembrando que $N \trianglelefteq G$. Então, pelo Teorema de Baer-Rosenlicht $[N,H]$ é finito de ordem $\{r,s\}$-limitada. □

Teorema 2.4.2. *(Baer) Seja G um grupo. Se $|G:Z_i(G)| = n$, com $i \geq 1$, então o $(i+1)$-ésimo termo da série central inferior $\gamma_{i+1}(G)$ é finito, de ordem n-limitada.*

Demonstração. Temos que $|G:Z_i(G)| = n$. Demonstraremos por indução sobre i. O caso $i = 1$ é exatamente o Teorema de Schur. Argumentaremos para $i > 1$. Pela Proposição 1.2.18, temos que $Z_{i-1}(G/Z(G)) = Z_i(G)/Z(G)$. Daí,

$$|G/Z(G) : Z_{i-1}(G/Z(G))| = |G/Z(G) : Z_i(G)/Z(G)| = |G:Z_i(G)| = n.$$

Por hipótese de indução $\gamma_i(G/Z(G))$ é finito de ordem n-limitada. Pelo Lema 1.2.17 temos que, $\gamma_i(G/Z(G)) = \gamma_i(G)Z(G)/Z(G)$ e, assim, $\gamma_i(G)Z(G)/Z(G)$ é finito de ordem n-limitada.

Sejam $H = \gamma_i(G)Z(G)$, $K = Z_i(G)$, $M = Z(G)$ e $N = G$. Assim, pela observação acima $|H:M| = |\gamma_i(G)Z(G):Z(G)|$ é limitado em função de n e $|N:K| = |G:Z_i(G)| = n$, por hipótese. Além disso, $[N,M] = [G,Z(G)] = 1$ e $[H,K] = [\gamma_i(G)Z(G),Z_i(G)] = [\gamma_i(G),Z_i(G)] = 1$, pelo Lema 1.2.16. Segue do Lema 2.4.1 que

$$[N,H] = [G,\gamma_i(G)Z(G)] = [G,\gamma_i(G)][G,Z(G)] = [G,\gamma_i(G)] = \gamma_{i+1}(G)$$

é finito de ordem n-limitada. □

Capítulo 3

Comutadores e seus Produtos

É bem conhecido que o produto de dois comutadores em um grupo (arbitrário) não é, necessariamente, um comutador. O primeiro a estabelecer este fato foi W. B. Fite [3, Capítulo 3]. Desde então vários exemplos foram apresentados. Por exemplo, [1], [4], [6].

Os grupos com os quais os alunos de um primeiro curso de álgebra estão familiarizados tendem a ter ordens pequenas ou estruturas mais "simples". Aparentemente, produtos de comutadores em tais grupos tendem a ser comutadores. Assim, parece razoável supor que elementos "não comutadores" são raros. Nosso objetivo é mostrar que elementos "não comutadores" existem em uma infinidade de grupos. Mais ainda, tais grupos são p-grupos finitos de classe 2 ("grupos de matrizes"). Este capítulo é baseado no trabalho de Ian D. MacDonald [9].

3.1 Elementos não comutadores em grupos

Neste capítulo estamos interessados em descrever p-grupos G nos quais o subgrupo comutador G' é diferente do conjunto de todos os comutadores $\Gamma(G)$, isto é, $G' \setminus \Gamma(G) \neq \emptyset$. Daí, para simplificar a escrita dos nossos resultados introduziremos a definição de elementos não comutadores em um grupo.

Definição 3.1.1. *Seja G um grupo. Dizemos que um elemento $\alpha \in G'$ é um elemento não comutador (em G) se não existem elementos $x, y \in G$ tais que $\alpha = [x, y]$.*

Lema 3.1.2. *Seja G um grupo. Suponha que*

$$|G : Z(G)|^2 < |G'|,$$

então existem elementos não comutadores (em G).

Demonstração. Suponha que $|G : Z(G)| = n$. Então, o conjunto de comutadores

$$\Gamma(G) = \{[x,y] \mid x,y \in G\}$$

tem, no máximo, n^2 elementos, pelo Lema 2.1.1. Por hipótese, $|G : Z(G)|^2 < |G'|$, e assim,

$$|\Gamma(G)| \leq n^2 = |G : Z(G)|^2 < |G'|.$$

Então, existe pelo menos um elemento em G' que não é um comutador. □

Lema 3.1.3. *Seja G um grupo. Suponha que $G = \langle a_1, a_2, \ldots, a_n \rangle$. Então cada elemento $a \in G$ pode ser escrito como*

$$a = a_1^{k_1} a_2^{k_2} \ldots a_n^{k_n} \alpha,$$

sendo que $k_1, k_2, \ldots, k_n$ são números inteiros e $\alpha \in G'$.

Demonstração. De fato, como G é gerado pelos elementos $a_1, a_2, \ldots, a_n$, temos que G/G' é gerado pelos elementos $a_1G', a_2G', \ldots, a_nG'$. Dado qualquer $a \in G$ e lembrando que o grupo quociente G/G' é abeliano, existem números inteiros $k_1, k_2, \ldots, k_n$ tais que

$$aG' = a_1^{k_1} G' a_2^{k_2} G' \ldots a_n^{k_n} G' = a_1^{k_1} a_2^{k_2} \ldots a_n^{k_n} G'.$$

Daí, $(a_1^{k_1} a_2^{k_2} \ldots a_n^{k_n})^{-1} a \in G'$ e, assim, existe $\alpha \in G'$ tal que $\alpha = (a_1^{k_1} a_2^{k_2} \ldots a_n^{k_n})^{-1} a$. Portanto,

$$a = a_1^{k_1} a_2^{k_2} \ldots a_n^{k_n} \alpha.$$

□

Observação 3.1.4. *Lembrando, se um grupo G é nilpotente de classe 2, então $\gamma_3(G) = 1$. Assim, $1 = \gamma_3(G) = [\gamma_2(G), G] = [G', G]$ e $G' \leq Z(G)$.*

Lema 3.1.5. *Seja G um grupo nilpotente de classe 2. Suponha que $G = \langle a_1, a_2, \ldots, a_n \rangle$. Se $a, b \in G$, então*

$$[a,b] = \prod_{i<j} [a_i, a_j]^{k_i l_j - k_j l_i},$$

sendo que $k_1, k_2, \ldots k_n$, $l_1, l_2, \ldots l_n \in \mathbb{Z}$. Mais ainda, o subgrupo comutador G' é gerado pelos comutadores $[a_i, a_j]$, com $1 \leq i < j \leq n$.

Demonstração. Dados $a,b \in G$, temos que $a = a_1^{k_1}a_2^{k_2}\dots a_n^{k_n}\alpha$ e $b = a_1^{l_1}a_2^{l_2}\dots a_n^{l_n}\beta$, sendo que $k_1,k_2,\dots k_n$, $l_1,l_2,\dots l_n \in \mathbb{Z}$ e $\alpha,\beta \in G'$. Como G é nilpotente de classe 2, temos que $\alpha,\beta \in Z(G)$. Segue pelos itens (a), (b) e (c) do Lema 1.2.9 que

$$\begin{aligned}
[a,b] &= [a_1^{k_1}a_2^{k_2}\dots a_n^{k_n}\alpha, a_1^{l_1}a_2^{l_2}\dots a_n^{l_n}\beta] = [a_1^{k_1}a_2^{k_2}\dots a_n^{k_n}, a_1^{l_1}a_2^{l_2}\dots a_n^{l_n}]\\
&= \prod_{i=1}^{n}[a_i^{k_i}, a_1^{l_1}a_2^{l_2}\dots a_n^{l_n}] = \prod_{i=j=1}^{n}[a_i^{k_i}, a_i^{l_i}]\prod_{i<j}[a_i^{k_i}, a_j^{l_j}]\prod_{i>j}[a_i^{k_i}, a_j^{l_j}]\\
&= \prod_{i<j}[a_i^{k_i}, a_j^{l_j}]\prod_{i>j}[a_i^{k_i}, a_j^{l_j}] = \prod_{i<j}[a_i^{k_i}, a_j^{l_j}]\prod_{i>j}[a_j^{l_j}, a_i^{k_i}]^{-1}\\
&= \prod_{i<j}[a_i,a_j]^{k_il_j}\prod_{i>j}[a_j,a_i]^{-l_jk_i} = \prod_{i<j}[a_i,a_j]^{k_il_j}\prod_{i<j}[a_i,a_j]^{-k_jl_i}\\
&= \prod_{i<j}[a_i,a_j]^{k_il_j-k_jl_i},
\end{aligned}$$

pois $\prod_{i=j=1}^{n}[a_i^{k_i}, a_i^{l_i}] = 1$ e $\prod_{i>j}[a_j,a_i]^{-l_jk_i} = \prod_{i<j}[a_i,a_j]^{-k_jl_i}$, o que completa a demonstração. □

Observação 3.1.6. *A partir do lema acima, se $G = \langle a_1,a_2,\dots,a_n\rangle$ é nilpotente de classe ≤ 2, então G' é gerado por, no máximo, $\dfrac{n(n-1)}{2}$ comutadores.*

3.2 Cálculos com matrizes

Os cálculos que estamos interessados envolvem matrizes com entradas inteiras $\mathbb{Z}$ (ou, no corpo dos inteiros módulo p, $\mathbb{Z}_p$).

Definição 3.2.1. *Seja m um inteiro positivo. Definimos $E(i,j)$ para $1 \leq i < j \leq m$, como sendo a matriz com o inteiro 1 na linha i e coluna j, e 0 em todas as outras entradas. Denotaremos por I, a matriz identidade $m \times m$, isto é, $I = (a_{ij})$, onde $a_{ij} = 1$, se $i = j$ e $a_{ij} = 0$, se $i \neq j$.*

Exemplo 3.2.2. *Alguns exemplos associados a definição acima:*

(a) Se $m = 3$, então as matrizes

$$I = \begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix};\ E(1,2) = \begin{pmatrix}0&1&0\\0&0&0\\0&0&0\end{pmatrix}\ e\ E(2,3) = \begin{pmatrix}0&0&0\\0&0&1\\0&0&0\end{pmatrix}$$

(b) Se $m = 4$, então as matrizes

$$I = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}; E(1,2) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \text{ e } E(3,4) = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

(c) Se $m = 6$, então temos

$$I = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}; E(2,5) = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix};$$

$$E(3,5) = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \text{ e } E(4,6) = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

O resultado a seguir é semelhante ao resultado do trabalho de Ian D. MacDonald [9], apenas incluímos mais alguns itens e reforçamos algumas hipóteses (cf. Observação 3.2.4). Este resultado nos ajudará a simplificar algumas contas no decorrer do trabalho. Principalmente no cálculo de alguns comutadores "de matrizes".

Proposição 3.2.3. *Sejam $m \in \mathbb{N}$ e $q_1, q_2, \dots, q_r \in \mathbb{Z}$. Tomemos*

$$1 \leq i, j, k, l, i_1, i_2, \dots, i_r, j_1, j_2, \dots, j_r \leq m,$$

com índices $i_1 < j_1, \dots, i_r < j_r$, $i < j$ e $k < l$; e as matrizes $m \times m$ dadas por

$$A = I + E(i,j),\ B = I + E(k,l) \text{ e } C = I + q_1 E(i_1, j_1) + \dots + q_r E(i_r, j_r).$$

Vale que:

(a) Se $j = k$, então $E(i,j)E(k,l) = E(i,l)$ e, se $j \neq k$ então $E(i,j)E(k,l) = 0$;

(b) $AB = I + E(i,j) + E(k,l) + E(i,j)E(k,l)$;

(c) $A^{-1} = I - E(i,j)$;

(d) *Se* $\{i_1, i_2, \ldots, i_r\} \cap \{j_1, j_2, \ldots j_r\} = \emptyset$, *então* $C^{-1} = I - q_1E(i_1, j_1) - \ldots - q_rE(i_r, j_r)$;

(e) *Se* $j = k$, *então* $[A,B] = I + E(i,l)$;

(f) *Se* $i = l$, *então* $[A,B] = I - E(k, j)$;

(g) *Se* $j \neq k$ *e* $i \neq l$, *então* $AB = BA$, *isto é,* $[A,B] = I$;

(h) *Se* $\{i, i_1, i_2, \ldots, i_r\} \cap \{j, j_1, j_2, \ldots j_r\} = \emptyset$, *então* $[A,C] = I$.

Demonstração. (a) Veja que, o elemento da linha i e coluna l da matriz $E(i, j)E(k,l)$ é 1, se $j = k$, e 0 se $j \neq k$. Logo, $E(i, j)E(k,l) = E(i,l)$, se $j = k$, e $E(i, j)E(k,l) = 0$, se $j \neq k$.

(b) Segue da propriedade distributiva de matrizes que

$$AB = (I + E(i, j))(I + E(k,l)) = I + E(i, j) + E(k,l) + E(i, j)E(k,l).$$

(c) De fato,

$$\begin{aligned} A(I - E(i, j)) &= (I + E(i, j))(I - E(i, j)) \\ &= I - E(i, j) + E(i, j) - E(i, j)E(i, j) \\ &= I \end{aligned}$$

e do mesmo modo, $(I - E(i, j))A = I$, pois, $i \neq j$, e assim, $E(i, j)E(i, j) = 0$. Portanto, $A^{-1} = I - E(i, j)$.

(d) De fato,

$$\begin{aligned} C(I - \sum_{r=1}^{s}(q_rE(i_r, j_r)) &= (I + \sum_{r=1}^{s}(q_rE(i_r, j_r))(I - \sum_{r=1}^{s}(q_rE(i_r, j_r)) \\ &= I - \sum_{r=1}^{s}(q_rE(i_r, j_r) + \sum_{r=1}^{s}(q_rE(i_r, j_r) - \sum_{r=1}^{s}\sum_{t=1}^{s} q_rq_tE(i_r, j_r)E(i_t, j_t) \\ &= I \end{aligned}$$

e do mesmo modo podemos mostrar que $(I - \sum_{r=1}^{s}(q_rE(i_r, j_r))C = I$, pois por hipótese, $\{i_1, i_2, \ldots, i_r\} \cap \{j_1, j_2, \ldots j_r\} = \emptyset$ e, assim, $\sum_{r=1}^{s}\sum_{t=1}^{s} q_rq_tE(i_r, j_r)E(i_t, j_t) = 0$.

Portanto, $C^{-1} = I - \sum_{r=1}^{s}(q_rE(i_r, j_r))$.

Agora vamos demonstrar (e), (f) e (g). Temos que $A^{-1} = I - E(i,j)$ e $B^{-1} = I - E(k,l)$, pelo item (c). Note que,

$$\begin{aligned}
[A,B] &= A^{-1}B^{-1}AB = (I - E(i,j))(I - E(k,l))(I + E(i,j))(I + E(k,l)) \\
&= (I - E(i,j) - E(k,l) + E(i,j)E(k,l))(I + E(i,j) + E(k,l) + E(i,j)E(k,l)) \\
&= I + E(i,j) + E(k,l) + E(i,j)E(k,l) - E(i,j) - E(i,j)E(k,l) - E(k,l) - \\
&- E(k,l)E(i,j) - E(k,l)E(i,j)E(k,l) + E(i,j)E(k,l) + \\
&+ E(i,j)E(k,l)E(i,j) + (E(i,j)E(k,l))^2 \\
&= I - E(k,l)E(i,j) - E(k,l)E(i,j)E(k,l) + E(i,j)E(k,l) + \\
&+ E(i,j)E(k,l)E(i,j) + (E(i,j)E(k,l))^2.
\end{aligned}$$

Usando o item (a): Se $j = k$, $i < j = k < l$, e assim, $i \neq l$. Logo,

$$[A,B] = I + E(i,l).$$

Se $i = l$, $k < l = i < j$, e assim, $k \neq j$. Assim,

$$[A,B] = I - E(k,j).$$

Se $j \neq k$, $i \neq l$, temos que

$$[A,B] = I.$$

E demonstramos (e), (f) e (g).

(h) Suponha que $\{i, i_1, i_2, \ldots, i_r\} \cap \{j, j_1, j_2, \ldots j_r\} = \emptyset$. Note que:

$$\begin{aligned}
A^{-1}C^{-1} &= (I - E(i,j))(I - q_1E(i_1,j_1) - \ldots - q_rE(i_r,j_r)) \\
&= I - q_1E(i_1,j_1) - \ldots - q_rE(i_r,j_r) \\
&- E(i,j) + q_1E(i,j)E(i_1,j_1) + \ldots + q_rE(i,j)E(i_r,j_r) \\
&= I - q_1E(i_1,j_1) - \ldots - q_rE(i_r,j_r) - E(i,j),
\end{aligned}$$

e $AC = I + q_1E(i_1,j_1) + \ldots + q_rE(i_r,j_r) + E(i,j)$. Então, [A,C] = I. □

Observação 3.2.4. *No artigo de Ian D. MacDonald [9, p. 442] está mencionado que a matriz*

$$I + q_1E(i_1,j_1) + \ldots + q_rE(i_r,j_r),$$

onde $q_1, q_2, \ldots, q_r$ são números inteiros, tem inversa

$$I - q_1E(i_1, j_1) - \ldots - q_rE(i_r, j_r)$$

e também que $[A,B] = I$, se $j \neq k$, onde $A = I + E(i, j)$ e $B = I + E(k,l)$. Entretanto isso não é válido. Considere a matriz 6×6,

$$I + 2E(2,3) + 3E(3,5) + 4E(5,6).$$

Note que,

$$\begin{aligned}
&(I + 2E(2,3) + 3E(3,5) + 4E(5,6))(I - 2E(2,3) - 3E(3,5) - 4E(5,6)) = \\
&= I - 2E(2,3) - 3E(3,5) - 4E(5,6) + 2E(2,3) \\
&- 6E(2,5) + 3E(3,5) - 12E(3,6) + 4E(5,6) \\
&= I - 6E(2,5) - 12E(3,6) \neq I.
\end{aligned}$$

Agora, considere as matrizes 5×5, $A = I + E(3,5)$ e $B = I + E(2,3)$. Veja que, $5 \neq 2$, mas

$$\begin{aligned}
[A,B] &= (I - E(3,5))(I - E(2,3))(I + E(3,5))(I + E(2,3)) \\
&= (I - E(2,3) - E(3,5))((I + E(2,3) + E(3,5)) \\
&= I + E(2,3) + E(3,5) - E(2,3) - E(2,5) - E(3,5) \\
&= I - E(2,5) \neq I.
\end{aligned}$$

3.3 Exemplos de Grupos Nilpotentes de Classe 2 (Parte 1)

Nesta seção vamos construir exemplos de grupos de matrizes nilpotentes de classe 2 (com um número pequeno de geradores). O próximo resultado sobre matrizes também será útil no restante.

Lema 3.3.1. *Sejam m e n inteiros positivos. Tomemos $1 \leq i_1, \ldots, i_r, j_1, \ldots, j_r \leq m$, sendo que $\{i_1, i_2, \ldots i_r\} \cap \{j_1, j_2, \ldots, j_r\} = \emptyset$, $i_1 < j_1, \ldots, i_r < j_r$ e a matriz $m \times m$*

$$A = I + E(i_1, j_1) + \ldots + E(i_r, j_r).$$

Então,

$$A^n = I + nE(i_1, j_1) + \ldots + nE(i_r, j_r).$$

Demonstração. Demonstraremos por indução sobre n. Para $n = 1$ é imediato. Suponhamos que a identidade seja válida para algum n. Então,

$$\begin{aligned}
A^{n+1} &= A^n A = (I + nE(i_1, j_1) + \ldots + nE(i_r, j_r))(I + E(i_1, j_1) + \ldots + E(i_r, j_r)) \\
&= I + E(i_1, j_1) + \ldots + E(i_r, j_r) + nE(i_1, j_1) + nE(i_1, j_1)E(i_1, j_1) + \ldots + \\
&+ nE(i_1, j_1)E(i_r, j_r) + \ldots + nE(i_r, j_r) + nE(i_r, j_r)E(i_1, j_1) + \ldots + nE(i_r, j_r)E(i_r, j_r) \\
&= I + E(i_1, j_1) + \ldots + E(i_r, j_r) + nE(i_1, j_1) + \ldots + nE(i_r, j_r) \\
&= I + (n+1)E(i_1, j_1) + \ldots + (n+1)E(i_r, j_r),
\end{aligned}$$

já que, pela Proposição 3.2.3, o produto $nE(i_k, j_k)E(i_l, j_l) = 0$, com $1 \leq k, l \leq r$, visto que $\{i_1, i_2, \ldots i_r\} \cap \{j_1, j_2, \ldots, j_r\} = \emptyset$. O que completa a demonstração. $\square$

Observação 3.3.2. *Veja que não existe inteiro positivo n tal que $A^n = I$. Para os grupos que pretendemos construir, tomaremos uma quantidade finita de geradores da forma da matriz $m \times m$ do lema anterior, isto é, matrizes $m \times m$ da forma $A = I + E(i_1, j_1) + \ldots + E(i_r, j_r)$, com $\{i_1, i_2, \ldots i_r\} \cap \{j_1, j_2, \ldots, j_r\} = \emptyset$, sob algumas condições envolvendo os índices. Com isso, os grupos desejados são infinitos.*

Por uma questão de completude apresentaremos uma análise detalhada dos subgrupos $Z(G)$ e G' para um dado grupo de matrizes G (3-gerado):

Exemplo 3.3.3. *Construiremos um grupo G 3-gerado, nilpotente de classe 2, em que o subgrupo comutador G' é gerado por $\dfrac{3(3-1)}{2} = 3$ comutadores.*

Demonstração. Primeiro considere as matrizes 9×9:

$$\begin{aligned}
A_1 &= I + E(1,2); \\
A_2 &= I + E(3,4) + E(2,7); \\
A_3 &= I + E(5,6) + E(2,8) + E(4,9).
\end{aligned}$$

Aplicando a Proposição 3.2.3:

$$\begin{aligned}
A_1^{-1}A_2^{-1} &= (I - E(1,2))(I - E(3,4) - E(2,7)) \\
&= I - E(3,4) - E(2,7) - E(1,2) + E(1,2)E(2,7) \\
&= I - E(3,4) - E(2,7) - E(1,2) + E(1,7),
\end{aligned}$$

$$eA_1A_2 = I + E(3,4) + E(2,7) + E(1,2) + E(1,7).$$

Logo,

$$\begin{aligned}
A_1^{-1}A_2^{-1}A_1A_2 &= I+E(3,4)+E(2,7)+E(1,2)+E(1,7)-E(3,4)-E(2,7)-E(1,2)-\\
&-E(1,2)E(2,7)+E(1,7)\\
&= I+E(1,7).
\end{aligned}$$

Do mesmo modo,

$$\begin{aligned}
A_1^{-1}A_3^{-1} &= (I-E(1,2))(I-E(5,6)-E(2,8)-E(4,9))\\
&= I-E(5,6)-E(2,8)-E(4,9)-\\
&-E(1,2)+E(1,2)E(5,6)+E(1,2)E(2,8)+E(1,2)E(4,9)\\
&= I-E(5,6)-E(2,8)-E(4,9)-E(1,2)+E(1,8);
\end{aligned}$$

$$A_1A_3 = I+E(5,6)+E(2,8)+E(4,9)+E(1,2)+E(1,8).$$

Assim,

$$\begin{aligned}
A_1^{-1}A_3^{-1}A_1A_3 &= I+E(5,6)+E(2,8)+E(4,9)+E(1,2)+E(1,8)-E(5,6)-E(2,8)-\\
&-E(4,9)-E(1,2)-E(1,2)E(2,8)+E(1,8)\\
&= I+E(1,8);
\end{aligned}$$

Também,

$$\begin{aligned}
A_2^{-1}A_3^{-1} &= (I-E(3,4)-E(2,7))(I-E(5,6)-E(2,8)-E(4,9))\\
&= I-E(5,6)-E(2,8)-E(4,9)\\
&-E(3,4)+E(3,4)E(5,6)+E(3,4)E(2,8)+E(3,4)E(4,9)\\
&-E(2,7)+E(2,7)E(5,6)+E(2,7)E(2,8)+E(2,7)E(4,9)\\
&= I-E(5,6)-E(2,8)-E(4,9)-E(3,4)+E(3,9)-E(2,7)
\end{aligned}$$

e,

$$A_2A_3 = I+E(5,6)+E(2,8)+E(4,9)+E(3,4)+E(3,9)+E(2,7).$$

Então,

$$\begin{aligned} A_2^{-1}A_3^{-1}A_2A_3 &= I+E(5,6)+E(2,8)+E(4,9)+E(3,4)+E(3,9)+E(2,7)-E(5,6)- \\ &-E(2,8)-E(4,9)-E(3,4)-E(3,4)E(4,9)+E(3,9)-E(2,7) \\ &= I+E(3,9). \end{aligned}$$

Portanto, $[A_1,A_2]=I+E(1,7)$, $[A_1,A_3]=I+E(1,8)$ e $[A_2,A_3]=I+E(3,9)$.

Agora vamos verificar que G é nilpotente de classe 2, aplicando item (h) da Proposição 3.2.3:

- De $[A_1,A_2]=I+E(1,7)$, $A_1=I+E(1,2)$ e $\{1\}\cap\{2,7\}=\emptyset$, logo
$$[[A_1,A_2],A_1]=I$$
- De $[A_1,A_2]=I+E(1,7)$, $A_2=I+E(3,4)+E(2,7)$ e $\{1,2,3\}\cap\{4,7\}=\emptyset$, temos
$$[[A_1,A_2],A_2]=I;$$
- De $[A_1,A_2]=I+E(1,7)$, $A_3=I+E(5,6)+E(2,8)+E(4,9)$ e também temos que $\{1,2,4,5\}\cap\{6,7,8,9\}=\emptyset$, logo
$$[[A_1,A_2],A_3]=I;$$
- De $[A_1,A_3]=I+E(1,8)$, $A_1=I+E(1,2)$ e $\{1\}\cap\{2,8\}=\emptyset$, temos
$$[[A_1,A_3],A_1]=I;$$
- De $[A_1,A_3]=I+E(1,8)$, $A_2=I+E(3,4)+E(2,7)$ e $\{1,2,3\}\cap\{4,7,8\}=\emptyset$. Logo,
$$[[A_1,A_3],A_2]=I;$$
- De $[A_1,A_3]=I+E(1,8)$ $A_3=I+E(5,6)+E(2,8)+E(4,9)$ e também temos que $\{1,2,4,5\}\cap\{6,8,9\}=\emptyset$, logo
$$[[A_1,A_3],A_3]=I;$$
- De $[A_2,A_3]=I+E(3,9)$, $A_1=I+E(1,2)$ e $\{1,3\}\cap\{2,9\}=\emptyset$, temos
$$[[A_2,A_3],A_1]=I;$$

- De $[A_2,A_3] = I + E(3,9)$ e $A_2 = I + E(3,4) + E(2,7)$ e $\{2,3\} \cap \{4,7,9\} = \emptyset$, temos
$$[[A_2,A_3],A_2] = I;$$
- De $[A_2,A_3] = I + E(3,9)$, $A_3 = I + E(5,6) + E(2,8) + E(4,9)$ e $\{2,3,4,5\} \cap \{6,8,9\} = \emptyset$, temos,
$$[[A_2,A_3],A_3] = I.$$

Então, $G' \leq Z(G)$, e assim, G é nilpotente de classe 2. Mais ainda, $G' = Z(G)$. De fato, se $z \in Z(G)$, então existem $l_1, l_2, l_3 \in \mathbb{Z}$ tais que
$$z = A_1^{l_1} A_2^{l_2} A_3^{l_3} \alpha,$$
sendo que $\alpha \in G' \leq Z(G)$. Pelo Lema 1.2.9
$$I = [A_1, z] = [A_1, A_1^{l_1} A_2^{l_2} A_3^{l_3} \alpha] = [A_1, A_1^{l_1} A_2^{l_2} A_3^{l_3}] = [A_1, A_2]^{l_2} [A_1, A_3]^{l_3},$$
ou seja, $(I + E(1,7))^{l_2} = [A_1,A_2]^{l_2} = [A_1,A_3]^{-l_3} = (I + E(1,8))^{-l_3}$. Pelo Lema 3.3.1 temos que, $(I + l_2 E(1,7)) = (I - l_3 E(1,8))$, e assim, $l_2 E(1,7) = -l_3 E(1,8)$. Daí, $l_2 = l_3 = 0$ e $z = A_1^{l_1} \alpha$. Do mesmo modo, $I = [A_2, z] = [A_2, A_1^{l_1} \alpha] = [A_2, A_1^{l_1}] = [A_2, A_1]^{l_1} = [A_1, A_2]^{-l_1}$. Logo, $l_1 = 0$ e $z = \alpha \in G'$. Portanto, $Z(G) \leq G'$ e concluímos a demonstração. □

Observação 3.3.4. *A escolha dos números na apresentação do grupo acima não é única! Poderíamos escolher:* $G = \langle B_1, B_2, B_3 \rangle$, *sendo que*
$$\begin{aligned} B_1 &= I + E(1,2) \\ B_2 &= I + E(3,4) + E(2,9) \\ B_3 &= I + E(5,6) + E(2,8) + E(4,7). \end{aligned}$$

A seguir incluimos exemplos de grupos m-gerados nilpotentes de classe 2 com $4 \leqslant m \leqslant 6$:

Exemplo 3.3.5. *Considere* $G = \langle A_1, A_2, A_3, A_4 \rangle$, *sendo que*
$$\begin{aligned} A_1 &= I + E(1,2) \\ A_2 &= I + E(3,4) + E(2,9) \\ A_3 &= I + E(5,6) + E(2,10) + E(4,12) \\ A_4 &= I + E(7,8) + E(2,11) + E(4,13) + E(6,14). \end{aligned}$$

são matrizes 14×14*. Os 6 elementos que geram o subgrupo comutador* G' *são:*

$$\begin{array}{lll} [A_1,A_2] = I + E(1,9) & [A_1,A_3] = I + E(1,10) & [A_1,A_4] = I + E(1,11) \\ [A_2,A_3] = I + E(3,12) & [A_2,A_4] = I + E(3,13) & [A_3,A_4] = I + E(5,14). \end{array}$$

De modo análogo, podemos verificar que $G' = Z(G)$*, isto é,* G *é nilpotente de classe* 2*.*

Exemplo 3.3.6. *Considere* $G = \langle A_1,A_2,A_3,A_4,A_5 \rangle$*, sendo que*

$$\begin{aligned} A_1 &= I + E(1,2) \\ A_2 &= I + E(3,4) + E(2,11) \\ A_3 &= I + E(5,6) + E(2,12) + E(4,15) \\ A_4 &= I + E(7,8) + E(2,13) + E(4,16) + E(6,18) \\ A_5 &= I + E(9,10) + E(2,14) + E(4,17) + E(6,19) + E(8,20). \end{aligned}$$

são matrizes 20×20*. Os 10 elementos que geram o subgrupo comutodor* G' *são:*

$$\begin{array}{lll} [A_1,A_2] = I + E(1,11) & [A_1,A_3] = I + E(1,12) & [A_1,A_4] = I + E(1,13) \\ [A_1,A_5] = I + E(1,14) & [A_2,A_3] = I + E(3,15) & [A_2,A_4] = I + E(3,16) \\ [A_2,A_5] = I + E(3,17) & [A_3,A_4] = I + E(5,18) & [A_3,A_5] = I + E(5,19) \\ [A_4,A_5] = I + E(7,20). & & \end{array}$$

Também é possível verificar que $G' = Z(G)$ *e* G *é um grupo nilpotente de classe 2.*

Exemplo 3.3.7. *Agora considere* $G = \langle A_1,A_2,A_3,A_4,A_5,A_6 \rangle$ *sendo que*

$$\begin{aligned} A_1 &= I + E(1,2) \\ A_2 &= I + E(3,4) + E(2,13) \\ A_3 &= I + E(5,6) + E(2,14) + E(4,18) \\ A_4 &= I + E(7,8) + E(2,15) + E(4,19) + E(6,22) \\ A_5 &= I + E(9,10) + E(2,16) + E(4,20) + E(6,23) + E(8,25) \\ A_6 &= I + E(11,12) + E(2,17) + E(4,21) + E(6,24) + E(8,26) + E(10,27). \end{aligned}$$

matrizes 27×27. *Os 15 geradores que* G' *são:*

$$\begin{array}{lll}
[A_1,A_2] = I + E(1,13) & [A_1,A_3] = I + E(1,14) & [A_1,A_4] = I + E(1,15) \\
[A_1,A_5] = I + E(1,16) & [A_1,A_6] = I + E(1,17) & [A_2,A_3] = I + E(3,18) \\
[A_2,A_4] = I + E(3,19) & [A_2,A_5] = I + E(3,20) & [A_2,A_6] = I + E(3,21) \\
[A_3,A_4] = I + E(5,22) & [A_3,A_5] = I + E(5,23) & [A_3,A_6] = I + E(5,24) \\
[A_4,A_5] = I + E(7,25) & [A_4,A_6] = I + E(7,26) & [A_5,A_6] = I + E(9,27).
\end{array}$$

Do mesmo modo, $G' = Z(G)$ *e temos que* G *é nilpotente de classe 2.*

3.4 Exemplos de Grupos Nilpotentes de Classe 2 (Parte 2)

Seja p um número primo. A partir de agora consideraremos os grupos de matrizes G nos quais as entradas estão em $\mathbb{Z}_p$, corpo dos inteiros módulo p. Todos os argumentos e construções dadas anteriormente continuam válidos com a vantagem dos "novos" grupos serem finitos.

Ian D. MacDonald menciona em [9] que matrizes $m \times m$ da forma $I + E(i, j)$ têm ordem p. Além disso, podemos verificar que matrizes da forma $I + E(i_1, j_1) + \ldots + E(i_r, j_r)$, sobe algumas condições envolvendo os índices também têm ordem p, como veremos no lema a seguir. Na verdade o próximo resultado é equivalente ao do Lema 3.3.1, a diferença é que aqui as matrizes consideradas têm entradas em $\mathbb{Z}_p$.

Lema 3.4.1. *Sejam* m *um inteiro positivo e* p *um número primo. Tomemos*

$$1 \leq i_1, \ldots, i_r, j_1, \ldots, j_r \leq m,$$

sendo que $\{i_1, i_2, \ldots i_r\} \cap \{j_1, j_2, \ldots, j_r\} = \emptyset$, $i_1 < j_1, \ldots, i_r < j_r$ *e a matriz* $m \times m$

$$A = I + E(i_1, j_1) + \ldots + E(i_r, j_r).$$

Então, $A^p = I$.

Demonstração. Pelo Lema 3.3.1,

$$\begin{aligned}
A^p &= (I + E(i_1, j_1) + \ldots + E(i_r, j_r))^p \\
&= I + pE(i_1, j_1) + \ldots + pE(i_r, j_r) \\
&= I
\end{aligned}$$

pois $pE(i_1, j_1) = \ldots = pE(i_r, j_r)) = 0$. □

Exemplo 3.4.2. *Considere o grupo* $G = G(3, p) = \langle A_1, A_2, A_3 \rangle$*, sendo que*

$$\begin{aligned} A_1 &= I + E(1,2); \\ A_2 &= I + E(3,4) + E(2,7); \\ A_3 &= I + E(5,6) + E(2,8) + E(4,9). \end{aligned}$$

são 9×9*. Então,* G *é* p*-grupo nilpotente de classe 2, onde* $Z(G) = G'$*,* $|G/Z(G)| = p^3$*,* $|G'| = p^3$ *e* $|G| = p^6$*.*

Demonstração. De fato, pelo Exemplo 3.3.3, $G' = Z(G)$ e G é nilpotente de classe 2. Considere os subgrupos $H_1 = \langle [A_1, A_2] \rangle$, $H_2 = \langle [A_1, A_3] \rangle$ e $H_3 = \langle [A_2, A_3] \rangle$, e assim, $G' = H_1 H_2 H_3$. Observe que cada um destes subgrupo tem ordem p pois:

- $[A_1, A_2]^p = (I + E(1,7))^p = I + pE(1,7) = I$;
- $[A_1, A_3]^p = (I + E(1,8))^p = I + pE(1,8) = I$;
- $[A_2, A_3]^p = (I + E(3,9))^p = I + pE(3,9) = I$.

Além disso, $H_i \lhd G'$, $i = 1,2,3$, pois o subgrupo comutador $G' = Z(G)$ é abeliano. Dado $x \in H_1 \cap H_2 H_3$, então $x = [A_1, A_2]^{l_1} = [A_1, A_3]^{l_2} [A_2, A_3]^{l_3}$, com $l_1, l_2, l_3 \in \mathbb{Z}$. Pela Proposição 3.3.1,

$$\begin{aligned} I + l_1 E(1,7) = [A_1, A_2]^{l_1} = [A_1, A_3]^{l_2} [A_2, A_3]^{l_3} &= (I + l_2 E(1,8))(I + l_3 E(3,9)) \\ &= I + l_3 E(3,9) + l_2 E(1,8) + l_2 l_3 E(1,8) E(3,9)) = I + l_3 E(3,9) + l_2 E(1,8). \end{aligned}$$

Daí, $l_1 = l_2 = l_3 = 0$ e $x = I$. Pontanto, $H_1 \cap H_2 H_3 = I$. Do mesmo modo podemos verificar que $H_2 \cap H_1 H_3 = I$ e $H_3 \cap H_1 H_2 = I$. Então, $G' \cong H_1 \times H_2 \times H_3$ e $|G'| = p^3$.

Agora considere, $N_1 = \langle A_1 Z(G) \rangle$, $N_2 = \langle A_2 Z(G) \rangle$ e $N_3 = \langle A_3 Z(G) \rangle$. Temos que, o grupo quociente $G/Z(G) = N_1 N_2 N_3$, pois $G/Z(G)$ é abeliano e gerado por $A_1 Z(G)$, $A_2 Z(G)$ e $A_3 Z(G)$. Além disso, pela Proposição 3.4.1, A_1, A_2 e A_3 tem ordem p, e assim, cada $|N_i| = p$, $i = 1,2,3$. Dado $y \in N_1 \cap N_2 N_3$, $y = A_1^{k_1} Z(G) = A_2^{k_2} A_3^{k_3} Z(G)$, com $k_1, k_2, k_2 \in \mathbb{Z}$. Assim, $A_1^{-k_1} A_2^{k_2} A_3^{k_3} \in Z(G)$. Logo, pelo Lema 1.2.9 $I = [A_1, A_1^{-k_1} A_2^{k_2} A_3^{k_3}] = [A_1, A_2]^{k_2} [A_1, A_3]^{k_3}$ ou seja,

$$\begin{aligned} I &= (I + k_2 E(1,7))(I + k_3 E(1,8)) \\ &= I + k_3 E(1,8) + k_2 E(1,7) + k_2 k_3 E(1,7) E(1,8) \\ &= I + k_3 E(1,8) + k_2 E(1,7), \end{aligned}$$

mas isso vale se, e somente $k_2 = k_3 = 0$. Do mesmo modo, $I = [A_2, A_1^{-k_1}] = [A_1, A_2]^{k_1}$, e assim, $k_1 = 0$. Daí, $y = Z(G)$. Portanto, $N_1 \cap N_2N_3 = Z(G)$. Analogamente, podemos verificar que $N_2 \cap N_1N_3 = N_3 \cap N_1N_3 = Z(G)$. Então, $G/Z(G) \cong N_1 \times N_2 \times N_3$ e $|G/Z(G)| = p^3$. Por fim, $|G| = p^6$. $\square$

Exemplo 3.4.3. *Sejam p um primo e $G = G(4, p) = \langle A_1, A_2, A_3, A_4 \rangle$, com matrizes 14×14 dadas por*

$$\begin{aligned}
A_1 &= I + E(1,2)\\
A_2 &= I + E(3,4) + E(2,11)\\
A_3 &= I + E(5,6) + E(2,10) + E(4,13)\\
A_4 &= I + E(7,8) + E(2,9) + E(4,12) + E(6,14).
\end{aligned}$$

Como no exemplo anterior, podemos mostrar que G é p-grupo nilpotente de classe 2. Mais ainda, $|G| = p^{10}$, com $|G/Z(G)| = p^4$ e $|G'| = p^6$.

Exemplo 3.4.4. *Considere $G = G(5, p) = \langle A_1, A_2, A_3, A_4, A_5 \rangle$, sendo que*

$$\begin{aligned}
A_1 &= I + E(1,2)\\
A_2 &= I + E(3,4) + E(2,11)\\
A_3 &= I + E(5,6) + E(2,12) + E(4,15)\\
A_4 &= I + E(7,8) + E(2,13) + E(4,16) + E(6,18)\\
A_5 &= I + E(9,10) + E(2,14) + E(4,17) + E(6,19) + E(8,20).
\end{aligned}$$

são matrizes 20×20. Podemos verificar que G é p-grupo nilpotente de classe 2 com $G' = Z(G)$, $|G/Z(G)| = p^5$, $|G'| = p^{10}$ e $|G| = p^{15}$.

Exemplo 3.4.5. *Considere $G = G(6, p) = \langle A_1, A_2, \ldots, A_6 \rangle$, sendo que*

$$\begin{aligned}
A_1 &= I + E(1,2)\\
A_2 &= I + E(3,4) + E(2,13)\\
A_3 &= I + E(5,6) + E(2,14) + E(4,18)\\
A_4 &= I + E(7,8) + E(2,15) + E(4,19) + E(6,22)\\
A_5 &= I + E(9,10) + E(2,16) + E(4,20) + E(6,23) + E(8,25)\\
A_6 &= I + E(11,12) + E(2,17) + E(4,21) + E(6,24) + E(8,26) + E(10,27),
\end{aligned}$$

matrizes 27×27. Então, G é um p-grupo nilpotende de classe 2. Mais ainda, $G' = Z(G)$, $|G/Z(G)| = p^6$, $|G'| = p^{15}$ e $|G| = p^{21}$.

Demonstração. De fato, os 15 elementos que geram subgrupo comutador G' são:

$$
\begin{array}{lll}
[A_1,A_2] = I + E(1,13) & [A_1,A_3] = I + E(1,14) & [A_1,A_4] = I + E(1,15) \\
[A_1,A_5] = I + E(1,16) & [A_1,A_6] = I + E(1,17) & [A_2,A_3] = I + E(3,18) \\
[A_2,A_4] = I + E(3,19) & [A_2,A_5] = I + E(3,20) & [A_2,A_6] = I + E(3,21) \\
[A_3,A_4] = I + E(5,22) & [A_3,A_5] = I + E(5,23) & [A_3,A_6] = I + E(5,24) \\
[A_4,A_5] = I + E(7,25) & [A_4,A_6] = I + E(7,26) & [A_5,A_6] = I + E(9,27).
\end{array}
$$

Primeiro vamos mostrar que $Z(G) = G'$. Observe que $[[A_i,A_j],A_k] = I$, $1 \le i,j,k \le 6$, pelo item (h) da Proposião 3.2.3. Assim, temos que $G' \le Z(G)$. Reciprocamente, tome qualquer $z \in Z(G)$, então existem $l_1, l_2, \ldots, l_6 \in \mathbb{Z}$ e $\alpha \in G'$ tais que $z = A_1^{l_1}A_2^{l_2}A_3^{l_3}A_4^{l_4}A_5^{l_5}A_6^{l_6}\alpha$. Aplicando os Lemas 1.2.9 e 3.3.1:

$$
\begin{aligned}
I = [A_1,z] &= [A_1, A_1^{l_1}A_2^{l_2}A_3^{l_3}A_4^{l_4}A_5^{l_5}A_6^{l_6}\alpha] = [A_1, A_1^{l_1}A_2^{l_2}A_3^{l_3}A_4^{l_4}A_5^{l_5}A_6^{l_6}] \\
&= [A_1,A_2]^{l_2}[A_1,A_3]^{l_3}[A_1,A_4]^{l_4}[A_1,A_5]^{l_5}[A_1,A_6]^{l_6} \\
&= (I + l_2E(1,13))(I + l_3E(1,14))(I + l_4E(1,15))(I + l_5E(1,16))(I + l_6E(1,17)) \\
&= (I + l_3E(1,14) + l_2E(1,13))(I + l_5E(1,16) + l_4E(1,15))(I + l_6E(1,17)) \\
&= (I + l_5E(1,16) + l_4E(1,15) + l_3E(1,14) + l_2E(1,13))(I + l_6E(1,17)) \\
&= I + l_6E(1,17) + l_5E(1,16) + l_4E(1,15) + l_3E(1,14) + l_2E(1,13).
\end{aligned}
$$

Logo, $l_2 = l_3 = l_4 = l_5 = l_6 = 0$ e $z = A_1^{l_1}\alpha$. Do mesmo modo,

$$I = [A_2,z] = [A_2, A_1^{l_1}\alpha] = [A_2, A_1^{l_1}] = [A_1,A_2]^{-l_1}.$$

Logo, $l_1 = 0$ e $z = \alpha \in G'$ e $Z(G) \le G'$. Portanto, $G' = Z(G)$.

Agora vamos calcular as ordens $|Z(G)|$ e $|G/Z(G)|$. Pelo Lema 3.4.1 Temos que:

- $A_1^p = I + pE(1,2) = I$;
- $A_4^p = I + pE(7,8) + pE(2,15) + pE(4,19) + pE(6,22) = I$;
- $[A_1,A_2]^p = I + pE(1,13) = I$;
- $[A_2,A_3]^p = I + pE(3,18) = I$.

Os demais gerados de G e G' têm ordem p. Agora, considere os subgrupos:

$$\begin{array}{lll}
H_1 = \langle [A_1,A_2] \rangle; & H_2 = \langle [A_1,A_3] \rangle; & H_3 = \langle [A_1,A_4] \rangle; \\
H_4 = \langle [A_1,A_5] \rangle; & H_5 = \langle [A_1,A_6] \rangle; & H_6 = \langle [A_2,A_3] \rangle; \\
H_7 = \langle [A_2,A_4] \rangle; & H_8 = \langle [A_2,A_5] \rangle; & H_9 = \langle [A_2,A_6] \rangle; \\
H_{10} = \langle [A_3,A_4] \rangle; & H_{11} = \langle [A_3,A_5] \rangle; & H_{12} = \langle [A_3,A_6] \rangle; \\
H_{13} = \langle [A_4,A_5] \rangle; & H_{14} = \langle [A_4,A_6] \rangle; & H_{15} = \langle [A_5,A_6] \rangle.
\end{array}$$

Estes subgrupos têm ordem p e são normais em G', pois $G' = Z(G)$ é abeliano. Além disso, $G' = H_1H_2\ldots H_{15}$. Dado $x \in H_1 \cap (H_2H_3\ldots H_{15})$, existem elementos $m_1, m_2, \ldots, m_{15} \in \mathbb{Z}$ tais que

$$[A_1,A_2]^{m_1} = [A_1,A_3]^{m_2}\ldots[A_1,A_6]^{m_5}[A_2,A_3]^{m_6}\ldots[A_2,A_6]^{m_9}[A_3,A_4]^{m_{10}}\ldots[A_5,A_6]^{m_{15}}$$

Assim,

$$\begin{aligned}
I + m_1E(1,13) = I &+ m_2E(1,14) + m_3E(1,15) + m_4E(1,16) + m_5E(1,17) + m_6E(3,18) + \\
&+ m_7E(3,19) + m_8E(3,20) + +m_9E(3,21) + m_{10}E(5,22) + m_{11}E(5,23) + \\
&+ m_{12}E(5,24) + m_{13}E(7,25) + m_{14}E(7,26) + m_{15}E(9,27).
\end{aligned}$$

Logo, $m_1 = m_2 = \ldots = m_{15} = 0$ e $x = I$. Pontanto, $H_1 \cap (H_2H_3\ldots H_{15}) = I$. Do mesmo modo, podemos mostrar que $H_i \cap (H_1\ldots H_{i-1}H_{i+1}\ldots H_{15}) = I$, com $1 \leq i \leq 15$. Com isso, $G' \cong H_1 \times H_2 \times \ldots \times H_{15}$. Portanto, $|G'| = p^{15}$.

Sabemos que $G/Z(G) = \langle A_1Z(G), A_2Z(G), A_3Z(G), A_4Z(G), A_5Z(G), A_6Z(G) \rangle$. Agora, considere:

$$\begin{array}{lll}
N_1 = \langle A_1Z(G) \rangle; & N_2 = \langle A_2Z(G) \rangle; & N_3 = \langle A_3Z(G) \rangle; \\
N_4 = \langle A_4Z(G) \rangle; & N_5 = \langle A_5Z(G) \rangle; & N_6 = \langle A_6Z(G) \rangle.
\end{array}$$

Estes subgrupos têm ordem p e também são normais em $G/Z(G)$, pois $Z(G) = G'$ e G/G' é abeliano. Mais ainda, $G/Z(G) = N_1N_2\ldots N_6$. Dado $y \in N_1 \cap (N_2N_3\ldots N_6)$, existem $k_1, k_2, \ldots k_6 \in \mathbb{Z}$ tais que $A_1^{k_1}Z(G) = A_2^{k_2}A_3^{k_3}\ldots A_6^{k_6}Z(G)$. Daí, $A_1^{-k_1}A_2^{k_2}A_3^{k_3}A_4^{k_4}A_5^{k_5}A_6^{k_6} \in Z(G)$. Pelo mesmo argumento dado no início da demonstração, temos que $k_1 = k_2 = \ldots = k_6 = 0$. Logo, $y = Z(G)$ e $N_1 \cap (N_2N_3\ldots N_6) = Z(G)$. Para finalizar, podemos também verificar que cada $N_j \cap (N_1\ldots N_{j-1}N_{j+1}\ldots N_6) = Z(G)$, com $1 \leq j \leq 6$. Logo,

$$G/Z(G) \cong N_1 \times N_2 \times \ldots \times N_6.$$

Assim, $|G/Z(G)| = p^6$. Por fim, pelo Teorema de Lagrange, $|G| = p^{21}$. $\square$

Uma consequência de [9, Proposição 2] é:

Teorema 3.4.6. *(MacDonald) Seja p um número primo. O grupo $G = G(6, p)$ contém um elemento $\alpha \in G'$ tal que α não é um comutador.*

Demonstração. Pelo Exemplo 3.4.5, temos que $|G : Z(G)| = p^6$ e $|G'| = p^{15}$. Observe que,

$$|G : Z(G)|^2 = p^{12} < p^{15} = |G'|.$$

Então, pelo Lema 3.1.2, o subgrupo comutador G' contém um elemento α que não é um comutador. Mais ainda, existem, pelo menos, $p^{15} - p^{12}$ elementos não comutadores em G. $\square$

Observação 3.4.7. *Em vista do Lema 3.1.2, podemos dizer que o resultado acima não é o melhor possível. Isso está explícito no trabalho [9]. Usando o GAP, é possível mostrar que o grupo $G(2,4)$ (de ordem 2^{10}) possui elementos não comutadores.*

A grosso modo, os exemplos explicitados no Teorema 3.4.6 nos fornecem uma "máquina" capaz de gerar p-grupos com elementos não comutadores (a partir de uma determinada ordem). Mais precisamente:

Exemplo 3.4.8. *Sejam p um número primo, H um p-grupo abeliano finito e $G = G(6, p)$. Então, $K = G \times H$ possui elementos que não são comutadores.*

Demonstração. De fato, $Z(K) = Z(G) \times H$ e o subgrupo comutador $K' = G' \times 1$. Suponhamos que $|H| = p^n$, para algum inteiro positivo n. Como $|G| = p^{21}$ e $|G'| = |Z(G)| = p^{15}$, temos que, as ordens de K e de $Z(K)$ são p^{n+21} e p^{n+15}, respectivamente. Assim, o índice $|K : Z(K)| = \dfrac{p^{n+21}}{p^{n+15}} = p^6$ e $|K'| = |G'| = p^{15}$. Argumentando como no Teorema 3.4.6, temos que existem elementos não comutadores em K. $\square$

Finalmente, combinando o Teorema 3.4.6 e o Exemplo 3.4.8, podemos reescrever o teorema anterior como:

Teorema 3.4.9. *Seja p um primo. Para cada $m \geqslant 21$, existe um p-grupo de ordem p^m de classe 2 com elementos não comutadores.*

Bibliografia

[1] Cassidy, P. J. (1979). Products of commutators are not always commutators: an example. *The American Mathematical Monthly*, 86(9):772–772.

[2] Dixon, J. D. (2007). *Problems in Group Theory*. Dover.

[3] Fite, W. B. (1902). On metabelian groups. *Transactions of the American Mathematical Society*, 3(3):331–353.

[4] Gallagher, P. (1965). The generation of the lower central series. *Canadian Journal of Mathematics*, 17:405–410.

[5] Gonçalves, A. (1979). *Introdução à álgebra*. Projeto Euclides, Impa.

[6] Guralnick, R. M. (1980). Expressing group elements as commutators. *The Rocky Mountain Journal of Mathematics*, 10(3):651–654.

[7] Kerber, A. (2013). *Applied finite group actions*, volume 19. Springer Science & Business Media.

[8] Lima, E. L., Carvalho, P. C. P., Wagner, E., and Morgado, A. (2016). *A matemática do ensino médio*, volume 2. Coleção do Professor de Matemática, SBM.

[9] Macdonald, I. (1986). Commutators and their products. *The American Mathematical Monthly*, 93(6):440–444.

[10] Robinson, D. J. (2012). *A Course in the Theory of Groups*, volume 80. Springer Science & Business Media.

[11] Rosenlicht, M. (1962). On a result of Baer. *Proceedings of the American Mathematical Society*, 13(1):99–101.

[12] Wiegold, J. (1957). Groups with boundedly finite classes of conjugate elements. *Proceedings of the Royal Society. London. Series A. Mathematical, Physical and Engineering Sciences*, 238:389–401.