Universidade Federal de Minas Gerais

Instituto de Ciências Exatas - ICEx

Programa de Pós-Graduação em Matemática

Dissertação de Mestrado

Sobre p-grupos metahamiltonianos finitos

Maria Luiza Oliveira Santos

Belo Horizonte, Brasil

2017

Maria Luiza Oliveira Santos

Sobre p-grupos metahamiltonianos finitos

Dissertação submetida à banca examinadora, designada pelo Programa de Pós-Graduação em Matemática da UFMG, como requisito parcial para a obtenção do título de mestre em Matemática.

Orientadora: Ana Cristina Vieira

Belo Horizonte, Brasil
2017

Santos, Maria Luiza Oliveira.

S237s Sobre p-grupos metahamiltonianos finitos [manuscrito] / Maria Luiza Oliveira Santos. - 2017.
74 f. il.

Orientadora: Ana Cristina Vieira.
Dissertação (mestrado) - Universidade Federal de Minas Gerais, Instituto de Ciências Exatas, Departamento de Matemática.
Referências: f.73-74
.
1. Matemática – Teses. 2. Grupos metahamiltonianos – Teses. 3. Sistemas hamiltonianos – Teses. 4. Grupos dedekindianos – Teses. I. Vieira ,Ana Cristina. II. Universidade Federal de Minas Gerais; Instituto de Ciências Exatas, Departamento de Matemática. III.Título.

CDU 51(043)

Ficha catalográfica elaborada pela bibliotecária Belkiz Inez Rezende Costa
CRB 6ª Região nº 1510

Universidade Federal de Minas Gerais
Departamento de Matemática
Programa de Pós-Graduação em Matemática

FOLHA DE APROVAÇÃO

Sobre p-grupos metahamiltonianos finitos

MARIA LUIZA OLIVEIRA SANTOS

Dissertação defendida e aprovada pela banca examinadora constituída pelos Senhores:

Ana Cristina Vieira

Profa. Ana Cristina Vieira
UFMG

John MacQuarrie

Prof. John William MacQuarrie
UFMG

L Calixto

Prof. Lucas Henrique Calixto
UFMG

Belo Horizonte, 10 de março de 2017.

Av. Antônio Carlos, 6627 – Campus Pampulha - Caixa Postal: 702
CEP-31270-901 - Belo Horizonte – Minas Gerais - Fone (31) 3409-5963
e-mail: pgmat@mat.ufmg.br - home page: http://www.mat.ufmg.br/pgmat

Agradecimentos

A Deus, meu refúgio e minha fortaleza, pelo cuidado e por sempre guiar os meus passos. Agradeço por toda proteção, bênçãos e por sempre colocar pessoas maravilhosas no meu caminho. Obrigada por mais essa conquista.

Aos meus pais, Antônio e Liliana, que são minha base e os meus maiores exemplos. Obrigada pelo amor e apoio incondicional e por sempre terem feito de tudo para me dar condições de chegar até aqui. Muito obrigada!

Ao meu namorado Weberson pelo amor, incentivo, atenção, cuidado e pelas risadas que tornaram meus dias mais leves, mesmo nos tempos mais difíceis.

Ao meu irmão Pedro, à minha cunhada Angélica e aos meus sobrinhos Ana Clara e Pedro Henrique por todos os momentos de alegria.

À minha família pela torcida e orações.

À minha orientadora Ana Cristina Vieira por todos os ensinamentos, pela paciência, atenção e confiança em mim depositada. Tenho em você uma inspiração e um exemplo de pessoa e de profissional. Obrigada por tudo.

Aos meus amigos e presentes da Matemática UFMG, Dafne, Hellen, Marcos, Ayane e Cajeh, pelo companheirismo, pelas horas de estudo e pelos momentos de descontração. Aos amigos da graduação, em especial, à Fernanda, Cadu, Jessé e Mateus.

Às minhas queridas amigas Neise, Noara, Regiane, Lilian e Érika pela amizade, pelas orações, por serem abrigo nos tempos mais difíceis e por vibrarem comigo a cada conquista.

A todos os professores e funcionários do Departamento de Matemática da UFMG por contribuírem para minha formação.

A FAPEMIG pelo apoio financeiro.

A todos que estiveram comigo durante essa jornada e que involuntariamente não foram citados, muito obrigada!

Resumo

Um grupo não abeliano é dito metahamiltoniano se todos seus subgrupos não abelianos são normais. Desde que já existem resultados sobre os grupos metahamiltonianos infinitos e metahamiltonianos não nilpotentes finitos, pretende-se obter mais informações sobre o caso nilpotente finito. Mas, para este caso, é suficiente concentrar-se na investigação dos p-grupos metahamiltonianos finitos. Portanto, nesta dissertação, desenvolveremos algumas propriedades importantes de p-grupos metahamiltonianos, provadas em [1] por L. J. An e Q. H. Zhang, a fim de propiciar o estudo da classificação destes grupos.

Palavras chaves: Grupos metahamiltonianos, p-grupos metahamiltonianos, grupos hamiltonianos, grupos dedekindianos.

Abstract

A non-abelian group is called metahamiltonian if all its non-abelian subgroups are normal. Since there are results on infinite metahamiltonian groups and finite non-nilpotent metahamiltonian groups, we intend to obtain information on the finite nilpotent case. In this case, it is enough to focus on the study of finite metahamiltonian p-groups. In this dissertation, we will develop important properties of the metahamiltonian p-groups proved by L. J. An e Q. H. Zhang in [1].

Keywords: Metahamiltonian groups, metahamiltonian p-groups, hamiltonian groups, dedekindian groups.

Lista de Símbolos

- $H \trianglelefteq G$: H é subgrupo normal de G.
- $H \leq G$: H é subgrupo de G.
- $H < G$: H é subgrupo próprio de G.
- $ker\varphi$: Núcleo de um homomorfismo φ.
- $Im\varphi$: Imagem de um homomorfismo φ.
- $Z(G)$: Centro do grupo G.
- $[G : H]$: Índice de H em G.
- $G \cong H$: G e H são isomorfos.
- $G \times H$: O produto direto de G e H.
- $G \rtimes H$: O produto semidireto de G por H.
- $exp(G)$: Expoente do grupo G.
- $H\ char\ G$: H é subgrupo característico em G.
- C_n: Grupo cíclico de ordem n.
- C_n^m: Produto direto de m grupos cíclios de ordem n.
- Q_8: Grupo dos quatérnios de ordem 8.
- D_4: Grupo diedral de ordem 8.
- $C(x)$: Classe de conjugação do elemento x de um grupo.
- $C_G(x)$: Centralizador do elemento no grupo.

- $C_G(H)$: Centralizador de H em G.
- $N_G(H)$: Normalizador de H em G.
- $|G|$: Ordem do grupo G.
- $o(x)$: Ordem do elemento x de um grupo.
- $cl(G)$: Classe de nilpotência do grupo G.
- $p \mid q$: p divide q.
- $p \nmid q$: p não divide q.
- $d(G)$: número minimal de geradores do grupo.

Índice

Introdução

A teoria de grupos é um dos ramos mais antigos da álgebra moderna. Suas origens podem ser encontradas, por exemplo, nos trabalhos de J. Lagrange (1736-1813), P. Ruffini (1765-1822) e E. Galois (1811-1832) sobre teoria de equações algébricas. Ao passar dos anos, com o término da classificação dos grupos simples finitos, resultado esse, que mobilizou empenho e esforço de diversas gerações de matemáticos, a teoria de grupos foi dividida em várias áreas de interesse.

Conhecendo as propriedades dos subgrupos de um grupo, o que podemos dizer sobre este grupo? Este é um dos temas que tem sido de interesse consistente na teoria de grupos, tanto que alguns autores se dedicaram, por exemplo, ao estudo de grupos cuja totalidade ou parte dos seus subgrupos apresentam uma mesma propriedade. Foi assim com Dedekind (1831-1916) que se concentrou no estudo de grupos cujos todos os seus subgrupos são normais, os chamados grupos de Dedekind ou grupos dedekindianos. Em 1897, Dedekind classificou os grupos dedekindianos finitos [6]. Em 1933, Baer (1902-1979) classificou os grupos dedekindianos infinitos [3].

Em particular, um grupo de Dedekind não abeliano é dito hamiltoniano. A estrutura de um dado grupo não abeliano que contém somente subgrupos normais é bem conhecida, sendo da forma $K \times A \times E$, onde K é isomorfo ao grupo dos quatérnios de ordem 8, A é um grupo abeliano com todos elementos de ordem ímpar e E é um 2-grupo abeliano elementar.

Sendo assim, chegamos nos grupos metahamiltonianos: grupos não abelianos em que todos os seus subgrupos não abelianos são normais. Tal conceito é uma generalização natural dos hamiltonianos.

A classe dos grupos metahamiltonianos foi introduzida numa série de artigos por G. M. Romalis e N.F. Sesekin, que investigaram propriedades dos metahamiltonianos infinitos ([15], [16], [17]). Já Nagrebeckii ([10], [11], [12]) se dedicou ao estudo de grupos metahamiltonianos finitos e, neste caso, uma caracterização dos metahamiltonianos não nilpotentes foi dada em ([11]):

Teorema 0.1. *Suponha que G é um grupo não nilpotente finito. Então G é metahamiltoniano se, e somente se, $G = SZ(G)$, onde S é um dos seguintes grupos:*
(i) $P \rtimes Q$, onde P é um p-grupo abeliano elementar, Q é cíclico e $mdc(p, |Q|) = 1$.
(ii) $Q_8 \rtimes Q$, onde Q é cíclico e $mdc(|Q|, 2) = 1$.
(iii) $P \rtimes Q$, onde $|P| = p^3$, $p \geq 5$, Q é cíclico e $mdc(p, |Q|) = 1$.

Para o caso dos grupos nilpotentes finitos, pouco se sabe. Mas, uma vez que um grupo nilpotente finito pode ser escrito como produto direto dos seus p-subgrupos de Sylow, o problema se reduz a investigação dos p-grupos metahamiltonianos finitos. Situação essa, um pouco mais complexa que a dos grupos não-nilpotentes.

Portanto, o objetivo desse trabalho é conhecer e explorar algumas propriedades dos p-grupos metahamiltonianos finitos, para que através destas, seja possível identificar alguns grupos que pertecem a essa classe. Além disso, entendemos que tais propriedades são essenciais para o estudo da classificação destes grupos. Como referência, nos basearemos principalmente em [1].

No Capítulo 1, abordaremos alguns conceitos da teoria de grupos e desenvolveremos alguns resultados que serão importantes ao longo da dissertação.

Já no Capítulo 2, estudaremos os grupos hamiltonianos e suas propriedades. Além disso, demonstraremos o teorema que classifica estes grupos. Observamos que este capítulo é uma motivação para o estudo do Capítulo 3, onde trataremos dos grupos que generalizam o conceito de grupos hamiltonianos.

Finalmente, no Capítulo 3, vamos apresentar os grupos metahamiltonianos. Mais especificamente, trabalharemos algumas propriedades dos p-grupos metahamiltonianos finitos e desenvolveremos um teorema que os caracteriza.

Capítulo 1

Conceitos iniciais

Neste capítulo, abordaremos alguns conceitos iniciais da Teoria de Grupos finitos que se farão necessários no decorrer desse trabalho. Mais especificamente, conceituaremos os comutadores, grupos nilpotentes, séries centrais, p-grupos, subgrupo de Frattini, bem como estudaremos suas propriedades. Também falaremos sobre grupos não abelianos minimais, grupos que satisfazem a condição de Engel, p-grupos extra-especiais, entre outros.

As principais referências utilizadas neste capítulo foram [7], [8], [14] e [18].

1.1 Resultados gerais sobre grupos

Nesta seção, introduziremos de forma breve e objetiva algumas definições e resultados relacionados a grupos finitos.

Primeiramente, recordemos que um automorfismo de um grupo G é um isomorfismo $\varphi : G \to G$. Denotaremos o conjunto dos automorfismos de G por $Aut(G)$. É fácil ver que $Aut(G)$ é um grupo com a operação de composição de funções.

Exemplo 1.1. *Seja K um grupo de Klein, isto é, um grupo de ordem 4, tal que todo elemento não trivial tem ordem 2. Vamos encontrar $Aut(K)$. Sendo assim, suponha $K = \{1, a, b, ab\}$. Desde que os automorfismos preservam a ordem dos elementos, os automorfismos de K são dados por:*

$$\begin{array}{rcl} \varphi_1 : & K_4 \longrightarrow K_4 \\ & a \longmapsto a \\ & b \longmapsto b. \end{array} \quad \begin{array}{rcl} \varphi_2 : & K_4 \longrightarrow K_4 \\ & a \longmapsto a \\ & b \longmapsto ab. \end{array} \quad \begin{array}{rcl} \varphi_3 : & K_4 \longrightarrow K_4 \\ & a \longmapsto b \\ & b \longmapsto a. \end{array}$$

$$\begin{aligned} \varphi_4 : \quad K_4 &\longrightarrow K_4 & \varphi_5 : \quad K_4 &\longrightarrow K_4 & \varphi_6 : \quad K_4 &\longrightarrow K_4 \\ a &\longmapsto b & a &\longmapsto ab & a &\longmapsto ab \\ b &\longmapsto ab. & b &\longmapsto a. & b &\longmapsto b. \end{aligned}$$

Logo, $|Aut(K)| = 6$. Além disso, $Aut(K)$ não é abeliano, pois $\varphi_2\varphi_3 = \varphi_5$ e $\varphi_3\varphi_2 = \varphi_4$. Portanto, $Aut(K) \cong S_3$.

Definição 1.1. *Sejam G um grupo e H um subgrupo de G. O subgrupo H é chamado de característico em G, sendo denotado por H char G, se $\varphi(H) = H$, para todo automorfismo φ de G.*

Uma vez que para cada $g \in G$, temos que

$$\begin{aligned} \varphi : \ G &\longrightarrow G \\ x &\longmapsto g^{-1}xg \end{aligned}$$

é um automorfismo de G, segue que todo subgrupo característico em G é normal em G.

Lema 1.1. *Sejam G grupo e H, K subgrupos de G. Então:*

(i) Se H char K e K char G, então H char G.

(ii) Se H char K e $K \trianglelefteq G$, então $H \trianglelefteq G$.

Demonstração. (i) Se $\varphi \in Aut(G)$, então $\varphi(K) = K$ e, assim, a restrição $\varphi|_K : K \longrightarrow K$ é um automorfismo de K. Desde que H *char* K, segue que $\varphi(H) = (\varphi|_K)(H) = H$, o que implica em H *char* G.

(ii) Sejam $a \in G$ e

$$\begin{aligned} \varphi : \ G &\longrightarrow G \\ x &\longmapsto a^{-1}ga \end{aligned}$$

Desde que $K \trianglelefteq G$, temos que $\varphi|_K : K \longrightarrow K$ é um automorfismo de K. E como H *char* K, $(\varphi|_K)(H) = H$. Isto quer dizer que se $h \in H$, então $a^{-1}ha = \varphi(h) \in H$ e temos $H \trianglelefteq G$. □

Definição 1.2. *Sejam G um grupo e H um subgrupo de G. Definimos o normalizador de H em G, denotado por $N_G(H)$, como:*

$$N_G(H) = \{g \in G \mid g^{-1}Hg = H\}.$$

Definição 1.3. *Sejam G um grupo e H um subgrupo de G. Definimos o centralizador de H em G, denotado por $C_G(H)$, como:*

$$C_G(H) = \{g \in G \mid gh = hg, \forall\ h \in H\}.$$

É fácil verificar que $N_G(H)$ e $C_G(H)$ são subgrupos de G e que $C_G(H)$ está contido em $N_G(H)$. Sendo assim:

Teorema 1.1. *(Teorema do Normalizador-Centralizador) Sejam G um grupo e H um subgrupo de G. Temos que:*

$$C_G(H) \trianglelefteq N_G(H) \quad e \quad \frac{N_G(H)}{C_G(H)} \text{ é isomorfo a um subgrupo de } Aut(H).$$

Demonstração. Se tomarmos $g \in N_G(H)$ e $x \in C_G(H)$, vamos ter que $g^{-1}xg \in C_G(H)$. De fato, se $h \in H$, então:

$$\begin{aligned}(g^{-1}xg)h =& g^{-1}x(gh)\\ =& g^{-1}x(h_1g), \quad \text{para algum} \quad h_1 \in H\\ =& g^{-1}h_1xg\\ =& h(g^{-1}xg).\end{aligned}$$

Portanto, $C_G(H) \trianglelefteq N_G(H)$.

Agora, uma vez que se $g \in N_G(H)$, temos $g^{-1}hg \in H$, para todo $h \in H$, considere os automorfismos:

$$\begin{aligned}\varphi_g : H &\longrightarrow H\\ h &\longmapsto g^{-1}hg.\end{aligned}$$

Seja:

$$\begin{aligned}\varphi : N_G(H) &\longrightarrow Aut(H)\\ g &\longmapsto \varphi_g.\end{aligned}$$

Para todo $h \in H$ e quaisquer $g_1, g_2 \in G$, temos:

$$\begin{aligned}\varphi_{g_1g_2}(h) =& (g_1g_2)^{-1}hg_1g_2\\ =& g_2^{-1}g_1^{-1}hg_1g_2\\ =& g_2^{-1}\varphi_{g_1}(h)g_2\\ =& \varphi_{g_2}(\varphi_{g_1}(h)).\end{aligned}$$

Logo, φ é um homomorfismo. Além disso, note que:

$$\begin{aligned}Ker\varphi =& \{g \in N_G(H) \mid \varphi_g = Id\}\\ =& \{g \in N_G(H) \mid \varphi_g(h) = h, \forall\ h \in H\}\\ =& \{g \in N_G(H) \mid hg = gh, \forall\ h \in H\}\\ =& C_G(H),\end{aligned}$$

já que $C_G(H) \leq Ker\varphi$. Mas então pelo Teorema do isomorfismo,

$$\frac{N_G(H)}{C_G(H)} \cong Im\varphi \leq Aut(H).$$

□

1.2 Cálculo de comutadores

Definição 1.4. *Sejam G um grupo e x, y elementos de G. O conjugado de x por y será dado por $x^y = y^{-1}xy$. Além disso, definimos o comutador de x e y como:*

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

Desta forma, temos que x comuta com y se, e somente se, $[x, y] = 1$. Definimos ainda, indutivamente, os comutadores de comprimento $n \geq 2$ como:

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

Definição 1.5. *O comutador de dois subgrupos H e K de um grupo G é definido como:*

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

Veremos, a seguir, algumas propriedades de comutadores.

Proposição 1.1. *Sejam x, y, z elementos de um grupo. Então:*

(i) $[x, y] = [y, x]^{-1}$.
(ii) $x^y = x[x, y]$.
(iii) $[x, y]^z = [x^z, y^z]$.
(iv) $[xy, z] = [x, z]^y[y, z]$.
(v) $[x, yz] = [x, z][x, y]^z$.
(vi) Identidade de Witt: $[x, y^{-1}, z]^y[y, z^{-1}, x]^z[z, x^{-1}, y]^x = 1$.

Demonstração. *(i)* $[y, x]^{-1} = (y^{-1}x^{-1}yx)^{-1} = x^{-1}y^{-1}xy = [x, y]$.
(ii) $x^y = xx^{-1}y^{-1}xy = x[x, y]$.
(iii) $[x, y]^z = z^{-1}x^{-1}zz^{-1}y^{-1}zz^{-1}xzz^{-1}yz = [x^z, y^z]$.
(iv) $[xy, z] = (xy)^{-1}z^{-1}(xy)z = y^{-1}x^{-1}z^{-1}xyz = [x, z]^y[y, z]$.

(v) Análogo ao item anterior.

(vi) Sejam $u = xzx^{-1}yx$, $v = yxy^{-1}zy$ e $w = zyz^{-1}xz$. Então:

$$\begin{aligned}[x, y^{-1}, z]^y = [x^{-1}yxy^{-1}, z]^y &= y^{-1}(yx^{-1}y^{-1}xz^{-1}x^{-1}yxy^{-1}z)y \\ &= (x^{-1}y^{-1}xz^{-1}x^{-1})(yxy^{-1}zy) \\ &= u^{-1}v,\end{aligned}$$

e, similarmente, obtemos $[y, z^{-1}, x]^z = v^{-1}w$ e $[z, x^{-1}, y]^x = w^{-1}u$, donde segue que:

$$[x, y^{-1}, z]^y[y, z^{-1}, x]^z[z, x^{-1}, y]^x = u^{-1}vv^{-1}ww^{-1}u = 1,$$

como queríamos. □

Definição 1.6. *Seja G um grupo e $X \subseteq G$. Definimos o fecho normal de X em G, denotado por X^G, como*

$$X^G = \langle g^{-1}xg \mid x \in X, g \in G\rangle.$$

Vale dizer que X^G é o menor subgrupo normal de G contendo X, ou seja, $X^G = \bigcap_{N \trianglelefteq G,\ X \subseteq N} N$.

Proposição 1.2. *Seja X um subconjunto e K um subgrupo de um grupo G. Então $X^K = \langle X, [X, K]\rangle$.*

Demonstração. Seja $x^k \in X^K$, com $x \in K, k \in K$. Note que $x^k = x[x, k] \in \langle X, [X, K]\rangle$. Por outro lado, uma vez que $X \leq X^K$ e $[X, K] \leq X^K$, temos $\langle X, [X, K]\rangle \leq X^K$. □

Proposição 1.3. *$[H, K] \leq H$ se, e somente se, $K \leq N_G(H)$.*

Demonstração. Note que $[h, k] = h^{-1}k^{-1}hk \in H$ se, e somente se, temos $k^{-1}hk \in H$, para todo $k \in K$, ou seja, se, e somente se, $K \leq N_G(H)$. □

Lema 1.2. *(Lema dos Três Subgrupos) Sejam X, Y e Z subgrupos de um grupo G e N um subgrupo normal em G. Se $[X, Y, Z]$, $[Y, Z, X] \leq N$, então $[Z, X, Y] \leq N$.*

Demonstração. Sejam $x \in X$, $y \in Y$ e $z \in Z$. Desde que N é normal em G e $[X, Y, Z]$, $[Y, Z, X] \leq N$, temos que $[x, y^{-1}, z]^y$ e $[y, z^{-1}, x]^z$ são elementos de N. Assim, pela identidade de Witt:

$$\left([x, y^{-1}, z]^y[y, z^{-1}, x]^z\right)^{-1} = [z, x^{-1}, y]^x \in N.$$

Ao conjugarmos $[z, x^{-1}, y]^x$ por x^{-1}, obtemos que $[z, x^{-1}, y] \in N$. Fazendo $x' = x^{-1}$, temos que $[z, x', y] \in N$, para todo $z \in Z$, $x' \in X$ e $y \in Y$. Desde que $[Z, X, Y]$ é gerado por elementos dessa forma, obtemos que $[Z, X, Y] \leq N$, como afirmado. □

Proposição 1.4. *Sejam H, K e L subgrupos normais em G. Então:*

$$[HK, L] = [H, L][K, L] \quad e \quad [L, HK] = [L, H][L, K].$$

Demonstração. Claramente temos que $[H, L][K, L] \leq [HK, L]$. Por outro lado, se $x \in [HK, L]$, então $x = [hk, l]$, onde $h \in H,\ k \in K,\ l \in L$. Mas observe que pela Proposição 1.1:

$$x = [hk, l] = [h, l]^k [k, l] = [h^k, l^k][k, l] \in [H, L][K, L].$$

A segunda igualdade segue analogamente. □

Definição 1.7. *Seja G um grupo. Definimos o subgrupo derivado ou subgrupo comutador de G, denotado por G', como:*

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

Ou seja, G' é gerado pelos comutadores dos elementos de G.

Não é difícil verificar que G' é um subgrupo normal em G.

Proposição 1.5. *Sejam G um grupo e x, y elementos de G. Considere ainda, H, K e L subgrupos de G e $\varphi : G \to H$ um homomorfismo de grupos. Então:*

(i) $\varphi([x, y]) = [\varphi(x), \varphi(y)]$.
(ii) $\varphi([H, K]) = [\varphi(H), \varphi(K)]$. *Em particular, o subgrupo comutador de dois subgrupos característicos em G é ainda característico.*

(iii) Se $N \trianglelefteq G$, então $\left[\dfrac{HN}{N}, \dfrac{KN}{N}\right] = \dfrac{[H, K]N}{N}$.

Demonstração. Segue diretamente da definição de homomorfismo e do Teorema da Correspondência de grupos. □

Pela proposição acima, temos que G' é característico em G.

Lema 1.3. *Seja $H = \langle x, y \rangle$ um grupo tal que $[x, y] \in Z(H)$. Então, verificamos as seguintes afirmações para $r \geq 2$, $r \in \mathbb{N}$:*

(i) $[x^r, y] = [x, y]^r = [x, y^r]$.
(ii) $(xy)^r = x^r y^r [y, x]^{\binom{r}{2}}$.

Demonstração. (i) Vamos provar que $[x^r, y] = [x, y]^r$. Para isso, usaremos indução sobre $r \in \mathbb{N}$. Se $r = 1$, o resultado é imediato. Suponhamos, então, que a igualdade é válida para algum $r - 1$, com $r > 1$. Vamos verificar que vale para r. De fato, utilizando a Proposição 1.1 e o fato de que $[x, y] \in Z(H)$, obtemos:

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

A segunda igualdade segue de forma análoga.
(ii) Usaremos indução sobre $r \geq 2$, $r \in \mathbb{N}$. Para $r = 2$ temos, ao aplicar que $[x, y] \in Z(H)$, o seguinte:

$$x^2y^2[y, x]^{\binom{r}{2}} = x^2y^2[y, x] = x^2y[y, x]y = (xy)^2.$$

Agora, vamos assumir que a igualdade é válida para algum $n > 2$, isto é, que $(xy)^n = x^ny^n[y, x]^{\binom{n}{2}}$. Verificaremos que a afirmação é válida para $n + 1$. De fato, temos

$$(xy)^{n+1} = (xy)^n(xy) = x^ny^n[y, x]^{\binom{n}{2}}xy = x^ny^nxy[y, x]^{\binom{n}{2}}.$$

Como

$$y^nx = xy^ny^{-n}x^{-1}y^nx = xy^n[y^n, x] = xy^n[y, x]^n,$$

ao substituirmos na expressão anterior, temos o seguinte:

$$(xy)^{n+1} = x^nxy^n[y, x]^ny[y, x]^{\binom{n}{2}} = x^{n+1}y^{n+1}[y, x]^{\binom{n+1}{2}},$$

como esperávamos. $\square$

A seguir, destacamos algumas propriedades relacionadas ao subgrupo comutador.

Proposição 1.6. *Sejam G um grupo e H um subgrupo normal em G. Então, o grupo quociente G/H é abeliano se, e somente se, $G' \leq H$.*

Demonstração. Se G/H é abeliano, então:

$$xyH = yxH \Rightarrow x^{-1}y^{-1}xyH = H \Rightarrow [x, y] \in H, \text{ para todo } x, y \in G \Rightarrow G' \leq H.$$

Reciprocamente, se $G' \leq H$, temos o seguinte:

$$xyH = yxx^{-1}y^{-1}xyH = yx\underbrace{[x, y]}_{\in G'}H = yxH.$$

E, portanto, G/H é abeliano. $\square$

Ressaltamos que, pela proposição acima, G/G' é o maior quociente abeliano do grupo G. Ou, equivalentemente, G' é o subgrupo de menor ordem em G, tal que o quociente G/G' é abeliano.

Lema 1.4. *Seja $G = \langle X\rangle$, então $G' = \langle [x,y] | x, y \in X\rangle^G$.*

Demonstração. Vamos denotar $N = \langle [x,y] | x, y \in X\rangle^G$. Claramente, $N \leq G'$. Agora, precisamos mostrar a inclusão inversa. Para isso, vamos mostrar que o quociente G/N é abeliano.

De fato, pois se $x_i, x_j \in X$, onde $i \neq j$, então:

$$x_i x_j N = x_j x_i \underbrace{x_i^{-1} x_j^{-1} x_i x_j}_{\in N} N = x_j x_i N.$$

Isto é, os geradores comutam. Logo G/N é abeliano e pela proposição acima, $G' \leq N$. Logo, $G' = \langle [x,y] | x, y \in X\rangle^G$. $\square$

Observação 1.1. *Se $G = \langle x, y\rangle$, então pelo Lema acima, temos que $G' = \langle [x,y]\rangle^G$. Mas, note que se $G = \langle x, y\rangle$ e $[x,y] \in Z(G)$, então $G' = \langle [x,y]\rangle$.*

Exemplo 1.2. *Vamos considerar o grupo dos quatérnios de ordem 8, cuja apresentação é dada por:*

$$Q_8 = \langle a, b \mid a^4 = 1,\ a^2 = b^2,\ [a,b] = a^2\rangle.$$

O reticulado de subgrupos do Q_8 é o seguinte

$$\begin{tikzcd}
& Q_8 \arrow[dl, equal] \arrow[d, equal] \arrow[dr, equal] & \\
\langle ab\rangle \arrow[dr, dash] & \langle a\rangle \arrow[d, equal] & \langle b\rangle\ , \arrow[dl, dash] \\
& \langle a^2\rangle \arrow[d, equal] & \\
& \{1\} &
\end{tikzcd}$$

onde $\langle ab\rangle$, $\langle a\rangle$, $\langle a^2\rangle$ e $\langle b\rangle$ são subgrupos normais de Q_8, $\langle a^2\rangle$ é subgrupo de $\langle ab\rangle$ e de $\langle b\rangle$ e é um subgrupo normal de $\langle a\rangle$.

Sabemos que Q_8 é um grupo não abeliano de ordem 8 e, portanto, $|Z(Q_8)| = 2$. Desde que os subgrupos próprios de Q_8 são cíclicos e a^2 é o único elemento de ordem 2 em Q_8, temos que $Z(Q_8) = \langle a^2\rangle$. Uma vez que $[a,b] = a^2$, pela observação acima, temos que $Q_8' = \langle a^2\rangle = \langle [a,b]\rangle$.

Definição 1.8. *Um grupo G é dito metabeliano, se existe N um subgrupo abeliano e normal em G, tal que G/N é abeliano.*

Observe que a definição acima, implica que G é metabeliano se, e somente se, G' é abeliano, já que G/N é abeliano se, e somente se, $G' \leq N$.

1.3 Grupos nilpotentes

Definição 1.9. *Um grupo G é nilpotente se contém uma série de subgrupos:*

$$\{1\} = G_0 \leq G_1 \leq ... \leq G_n = G,$$

tal que cada subgrupo G_i é normal em G e $\frac{G_{i+1}}{G_i} \leq Z(\frac{G}{G_i})$. Uma série com esta propriedade é chamada uma série central de G.

Definição 1.10. *Se G é um grupo nilpotente, então a classe de nilpotência de G, denotada por $cl(G)$, é o comprimento da menor série central de G. Se $G = \{1\}$, então $cl(G) = 0$.*

Definição 1.11. *Dado um grupo G, definimos:*

$$Z_0(G) = 1, \quad Z_1(G) = Z(G) \quad e \quad \frac{Z_{i+1}(G)}{Z_i(G)} = Z\left(\frac{G}{Z_i(G)}\right), \ para\ i \geq 1,\ i \in \mathbb{Z}.$$

Como $Z_i(G) \leq Z_{i+1}(G)$, temos a seguinte série:

$$\{1\} = Z_o(G) \leq Z_1(G) = Z(G) \leq ... \leq Z_i(G) \leq ...$$

Esta série ascendente de subgrupos de G é chamada de série central superior de G.

Observação 1.2. *Ressaltamos que:*

$$\frac{Z_{i+1}(G)}{Z_i(G)} = Z\left(\frac{G}{Z_i(G)}\right) \Rightarrow \left[\frac{Z_{i+1}(G)}{Z_i(G)}, \frac{G}{Z_i(G)}\right] = \{\bar{1}\} \Rightarrow [Z_{i+1}(G), G] \leq Z_i(G).$$

Observação 1.3. *Observamos que cada termo $Z_i(G)$ é um subgrupo característico em G e, consequentemente, cada $Z_i(G)$ é normal em G, $i \geq 1$.*

De fato, vamos mostrar usando indução sobre i. Para $i = 1$, temos que $Z(G)$ char G, pois se $a \in Z(G)$ e $\varphi \in Aut(G)$, usando a Proposição 1.5:

$$[\varphi(a), G] = [\varphi(a), \varphi(G)] = \varphi([a, G]) = \varphi(1) = 1.$$

Agora, suponhamos que o resultado é válido para algum $n > 1$, isto é, $Z_n(G)$ char G. Sejam $a \in Z_{n+1}(G)$ e $\varphi \in Aut(G)$. Pela observação anterior, obtemos:

$$[\varphi(a), G] = [\varphi(a), \varphi(G)] = \varphi\left([a, G]\right) \leq \varphi(Z_n(G)) = Z_n(G).$$

Logo, $\varphi(a) \in Z_{n+1}(G)$ e, portanto, $Z_{n+1}(G)$ char G.

Exemplo 1.3. *Todo grupo abeliano G é nilpotente, pois:*

$$\{1\} = Z_0(G) < Z(G) = G.$$

Neste caso, temos que $cl(G) = 1$.

Definição 1.12. *Seja G um grupo. Definimos indutivamente:*

$$\gamma_1(G) = G$$

$$\gamma_2(G) = [\gamma_1(G), G] = [G, G] = G'$$

$$\vdots$$

$$\gamma_i(G) = [\gamma_{i-1}(G), G],\ i \geq 3.$$

Lema 1.5. *Seja G um grupo. Então $\gamma_i(G)$ é um subgrupo característico em G, para todo $i \geq 1$, $i \in \mathbb{Z}$. Desse modo, segue que a seguinte cadeia descendente de subgrupos de G:*

$$G = \gamma_1(G) \geq \gamma_2(G) \geq ... \geq \gamma_i(G) \geq ...$$

é uma série central e é chamada de série central inferior de G.

Demonstração. Vamos verificar que cada termo $\gamma_i(G)$ é um subgrupo característico em G usando indução sobre i.

Se $i = 1$, então $\gamma_1(G) = G$ e o resultado já vale. Suponhamos que o resultado é válido para algum $i > 1$, isto é, $\gamma_i(G)$ *char* G. Tome $\varphi \in Aut(G)$. Pela Proposição 1.5:

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

Assim, $\gamma_i(G)$ *char* G e, consequentemente, $\gamma_i(G) \trianglelefteq G$, para todo $i \geq 1$.

Além disso, desde que $\gamma_i(G) = [\gamma_{i-1}(G), G]$, temos:

$$1 = \left[\frac{\gamma_{i-1}(G)}{\gamma_i(G)}, \frac{G}{\gamma_i(G)}\right] \text{ implicando em } \frac{\gamma_{i-1}(G)}{\gamma_i(G)} \leq Z\left(\frac{G}{\gamma_i(G)}\right), \text{ para todo } i \geq 1.$$

Portanto, temos uma série central, como afirmado. $\square$

Destacamos que as séries centrais inferior e superior podem estabilizar a partir de um determinado termo. Mas, se para um grupo G, tem-se $\gamma_{d+1}(G) = \{1\}$ e $\gamma_d(G) \neq 1$, então G é nilpotente e segue que $cl(G) = d$. Da mesma forma, se $Z_c(G) = G$ e $Z_{c-1}(G) \neq G$, então G é nilpotente e $cl(G) = c$. Além disso, temos que se G é um grupo nilpotente, então suas séries centrais inferior e superior têm o mesmo comprimento e este número é a classe de nilpotência de G, como pode ser visto no exemplo abaixo. Tais afirmações podem ser verificadas em [14].

Exemplo 1.4. *O grupo dos quatérnios de ordem 8 é nilpotente. Observe as séries centrais de* Q_8*.*

A série central inferior de Q_8 *é dada por:*

$$Q_8 = \gamma_1(Q_8) > \gamma_2(Q_8) > \gamma_3(Q_8) = \{1\},$$

pois $Q_8' = \gamma_2(Q_8) = Z(Q_8)$ *e* $\gamma_3(Q_8) = [\gamma_2(Q_8), Q_8] = [Z(Q_8), Q_8] = \{1\}$.

Já a série central superior de Q_8 *é dada por:*

$$\{1\} = Z_o(Q_8) < Z(Q_8) < Z_2(Q_8) = Q_8,$$

pois $\dfrac{Z_2(Q_8)}{Z(Q_8)} = Z\left(\dfrac{Q_8}{Z(Q_8)}\right) = \dfrac{Q_8}{Z(Q_8)} \Rightarrow Z_2(Q_8) = Q_8.$

Note que as séries possuem o mesmo comprimento e, portanto, $cl(Q_8) = 2$.

A seguir, veremos algumas propriedades relacionadas aos termos das séries centrais de um grupo G.

Teorema 1.2. *Sejam* G *um grupo e* N *um subgrupo normal em* G*. Então:*

$$\gamma_i\left(\frac{G}{N}\right) = \frac{\gamma_i(G)N}{N}, \quad \textit{para todo} \quad i \geq 1.$$

Particularmente, se $N \leq \gamma_i(G)$*, então* $\gamma_i\left(\dfrac{G}{N}\right) = \dfrac{\gamma_i(G)}{N}$.

Demonstração. Vamos fazer indução sobre i. Se $i = 1$, temos que:

$$\gamma_1\left(\frac{G}{N}\right) = \frac{G}{N} = \frac{\gamma_1(G)N}{N},$$

e o resultado é válido.

Agora, suponhamos que o resultado seja válido para algum $i - 1 > 1$. Então, temos:

$$\gamma_{i-1}\left(\frac{G}{N}\right) = \frac{\gamma_{i-1}(G)N}{N}.$$

Desse modo, utilizando as Proposições 1.4 e 1.5, obtemos que:

$$\begin{aligned}
\gamma_i\left(\frac{G}{N}\right) &= \left[\gamma_{i-1}\left(\frac{G}{N}\right), \frac{G}{N}\right] \\
&= \left[\frac{\gamma_{i-1}(G)N}{N}, \frac{G}{N}\right] \\
&= \frac{[\gamma_{i-1}(G)N, G]N}{N} \\
&= \frac{[\gamma_{i-1}(G), G][N, G]N}{N} \\
&= \frac{\gamma_i(G)N}{N},
\end{aligned}$$

como queríamos. □

Teorema 1.3. *Para todo grupo G, temos $[\gamma_i(G), \gamma_j(G)] \leq \gamma_{i+j}(G)$, para i, j inteiros positivos.*

Demonstração. Usaremos indução sobre i. Se $i = 1$, então:

$$[\gamma_1(G), \gamma_j(G)] = [G, \gamma_j(G)] = \gamma_{1+j}(G),$$

e o resultado é válido. Suponhamos que também é válido para algum $i - 1 > 1$. Então, pela hipótese de indução:

$$[\gamma_{i-1}(G), \gamma_j(G), G] \leq [\gamma_{i+j-1}(G), G] = \gamma_{i+j}(G) \ \text{ e}$$

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

Sendo assim, pelo Lema dos Três Subgrupos, temos que:

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

Uma vez que $[G, \gamma_{i-1}(G), \gamma_j(G)] = [\gamma_i(G), \gamma_j(G)]$, obtemos o resultado. □

Proposição 1.7. *Seja G um grupo de classe de nilpotência c. Então $\gamma_{c-i+1}(G) \leq Z_i(G)$, onde $i \geq 0,\ i \in \mathbb{Z}$.*

Demonstração. Vamos mostrar por indução sobre i. Se $i = 0$, então $\gamma_{c+1}(G) = 1 = Z_0(G)$.

Suponhamos que o resultado é válido para algum $i-1>0$, ou seja, $\gamma_{c+1-(i-1)}(G) \leq Z_{i-1}(G)$. Sendo assim, pela hipótese de indução, obtemos:

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

E, pela Observação 1.2, segue que $\gamma_{c+1-i}(G) \leq Z_i(G)$. □

Agora, exploremos alguns resultados de grupos nilpotentes.

Teorema 1.4. *Seja $G \neq \{1\}$ um grupo nilpotente, então $Z(G) \neq \{1\}$.*

Demonstração. Como G é nilpotente, existe $n>0$, tal que $Z_n(G)=G$. Mas, se tivermos $Z(G)=1$, então $Z_n(G)=1$, para todo $n \geq 1$, uma contradição. Logo, se G é nilpotente, temos $Z(G) \neq \{1\}$. □

Exemplo 1.5. *Consideremos o grupo simétrico de grau n, S_n, $n \geq 3$. Afirmamos que S_n não é um grupo nilpotente. De fato, como $Z(S_n) = \{1\}$, segue pelo teorema acima que S_n não é um grupo nilpotente.*

Teorema 1.5. *Se G é nilpotente e H é um subgrupo normal não trivial de G, então $H \cap Z(G) \neq 1$.*

Demonstração. Se G é um grupo nilpotente, então $G = Z_n(G)$, para algum n. Assim, existe um menor inteiro i, tal que $H \cap Z_i(G) \neq \{1\}$, com $i \geq 1$. Como $[H, G] \leq H$, pela Observação 1.2, obtemos:

$$[H \cap Z_i(G), G] \leq H \cap Z_{i-1}(G) = \{1\}.$$

Assim, $\{1\} \neq H \cap Z_i(G) \leq Z(G)$ e, portanto, $\{1\} \neq H \cap Z_i(G) \leq H \cap Z(G)$. Desde que $H \cap Z(G) \leq H \cap Z_i(G)$, obtemos $H \cap Z(G) = H \cap Z_i(G) \neq \{1\}$, como queríamos. □

Antes de vermos uma consequência do teorema acima, recordemos que H é um subgrupo normal minimal de um grupo G, se $H \neq \{1\}$ e se para qualquer outro subgrupo normal K de G satisfazendo $\{1\} \leq K \leq H$, implicar que ou $K = \{1\}$ ou $K = H$.

Corolário 1.1. *Sejam G um grupo nilpotente e H um subgrupo normal minimal de G. Então H está contido no centro de G.*

Demonstração. Pelo teorema anterior, já temos que $H \cap Z(G) \neq 1$. Como $H \cap Z(G) \trianglelefteq G$, pela minimalidade de H, segue que $H \cap Z(G) = H$. □

Para finalizar esta seção, veremos de forma breve os grupos de Engel, que de certa forma generalizam a ideia de grupo nilpotente. Em particular, destacaremos resultados que nos fornecerão a classe de nilpotência dos grupos que satisfazem a segunda condição de Engel.

Definição 1.13. *Sejam n um inteiro positivo e G um grupo. Dizemos que $g \in G$ é n-Engel se:*

$$[x,\ _n g] = [x, \underbrace{g, \cdots, g}_{n \text{ vezes}}] = 1, \text{ para todo } x \in G.$$

Dizemos que g é Engel, se para qualquer $x \in G$, existe $n_x = n(x, g) \geq 1$, tal que:

$$[x,\ _{n_x} g] = [x, \underbrace{g, \cdots, g}_{n_x \text{ vezes}}] = 1.$$

Definição 1.14. *Sejam G um grupo e n um inteiro positivo. Dizemos que G satisfaz a n-ésima condição de Engel, ou simplesmente, que G é n-Engel, se todos os seus elementos são n-Engel. Equivalentemente, G satisfaz a identidade:*

$$[x,\ _n y] = [x, \underbrace{y, \cdots, y}_{n \text{ vezes}}] = 1, \text{ para todo } x, y \in G.$$

Note que se um grupo G é 1-Engel, então G é abeliano. Assim, dizemos que G é um grupo de Engel se G é n-Engel, para algum $n \geq 1$.

O próximo resultado, cuja demonstração pode ser encontrada em [14], nos dá uma condição suficiente para que um grupo de Engel seja nilpotente.

Teorema 1.6. *([14], Teorema 12.3.4)(Zorn) Todo grupo de Engel finito é nilpotente.*

Desde que estaremos interessados em grupos que satisfazem a segunda condição de Engel, isto é, grupos 2-Engel, o resultado abaixo nos fornece informações sobre a classe de nilpotência destes grupos.

Teorema 1.7. *Se $[x, y, y] = 1$, para todo $x, y \in G$, então G é nilpotente e $cl(G) \leq 3$. Além disso, se G não tem elemento de ordem 3, então $cl(G) \leq 2$.*

Demonstração. Ver [8] e [14]. $\square$

1.4 p-Grupos finitos

Agora, estudaremos alguns resultados sobre p-grupos finitos que serão essenciais ao longo do trabalho.

Definição 1.15. *Sejam G um grupo e p um primo. Dizemos que G é um p-grupo se todo elemento de G tem ordem potência de p. Em particular, se G é finito, então G tem ordem potência de p.*

Exemplo 1.6. *Sabemos que o conjunto das raízes n-ésimas da unidade formam um grupo multiplicativo. Sendo assim, sejam p um primo e $f_n(x) = x^{p^n} - 1$, $n \geq 1$. Considere os seguintes grupos formados pelas raízes de $f_n(x)$, $n \geq 1$, ou seja, formados pelas raízes p^n-ésimas da unidade:*

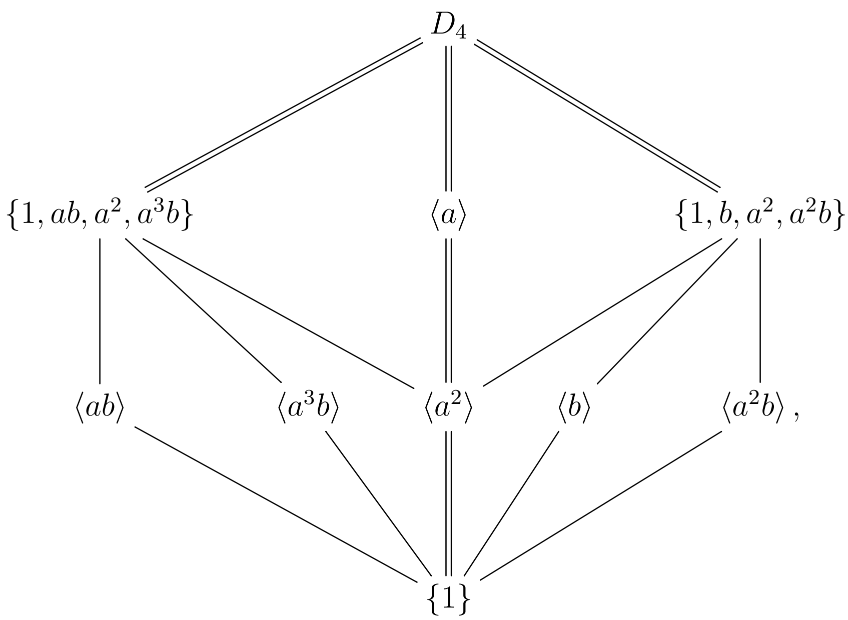
$$\begin{gathered} K_1 = \{\textit{raízes de } f_1(x) = x^p - 1\} \\ K_2 = \{\textit{raízes de } f_2(x) = x^{p^2} - 1\} \\ \vdots \\ K_i = \{\textit{raízes de } f_i(x) = x^{p^i} - 1\} \\ \vdots \end{gathered}$$

Agora, ao tomarmos o conjunto $K_\infty = \{\textit{raízes de } f_n(x) = x^{p^n} - 1,\ n \geq 1\}$, isto é, o conjunto formado pelas raízes de todos os polinômios $f_n(x) = x^{p^n} - 1$, $n \geq 1$, obtemos um p-grupo infinito. De fato, pois desde que $K_1 \subseteq K_2 \subseteq \cdots \subseteq K_i \subseteq \cdots$, temos que K_∞ é um grupo infinito. Além disso, como cada elemento em K_∞ satisfaz $x^{p^n} = 1$, segue que todo elemento em K_∞ tem ordem potência de p. Portanto, K_∞ é um p-grupo.

Exemplo 1.7. *O grupo diedral de ordem 8, cuja apresentação é dada por:*

$$D_4 = \left\langle a, b \mid a^4 = b^2 = 1;\ bab^{-1} = a^{-1} \right\rangle,$$

é um exemplo de 2-grupo finito. Observe o reticulado de subgrupos do D_4:



onde

$\langle ab\rangle, \langle a^3b\rangle, \langle b\rangle, \langle a^2b\rangle$ são subgrupos de D_4 e $\{1, ab, a^2, a^3b\}, \langle a\rangle, \langle a^2\rangle, \{1, b, a^2, a^2b\}$ são subgrupos normais de D_4;

$\langle ab\rangle, \langle a^3b\rangle, \langle a^2\rangle$ são subgrupos de $\{1, ab, a^2, a^3b\}$;

$\langle a^2\rangle, \langle b\rangle, \langle a^2b\rangle$ são subgrupos de $\{1, b, a^2, a^2b\}$;

$\langle a^2\rangle$ é subgrupo normal de $\langle a\rangle$.

Definição 1.16. *Um p-grupo G é denominado p-grupo abeliano elementar se G é abeliano e se todo elemento não trivial de G tem ordem p.*

Teorema 1.8. *Seja G um p-grupo finito, então $Z(G) \neq 1$.*

Demonstração. De fato, se $G \neq \{1\}$ é abeliano, então $Z(G) = G$ e o resultado está provado. Então, suponhamos que G é não abeliano. Logo, pela equação das classes ([14], página 38), temos que:

$$|G| = |Z(G)| + \sum_{x \notin Z(G)} |C(x)| = |Z(G)| + \sum_{x \notin Z(G)} [G : C_G(x)],$$

onde $C(x)$ é a classe de conjugação de x em G e $C_G(x) = \{x \in G \mid xg = gx\}$.

Sabemos que p divide $|G|$ e como p divide $[G : C_G(x)]$, concluímos que p divide $Z(G)$ e, portanto, $Z(G) \neq 1$. □

Proposição 1.8. *Todo p-grupo finito é nilpotente.*

Demonstração. Se $G = \{1\}$, não há o que demonstrar. Suponhamos então $G \neq \{1\}$. Se G é abeliano, então G é nilpotente. Agora, se G é não abeliano, sabemos que $Z(G) \neq G$. Além disso, pelo teorema acima, $Z(G) \neq \{1\}$. Mas então, o quociente $G/Z(G)$ é um p-grupo finito, tal que:

$$1 < \left|\frac{G}{Z(G)}\right| < |G|.$$

Por isso, $Z\left(\frac{G}{Z(G)}\right) \neq 1$. Então, pelo Teorema da Correspondência, existe $Z_2(G)$ subgrupo de G, tal que $\frac{Z_2(G)}{Z(G)} \leq Z\left(\frac{G}{Z(G)}\right)$. E, assim, temos a série $\{1\} < Z(G) < Z_2(G)$. Como cada inclusão é estrita e G é finito, segue que a série alcançará G e, portanto, G é nilpotente. □

Abaixo, veremos uma caracterização dos grupos nilpotentes finitos que será útil para o desenvolvimento de algumas propriedades importantes de p-grupos finitos.

Teorema 1.9. *(Teorema de Caracterização dos Grupos Nilpotentes Finitos) Seja G um grupo finito. Então as seguintes propriedades são equivalentes:*

(i) *G é nilpotente.*
(ii) *Se $H \leq G$, então existe uma série $K_0 = H \trianglelefteq K_1 \trianglelefteq \cdots \trianglelefteq K_c = G$.*
(iii) *Se $H < G$, então $H < N_G(H)$.*
(iv) *Se $M < G$ é maximal, então $M \trianglelefteq G$.*
(v) *G é o produto direto de seus subgrupos de Sylow.*

Demonstração. $(i) \Rightarrow (ii)$ Suponha que G é nilpotente de classe c. Então:

$$1 = Z_0(G) \leq Z_1(G) \leq \cdots \leq Z_c(G) = G.$$

Logo,

$$H = HZ_0(G) \leq HZ_1(G) \leq \cdots \leq HZ_c(G) = G.$$

Vamos verificar que $HZ_i(G) \trianglelefteq HZ_{i+1}(G)$. De fato, dado $hz \in HZ_i(G)$, para todo $h_1 \in H$, temos que $(hz)^{h_1} = h^{h_1} z^{h_1} \in HZ_i(G)$, logo $H \leq N_G(HZ_i(G))$. Por outro lado,

$$[HZ_i(G), Z_{i+1}(G)] \leq [G, Z_{i+1}(G)] \leq Z_i(G) \leq HZ_i(G).$$

Donde segue, pela Proposição 1.3, que $Z_{i+1}(G) \leq N_G(HZ_i(G))$. Logo, $HZ_{i+1}(G) \leq N_G(HZ_i(G))$ e, portanto, $HZ_i(G) \trianglelefteq HZ_{i+1}(G)$, donde segue o resultado.

$(ii) \Rightarrow (iii)$ Por hipótese, temos que $K_0 = H \trianglelefteq K_1 \trianglelefteq \cdots \trianglelefteq K_c = G$. Como $H < G$, seja i o menor inteiro positivo, tal que $H \neq K_i$. Logo, temos que $H = K_{i-1} \trianglelefteq K_i$ e, portanto, temos $H < K_i \leq N_G(H)$.

$(iii) \Rightarrow (iv)$ Seja $M < G$ maximal. Por hipótese, segue que $M < N_G(M) \leq G$. Mas, a maximalidade de M implica em $N_G(M) = G$ e, portanto, $M \trianglelefteq G$.

$(iv) \Rightarrow (v)$ Seja P um p-subgrupo de Sylow de G. Vamos mostrar que $P \trianglelefteq G$. Para tanto, mostraremos que $N_G(P) = G$. Suponhamos que não, ou seja, $N_G(P) \neq G$. Então, existe um subgrupo maximal M, tal que $N_G(P) \leq M$. Sabemos que $P \leq N_G(P) \leq M$. E, por hipótese, temos que $M \trianglelefteq G$ e, assim, $g^{-1}Pg \leq g^{-1}Mg = M$, para todo $g \in G$. Como $g^{-1}Pg$ é p-subgrupo de Sylow de M, temos que existe $m \in M$, tal que $g^{-1}Pg = m^{-1}Pm$.

Mas, então $gm^{-1} \in N_G(P) \leq M$ e, portanto, $g \in M$, para todo $g \in G$, uma contradição. Assim, $P \trianglelefteq G$.

Como G é um grupo finito, suponhamos que $|G| = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, onde p_i são primos distintos e $\alpha_i > 0$, para todo i. Além disso, sejam $P_1, \cdots, P_k$ os p_i- subgrupos (próprios e normais) de Sylow de G correspondentes. Como $|P_i| = p_i^{\alpha_i}$, temos que $P_i \cap P_j = \{1\}$, sempre que $i \neq j$. Da mesma forma, se tomarmos $P^* = P_1 \cdots P_{i-1}P_{i+1}P_k$, temos $P^* \leq G$ e que a ordem de todo elemento de P^* divide $p_1 \cdots p_{i-1}p_{i+1} \cdots p_k$. Consequentemente, $P_i \cap P^* = \{1\}$ e $P_1 \cdots P_k = P_1 \times \cdots \times P_k$. Uma vez que $|G| = p_1^{\alpha_1} \cdots p_k^{\alpha_k} = |P_1 \cdots P_k| = |P_1 \times \cdots \times P_k|$, concluímos que $G = P_1 \times \cdots \times P_k$.

$(v) \Rightarrow (i)$ Vimos que todo p-grupo finito é nilpotente. Além disso, como o produto direto de grupos nilpotentes é ainda nilpotente (ver [18]), segue o resultado. $\square$

Teorema 1.10. *Sejam G um p-grupo finito e M um subgrupo maximal de G. Então M é normal em G e $[G : M] = p$.*

Demonstração. Como G é p-grupo finito, sabemos que G é nilpotente. Então, pelo Teorema 1.9, Caracterização dos Grupos Nilpotentes Finitos, M maximal em G, implica que M é normal em G.

Além disso, afirmamos que $[G : M] = p$. Suponhamos que não, isto é, $[G : M] \neq p$. Claramente, temos que $[G : M] \neq 1$, já que caso contrário, teríamos $G = M$. Sendo assim, temos $[G : M] = p^\alpha, \alpha > 1$. Então, pelo Teorema de Sylow ([14], Teorema 1.6.16), sabemos que existe um subgrupo não trivial H/M de G/M. Mas, pelo Teorema da Correspondência, $H/M \leq G/M$ é tal que $H \leq G$ e $M \trianglelefteq H$, ou seja, $M < H \leq G$, o que contraria a maximalidade de M. Portanto, só podemos ter $[G : M] = p$. $\square$

Lema 1.6. *Se G é um p-grupo não abeliano finito que possui um subgrupo abeliano de índice p, então $|G| = p|G'||Z(G)|$.*

Demonstração. Seja A o subgrupo abeliano de G que tem índice p. Tome g em $G \backslash A$ e considere:

$$\begin{aligned} \varphi_g : A &\longrightarrow A \\ a &\longmapsto [a, g]. \end{aligned}$$

Note que como $[G : A] = p$, temos que $A \trianglelefteq G$ e, assim, $[a, g] \in A$. Além disso, φ_g é um homomorfismo de grupos, já que usando as propriedades do comutador:

$$\text{Se } \ a_1, a_2 \in A, \ \text{ então } \ \varphi_g(a_1a_2) = [a_1a_2, g] = [a_1, g]^{a_2}[a_2, g] = \varphi_g(a_1)\varphi_g(a_2).$$

Logo, pelo 1º Teorema do Isomorfismo:

$$\frac{A}{Ker\varphi_g} \cong Im\varphi_g.$$

Daí segue que $|A| = |Im\varphi_g|.|Ker\varphi_g|$.

Agora, se pudermos mostrar que $Ker\varphi_g = Z(G)$ e $Im\varphi_g = G'$, o resultado estará provado, pois teremos que $|A| = |G'|.|Z(G)|$. E como, pelo Teorema de Lagrange, $|G| = [G : A].|A|$, obteremos que $|G| = p.|G'|.|Z(G)|$, como desejado. Sendo asssim, vamos mostrar que $Ker\varphi_g = Z(G)$ e $Im\varphi_g = G'$.

Primeiramente, afirmamos que $G = \langle A, g\rangle$. Suponhamos que não, então $A < \langle A, g\rangle < G$, uma contradição, pois como $|G/A| = p$, não existe $H \leq G$ tal que $A \leq H$. Daí também concluímos que A é um subgrupo maximal de G.

$$\begin{tikzcd}
& G = \langle A, g\rangle \arrow[dl, equal, "p"'] \arrow[dr, dash] & \\
A \arrow[dr, dash] & & \langle g\rangle \arrow[dl, equal, "p"] \\
& A \cap \langle g\rangle \arrow[d, dash] & \\
& \{1\} &
\end{tikzcd}$$

Agora, note que $Ker\varphi_g = \{a \in A \mid [a, g] = 1\} = C_A(g) \leq Z(G)$. De fato, se x está em $C_A(g)$, então $x \in A$ comuta com todo elemento em A e comuta com g, logo x comuta com todo elemento em $G = \langle A, g\rangle$.

Afirmamos que $C_A(g) = Z(G)$. Suponhamos que não, então $C_A(g) < Z(G)$ e, assim, existe x em $Z(G)$ tal que x não está em $C_A(g)$. Mas então x não está em A e, então, $G = \langle A, x\rangle$, o que implica em G abeliano, uma contradição. Logo $C_A(g) = Z(G)$ e temos $Ker\varphi_g = Z(G)$.

Por outro lado, seja $K = Im\varphi_g$. Pela definição do homomorfismo φ_g, já temos $K \leq G'$. Logo, para garantirmos que $K = G'$, basta verificarmos a inclusão inversa $G' \leq K$. Para isso, provaremos que G/K é abeliano.

Começaremos mostrando que $K \trianglelefteq G$. De fato, observe que os elementos em $G = \langle A, g\rangle$ são da forma:

$$x = a_1 g^{l_1} a_2 g^{l_2} \ldots a_n g^{l_n}, l_i \in \mathbb{Z}, a_i \in A.$$

Sendo assim, para assegurarmos que K é fechado pelas conjugações por elementos de G, precisamos considerar $[a, g]$ conjugado por elementos em A e por elementos em $\langle g\rangle$.

Assim:
$$[a,g]^{a_1} = a_1^{-1}[a,g]a_1 = [a,g] \in K, \text{ pois } A \text{ é abeliano.}$$
E
$$[a,g]^{g^{l_1}} = [a^{g^{l_1}}, g] \in K, \text{ pois } a^{g^{l_1}} \in A \trianglelefteq G.$$
Diante do exposto, verificamos que $K \trianglelefteq G$.

Finalmente, para vermos que $G/K = \langle \frac{A}{K}, gK \rangle$ é abeliano, basta verificarmos que gK centraliza A/K. Logo, seja $\overline{a} \in A/K$, então:
$$gaK = agK \Leftrightarrow a^{-1}g^{-1}ag \in K, \text{ isto é, } gaK = agK \Leftrightarrow [a,g] \in K.$$
Uma vez que $[a,g]$ está em K, para todo elemento a em A, segue que G/K é abeliano, donde segue que $K = G'$. E assim, concluímos a demonstração. □

Definição 1.17. *Seja G um grupo. Se existe um inteiro positivo m, tal que $g^m = 1$, para todo $g \in G$, dizemos que G tem expoente limitado e denotamos o menor inteiro m com tal propriedade por $exp(G) = m$. Caso contrário, G tem expoente ilimitado.*

Lema 1.7. *Sejam G um p-grupo abeliano de expoente limitado e $g \in G$ um elemento de ordem maximal. Então $\langle g \rangle$ é um somando direto de G, ou seja, existe um subgrupo M de G tal que $G = M \times \langle g \rangle$.*

Demonstração. Seja:
$$S = \{N \subseteq G \mid N \text{ subgrupo de } G \text{ e } N \cap \langle g \rangle = \{1\}\}.$$
Uma vez que o conjunto S é não vazio, pelo Lema de Zorn, existe um subgrupo M de G maximal em S. Se pudermos mostrar que $G = M\langle g \rangle$, ao usarmos que $M \cap \langle g \rangle = 1$ e que os sugbrupos de G são normais, obtemos $G = M \times \langle g \rangle$, como afirmado.

Sendo assim, vamos demonstrar que $G = M\langle g \rangle$. Para tanto, suponhamos, por absurdo, que $G \neq M\langle g \rangle$. Então, tome $x \in G \backslash M\langle g \rangle$ de tal forma que x é o elemento de menor ordem com esta característica. Suponhamos $x^p = 1$. Uma vez que $x \notin M$ e $x \notin \langle g \rangle$, temos que $\langle x \rangle \nsubseteq M$ e $\langle x \rangle \nsubseteq \langle g \rangle$. Logo, pela maximalidade de M em S, segue que $\langle x \rangle \cap \langle g \rangle \neq 1$. E assim, existem inteiros n, l, satisfazendo $x^n = g^l \neq 1$. Daí segue que $p \nmid n$, e portanto, existem inteiros q, r, tais que $pq + nr = 1$. Logo, temos que $x = x^{pq}x^{nr} = x^{nr}$, o que implica que $x \in \langle g \rangle$, absurdo. Sendo assim, $x^p \neq 1$.

Desde que $x^p \neq 1$, claramente, $o(x^p) < o(x)$. E pela minimalidade da ordem de x, segue que $x^p \in M\langle g \rangle$. Logo, $x^p = yg^l$, com $y \in M$ e $g^l \in \langle g \rangle, l \in \mathbb{Z}$. Suponhamos que $o(g) = p^n$. Desde que g tem ordem máxima e que todo elemento de G tem ordem potência de p, temos $x^{p^n} = 1$. Daí e do fato de G ser abeliano:

$$1 = x^{p^n} = (x^p)^{p^{n-1}} = (yg^l)^{p^{n-1}} = y^{p^{n-1}} g^{lp^{n-1}},$$

que implica:

$$g^{lp^{n-1}} = (y^{p^{n-1}})^{-1} \in M \cap \langle g \rangle = \{1\}.$$

Como $1 = g^{lp^{n-1}}$ e $o(g) = p^n$ temos que $p^n \mid lp^{n-1}$ e assim $p \mid l$. Suponhamos $l = pl_1$. Note que:

$$(xg^{-l_1})^p = x^p g^{-l_1 p} = yg^l g^{-l_1 p} = yg^{l_1 p} g^{-l_1 p} = y \in M.$$

Mas $(xg^{-l_1}) \notin M$ e assim $\langle xg^{-l_1} \rangle \not\subseteq M$. Logo, devido a maximalidade de M em S temos $\langle xg^{-l_1} \rangle \cap \langle g \rangle \neq 1$. Por isso, existe um elemento tal que:

$$(xg^{-l_1})^m = g^k \neq 1.$$

Observe que $(xg^{-l_1})^m \in \langle xg^{-l_1} \rangle$, mas $(xg^{-l_1})^m \notin M$. E uma vez que $(xg^{-l_1})^p \in M$, temos que p não divide m, pois caso contrário $(xg^{-l_1})^m = ((xg^{-l_1})^p)^q \in M$ e teríamos uma contradição, já que $M \cap \langle g \rangle = \{1\}$. Assim:

$$p \nmid m \Longrightarrow m = pq + u, \quad com \quad q, u \in \mathbb{Z} \quad e \quad 0 < u < p.$$

Então:

$$(xg^{-l_1})^m = (xg^{-l_1})^{pq} (xg^{-l_1})^u = g^k \neq 1. \qquad (*).$$

Como $p \nmid u$, temos $mdc(p, u) = 1$. Logo, existem inteiros r, s tais que $1 = rp + su$. Portanto:

$$x = x^{rp+su} = x^{rp} x^{su}.$$

Como $o(x^{rp}) < o(x)$ e $x^p \in M\langle g \rangle$, temos que $x^{rp} \in M\langle g \rangle$. Por outro lado, de $(*)$ obtemos que $(xg^{-l_1})^u = x^u g^{-l_1 u} \in M\langle g \rangle$, implicando em $x^u \in M\langle g \rangle$ e assim $x^{su} \in M\langle g \rangle$, donde concluímos que $x \in M\langle g \rangle$, uma contradição. Portanto $G = M\langle g \rangle$ e assim $\langle g \rangle$ é um somando direto de G, como queríamos.

□

1.5 Subgrupo de Frattini

Nesta seção, conceituaremos o subgrupo de Frattini de um grupo e exploraremos suas importantes propriedades.

Definição 1.18. *Seja G um grupo. O subgrupo de Frattini de G, denotado por $\Phi(G)$, é a interseção de todos os subgrupos maximais de G. Quando um grupo G não tem subgrupos maximais definimos $\Phi(G) = G$.*

Se G é finito, então G sempre tem subgrupo maximal. Agora, se G é infinito, G pode ter ou não subgrupos maximais. Por exemplo, considere $\mathbb{Q}$, o subgrupo aditivo dos racionais. Desde que $\mathbb{Q}$ é abeliano, um subgrupo maximal H de $\mathbb{Q}$ é normal e, então, o quociente $\mathbb{Q}/H$ deve ser um grupo abeliano simples. Por isso, $\mathbb{Q}/H$ deve ser finito e de ordem prima. Mas $\mathbb{Q}$ não tem subgrupos próprios de índice finito. De fato, suponhamos, por absurdo, que existe H subgrupo próprio de $\mathbb{Q}$, tal que $[\mathbb{Q} : H] = n = |\mathbb{Q}/H|$, n inteiro positivo. Então, para todo $q \in \mathbb{Q}$, temos que

$$n(q + H) = 0 + H.$$

Ou seja, $nq \in H$, para todo $q \in \mathbb{Q}$. Daí segue que $n\mathbb{Q} \subseteq H$, mas desde que $n\mathbb{Q} = \mathbb{Q}$, obtemos $\mathbb{Q} = H$, uma contradição.

Portanto, concluímos que $\mathbb{Q}$ não possui subgrupos maximais e, assim, $\Phi(\mathbb{Q}) = \mathbb{Q}$.

Agora, por outro lado, temos que $\mathbb{Z}$ possui subgrupos maximais, que são da forma $p\mathbb{Z}$, p primo. Logo, $\Phi(\mathbb{Z}) \neq \mathbb{Z}$.

Definição 1.19. *Seja G um grupo. Dizemos que $g \in G$ é um elemento não gerador se, e somente se, $G = \langle X, g\rangle$, $X \subseteq G$, então $G = \langle X\rangle$.*

Veremos abaixo que o subgrupo de Frattini é o conjunto de elementos não geradores de G.

Proposição 1.9. *Dado um grupo G, tal que $\Phi(G) \neq G$, então temos que $\Phi(G)$ é o conjunto de todos os não geradores de G.*

Demonstração. Sejam x um elemento não gerador de G e M um subgrupo maximal de G. Então $M \leq \langle M, x\rangle$ e desde que M é maximal, segue que $\langle M, x\rangle = M$ ou $\langle M, x\rangle = G$. Se $\langle M, x\rangle = G$, então pela definição de um elemento não gerador, temos que $G = \langle M, x\rangle = M$, uma contradição. Portanto, temos $\langle M, x\rangle = M$ e, assim, $x \in M$. Como é válido para todo subgrupo maximal de G, segue que $x \in \Phi(G)$.

Reciprocamente, seja $x \in \Phi(G)$. Suponha que G é gerado por algum conjunto Y e por x, ou seja, $G = \langle Y, x\rangle$. Suponhamos, por absurdo, que $\langle Y\rangle \neq G$. Então, $\langle Y\rangle$ está contido em algum subgrupo maximal, digamos M, de G. Mas $x \in M$ e assim $\langle Y, x\rangle \leq M < G$, uma contradição. Logo, $G = \langle Y\rangle$, para todo conjunto Y, tal que $G = \langle Y, x\rangle$ e, portanto, x é um não gerador. $\square$

Proposição 1.10. *Seja G um grupo. O subgrupo de Frattini de G é um subgrupo característico em G.*

Demonstração. Se G não possui maximais, então $\Phi(G) = G$ e não há nada a fazer. Agora, se M é um subgrupo maximal de G, então $\varphi(M)$ também é um maximal em G, para qualquer automorfismo $\varphi \in Aut(G)$. Desse modo, pela definição de Frattini de G, segue o resultado. $\square$

Teorema 1.11. *Seja G um grupo e N um subgrupo normal em G. Então:*

$$\frac{\Phi(G)N}{N} \leq \Phi\left(\frac{G}{N}\right).$$

Em particular, se N é normal em $\Phi(G)$, temos:

$$\frac{\Phi(G)}{N} = \Phi\left(\frac{G}{N}\right).$$

Demonstração. Considere $\overline{G} = G/N$. Se $\overline{M}$ é um subgrupo maximal de $\overline{G}$, pelo Teorema da Correspondência, existe M maximal de G, com N normal em M, tal que $\overline{M} = M/N$. Então:

$$\frac{\Phi(G)N}{N} \leq \frac{M}{N} = \overline{M}.$$

Como vale para todo maximal $\overline{M}$ de $\overline{G}$, temos:

$$\frac{\Phi(G)N}{N} \leq \Phi\left(\frac{G}{N}\right).$$

Agora, vamos verificar que se N é normal em $\Phi(G)$, então $\Phi(G)/N = \Phi\left(\frac{G}{N}\right)$. Suponhamos que não, então pelo exposto acima, segue que $\Phi(G)/N < \Phi\left(\frac{G}{N}\right)$. Logo, existe $\overline{g} \in \Phi\left(\frac{G}{N}\right)$, tal que $\overline{g} \notin \Phi(G)/N$. Logo, $\overline{g} \in \overline{M}$, para todo $\overline{M}$ maximal em $\overline{G}$. Mas, pelo Teorema da Correspondência, sabemos que $\overline{M} = M/N$, onde M maximal em G. Mas então, $g \notin N$ e $g \in M$, para todo M maximal em G e, portanto, $g \in \Phi(G)$, que implica em $\overline{g} \in \Phi(G)/N$. $\square$

Agora, abordaremos alguns resultados sobre o subgrupo de Frattini de um p-grupo finito e veremos que este assume particularidades interessantes, que merecem ser detalhadas e que serão frequentemente utilizadas ao longo desse trabalho.

Exemplo 1.8. *Pelo reticulado de subgrupos do Q_8 que vimos no Exemplo 1.2, temos que $\langle a^2 \rangle$ é a interseção dos subgrupos maximais de Q_8, logo $\Phi(Q_8) = \langle a^2 \rangle$.*

Teorema 1.12. *Se G é um p-grupo, então $G/\Phi(G)$ é um p-grupo abeliano elementar. Além disso, $\Phi(G) = 1$ se, e somente se, G é abeliano elementar.*

Demonstração. Queremos mostrar que:

$$xy\Phi(G) = yx\Phi(G) \text{ e } (x\Phi(G))^p = \Phi(G), \text{ para todo } x, y \in G.$$

Isto é, precisamos mostrar que $x^{-1}y^{-1}xy, x^p \in M$, para todo subgrupo maximal M de G. Já vimos que todo subgrupo maximal M de G é normal e que $[G : M] = p$. Logo, G/M é abeliano e, portanto, $G' \leq G$ e $x^{-1}y^{-1}xy \in M$, para todo $x, y \in G$. Por outro lado, observamos que todo elemento não trivial em G/M tem ordem p e, assim, $x^p \in M$, para todo $x \in G$, como queríamos.

Em particular, se $\Phi(G) = 1$, temos que G é abeliano elementar. Por outro lado, se G é p-grupo abeliano elementar, então G possui uma base $x_i, 1 \leq i \leq n$, isto é, $G = \langle x_1, ..., x_n\rangle$, onde $x_i^p = 1$, para todo i. Para cada $j = 1, ..., n$, considere o subgrupo $H_j = \langle x_i \mid 1 \leq i \leq n, i \neq j\rangle$ maximal em G. Assim, $\Phi(G) \leq \bigcap_{j=1}^{n} H_j = \{1\}$ e, portanto, $\Phi(G) = 1$. □

Observação 1.4. *Note que pelo teorema anterior e pelo Teorema 1.11 temos que se G é p- grupo finito, $\Phi(G)$ é o menor subgrupo de G, tal que $G/\Phi(G)$ é abeliano elementar. De fato, pois se N é normal em G, tal que G/N é abeliano elementar, temos que:*

$$\frac{\Phi(G)N}{N} \leq \Phi\left(\frac{G}{N}\right) = \overline{1} \Rightarrow \Phi(G) \leq N.$$

Definição 1.20. *Seja G um p-grupo. Para $i \geq 0$, definimos:*

$$\Omega_i(G) = \langle x \in G \mid x^{p^i} = 1\rangle,$$

o subgrupo de G gerado por elementos com ordem $\leq p^i$. E ainda,

$$\mho_i(G) = \langle x^{p^i} \mid x \in G\rangle.$$

Ressaltamos que $\Omega_i(G)$ e $\mho_i(G)$ são subgrupos característicos em G e, portanto, são normais em G. Além disso, o subgrupo $\mho_1(G) = \langle x^p \mid x \in G\rangle$ está relacionado ao subgrupo de Frattini de um p-grupo, como veremos abaixo.

Teorema 1.13. *Seja G um p-grupo finito. Então $\Phi(G) = G'\mho_1(G)$.*

Demonstração. Vimos na demonstração do teorema anterior que $x^{-1}y^{-1}xy, x^p \in M$, para todo $x, y \in G$ e para todo M subgrupo maximal de G. Logo, já temos que $G'\mho_1(G) \leq G$. Reciprocamente, uma vez que o quociente $G/G'\mho_1(G)$ é abeliano elementar, pela observação anterior, segue que $\Phi(G) \leq G'\mho_1(G)$ e obtemos a igualdade desejada. □

Definição 1.21. *Um conjunto minimal de geradores de um grupo G é um subconjunto X de G que gera G e tal que nenhum subconjunto próprio de X gera G. Assim, o menor número de elementos em X é o número minimal de geradores de G e será denotado por $d(G)$.*

Se um grupo G é tal que $d(G) = n$, então dizemos que G é um grupo n-gerado.

Definição 1.22. *Seja G um grupo e X um conjunto minimal de geradores de G. Cada elemento $x \in X$ é chamado de gerador essencial de G.*

Note que se G é um grupo e $g \in G$ é um gerador essencial, então $g \notin \Phi(G)$.

Teorema 1.14. *(Teorema da Base de Burnside) Seja G um p-grupo finito. Então:*

(i) O conjunto $\{x_1, ..., x_n\}$ é um conjunto gerador minimal de geradores de G se, e somente se, $\{x_1\Phi(G), ..., x_n\Phi(G)\}$ é uma base de $G/\Phi(G)$ como espaço vetorial sobre $\mathbb{Z}_p$.
(ii) $[G : \Phi(G)] = p^n$.

Demonstração. (i) Seja $X = \{x_1, ..., x_n\}$ um conjunto minimal de geradores de G. Dessa forma, sendo $\overline{x_i} = x_i\Phi(G) \in G/\Phi(G)$, temos que $\overline{X} = \{\overline{x_1}, \cdots, \overline{x_n}\}$ é um conjunto gerador de $G/\Phi(G)$. Afirmamos que o conjunto $\overline{X}$ é linearmente independente. De fato, suponhamos que $\overline{X}$ seja linearmente dependente, então podemos assumir, reordenando os elementos se necessário, que $\overline{x_1} \in \langle \overline{x_2}, \cdots, \overline{x_n} \rangle$. Assim, $x_1\Phi(G) \in \langle \overline{x_2}, \cdots, \overline{x_n} \rangle \Phi(G)$ e existe $y \in \langle \overline{x_2}, \cdots, \overline{x_n} \rangle$, tal que $y^{-1}x_1 \in \Phi(G)$.

Logo, como $X = \{x_1, \cdots, x_n\}$ gera G e $y \in \langle x_2, \cdots, x_n \rangle$, segue que $\{y^{-1}x_1, \cdots, x_n\}$ gera G. Mas, como $y^{-1}x_1 \in \Phi(G)$, $y^{-1}x_1$ é um não gerador e temos que $\{x_2, \cdots, x_n\}$ gera G, uma contradição, pois X é um conjunto minimal de geradores. Logo, $\overline{X}$ é uma base de $G/\Phi(G)$ visto como espaço vetorial sobre $\mathbb{Z}_p$.

Reciprocamente, temos que se $\overline{X}$ é uma base de $G/\Phi(G)$, então $G = \langle X, \Phi(G) \rangle$, o que implica em $G = \langle X \rangle$ e, portanto, X é um conjunto minimal de geradores de G.

Portanto, concluímos que a dimensão de $G/\Phi(G)$ como espaço vetorial sobre $\mathbb{Z}_p$ coincide com $n = d(G)$, para qualquer subconjunto minimal de geradores de X.

(ii) Se $G/\Phi(G)$ tem uma base com n elementos, então $G/\Phi(G) \cong {\mathbb{Z}_p}^n$ e, portanto, $[G : \Phi(G)] = p^n$. □

Observamos que, pelo teorema acima, quando G é um p-grupo finito, podemos encontrar o número minimal de geradores de G através do subgrupo de Frattini.

1.6 p-Grupos não abelianos minimais

Definição 1.23. *Um grupo finito G é não abeliano minimal, se G é não abeliano e todo subgrupo próprio de G é abeliano.*

Exemplo 1.9. *O grupo simétrico de grau 3 é não abeliano minimal. De fato, sabemos que S_3 é um grupo não abeliano e que todo subgrupo próprio de S_3 tem ordem 2 ou 3, ou seja, todo subgrupo próprio de S_3 é abeliano.*

Claramente, temos que se G é um p-grupo não abeliano, tal que todos seus subgrupos próprios são abelianos, então G é um p-grupo não abeliano minimal.

Exemplo 1.10. *O grupo dos quatérnios de ordem 8 é um 2-grupo não abeliano minimal. De fato, pois Q_8 é não abeliano e todo subgrupo próprio de Q_8 é de ordem 2 ou 4.*

A seguir, veremos uma caracterização dos p-grupos não abelianos minimais finitos que será de grande importância, principalmente para o último capítulo deste trabalho.

Teorema 1.15. *Seja G um p-grupo finito. São equivalentes:*

(i) G é p-grupo não abeliano minimal.
(ii) $d(G) = 2$ e $\mid G' \mid = p$.
(iii) $d(G) = 2$ e $Z(G) = \Phi(G)$.

Demonstração. Vamos mostrar primeiro que $(ii) \Rightarrow (iii) \Rightarrow (i)$.
$(ii) \Rightarrow (iii)$ Supondo $d(G) = 2$ e $|G'| = p$, queremos mostrar que $Z(G) = \Phi(G)$. Claramente temos que G é não abeliano. Além do mais, como $|G'| = p$ e $G' \trianglelefteq G$, temos que G' é um subgrupo normal minimal de G e, assim, temos $Z(G) \cap G' = G'$. Daí obtemos que $G' \leq Z(G)$. Por outro lado, como $G = \langle x, y \rangle$ e $[x, y] \in Z(G)$, pela Proposição 1.1, segue que:

$$1 = [x, y]^p = [x^p, y] = [x, y^p] \Rightarrow x^p, y^p \in Z(G) \Rightarrow \langle x^p, y^p, G' \rangle = \mho_1(G) \leq Z(G).$$

Logo, $\mho_1(G)G' = \Phi(G) \leq Z(G)$.

Afirmamos que $\Phi(G) = Z(G)$. Suponhamos que não, então $\Phi(G) < Z(G)$. Assim, existe um elemento $g \in Z(G)$, tal que $g \notin \Phi(G)$. Mas então g é um gerador essencial que comuta com todos os outros geradores essenciais de G, uma contradição, já que G é não abeliano. Portanto, $\Phi(G) = Z(G)$.

$(iii) \Rightarrow (i)$ Agora, supondo $d(G) = 2$ e $Z(G) = \Phi(G)$, queremos mostrar que G é não abeliano e que todo subgrupo próprio de G é abeliano. De fato, observamos que como $d(G) = 2$, pelo Teorema da Base de Burnside, $[G : \Phi(G)] = p^2$. Desde que, por hipótese, $Z(G) = \Phi(G)$, temos $[G : Z(G)] = p^2$ e, assim, G é não abeliano.

Agora, vamos tomar H um subgrupo maximal de G. Se mostrarmos que H é abeliano, o resultado estará provado, já que todo subgrupo próprio de G ou é maximal ou está contido em algum maximal.

Afirmamos, primeiramente, que $Z(G) \leq Z(H)$. De fato, já temos que $Z(G) = \Phi(G) \leq H$. Além disso, $Z(G) \leq Z(H)$, pois se $g \in Z(G)$, então $g \in H$ e uma vez que g comuta com todo elemento em H, segue que $g \in Z(H)$. Temos o seguinte:

$$\begin{tikzcd}[arrows=dash]
G \arrow[d, "p"] \\
H \arrow[d] \\
Z(H) \arrow[d] \\
Z(G) = \Phi(G)
\end{tikzcd}$$

Já temos que $[G : \Phi(G)] = p^2$. Além do mais, como H é maximal, sabemos que $[G : H] = p$. Assim, obtemos que $Z(H) = Z(G)$ ou $Z(H) = H$.

Se $Z(H) = Z(G)$, então $|H/Z(H)| = p$, e assim $H/Z(H)$ é cíclico, implicando em H abeliano. Mas, então $H = Z(H)$, contrariando o fato de que $|H/Z(H)| = p$. Assim, concluímos que $Z(H) = H$ e, portanto, H é abeliano, como queríamos.

Agora, vamos provar que $(i) \Rightarrow (iii) \Rightarrow (ii)$.

$(i) \Rightarrow (iii)$ Como, por hipótese, G é não abeliano, existem pelo menos dois elementos x, y em G, tais que $[x, y] \neq 1$. Considerando $H = \langle x, y \rangle$, temos que H é um subgrupo não abeliano de G. Mas então a minimalidade de G implica em $G = H$, donde segue que $d(G) = 2$. E se $d(G) = 2$, pelo Teorema da Base de Burnside, sabemos que $[G : \Phi(G)] = p^2$.

Sendo assim, afirmamos que G possui pelo menos dois subgrupos maximais distintos. De fato, caso contrário, se G tivesse apenas um subgrupo maximal A, teríamos $\Phi(G) = A$ e, assim, $[G : \Phi(G)] = p$, contrariando o fato de que $[G : \Phi(G)] = p^2$. Logo, podemos tomar A e B subgrupos maximais distintos de G. Note que A e B são abelianos.

Além disso, temos que $\Phi(G) \leq A \cap B \leq Z(G)$. De fato, como A e B são maximais, temos que $\Phi(G) \leq A$ e $\Phi(G) \leq B$, logo $\Phi(G) \leq A \cap B$. Por outro lado, se $g \in A \cap B$, então g comuta com os elementos em A e g comuta com os elementos em B e, assim, g comuta com todo elemento em $G = AB$, donde segue que $g \in Z(G)$. Então:

$$\begin{tikzcd}[arrows=-] G = AB \arrow[d] \\ Z(G) \arrow[d] \\ A \cap B \arrow[d] \\ \Phi(G) \end{tikzcd}$$

Pelo esquema acima, como $[G : \Phi(G)] = p^2$ e G é não abeliano, segue que $Z(G) = A \cap B$. Logo:

$$\begin{tikzcd}[arrows=-] G = AB \arrow[d, "p"] \\ Z(G) = A \cap B \arrow[d, "p"] \\ \Phi(G) \end{tikzcd}$$

Observe que se $|G/Z(G)| = p$, então $G/Z(G)$ é cíclico, o que implica em G abeliano, uma contradição. Portanto, só poderemos ter $Z(G) = A \cap B = \Phi(G)$.

$(iii) \Rightarrow (ii)$ Supondo $d(G) = 2$ e que $\Phi(G) = Z(G)$, queremos mostrar que $|G'| = p$. Note que, pelo Teorema da Base de Burnside, G é não abeliano. Logo, é possível tomarmos um subgrupo abeliano maximal A de G. Sendo assim, desde que $[G : A] = p$, pelo Lema 1.6, temos que:

$$|G| = p.|G'|.|Z(G)|.$$

Usando que $|G/Z(G)| = |G/\Phi(G)| = p^2$, obtemos que $|G'| = p$, como queríamos. $\square$

Teorema 1.16. *Um p-grupo finito não abeliano é gerado por subgrupos não abelianos minimais.*

Demonstração. Ver [4]. $\square$

Definição 1.24. *Para p um primo e m, n naturais, usaremos $M_p(m,n)$ para denotar os grupos:*

$$\langle a, b \mid a^{p^m} = b^{p^n} = 1,\ a^b = a^{1+p^{m-1}}\rangle,\ \text{onde } m \geq 2.$$

E para $m \geq n$ usaremos $M_p(m,n,1)$ para denotar os grupos:

$$\langle a, b, c \mid a^{p^m} = b^{p^n} = c^p = 1,\ [a,b] = c,\ [c,a] = [c,b] = 1\rangle,$$

onde $m + n \geq 3$ para $p = 2$.

Teorema 1.17. *Seja G um p-grupo finito não abeliano minimal. Então G é isomorfo a Q_8 ou $M_p(m,n)$ ou $M_p(m,n,1)$.*

Demonstração. Ver [13]. □

Agora, apresentaremos, de forma breve, os p-grupos extra-especiais.

Definição 1.25. *Seja G um p-grupo não abeliano finito. Dizemos que G é extra-especial se $Z(G) = G'$ e $|Z(G)| = p$.*

Proposição 1.11. *Todo grupo não abeliano de ordem p^3 é extra-especial.*

Demonstração. Seja G um grupo não abeliano de ordem p^3. Queremos mostrar que $Z(G) = G'$ e $|Z(G)| = p$. De fato, como G é um p-grupo, pelo Teorema 1.8, já temos que $Z(G) \neq 1$ e desde que G é não abeliano, temos $|Z(G)| \neq p^3$. Sendo assim:

$$|Z(G)| = p \text{ ou } |Z(G)| = p^2.$$

Se $|Z(G)| = p^2$, então $|G/Z(G)| = p$ e $G/Z(G)$ é um grupo cíclico, implicando em G abeliano, uma contradição. Logo, $|Z(G)| = p$. Assim, $|G/Z(G)| = p^2$ e, portanto, $G/Z(G)$ é abeliano. Mas então, pela Proposição 1.6, temos $G' \leq Z(G)$ e, como $G' \neq \{1\}$, obtemos $G' = Z(G)$. Desse modo, concluímos que todo grupo de ordem p^3 é extra-especial.

□

Exemplo 1.11. *O grupo diedral de ordem 8 é um 2-grupo extra-especial. De fato, primeiramente recordemos a apresentação e os subgrupos de D_4 no Exemplo 1.7. Agora, como D_4 é não abeliano, sabemos que $|Z(D_4)| = 2$. Desde que $[a^2, b] = 1$, temos que $a^2 \in Z(D_4)$ e, assim, $\langle a^2\rangle \leq Z(D_4)$. Mas então, como $o(a^2) = 2$, segue que $Z(D_4) = \langle a^2\rangle$. Por outro lado, como $a^2 = [a,b]$, segue pela Observação 1.1 que $Z(D_4) = \langle a^2\rangle = D_4'$. E, portanto, D_4 é extra-especial, como afirmado.*

Exemplo 1.12. *O grupo dos quatérnios de ordem 8 também é extra-especial, pois vimos no exemplo 1.2 que ele satisfaz* $Z(Q_8) = Q_8' = \langle a^2 \rangle$ *e* $|Z(Q_8)| = 2$.

Veremos adiante que Q_8 e D_4 são os únicos subgrupos extra-especiais de ordem 2^3.

Teorema 1.18. *Seja* G *um grupo não abeliano tal que* $|G| = p^3$. *Temos que:*

(i) Se $p = 2$, *então* $G \cong D_4$ *ou* $G \cong Q_8$.
(ii) Se p *é ímpar, então* $G \cong M_p(2,1)$ *ou* $G \cong M_p(1,1,1)$.

Demonstração. Ver [7]. □

A classificação dos grupos extra-especiais nos diz que todo grupo extra-especial é o produto central de subgrupos não abelianos de ordem p^3, como pode ser visto em [7].

Para finalizar, enunciaremos o Teorema de Classificação dos grupos não abelianos de ordem 2^4 que será importante futuramente. Para mais detalhes, veja [5].

Teorema 1.19. *Se* G *é um grupo não abeliano de ordem* 2^4, *então* G *é isomorfo a um dos grupos abaixo:*

1. $C_8 \rtimes_3 C_2 = \left\langle a, b \mid a^8 = b^2 = 1,\ a^b = a^{-1} \right\rangle$
2. $C_8 \rtimes_5 C_2 = \left\langle a, b \mid a^8 = b^2 = 1,\ a^b = a^3 \right\rangle$
3. $C_8 \rtimes_7 C_2 = \left\langle a, b \mid a^8 = b^2 = 1,\ a^b = a^5 \right\rangle$
4. $Q_{16} = \left\langle a, b \mid a^8 = 1,\ b^2 = a^4,\ a^b = a^{-1} \right\rangle$
5. $C_4 \rtimes C_4 = \left\langle a, b \mid a^4 = b^4 = 1,\ a^b = a^3 \right\rangle$
6. $D_8 \times C_2 = \left\langle a, b, c \mid a^4 = b^2 = c^2 = 1,\ a^b = a^{-1},\ [a,c] = [b,c] = 1 \right\rangle$
7. $K_4 \rtimes C_4 = \langle a, b, c \mid a^4 = b^2 = c^2 = 1,\ [a,c] = b,\ [a,b] = [b,c] = 1 \rangle$
8. $Q_8 \times C_2 = \left\langle a, b, c \mid a^4 = c^2 = 1, a^2 = b^2,\ a^b = a^{-1},\ [a,c] = [b,c] = 1 \right\rangle$
9. $Q_8 \rtimes C_2 = \left\langle a, b, c \mid a^4 = c^2 = 1, a^2 = b^2, a^b = a^{-1},\ b^c = b^{-1},\ [a,c] = 1 \right\rangle$.

Note que $C_4 \rtimes C_4 = M_2(2,2)$.

Capítulo 2

Classificação dos grupos hamiltonianos

Um grupo hamiltoniano é um grupo não abeliano no qual todos os seus subgrupos são normais. Em 1897, Richard Dedekind investigou os grupos hamiltonianos e provou que todos eles contêm uma cópia do grupo dos quatérnios de ordem 8, como veremos adiante. Ele os nomeou assim, em homenagem a William Hamilton (1805-1865), o descobridor dos quatérnios.

Neste capítulo, nosso objetivo será classificar todos os grupos hamiltonianos e para isso, nos dedicaremos, a priori, ao desenvolvimento das propriedades destes grupos. As referências utilizadas foram [9] e [14].

2.1 Grupos hamiltonianos e suas propriedades

Um grupo G é dito ser dedekindiano, se todo subgrupo de G é normal em G. Equivalentemente, G é dedekindiano se todo subgrupo cíclico de G é normal em G. Obviamente, se o grupo é abeliano, então todos os seus subgrupos são normais e, portanto, grupos abelianos são dedekindianos. Aqui, estaremos interessados nos grupos dedekindianos não abelianos, que recebem o nome de hamiltonianos.

Definição 2.1. *Um grupo não abeliano G é dito ser hamiltoniano se todos os seus subgrupos são normais.*

Exemplo 2.1. *O grupo dos quatérnios de ordem 8 é um grupo hamiltoniano. De fato, desde que todo subgrupo próprio H de Q_8 é cíclico de ordem 2 ou 4, temos que:*

Se $|H| = 2$, então $H = Z(Q_8)$ e, assim, $H \trianglelefteq Q_8$. Por outro lado, se $|H| = 4$, então $[Q_8 : H] = 2$ e também obtemos que $H \trianglelefteq Q_8$.

Veremos abaixo que Q_8 é o exemplo mais importante de grupo hamiltoniano, pois está contido em todos os outros. Assim, vamos concluir que Q_8 é o grupo hamiltoniano de menor ordem.

Para os próximos resultados, a Proposição 1.1 e o Lema 1.3 se farão necessários.

Teorema 2.1. *Seja G um grupo hamiltoniano. Então G possui um subgrupo isomorfo ao Q_8.*

Demonstração. Como G é não abeliano, existem pelo menos dois elementos em G que não comutam. Logo, sejam $x, y \in G$, tais que $c = [x, y] \neq 1$. Desde que G é um grupo hamiltoniano, os subgrupos cíclicos $\langle x \rangle$ e $\langle y \rangle$ são normais em G. Então:

$$c \in \langle x \rangle \text{ e } c \in \langle y \rangle \Rightarrow c \in \langle x \rangle \cap \langle y \rangle.$$

Assim, existem inteiros positivos r e s tais que $c = [x, y] = x^r = y^s$. Então, considerando o subgrupo $H = \langle x, y \rangle$, temos que c pertence ao $Z(H)$. Por isso, usando o Lema 1.3:

$$c^r = [x, y]^r = [x^r, y] = [c, y] = 1.$$

Daí segue que $o(c) < \infty$, o que implica em $o(x) < \infty$ e $o(y) < \infty$. Além disso, pela Observação 1.1, temos que $H' = \langle c \rangle$. Mas, uma vez que as ordens de c, x e y são finitas e $H' = \langle c \rangle$, temos que H/H' é abeliano e finitamente gerado por elementos de ordem finita, logo, concluímos que H é finito.

Sendo assim, considere $o(x) = m$ e $o(y) = n$ e assuma que x e y foram escolhidos de tal forma que $m + n$ seja o menor possível. Seja p um primo que divide m. Temos que $o(x^p) < o(x)$ e, assim, pela minimalidade de $m + n$ segue que x^p e y comutam, ou seja:

$$1 = [x^p, y] = [x, y]^p = c^p.$$

Logo, $o(c) = p$. Observe que acabamos de mostrar que para qualquer primo p que divide a ordem de x, obtemos $o(c) = p$ e, por isso, concluímos que m e n são potências de p.

Vamos escrever $r = kp^{r_1}$ e $s = lp^{s_1}$, onde $mdc(k, p) = mdc(l, p) = 1$. Consequentemente, $mdc(k, o(x)) = mdc(l, o(y)) = 1$. Logo, pelo Lema de Bézout, existem inteiros k', q, l' e r, tais que:

$$kk' + o(x)q = 1 \;\text{ e }\; ll' + o(y)r = 1.$$

Donde obtemos k', l' satisfazendo:

$$kk' \equiv 1(mod\ \ o(x)) \quad e \quad ll' \equiv 1(mod\ \ o(y)).$$

Denotando por $x' = x^{l'}$ e $y' = y^{k'}$, verificamos o seguinte:

$$[x', y'] = [x^{l'}, y^{k'}] = [x, y]^{k'l'} = c^{k'l'}. \tag{2.1}$$

Por outro lado, obtemos:

$$\begin{aligned} (x')^{p^{r_1}} &= x^{l'p^{r_1}} = (x^{p^{r_1}})^{l'} \quad e \\ c^{k'} &= (x^{kp^{r_1}})^{k'} = (x^{kk'})^{p^{r_1}} = (x^{kk'-1}x)^{p^{r_1}} = x^{p^{r_1}}. \end{aligned} \tag{2.2}$$

Por (2.1) e (2.2) obtemos que $(x')^{p^{r_1}} = (x^{p^{r_1}})^{l'} = c^{k'l'}$. Assim, mostramos que $(x')^{p^{r_1}} = [x', y']$. Denotando por $c' = [x', y']$ e usando um raciocínio análogo ao anterior, obtemos que $c' = (y')^{p^{s_1}}$. Logo:

$$c' = (x')^{p^{r_1}} = (y')^{p^{s_1}}.$$

Agora, observe que:

$$(c')^p = (c^{k'l'})^p = (c^p)^{k'l'} = 1 \Rightarrow o(c') = p.$$

e

$$1 = (c')^p = ((x')^{p^{r_1}})^p = ((y')^{p^{s_1}})^p.$$

Daí segue que $o(x') = p^{r_1+1}$. De fato, pois se $o(x') < p^{r_1+1}$, então $c^{l'k'} = c' = (x')^{p^{r_1}} = 1$. Mas como $o(c) = p$, temos que $p|l'k'$, absurdo, já que $p \nmid l'$ e $p \nmid k'$. De forma análoga, chegamos em $o(y') = p^{s_1+1}$.

Sendo assim, a partir de agora, visando simplificar a notação, vamos escrever $x = x'$, $y = y'$ e $c = c'$. E vamos supor, sem perda de generalidade, que $r_1 \geq s_1$.

Ao tomarmos $y_1 = x^{-p^{r_1-s_1}}y \in H$ e novamente usando a Proposição 1.1:

$$[x, y_1] = [x, x^{-p^{r_1-s_1}}y] = [x, y]\underbrace{[x, x^{-p^{r_1-s_1}}]^y}_{1} = [x, y] = c \neq 1.$$

Logo x e y_1 não comutam. Mas então pela minimalidade de $m + n$, verificamos que $o(y_1) \geq o(y) = p^{s_1+1}$. Donde segue que $y_1^{p^{s_1}} \neq 1$. Logo, pelo Lema 1.3:

$$y_1^{p^{s_1}} = (x^{-p^{r_1-s_1}}y)^{p^{s_1}} = x^{-p^{r_1}}y^{p^{s_1}}[y, x^{-p^{r_1-s_1}}]^{\binom{p^{s_1}}{2}}.$$

Uma vez que $c = x^{p^{r_1}} = y^{p^{s_1}}$, segue que:

$$\begin{aligned} y_1^{p^{s_1}} = c^{-1}c[(x^{-p^{r_1-s_1}}, y]^{-1\binom{p^{s_1}}{2}} =& [x^{-1}, y]^{-p^{r_1-s_1}\binom{p^{s_1}}{2}} \\ =& [x, y]^{p^{r_1-s_1}\binom{p^{s_1}}{2}} \\ =& c^{\frac{p^{r_1}(p^{s_1}-1)}{2}}. \end{aligned}$$

Analisando a igualdade acima, temos que se p for um número ímpar, $p^{s_1} - 1$ é par. Mas como $o(c) = p$, teremos que p divide $\frac{p^{r_1}(p^{s_1}-1)}{2}$ e assim $y_1^{p^{s_1}} = 1$, uma contradição. Portanto, concluímos que a única possibilidade é $p = 2$ e $r_1 = 1$, pois caso contrário sempre vamos obter $y_1^{p^{s_1}} = 1$. Como estamos supondo $r_1 \geq s_1$, segue que $s_1 = 1$ e, assim, temos que $o(x) = o(y) = 4$. Com isso, x e y satisfazem:

$$x^4 = 1, \quad c = [x, y] = x^2 = y^2 \quad e \quad x^{-1} = y^{-1}xy.$$

E finalmente, obtemos que $K = \langle x, y \rangle$ é isomorfo ao Q_8, como queríamos.

$\square$

Observação 2.1. *Note que, de acordo com a demonstração acima, se G é um grupo hamiltoniano, então quaisquer dois elementos em G que não comutam devem ter ordem potência de 2.*

Destacamos que a recíproca do teorema acima não é verdadeira, isto é, se G é um grupo que possui um subgrupo isomorfo ao Q_8, então G não é necessariamente um grupo hamiltoniano. De fato, se considerarmos o grupo $GL(2, \mathbb{C})$, temos que as matrizes:

$$j = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \quad \text{e} \quad k = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

geram um subgrupo S isomorfo ao Q_8:

$$S = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \right.$$
$$\left. \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix} \right\}.$$

Mas verificamos que S não é um subgrupo normal em $GL(2, \mathbb{C})$, pois ao conjugarmos, por exemplo, $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in S$ por $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in GL(2, \mathbb{C})$, obtemos $\begin{pmatrix} 1 & 2 \\ -1 & -1 \end{pmatrix}$ que não está em S.

Portanto, o grupo $GL(2, \mathbb{C})$ não é hamiltoniano.

Através dos lemas a seguir, exploraremos algumas propriedades dos grupos hamiltonianos que serão fundamentais para demonstrarmos o Teorema de Classificação destes grupos.

A fim de simplificar a leitura, para os próximos quatro lemas, usaremos a seguinte hipótese.

Hipótese 2.1. *Seja G um grupo hamiltoniano e $K = \langle x, y \rangle$ um subgrupo de G que é isomorfo ao Q_8, ou seja,*

$$K = \langle x, y \mid x^4 = 1,\ x^2 = y^2 \text{ e } y^{-1}xy = x^{-1} \rangle.$$

Também usaremos que $C(g) = \{g^h \mid h \in G\}$, isto é, a classe de conjugação do elemento g em G, satisfaz $C(g) \subseteq \langle g \rangle$. De fato, pois desde que G é hamiltoniano, temos que $\langle g \rangle$ é normal em G, para todo $g \in G$ e, portanto, $g^h \in \langle g \rangle$, para todo $h \in G$.

Lema 2.1. *Seja $g \in G$. Se $o(g) = 2$, então $g \in Z(G)$.*

Demonstração. Seja $g \in G$. Como visto acima, temos que $C(g) \subseteq \langle g \rangle$. Sendo assim, desde que $o(g) = 2$, para $h \in H$, temos que:

$$h^{-1}gh = g \quad \text{ou} \quad h^{-1}gh = 1.$$

Se $h^{-1}gh = 1$, obtemos $g = 1$, uma contradição. Logo, concluímos que $h^{-1}gh = g$, donde segue que $g \in Z(G)$. $\square$

Observação 2.2. *Considerando a Hipótese 2.1, pelo lema acima, temos que se a é um elemento de ordem 4 em G, então $C(a) = \{a, a^{-1}\}$ em G. De fato, desde que $C(a) \subseteq \langle a \rangle$ e $o(a) = 4$, temos as seguintes possibilidades:*

$$g^{-1}ag = 1,\ a,\ a^2,\ \text{ou}\ \ a^3,\ \text{para todo } g \in G.$$

Note que se $g^{-1}ag = 1$, então $a = 1$, contradição. Agora, se $g^{-1}ag = a^2$, usando o lema anterior, obtemos $a = a^2$, novamente uma contradição. Logo, como $a^{-1} = a^3$, temos que $C(a) = \{a, a^{-1}\}$ em G, como afirmado.

Em particular, todo elemento $k \in K \cong Q_8$ possui classe de conjugação em K dada por $C(k) = \{k, k^{-1}\}$.

Lema 2.2. *$G = KC_G(K)$.*

Demonstração. Primeiramente, relembremos que:

$$C_G(K) = \{g \in G \mid gk = kg, \forall \ \ k \in K\}.$$

Agora, suponhamos, por absurdo, que existe $g \in G \backslash KC_G(K)$. Então g não comuta com x ou g não comuta com y. Sem perda de generalidade, vamos supor que g não comuta com y. Logo, $y^g \neq y$. Então, pela observação anterior, obtemos que $y^g = g^{-1}yg = y^{-1} = y^3$. Além disso, usando as relações em K:

$$ygx = gy^g x = gy^{-1}x = gxy.$$

Portanto, gx comuta com y. Como $gx \notin C_G(K)$, então deduzimos que gx não comuta com x. Assim, $x^{gx} \neq x$. Novamente pela observação anterior, segue que $x^{gx} = x^{-1}$. Sendo assim, de um lado:

$$x(gxy) = gxx^{gx}y = gy = gx^{-1}yx^{-1} = (gxy)x.$$

E por outro lado, usando que gx comuta com y:

$$y(gxy) = y(gx)y = (gxy)y.$$

Dessas duas igualdades, obtemos que $gxy \in C_G(K)$, donde concluímos que $g \in KC_G(K)$, uma contradição. Logo, $G = KC_G(K)$, como afirmado. □

Lema 2.3. *G é um grupo de torção.*

Demonstração. Primeiramente, dizemos que G é um grupo de torção se:

$$G = T(G) = \{g \in G \mid o(g) < \infty\},$$

isto é, G é um grupo de torção se todo elemento em G tem ordem finita.

Vimos no lema anterior que $G = KC_G(K)$. Logo, desde que $K \cong Q_8$ é um grupo de torção e uma vez que os elementos de K e $C_G(K)$ comutam, para mostrarmos que os elementos de G têm ordem finita, basta mostrarmos que os elementos de $C_G(K)$ têm ordem finita. Para tanto, seja $g \in C_G(K)$. Então:

$$[x, gy] = [x, y][x, g]^y = [x, y] = x^2 = y^2 \neq 1.$$

Como G é hamiltoniano, temos que $\langle x\rangle$ e $\langle gy\rangle$ são subgrupos normais de G. E, portanto, $1 \neq [x, gy] \in \langle x\rangle \cap \langle gy\rangle$. Logo, existem inteiros r e s, tais que $[x, gy] = x^r = (gy)^s$. Tome $H = \langle x, gy\rangle = \langle x\rangle\langle gy\rangle$. Temos que $[x, gy] \in Z(H)$ e assim:

$$[x, gy]^r = [x^r, gy] = [[x, gy], gy] = 1.$$

Donde segue que $o([x, gy]) < \infty$ e $o(gy) < \infty$ e, portanto, $o(g) < \infty$, como queríamos. $\square$

Lema 2.4. *$C_G(K)$ não contém elementos de ordem 4.*

Demonstração. Suponhamos, por absurdo, que existe $g \in C_G(K)$ com ordem 4. Logo, $o(gy) = 4$. Além disso, vimos na demonstração do lema anterior, que $[x, gy] \neq 1$ e $[x, gy] \in \langle gy\rangle$. Assim, temos as seguintes possibilidades para $[x, gy]$:

$$[x, gy] = (gy),\ (gy)^2 \text{ ou } (gy)^3.$$

Se $[x, gy] = (gy)$, então $x^{-1}(gy)^{-1}xgy = gy$, implicando em $gy = 1$, uma contradição.

Agora, se $[x, gy] = (gy)^3$, então $x^{-1}(gy)^{-1}xgy = (gy)^3$ e obtemos $x^2 = (gy)^{-1}$, uma contradição, pois $2 = o(x^2) \neq o\left((gy)^{-1}\right) = 4$.

Portanto, concluímos que:

$$[x, gy] = x^{-1}(gy)^{-1}xgy = (gy)^2 \Rightarrow (gy)^{-1} = (gy)^x.$$

Então, usando que $(gy)^{-1} = (gy)^x$:

$$[gy, x] = (gy)^{-1}x^{-1}gyx = (gy)^{-1}(gy)^x = (gy)^{-2} = g^{-2}y^{-2} = g^2y^2.$$

E por outro lado:

$$[gy, x] = [x, gy]^{-1} = [x, y]^{-1} = x^2 = y^2.$$

Logo, $g^2y^2 = y^2$ e obtemos que $g^2 = 1$, uma contradição, pois $o(g) = 4$. Sendo assim, concluímos que $C_G(K)$ não possui elementos de ordem 4, como afirmado. $\square$

2.2 Teorema de classificação

Chegamos ao Teorema de Classificação dos grupos hamiltonianos:

Teorema 2.2. *(Teorema de Classificação dos Grupos Hamiltonianos) Um grupo G é hamiltoniano se, e somente se, $G = K \times A \times E$, onde K é isomorfo ao grupo dos quatérnios de ordem 8, A é um grupo abeliano cujo todos os elementos possuem ordem ímpar e E é um 2-grupo abeliano elementar.*

Demonstração. Suponhamos que G é um grupo hamiltoniano. Vimos que G possui um subgrupo $K = \langle x, y\rangle$ isomorfo ao Q_8 e que $G = KC_G(K)$. Além disso, note que, pela Observação 2.1, segue que os elementos de ordem ímpar em $C_G(K)$ comutam com todos os elementos em G. Sendo assim, considerando o conjunto A formado pelos elementos de ordem ímpar em $C_G(K)$, obtemos que A é um subgrupo do $Z(G)$ e, portanto, A é abeliano.

Vimos ainda, Lema 2.4, que $C_G(K)$ não possui elementos de ordem 4. Dessa forma, afirmamos que se $h \in C_G(K)$ é um elemento não trivial com ordem potência de 2, então necessariamente $o(h) = 2$. De fato, suponhamos, por absurdo, que existe $h \in C_G(K)$, tal que $o(h) = 2^\alpha$, com $\alpha \geq 3$. Então, $h^{2^{\alpha-2}} \in C_G(K)$ e

$$\left(h^{2^{\alpha-2}}\right)^{2^2} = h^{2^\alpha} = 1.$$

Donde obtemos que $o(h^{2^{\alpha-2}}) = 2^2 = 4$, uma contradição. Portanto, se $h \in C_G(K)$ é um elemento não trivial de ordem par, então $o(h) = 2$ e, pelo Lema 2.1, temos que $h \in Z(G)$. Sendo assim, seja B o conjunto formado pelos elementos de ordem potência de 2 em $C_G(K)$. Note que o conjunto B está contido no $Z(G)$. Vamos verificar que B é um 2-grupo abeliano elementar. De fato, pois claramente B é um conjunto não vazio. Por outro lado, sejam $g, h \in B$ não triviais, então $o(g) = o(h) = 2$. Desde que $\langle g\rangle$ é normal em G:

$$(gh^{-1})^2 = gh^{-1}gh^{-1} = g\underbrace{h^{-1}gh}_{\in\langle g\rangle} = g^2 = 1.$$

E, assim, $gh^{-1} \in B$. Logo, B é um grupo abeliano, onde todo elemento não trivial tem ordem 2, ou seja, B é um 2-grupo abelino elementar.

Diante do exposto, afirmamos que $C_G(K) = B \times A$. De fato, claramente $A \cap B = \{1\}$. Temos ainda que A e B são normais em G e, consequentemente, são normais em $C_G(K)$. Além disso, $C_G(K) = BA$, pois se $h \in C_G(K)$ e $o(h) = 2$ ou $o(h)$ é ímpar, segue que $h \in BA$. Agora, se $o(h) = 2^\alpha m$, com m ímpar e $\alpha \geq 1$, temos necessariamente que $o(h) = 2m$. Uma vez que $mdc(2, m) = 1$, sabemos que existem inteiros r, s, tais que $2q + rm = 1$. Mas então $h = h^{rm}h^{2q} \in BA$.

Agora, observamos que $x^2 \in K$ e $o(x^2) = 2$. Logo $x^2 \in B$. Aplicando que x^2 tem ordem máxima em B e utilizando o Lema 1.7, obtemos $B = \langle x^2\rangle \times E$, onde E é um 2-grupo abeliano elementar.

Tendo em vista que x^2 é o único elemento de ordem 2 em K e, assim, $K \cap (E \times A) = \{1\}$, temos:

$$G = KC_G(K) = K(B \times A) = K(\langle x^2\rangle \times E \times A) = K \times E \times A,$$

como queríamos.

Reciprocamente, seja $G = K \times A \times E$, onde $K,\ A,\ E$ são como no enunciado. Desde que $K \cong Q_8$ é não abeliano, temos que G também é não abeliano. Sendo assim, para mostrarmos que G é hamiltoniano é suficiente provarmos que para cada g em G, temos $\langle g \rangle$ um subgrupo normal de G.

Então, seja $g \in G$, tal que $g = kab$, onde $k \in K,\ a \in A,\ b \in E$. Se $o(k) = 2$, segue que $k \in Z(K)$, logo $g \in Z(G)$ e assim $\langle g \rangle$ é normal em G. Agora, se $o(k) = 4$, sabemos que $C(k) = \{k, k^{-1}\}$ em G e, portanto, $C(g) = \{g, k^{-1}ab\}$ em G.

Queremos mostrar que $k^{-1}ab \in \langle g \rangle$. De fato, como $a \in A$, $o(a)$ é ímpar. Denote $o(a) = m$ e tome $s = 2m + 1$. Temos $s = \mathit{2m + 1} \equiv \mathit{3}(\mathit{mod}\ \mathit{4})$.

Afirmamos que $g^s = k^{-1}ab$.
Como $o(k) = 4$ e $s \equiv \mathit{3}(\mathit{mod}\ \mathit{4})$, segue que $4 \mid s + 1$ e assim:

$$k^{s+1} = 1 \Rightarrow k^s k = 1 \Rightarrow k^s = k^{-1}.$$

Além disso, como $s \equiv \mathit{1}(\mathit{mod}\ m)$, temos que $m \mid s - 1$:

$$a^{s-1} = 1 \Rightarrow a^s a^{-1} = 1 \Rightarrow a^s = a.$$

Finalmente, como $o(b) = 2$ e s é ímpar temos:

$$b^s = b^{2m+1} = b^{2m} b = b.$$

Portanto, $g^s = (kab)^s = k^s a^s b^s = k^{-1}ab$ e assim $k^{-1}ab \in \langle g \rangle$,. Logo, $C(g) \subseteq \langle g \rangle$ e concluímos que $\langle g \rangle$ é um subgrupo normal de G, como queríamos.

□

Observamos que de acordo com a estrutura de um grupo hamiltoniano, vista no teorema acima, temos que os p-grupos hamiltonianos são necessariamente 2-grupos da forma $K \times E$, onde $K \cong Q_8$ e E é um 2-grupo abeliano elementar.

Capítulo 3

p-Grupos metahamiltonianos finitos

Finalmente, vamos apresentar os grupos metahamiltonianos, grupos não abelianos onde todos os seus subgrupos não abelianos são normais. O conceito de metahamiltoniano é uma generalização dos grupos hamiltonianos vistos no capítulo anterior.

Neste capítulo, exploraremos algumas propriedades destes grupos. Além disso, enunciaremos e demonstraremos um importante teorema que os caracteriza. A referência deste capítulo é [1].

3.1 Grupos metahamiltonianos

Um grupo não abeliano G é dito metahamiltoniano se todos seus subgrupos não abelianos são normais. Como exemplos triviais, temos os grupos hamiltonianos e os grupos não abelianos minimais.

Lema 3.1. *Seja G um grupo, tal que $|G'| = p$, onde p é primo. Então G é metahamiltoniano.*

Demonstração. Primeiramente, note que G é não abeliano. Vamos verificar que se $|G'| = p$, então todo subgrupo não abeliano de G contém G' e, portanto, todo subgrupo não abeliano de G será normal em G, donde seguirá que G é metahamiltoniano. De fato, suponhamos, por absurdo, que existe $H \leq G$ não abeliano e tal que $G' \nleq H$. Desde que

$|G'| = p$, temos $G' \cap H = \{1\}$, logo:

$$\begin{tikzcd}
 & G \arrow[d, dash] & \\
 & G'H \arrow[dl, equal] \arrow[dr, dash] & \\
G' \arrow[dr, dash] & & H \arrow[dl, equal] \\
 & G' \cap H = \{1\} &
\end{tikzcd}$$

$$\frac{G'H}{G'} \cong \frac{H}{G' \cap H} = H.$$

Como $G'H/G' \leq G/G'$ é abeliano, obtemos que H também é abeliano, uma contradição. Logo, G' está contido em todo subgrupo não abeliano de G, como queríamos. □

Teorema 3.1. *Seja G um grupo metahamiltoniano finito. Então os quocientes não abelianos de G, bem como os subgrupos não abelianos de G são metahamiltonianos.*

Demonstração. De fato, seja G/H um quociente não abeliano de G e seja K/H um subgrupo não abeliano de G/H. Logo, $K \leq G$ é não abeliano e desde que G é metahamiltoniano, segue que K é normal em G e, portanto, K/H é normal em G/H.

Agora, seja H um subgrupo não abeliano de G, uma vez que os subgrupos de H são também subgrupos de G, segue que H é metahamiltoniano. □

3.2 Propriedades de p-grupos metahamiltonianos

Desde que estamos interessados em estudar os p-grupos metahamiltonianos finitos, abordaremos nesta seção algumas de suas propriedades.

Exemplo 3.1. *Todo p-grupo extra-especial é um p-grupo metahamiltoniano finito. De fato, se G é extra-especial, então sabemos que G é um p-grupo finito não abeliano e $|G'| = |Z(G)| = p$. Logo, pelo Lema 3.1, G é metahamiltoniano. Sendo assim, a classificação dos p-grupos extra-especiais, vista superficialmente no Capítulo 1, nos fornece alguns exemplos de p-grupos metahamiltonianos.*

Exemplo 3.2. *Grupos não abelianos de ordem p^4 são p-grupos metahamiltonianos finitos. De fato, sejam G um grupo não abeliano de ordem p^4 e H um subgrupo não abeliano* *de G. Nesta situação, a única possibilidade é que $|H| = p^3$. Mas então $[G : H] = p$ e, portanto, H é normal em G. Observamos que uma classificação dos grupos de ordem p^4 pode ser vista em [5].*

Teorema 3.2. *Seja G um p-grupo não abeliano finito. Então G é metahamiltoniano se, e somente se, todo subgrupo não abeliano minimal de G é normal em G.*

Demonstração. Se G é metahamiltoniano, então claramente todo subgrupo não abeliano minimal de G é normal. Reciprocamente, desde que pelo Teorema 1.16, um p-grupo não abeliano é gerado por subgrupos não abelianos minimais, temos que se todo subgrupo não abeliano minimal de G é normal, então todo subgrupo não abeliano de G é normal e, por isso, G é metahamiltoniano.

□

Teorema 3.3. *Seja G um p-grupo metahamiltoniano finito. Então para todo $x \in G$, $\langle x \rangle^G$ é abeliano ou não abeliano minimal.*

Demonstração. Suponhamos que $\langle x \rangle^G$ é não abeliano, para $x \in G$. Logo, existem g_1, g_2 em G, tais que:

$$[x^{g_1}, x^{g_2}] \neq 1 \Rightarrow [x^{g_1}, x^{g_2}]^{g_1{}^{-1}} \neq 1 \Rightarrow [x, x^{g_2 g_1{}^{-1}}] \neq 1.$$

Tomando $g = g_2 g_1{}^{-1}$, obtemos que $[x, x^g] \neq 1$. Então, consideremos o subgrupo $K = \langle x, x^g \rangle$ de G. Como K é não abeliano e G é metahamiltoniano, temos que K é normal em G e, por isso, $K = \langle x \rangle^G$. Sejam:

$$y = x^g$$

e

$$L = \langle x, x^y \rangle = \langle x, [x, y] \rangle.$$

Como $L < K$, temos que L não é normal em G e, por isso, L é abeliano. Daí, temos que $[[x, y], x] = 1$. Por outro lado, uma vez que $\langle y \rangle^G = \langle x^g \rangle^G = \langle x \rangle^G$, procedendo de forma similar, obtemos $[[x, y], y] = 1$. Portanto, $[x, y] \in Z(K)$.

Agora, seja $S = \langle x, y^p \rangle$. Desde que $S < K$, temos que S não é normal em G e, por isso, S é abeliano. Logo:

$$1 = [x, y^p].$$

Como $K = \langle x, y \rangle$ e $[x, y] \in Z(K)$, usando o Lema 1.3:

$$1 = [x, y^p] = [x, y]^p = [x^p, y].$$

Mas então $K' = \langle [x,y] \rangle$ tem ordem p e desde que $d(K) = 2$, pelo Teorema 1.15, concluímos que $K = \langle x \rangle^G$ é um p-grupo não abeliano minimal, como queríamos. $\square$

Teorema 3.4. *Seja G um p-grupo metahamiltoniano finito. Então $cl(G) \leq 3$. Em particular, G é metabeliano.*

Demonstração. Pelo teorema anterior, para todo elemento $x \in G$, $K = \langle x \rangle^G$ é abeliano ou não abeliano minimal. Então $K' = \{1\}$ ou $|K'| = p$.

Note que K' é normal em G, pois desde que K é normal em G:

$$[k_1, k_2]^g = [{k_1}^g, {k_2}^g] \in K', \text{ para todo } g \in G \text{ e } k_1, k_2 \in K.$$

Logo, pelo Teorema 1.5, $K' \leq Z(G)$.

Agora, seja $\overline{G} = G/Z(G)$. Então, para todo $\overline{x}$ em $\overline{G}$, $\langle \overline{x} \rangle^{\overline{G}}$ é abeliano. De fato, sejam $\overline{g}^{-1}\overline{x}^n\overline{g}$ e $\overline{q}^{-1}\overline{x}^m\overline{q} \in \langle \overline{x} \rangle^{\overline{G}}$, onde $\overline{g}, \overline{q} \in \overline{G}$ e m, n inteiros. Temos:

$$[g^{-1}x^n gZ(G), q^{-1}x^m qZ(G)] = \underbrace{[g^{-1}x^n g, q^{-1}x^m q]}_{\in K' \leq Z(G)} Z(G) = Z(G).$$

E, portanto, $[\overline{g}^{-1}\overline{x}^n\overline{g}, \overline{q}^{-1}\overline{x}^m\overline{q}] = \overline{1}$.

Além do mais, $\overline{G}$ satisfaz a segunda condição de Engel, pois para $\overline{g}, \overline{h} \in \overline{G}$, temos:

$$[\overline{g}, \overline{h}, \overline{h}] = [[\overline{g}, \overline{h}], \overline{h}] = \overline{1}, \text{ já que } \langle \overline{h} \rangle^{\overline{G}} \text{ é abeliano e } [\overline{g}, \overline{h}] \in \langle \overline{h} \rangle^{\overline{G}}.$$

Mas então, pelo Teorema 1.7, temos que $cl(\overline{G}) = 2$ para $p \neq 3$ e $cl(\overline{G}) \leq 3$ para $p = 3$. Observe, por exemplo, que se $cl(\overline{G}) \leq 3$, ao usarmos o Teorema 1.2 obtemos:

$$\overline{1} = \gamma_4\left(\frac{G}{Z(G)}\right) = \frac{\gamma_4(G)Z(G)}{Z(G)} \Rightarrow \gamma_4(G) \leq Z(G) \Rightarrow 1 = [\gamma_4(G), G] = \gamma_5(G) \Rightarrow cl(G) \leq 4.$$

Daí concluímos que $cl(G) \leq 3$ para $p \neq 3$ e $cl(G) \leq 4$ para $p = 3$.

Afirmamos que $cl(G) \leq 3$. Suponhamos que não, então, pelo argumento acima, $p = 3$. Considere ainda G um contra exemplo de ordem minimal, isto é, G é o 3-grupo metahamiltoniano de menor ordem, tal que $cl(G) > 3$. Diante do exposto acima, só poderemos ter $cl(G) = 4$.

Além disso, $|\gamma_4(G)| = p$. De fato, já temos que $\gamma_4(G) \neq \{1\}$. Suponha que $|\gamma_4(G)| \neq p$. Então existe $K < \gamma_4(G)$, tal que $K \neq \{1\}$. Como $[\gamma_4(G), G] = \gamma_5(G) = \{1\}$, temos que $\gamma_4(G) \leq Z(G)$ e, assim, K é normal em G. Agora, note que G/K é um quociente não abeliano de G, pois $G' \nleq K$. Daí, pelo Teorema 3.1, G/K é um p-grupo metahamiltoniano, tal que $|G/K| < |G|$. Mas então, pela minimalidade da ordem de G, temos que $cl(G/K) \leq 3$ e, consequentemente, $\gamma_4(G/K) = \{\overline{1}\}$. Assim,

$$\overline{1} = \gamma_4\left(\frac{G}{K}\right) = \frac{\gamma_4(G)}{K}.$$

Donde segue que $\gamma_4(G) = K$, uma contradição. Portanto, $|\gamma_4(G)| = p$.

Sendo assim, podemos assumir que $\gamma_4(G) = \langle [a, b, c, d] \rangle$, onde $a, b, c, d \in G \backslash \Phi(G)$. Sejam $x = [a, b, c]$ e $N = \langle x, d \rangle$. Note que $[x, d] \in Z(N)$. Logo, pela Observação 1.1, segue que $N' = \langle [x, d] \rangle$. Mas então, como N é 2-gerado e $N' = \gamma_4(G)$, pelo Teorema 1.15, N é não abeliano minimal.

Além disso, como todo subgrupo de G contendo N é normal, G/N é dedekindiano. E desde que $p = 3$, G/N é abeliano. Caso contrário, G/N seria hamiltoniano e, pelo Teorema 2.1, teria um subgrupo de ordem 2^3 isomorfo ao Q_8, o que claramente não é possível.

Uma vez que G/N é abeliano, segue que $G' \leq N$. Como $d \notin \Phi(G)$, temos $N \cap \Phi(G) < N$ e, por isso:

$$G' \leq N \cap \Phi(G) < N.$$

Daí obtemos que G' é abeliano, já que N é não abeliano minimal.

Além disso, pela identidade de Witt, temos o seguinte:

$$[c^{-1}, d^{-1}, [a, b]]^d [d, [a, b]^{-1}, c^{-1}]^{[a,b]} [[a, b], c, d]^{c^{-1}} = 1.$$

Note que $[c^{-1}, d^{-1}, [a, b]] = 1$, pois G' é abeliano. Também temos que $[d, [a, b]^{-1}, c^{-1}] = 1$, pois $d \in N$ e $[a, b]^{-1} \in G' < N$, logo $[d, [a, b]^{-1}] \in N' = \gamma_4(G) \leq Z(G)$. Então, resta-nos que:

$$[[a, b], c, d]^{c^{-1}} = 1 \Rightarrow [[a, b], c, d] = 1.$$

Mas então $\gamma_4(G) = \langle [a, b, c, d] \rangle = \{1\}$, contradição. Portanto, $cl(G) \leq 3$, como desejávamos.

Em particular, G é metabeliano, isto é, G' é abeliano. De fato, como $cl(G) \leq 3$, temos que $\gamma_4(G) = 1$. Logo, usando o Teorema 1.3:

$$[\gamma_2(G), \gamma_2(G)] \leq \gamma_4(G) = \{1\} \Rightarrow [\gamma_2(G), \gamma_2(G)] = 1,$$

e, portanto, $G' = \gamma_2(G)$ é abeliano. $\square$

3.3 Caracterização dos p-grupos metahamiltonianos finitos

Agora, utilizando as propriedades dos p-grupos metahamiltonianos finitos vistas na seção anterior, demonstraremos o teorema que caracteriza os p-grupos metahamiltonianos finitos.

Teorema 3.5. *Seja G um p-grupo não abeliano finito. G é metahamiltoniano se, e somente se, G' está contido em todo subgrupo não abeliano de G.*

Demonstração. Se G' está contido em todo subgrupo não abeliano de G, então todo subgrupo não abeliano de G é normal. Uma vez que G é não abeliano, concluímos que G é metahamiltoniano.

Reciprocamente, queremos mostrar que se G é metahamiltoniano, então G' está contido em todo subgrupo não abeliano de G. Mas uma vez que, pelo Teorema 1.16, todo p-grupo não abeliano é gerado por subgrupos não abelianos minimais, basta mostrarmos que G' está contido em todo subgrupo não abeliano minimal. Para tanto, vamos supor, por absurdo, que esta implicação é falsa e considerar G um contra exemplo de ordem minimal. Ou seja, G é um p-grupo metahamiltoniano de menor ordem, contendo um subgrupo não abeliano minimal N, tal que $G' \nleq N$. Pelo Teorema 1.15, sabemos que N é 2-gerado e, portanto, vamos considerar $N = \langle a, b\rangle$.

Desde que G é metahamiltoniano, N e os subgrupos contendo N são normais em G. Como G/N é não abeliano ($G' \nleq N$), temos que G/N é hamiltoniano e, portanto, G é um 2-grupo. Por isso, note que $|N'| = 2$. Além disso, pela minimalidade da ordem de G, segue que $G/N \cong Q_8$.

Sejam:

$$\frac{G}{N} = \langle xN, yN\rangle \ \text{ e } \ H = \langle x, y\rangle.$$

Temos:

$$G = HN, \quad \frac{H}{H \cap N} \cong Q_8 \ \text{ e } \ z := [x, y] \notin N.$$

De fato, como $G = \dot{\bigcup} gN$ e $G/N \cong Q_8$, temos:

$$G = N \,\dot{\cup}\, xN \,\dot{\cup}\, yN \,\dot{\cup}\, xyN \,\dot{\cup}\, x^2N \,\dot{\cup}\, x^3N \,\dot{\cup}\, x^2yN \,\dot{\cup}\, x^3yN.$$

Logo, se $g \in G$, então $g = x^i y^j n,$ onde $n \in N,$ e assim $g \in HN$. Daí segue a igualdade $G = HN$. Além disso, pelo Lema do Diamante, obtemos:

$$\begin{tikzcd}[column sep=small]
 & G = HN \arrow[dl, dash, shift left=0.5] \arrow[dl, dash, shift right=0.5] \arrow[dr, dash, shift left=0.5] \arrow[dr, dash, shift right=0.5] & \\
N \arrow[dr, dash, shift left=0.5] \arrow[dr, dash, shift right=0.5] & & H \arrow[dl, dash, shift left=0.5] \arrow[dl, dash, shift right=0.5] \\
 & H \cap N &
\end{tikzcd}$$

$$\frac{H}{H \cap N} \cong \frac{G}{N} \cong Q_8.$$

E, por último, $z \notin N$, pois caso contrário teríamos G/N abeliano, uma contradição.

Destacamos que como G é metahamiltoniano, pelo teorema anterior, temos $cl(G) \leq 3$, $\gamma_3(G) \leq Z(G)$ e G' abeliano. O mesmo vale para H e N, já que são subgrupos não abelianos de G e, portanto, também são metahamiltonianos.

Agora, verificaremos as seguintes afirmações:

$$(i)\ H \cap N \leq \Phi(H) \ \text{ e } \ (ii)\ H \cap N = \langle x^4, x^2y^2, x^2z \rangle^H.$$

(i) Como $H \cap N \trianglelefteq H$, pelo Teorema 1.11, temos que:

$$\frac{\Phi(H)(H \cap N)}{H \cap N} \leq \Phi\left(\frac{H}{H \cap N}\right) \cong \Phi(Q_8).$$

Sabemos que $|\Phi(Q_8)| = 2$, logo $\dfrac{\Phi(H)(H \cap N)}{H \cap N} = \{\overline{1}\}$ ou $\dfrac{\Phi(H)(H \cap N)}{H \cap N} = \Phi\left(\dfrac{H}{H \cap N}\right)$.
Se $\dfrac{\Phi(H)(H \cap N)}{H \cap N} = \{\overline{1}\}$, temos que $\Phi(H) \leq H \cap N$ e como $H' \leq \Phi(H)$, obtemos:

$$H' \leq \Phi(H) \leq H \cap N \leq N,$$

uma contradição, já que $z \notin N$. Resta-nos que $\dfrac{\Phi(H)(H \cap N)}{H \cap N} = \Phi\left(\dfrac{H}{H \cap N}\right)$, o que nos dá $H \cap N \leq \Phi(H)$, como afirmado.

(ii) Sabemos que $\dfrac{H}{H \cap N} \cong Q_8$, logo:

$$\begin{aligned}\frac{H}{H \cap N} =& \{H \cap N, x(H \cap N), y(H \cap N), x^2(H \cap N), x^3(H \cap N), xy(H \cap N), x^2y(H \cap N), \\ & x^3y(H \cap N)\}.\end{aligned}$$

Assim, $H \cap N$ é o fecho normal das relações definidoras de Q_8 e, portanto, $H \cap N = \langle x^4, x^2y^2, x^2z\rangle^H$.

Agora, como H é metahamiltoniano, pelo Teorema 3.3, $\langle x\rangle^H$ é abeliano ou não abeliano minimal. Uma vez que, pela Proposição 1.2, $\langle x\rangle^H = \langle z, x\rangle$, segue que $\langle z, x\rangle$ é abeliano ou não abeliano minimal. Por isso, $[z, x^2] = 1$. De modo análogo, obtemos $[z, y^2] = 1$. Com isso:

$$1 = [z, x^2] = [z, x][z, x]^x = [z, x]^2 \text{ e}$$

$$1 = [z, y^2] = [z, y][z, y]^y = [z, y]^2.$$

E então $exp(\gamma_3(G)) \leq 2$.

Observe que como H' é abeliano, z comuta com todo elemento em H' e z comuta com x^2 e y^2. Assim, desde que $\Phi(H) = \langle x^2, y^2, H'\rangle$, segue que $z \in Z(\Phi(H))$, isto é, $[\Phi(H), z] = 1$. Em particular, $[H \cap N, z] = 1$.

A seguir, deduziremos uma contradição em 5 casos.

Caso 1. $H \cap N = N = \langle a, b\rangle$.

Neste caso, $G = H = \langle x, y\rangle$. Como $[H \cap N, z] = 1$, temos $[N, z] = 1$.

Seja $M = \langle za, b\rangle$. Note que M é 2-gerado e $[za, b] \in Z(M)$. De fato, pois como

$$[za, b] = \underbrace{[z, b]^a}_{1, pois [N,z]=1.} [a, b] = [a, b],$$

temos que $[za, b] = [a, b]$ comuta com a, b e com za. Então:

$$M' = \langle [za, b]\rangle = \langle [a, b]\rangle = N'.$$

Assim, $|M'| = 2$ e, portanto, M é não abeliano minimal. Logo, $M \trianglelefteq G$ e G/M é dedekindiano. Desde que $z \notin M$, temos que $G' \nleq M$ e que G/M é não abeliano. Pela minimalidade da ordem de G, $H/M = G/M \cong Q_8$.

Mas então, como $H/H \cap N = H/N \cong Q_8$, obtemos que:

$$\langle za, b\rangle = M = \langle x^4, x^2y^2, x^2z\rangle^H = N = \langle a, b\rangle,$$

uma contradição, pois $z \notin N$.

Caso 2. $H \cap N < N$ e $H \cap N \nleq \Phi(N)$.

Neste caso, $H \cap N$ contém um gerador essencial de N. Sem perda de generalidade, vamos assumir que $a \in H \cap N$ e $b \notin H \cap N$. Logo, $[z, a] = 1$, já que $[H \cap N, z] = 1$. Além disso, observe que como N é não abeliano minimal, $H \cap N = \langle x^4, x^2y^2, x^2z \rangle^H$ é abeliano. Assim, usando que H' é abeliano:

$$1 = [x^2y^2, x^2z] = \underbrace{[x^2y^2, z]}_{z \in Z(\Phi(H))}[x^2y^2, x^2]^z = [x^2y^2, x^2] = [x^2, x^2]^{y^2}[y^2, x^2] = [y^2, x^2] \Rightarrow$$

$$[x^2, y^2] = 1.$$

Continuando os cálculos:

$$1 = [x^2, y^2] = [x^2, y][x^2, y]^y = [x, y]^x[x, y][x, y]^{xy}[x, y]^y = z^x z z^{xy} z^y.$$

Por outro lado, $z^x = z[z, y]$, $z^y = z[z, y]$ e $z^{xy} = z[z, xy] = z[z, y][z, x]^y = z[z, x][z, y]$. E substituindo estas relações na igualdade acima, obtemos:

$$1 = z^4[z, x]^2[z, y]^2 = z^4 \Rightarrow z^4 = 1,$$

Se $z^2 \neq 1$, então $\langle z^2 \rangle = \mho_1(H') = \langle h^2 \mid h \in H' \rangle$ é um subgrupo normal minimal de G. De fato, pois $\langle z^2 \rangle$ tem ordem 2 e é normal em G, já que:

$$\langle z^2 \rangle = \mho_1(H') \ char \ H' \ char \ H \Rightarrow \langle z^2 \rangle \ char \ H \trianglelefteq G \Rightarrow \langle z^2 \rangle \trianglelefteq G.$$

Mas então, pelo Corolário 1.1, $z^2 \in Z(G)$. Particularmente,

$$1 = [z^2, b] = \underbrace{[z, b]^z}_{\gamma_3(G) \leq Z(G)} [z, b] = [z, b]^2.$$

Subcaso 2.1. $[z, b] \neq [a, b]$.

Seja $M = \langle za, b \rangle$. Temos o seguinte:

$$[za, b] = [z, b]^a[a, b] = [z, b][a, b] \neq 1 \ \text{ e } \ [za, b]^2 = [z, b]^2[a, b]^2 = 1.$$

Além disso, como $M' = \langle [za, b] \rangle$, temos que $|M'| = 2$ e, portanto, M é não abeliano minimal. Logo, G/M é dedekindiano. Como $z \notin M$, temos G/M não abeliano e pela minimalidade da ordem de G, temos $G/M \cong Q_8$.

$$\begin{tikzcd}
& G = HM \arrow[dl, equal] \arrow[dr, equal] & \\
M \arrow[dr, equal] & & H \arrow[dl, equal] \\
& H \cap M &
\end{tikzcd}$$

$$\frac{G}{M} = \frac{HM}{M} \cong \frac{H}{H \cap M} \cong Q_8.$$

Mas então:

$$H \cap M = \langle x^4, x^2y^2, x^2z\rangle^H = H \cap N.$$

Mas $a \in H \cap N = H \cap M \leq M$ e com isso $z = (za)a^{-1} \in M$, uma contradição.

Subcaso 2.2. $[z, b] = [a, b]$.

Seja $L = \langle z, b\rangle \cap N$. Como N é normal em G e $\langle z, b\rangle$ é não abeliano minimal e, portanto, normal em G, segue que L é normal em G.

Note que como $a \notin L$, temos que $L < N$ e assim L é um maximal ou está contido em algum maximal. Seja K um subgrupo maximal de N contendo L e tal que K é normal em G.

Como $|G/N| = 2^3$ e $[N : K] = 2$, temos que $|G/K| = 2^4$. Além disso, G/K é não abeliano, tem dois geradores e possui um quociente isomorfo ao Q_8. De fato, primeiramente note que $N = \langle a\rangle K$, caso contrário, teríamos $K < \langle a\rangle K < N$, o que contraria a maximalidade de K. Assim:

$$\begin{tikzcd}
& N = \langle a\rangle K \arrow[dl, equal, "2"'] \arrow[dr, dash] & \\
K \arrow[dr, dash] & & \langle a\rangle \arrow[dl, equal, "2"] \\
& \langle a\rangle \cap K = \{1\} &
\end{tikzcd}$$

Logo,

$$G = HN = H\langle a\rangle K \underbrace{=}_{a \in H \cap N} HK$$

e temos $G/K = HK/K = \langle xK, yK\rangle$. Uma vez que $G' \nleq K$, temos que G/K é não abeliano. Por último, como N/K é normal em G/K, temos:

$$\frac{G/K}{N/K} \cong \frac{G}{N} \cong Q_8.$$

Sendo assim, pelo Teorema 1.19, que nos dá a classificação dos grupos não abelianos de ordem 2^4:

$$\frac{G}{K} = \langle xK, yK\rangle = \langle \overline{x}, \overline{y}\rangle \cong M_2(2, 2),$$

onde $M_2(2, 2) = \langle \overline{x}, \overline{y} \mid \overline{x}^4 = \overline{y}^4 = 1, \overline{x}^{\overline{y}} = \overline{x}^3\rangle$.

Agora, vamos mostrar que o conjugado $\overline{y}^{\overline{x}} \notin \langle \overline{y} \rangle$ e, portanto, $\langle \overline{y} \rangle$ não é normal em G/K. Como $o(\overline{y}) = 4$, segue que $\langle \overline{y} \rangle = \{\overline{1}, \overline{y}, \overline{y}^2, \overline{y}^3\}$ e, assim, temos as seguintes possibilidades para $\overline{y}^{\overline{x}}$:

$$\overline{y}^{\overline{x}} = \overline{1},\ \overline{y},\ \overline{y}^2 \text{ ou } \overline{y}^3.$$

Mas usando as relações em G/K, temos que:
Se $\overline{x}^{-1}\overline{yx} = \overline{1}$, então $\overline{y} = \overline{1}$, absurdo, já que $o(\overline{y}) = 4$.
Se $\overline{x}^{-1}\overline{yx} = \overline{y}$, então $\overline{yx} = \overline{xy}$, absurdo, já que G/K é não abeliano.
Se $\overline{x}^{-1}\overline{yx} = \overline{y}^2$, então $\overline{x}^2 = \overline{y}$, absurdo, já que $o(\overline{y}) = 4$.
Se $\overline{x}^{-1}\overline{yx} = \overline{y}^3$, então $\overline{x}^2 = \overline{y}^2$, absurdo, pois $M_2(2,2) \ncong Q_8$.

Portanto, $\overline{y}^{\overline{x}} \notin \langle \overline{y} \rangle$ e $\langle \overline{y} \rangle$ não é normal em G/K, como afirmado. Procedendo de forma análoga, obtemos que $\langle \overline{xy} \rangle$ não é normal em G/K.

Uma vez que $\langle \overline{y} \rangle$ e $\langle \overline{xy} \rangle$ não são normais em G/K, suas imagens inversas também não são normais em G e, por isso, $\langle y, K \rangle$ e $\langle xy, K \rangle$ são abelianos. Logo:

$$[y, K] = 1 \text{ e } 1 = [xy, K] = [x, K]^y [y, K] \Rightarrow [x, K] = 1.$$

Daí segue que $[H, K] = 1$, absurdo, pois contraria nossa hipótese de que $[z, b] = [a, b] \neq 1$.

Caso 3. $H \cap N < \Phi(N)$.

Primeiramente, afirmamos que $H \cap N \neq 1$. Suponhamos que não, então $G = H \times N$.

$$\begin{tikzcd}
 & G = HN \arrow[dl, equal] \arrow[dr, equal] & \\
N \arrow[dr, equal] & & H \arrow[dl, equal] \\
 & H \cap N = \{1\} &
\end{tikzcd}$$

Desde que $N \cong G/H$ é dedekindiano, temos $N \cong Q_8$. Logo, $N = \langle a, b \rangle \cong Q_8$, isto é:

$$N = \langle a, b \mid a^4 = 1,\ a^2 = b^2,\ [a, b] = a^2 \rangle = \{1, a, a^2, a^3, b, ab, a^2b, a^3b\}.$$

Por outro lado, observe que como $\langle x^4, x^2y^2, x^2[x, y] \rangle^H = H \cap N = \{1\}$, temos:

$$x^4 = 1, \quad x^2y^2 = 1 \Rightarrow x^2 = y^2 \ \text{ e } \ [x, y] = x^2.$$

Assim $H = \langle x, y \rangle \cong Q_8$.

Agora, considere $\langle xa, yb\rangle \leq G$. Usando as relações de N e H, obtemos que $\langle xa, yb\rangle \cong Q_8$, pois:

$$(xa)^4 = x^4a^4 = 1 = y^4b^4 = (yb)^4,$$

$$(xa)^2(yb)^2 = a^2x^2y^2b^2 = 1 \Rightarrow (xa)^2 = (yb)^2 \quad \text{e}$$

$$[xa, yb] = [xa, b][xa, y]^b = [x, b]^a[a, b][x, y]^{ab}[a, y]^b = [a, b][x, y] = [x, y][a, b] = x^2a^2 = (xa)^2.$$

Mas, note que

$$\langle xa, yb\rangle = \{1, (xa), (xa)^2, (xa)^3, (yb), (xa)(yb), (xa)(yb), (xa)^2(yb), (xa)^3(yb)\}$$

não é normal em G. Para comprovarmos, mostraremos que o conjugado $b^{-1}(ax)b = a^3x \notin \langle xa, yb\rangle$. Assim, tendo em vista a apresentação de $\langle xa, yb\rangle$, temos as seguintes possibilidades para $b^{-1}(ax)b = a^3x$:

- Se $a^3x = 1$, então $x = a$, absurdo, pois $[x, y] \neq 1$.
- Se $a^3x = ax$, então $a^2 = 1$, absurdo, pois $o(a) = 4$.
- Se $a^3x = a^2x^2$, então $a = x$, absurdo, pois $[x, y] \neq 1$.
- Se $a^3x = a^3x^3$, então $x^2 = 1$, absurdo, pois $o(a) = 4$.
- Se $a^3x = by$, então $ba = yx$, absurdo, pois $[x, y] \neq 1$.
- Se $a^3x = (xa)(yb)$, então $a^2b^{-1} = y$, absurdo, pois $[x, y] \neq 1$.
- Se $a^3x = (xa)^2(by)$, então $ab^{-1} = xy$, absurdo, pois $[x, y] \neq 1$.
- Se $a^3x = (xa)^3(by)$, então $b^{-1} = x^2y$, absurdo, pois $[x, y] \neq 1$.

Mas então $b^{-1}(ax)b = a^3x \notin \langle xa, yb\rangle$ e, portanto, $\langle xa, yb\rangle$ não é normal em G, uma contradição, já que $Q_8 \cong N$ e N é normal em G. Com isso, $H \cap N \neq 1$.

Também afirmamos que $N' \leq H \cap N$. Suponhamos que não, isto é, $N' \nleq H \cap N$, então o quociente $G/H \cap N$ é também um contra exemplo e contraria a minimalidade da ordem de G. De fato, note que $G/H \cap N$ é não abeliano, pois $G' \nleq H \cap N$. Logo, $G/H \cap N$ é metahamiltoniano. Mas se $N' \nleq H \cap N$, então $N/H \cap N$ é um subgrupo não abeliano de $G/H \cap N$ e, por isso, $N/H \cap N$ é normal em $G/H \cap N$. Mas,

$$\frac{G/H \cap N}{N/H \cap N} = \frac{G}{N} \cong Q_8$$

é não abeliano e assim $(G/H\cap N)' \nleq N/H\cap N$. Ou seja, $G/H\cap N$ é um metahamiltoniano com ordem menor que a ordem de G, contendo um subgrupo não abeliano $N/H\cap N$, tal que $(G/H\cap N)' \nleq N/H\cap N$, uma contradição. Por isso, $N' \leq H\cap N$.

Sejam:

$$\overline{G} = \frac{G}{H\cap N}, \quad \overline{H} = \frac{H}{H\cap N} = \langle \overline{x}, \overline{y}\rangle \ \text{ e } \ \overline{N} = \frac{N}{H\cap N} = \langle \overline{a}\rangle \times \langle \overline{b}\rangle.$$

Temos $\overline{G} = \overline{H}\times\overline{N}$. Note que $\overline{N}$ é abeliano, pois $N' \leq H\cap N$. Além disso, $exp(\overline{N}) \geq 4$, já que não podemos ter simultaneamente $\overline{a}^2 = \overline{b}^2 = \overline{1}$. De fato, suponhamos que $\overline{a}^2 = \overline{b}^2 = \overline{1}$. Então $\overline{N}$ é um 2-grupo abeliano elementar e, portanto, $\Phi(N) \leq H\cap N$, donde concluímos que $\Phi(N) = H\cap N$, contrariando nossa hipótese. Sendo assim, podemos assumir, sem perda de generalidade, que $o(\overline{a}) = 4$.

Agora, considere $\overline{K} = \langle \overline{xa}\rangle \times \langle \overline{b}\rangle$. Sem perda de generalidade, podemos supor $o(\overline{b}) = 2$. E como $\overline{H} \cong Q_8$, temos $o(\overline{x}) = 4$. Portanto, temos que:

$$C_4 \times C_2 \cong \overline{K} = \{\overline{1}, (\overline{xa}), (\overline{xa})^2, (\overline{xa})^3, \overline{b}, \overline{xab}, (\overline{xa})^2\overline{b}, (\overline{xa})^3\overline{b}\}.$$

Afirmamos que $\overline{K}$ não é normal em $\overline{G}$. Para comprovarmos a afirmação, vamos mostrar que o conjugado $(\overline{xa})^{\overline{y}} \notin \overline{K}$. De fato, pois temos as seguintes possiblidades para $(\overline{xa})^{\overline{y}} = \overline{x}^3\overline{a}$:

- Se $\overline{x}^3\overline{a} = \overline{1}$, então $\overline{x} = \overline{a}$, absurdo, pois $[\overline{x}, \overline{y}] \neq 1$.
- Se $\overline{x}^3\overline{a} = \overline{xa}$, então $\overline{x}^2 = 1$, absurdo, pois $o(\overline{x}) = 4$.
- Se $\overline{x}^3\overline{a} = (\overline{xa})^2$, então $\overline{x} = \overline{a}$, absurdo, $[\overline{x}, \overline{y}] \neq 1$.
- Se $\overline{x}^3\overline{a} = (\overline{xa})^3$, então $\overline{a}^2 = \overline{1}$, absurdo, pois $o(\overline{a}) = 4$.
- Se $\overline{x}^3\overline{a} = \overline{xab}$, então $[\overline{x}, \overline{y}] = \overline{b}$ e, assim, $[\overline{x}, \overline{y}] \in \overline{H}\cap\overline{N}$. Logo, $[\overline{x}, \overline{y}] = \overline{1}$, absurdo, pois $[x, y] \notin N$.
- Se $\overline{x}^3\overline{a} = (\overline{xa})^2\overline{b}$, então $\overline{x} = \overline{ba}$, absurdo, pois $[\overline{x}, \overline{y}] \neq 1$.
- Se $\overline{x}^3\overline{a} = (\overline{xa})^3\overline{b}$, então $\overline{a}^2 = \overline{b}$, absurdo, pois $\overline{N} \neq \langle \overline{a}\rangle$.

Portanto, $\overline{K}$ não é normal em $\overline{G}$, como afirmado. Mas se $\overline{K}$ não é normal em $\overline{G}$, sua imagem inversa também não é normal em G e, por isso:

$$1 = [xa, b] = [x, b]^a[a, b] \Rightarrow [x, b] = [b, a^{-1}].$$

Note que $[b, a^{-1}] \neq 1$, caso contrário, teríamos $[a, b] = 1$, um absurdo. Analogamente, obtemos $[y, b] = [b, a^{-1}]$ e $[xy, b] = [b, a^{-1}]$. E, finalmente, chegamos que:

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

uma contradição.

Caso 4. $H \cap N = \Phi(N) = N'$.

Neste caso,

$$|N| = 2^3, \quad |H| = 2^4 \ \text{ e } \ |G| = 2^6.$$

De fato, como $|H \cap N| = |N'| = 2$:

$$\begin{tikzcd}[column sep=small]
 & G = HN \arrow[dl, dash, "2^3"'] \arrow[dr, dash, "2^2"] & \\
N \arrow[dr, dash, "2^2"'] & & H \arrow[dl, dash, "2^3"] \\
 & H \cap N = N' &
\end{tikzcd}$$

Temos ainda que:

$$\frac{G}{N'} = \frac{HN}{N'} = \frac{H}{N'} \times \frac{N}{N'} = \frac{H}{N'} \times \langle aN' \rangle \times \langle bN' \rangle,$$

já que $N/N' = N/\Phi(N)$ é abeliano elementar.

Desde que $\langle aN' \rangle$ e $\langle bN' \rangle$ são normais em G/N', suas imagens inversas, $A = \langle a, N' \rangle$ e $B = \langle b, N' \rangle$ também são normais em G.

Vamos verificar que A e B são grupos de Klein. De fato, sabemos que $\mho_1(N)N' = \Phi(N)$ e, por hipótese, temos que $\Phi(N) = N'$. Logo, $\mho_1(N) \leq N'$. Sendo assim, temos que $a^2 \in N' = \langle [a, b] \rangle$. Desde que $|N'| = 2$, temos que:

$$a^2 = 1 \ \text{ ou } \ a^2 = [a, b].$$

Se $a^2 = 1$, então $A = \langle a, N' \rangle = \{1, a, [a, b], a[a, b]\}$. Note que A é um grupo de ordem 4, cujos elementos não triviais tem ordem 2, isto é, A é um grupo de Klein.
Se $a^2 = [a, b]$, da mesma forma, temos que $A = \langle a, N' \rangle = \{1, a, [a, b], a[a, b]\}$ e mais uma vez obtemos que A é um grupo de Klein.

Portanto, A é um grupo de Klein, como afirmamos. Analogamente, obtemos que B também é um grupo de Klein.

Afirmamos que $C_G(A)$ é maximal em G. De fato, como A é normal em G, temos $G = N_G(A)$ e, pelo Teorema do Normalizador-Centralizador, segue que: $N_G(A)/C_G(A) = G/C_G(A)$ é isomorfo a um subgrupo do $Aut(A)$. Mas, como A é um grupo de Klein, pelo Exemplo 1.1, temos que $Aut(A) \cong S_3$. Agora, desde que $G/C_G(A)$ é um 2-grupo, só poderemos ter $[G : C_G(A)] = 2$, donde concluímos que $C_G(A)$ é maximal. Da mesma forma, obtemos $C_G(B)$ maximal.

Seja $K = C_G(A) \cap C_G(B)$. Temos:

$$\begin{tikzcd}[column sep=small]
 & G = C_G(A)C_G(B) \arrow[dl, dash, shift left=0.5, "2"'] \arrow[dl, dash, shift right=0.5] \arrow[dr, dash, shift left=0.5, "2"] \arrow[dr, dash, shift right=0.5] & \\
C_G(A) \arrow[dr, dash, shift left=0.5] \arrow[dr, dash, shift right=0.5, "2"'] & & C_G(B) \arrow[dl, dash, shift left=0.5, "2"] \arrow[dl, dash, shift right=0.5] \\
 & K &
\end{tikzcd}$$

Assim, $|K| = 2^4$.

Vamos verificar que $K \cap N = Z(N) = N'$. De fato, se $c \in K \cap N$, então $c \in K$ e, assim, $c \in C_G(A)$ e $c \in C_G(B)$, ou seja, c comuta com os elementos em A e em B. Mas daí segue que c comuta com os elementos a e b, implicando que $c \in Z(N)$. Reciprocamente, seja $c \in Z(N)$. Note que $c \in K$, pois c comuta com $A < N$ e c comuta com $B < N$ e, assim, $c \in K \cap N$. Como N é não abeliano minimal, temos que $Z(N) = \Phi(N) = N'$, o que confirma $K \cap N = Z(N) = N'$.

Temos:

$$|KN| = \frac{|K||N|}{|K \cap N|} = \frac{2^4.2^3}{2} = 2^6.$$

Daí concluímos que $G = KN$. Além disso, $[K, N] = 1$, pois $[K, a] = 1$ e $[K, b] = 1$. Agora, desde que:

$$\begin{tikzcd}[column sep=small]
 & G = KN \arrow[dl, dash, shift left=0.5] \arrow[dl, dash, shift right=0.5] \arrow[dr, dash, shift left=0.5] \arrow[dr, dash, shift right=0.5] & \\
N \arrow[dr, dash, shift left=0.5] \arrow[dr, dash, shift right=0.5] & & K \arrow[dl, dash, shift left=0.5] \arrow[dl, dash, shift right=0.5] \\
 & K \cap N = N' &
\end{tikzcd}$$

Temos:

$$\frac{G}{N} = \frac{KN}{N} \cong \frac{K}{K \cap N} \cong Q_8.$$

Então, sem perda de generalidade, podemos assumir $H = K$. Afirmamos que:

$$(i) \quad H = \langle x, y \rangle \cong M_2(2,2) \;\text{ e }\; (ii) \quad N' = H \cap N = \langle x^2y^2 \rangle.$$

(i) Note primeiramente que H é um grupo não abeliano de ordem 2^4. Além disso, H tem dois geradores e possui um grupo quociente, $H/H \cap N$, isomorfo ao Q_8. Logo, pela classificação dos grupos de ordem 2^4, obtemos que $H = \langle x, y \rangle \cong M_2(2,2)$ e, portanto:

$$x^4 = y^4 = 1 \quad \text{e} \quad [x, y] = x^2.$$

(ii) Já sabemos que $N' = H \cap N = \langle x^4, x^2y^2, x^2[x, y] \rangle^H$ e uma vez que $[H, N] = 1$, segue que $N' = H \cap N = \langle x^4, x^2y^2, x^2[x, y] \rangle$. Usando as relações de $H \cong M_2(2,2)$, obtemos:

$$x^4 = 1 \quad \text{e} \quad x^2[x, y] = x^4 = 1,$$

e, portanto, $N' = H \cap N = \langle x^2y^2 \rangle$, como afirmado.

Agora, sem perda de generalidade, podemos assumir que $o(a) = 4$. Então $a^2 \neq 1$ e $a^2 \in N' = \langle x^2y^2 \rangle$, logo $a^2 = x^2y^2$. Temos:

$$[x, ay] = [x, y][x, a]^y = [x, y] = x^2, \quad \text{já que} \quad [H, N] = 1.$$

E

$$(ay)^2 = a^2y^2 = x^2 \;\text{ e }\; x^4 = (ay)^4 = 1.$$

Daí segue que $\langle x, ay \rangle \cong Q_8$, isto é,

$$\langle x, ay \rangle = \{1, x, x^2, x^3, ay, xay, x^2ay, x^3ay\}.$$

Logo, $\langle x, ay \rangle$ não é abeliano. Afirmamos que $\langle x, ay \rangle$ também não é normal, pois veremos que o conjugado $(ay)^b = a^by \notin \langle x, ay \rangle$. De fato, temos as seguintes possibilidades:

- Se $a^by = 1$, então $y = ba^{-1}b^{-1} \Rightarrow [x, y] = 1$, absurdo.
- Se $a^by = x$, então $b^{-1}ab = xy^{-1} \Rightarrow [xy^{-1}, x] = 1 \Rightarrow [x, y] = 1$, absurdo.
- Se $a^by = x^2$, então $b^{-1}ab = x^2y^{-1} \Rightarrow [x^2y^{-1}, x] = 1 \Rightarrow [x, y] = 1$,absurdo.
- Se $a^by = x^3$, então $x^3y^{-1} = a^b \Rightarrow [x^3y^{-1}, x] = 1 \Rightarrow [x, y] = 1$, absurdo.
- Se $a^by = ay$, então $ab = ba$, absurdo.
- Se $a^by = xay$, então $a^ba^{-1} = x \Rightarrow [x, y] = 1$, absurdo.

- Se $a^b y = x^2 ay$, então $a^b a^{-1} = x^2 \Rightarrow [x,y] = z \in N$, absurdo.

- Se $a^b y = x^3 ay$, então $a^b a^{-1} = x^3 = x^{-1} \Rightarrow [x^{-1}, y] = 1 \Rightarrow [x,y] = 1$, absurdo.

Portanto, $\langle x, ay \rangle$ não é nem abeliano nem normal em G, uma contradição.

Caso 5. $H \cap N = \Phi(N) \neq N'$.

Sejam:

$$\overline{G} = \frac{G}{K}, \quad \overline{H} = \frac{H}{K} = \langle \overline{x}, \overline{y} \rangle \ \text{ e } \ \overline{N} = \frac{N}{K} = \langle \overline{a} \rangle \times \langle \overline{b} \rangle,$$

onde K é um subgrupo maximal de $H \cap N$, tal que $K \trianglelefteq G$.

Temos $|\overline{G}| = 2^6$, $\ |\overline{H}| = 2^4\ $ e $\ |\overline{N}| = 2^3$, pois:

$$\begin{tikzcd}
 & G = HN \arrow[dl, dash, "2^2"'] \arrow[dr, dash, "2^3"] & \\
H \arrow[dr, dash, "2^3"'] & & N \arrow[dl, dash, "2^2"] \\
 & H \cap N = \Phi(N) \arrow[d, dash, "2"] & \\
 & K &
\end{tikzcd}$$

Uma vez que $\overline{G}$ é não abeliano ($G' \nleq K$), segue que $\overline{G}$ é metahamiltoniano. Então, pela minimalidade da ordem de G, $\overline{G}'$ está contido em todo subgrupo não abeliano minimal de $\overline{G}$ e, portanto, $\overline{G}'$ está contido em todo subgrupo não abeliano de $\overline{G}$. Como $\overline{G}/\overline{N} \cong G/N \cong Q_8$ é não abeliano, temos que $\overline{G}' \nleq \overline{N}$ e, assim, $\overline{N}$ é abeliano. Por isso, podemos supor, sem perda de generalidade que $o(\overline{a}) = 4$.

Note que $\overline{H}$ é um grupo não abeliano de ordem 2^4, gerado por dois elementos e contendo um subgrupo quociente, $H/(H \cap N)$, isomorfo ao Q_8. Então, pela classificação dos grupos de ordem 2^4, $\overline{H} \cong M_2(2,2)$ e, assim:

$$\overline{x}^4 = \overline{y}^4 = \overline{1} \quad e \quad [\overline{x}, \overline{y}] = \overline{x}^2.$$

Além disso,

$$(i)\ \ \overline{a}^2 = \overline{x}^2 \overline{y}^2 \quad \text{e} \quad (ii)\ \ [\overline{H}, \overline{N}] \leq \overline{H} \cap \overline{N} = \frac{\Phi(N)}{K} = \frac{H \cap N}{K} = \langle \overline{x}^2 \overline{y}^2 \rangle.$$

(i) Desde que $\overline{H} \cong M_2(2,2)$, temos que $\overline{x}^2$, $\overline{y}^2 \in Z(\overline{H})$ e, assim, $\langle \overline{x}^2\overline{y}^2 \rangle \in Z(\overline{H})$. Além disso, temos $(\overline{x}^2\overline{y}^2)^2 = \overline{x}^2\overline{y}^2\overline{x}^2\overline{y}^2 = \overline{x}^4\overline{y}^4 = \overline{1}$, isto é, $o(\overline{x}^2\overline{y}^2) = 2$. Portanto, usando as relações em $\overline{H}$ chegamos em $\overline{H} \cap \overline{N} = \langle \overline{x}^2\overline{y}^2 \rangle$.

Agora, como $\Phi(N) = N'\mho_1(N)$, temos que $a^2 \in \Phi(N)$ e $a^2 \notin K$, pois $\overline{a}^2 \neq \overline{1} \in \overline{N}$. Mas então

$$\overline{a}^2 \in \frac{\Phi(N)}{K} = \frac{H \cap N}{K} = \overline{H} \cap \overline{N} = \langle \overline{x}^2\overline{y}^2 \rangle.$$

Como $\overline{a}^2 \neq 1$, só poderemos ter $\overline{a}^2 = \overline{x}^2\overline{y}^2$.

(ii) Seja $[\overline{h}, \overline{n}] \in [\overline{H}, \overline{N}]$, com $\overline{h} \in \overline{H}$ e $\overline{n} \in \overline{N}$. Então $[\overline{h}, \overline{n}] \in \overline{H}$ e $[\overline{h}, \overline{n}] \in \overline{N}$, já que H e N são normais em G. Logo, $[\overline{h}, \overline{n}] \in \overline{H} \cap \overline{N}$, donde segue que $[\overline{H}, \overline{N}] \leq \overline{H} \cap \overline{N}$. Assim:

$$[\overline{H}, \overline{N}] \leq \overline{H} \cap \overline{N} = \frac{\Phi(N)}{K} = \frac{H \cap N}{K} = \langle \overline{x}^2\overline{y}^2 \rangle,$$

como afirmado. E uma vez que $|\langle \overline{x}^2\overline{y}^2 \rangle| = 2$, temos as seguintes possibilidades:

Subcaso 5.1 $[\overline{H}, \overline{N}] = \{\overline{1}\}$.

Neste subcaso, veremos que $\langle \overline{y}, \overline{b} \rangle$, $\langle \overline{xy}, \overline{b} \rangle$ e $\langle \overline{ax}, \overline{b} \rangle$ não são normais em G.

Primeiramente, note que como $\overline{y}^4 = \overline{1}$ e $\overline{b}^2 = \overline{1}$, temos o seguinte:

$$C_4 \times C_2 = \langle \overline{y}, \overline{b} \rangle = \{\overline{1}, \overline{y}, \overline{y}^2, \overline{y}^3, \overline{b}, \overline{y}\overline{b}, \overline{y}^2\overline{b}, \overline{y}^3\overline{b}\}.$$

Afirmamos que o conjugado $\overline{y}^{\overline{x}} \notin \langle \overline{y}, \overline{b} \rangle$ e, portanto, $\langle \overline{y}, \overline{b} \rangle$ não é normal em $\overline{G}$. De fato, temos as seguintes possibilidades:

- Se $\overline{x}^{-1}\overline{yx} = \overline{1}$, então $\overline{y} = \overline{1}$, absurdo.
- Se $\overline{x}^{-1}\overline{yx} = \overline{y}$, então $\overline{yx} = \overline{xy}$, absurdo.
- Se $\overline{x}^{-1}\overline{yx} = \overline{y}^2$, então $[\overline{y}, \overline{x}] = \overline{y} \Rightarrow \overline{x}^2 = \overline{y}$, absurdo.
- Se $\overline{x}^{-1}\overline{yx} = \overline{y}^3$, então $[\overline{x}, \overline{y}] = \overline{y}^2 \Rightarrow \overline{x}^2 = \overline{y}^2$, absurdo, pois $M_2(2,2) \ncong Q_8$.
- Se $\overline{x}^{-1}\overline{yx} = \overline{b}$, então $\overline{yx} = \overline{x}\overline{b} = \overline{b}\overline{x} \Rightarrow \overline{y} = \overline{b} \Rightarrow [\overline{x}, \overline{y}] = \overline{1}$, absurdo.
- Se $\overline{x}^{-1}\overline{yx} = \overline{y}\overline{b}$, então $[\overline{y}, \overline{x}] = \overline{b} \Rightarrow \overline{x}^2 = [\overline{x}, \overline{y}] = \overline{b} \Rightarrow [\overline{x}, \overline{y}] \in \overline{H} \cap \overline{N}$, absurdo.
- Se $\overline{x}^{-1}\overline{yx} = \overline{y}^2\overline{b}$, então $\overline{y}^{-1}[\overline{y}, \overline{x}] = \overline{b} \Rightarrow [\overline{y}^{-1}\overline{x}^2, \overline{x}] = \overline{1} \Rightarrow [\overline{x}, \overline{y}] = \overline{1}$, absurdo.

- Se $\overline{x}^{-1}\overline{yx} = \overline{y}^3\overline{b}$, então $\overline{yx}^{-1}\overline{yx} = \overline{b} \Rightarrow \overline{x}^2\overline{y}^2 = \overline{b}$, logo $\overline{a}^2 = \overline{b}$, absurdo, pois $\overline{N} \neq \langle \overline{a} \rangle$.

Portanto, $\langle \overline{y}, \overline{b} \rangle$ não é normal em $\overline{G}$. De maneira análoga, obtemos que $\langle \overline{xy}, \overline{b} \rangle$ e $\langle \overline{ax}, \overline{b} \rangle$ também não são normais em $\overline{G}$. Assim, segue que as imagens inversas de $\langle \overline{y}, \overline{b} \rangle$, $\langle \overline{xy}, \overline{b} \rangle$ e $\langle \overline{ax}, \overline{b} \rangle$ também não são normais em G e, por isso,

$$[y, b] = 1, \quad [xy, b] = 1 \ \ e \ \ [ax, b] = 1.$$

Assim:

$$1 = [xy, b] = [x, b]^y[y, b] = [x, b] \ \text{ e } \ 1 = [ax, b] = [a, b]^x[x, b] = [a, b],$$

uma contradição.

Subcaso 5.2 $[\overline{H}, \overline{N}] = \langle \overline{x}^2\overline{y}^2 \rangle$.

Temos que se $\overline{a} = Z(\overline{G})$, então $[\overline{H}, \overline{b}] = \langle \overline{x}^2\overline{y}^2 \rangle$, já que $[\overline{H}, \overline{a}] = \overline{1}$. Mas então $\langle \overline{x}, \overline{ay} \rangle$ não é abeliano e não é normal em $\overline{G}$. De fato, como:

$$\overline{x}^4 = \overline{a}^4\overline{y}^4 = \overline{1}, \quad [\overline{x}, \overline{ay}] = [\overline{x}, \overline{y}]\underbrace{[\overline{x}, \overline{a}]^{\overline{y}}}_{1} = \overline{x}^2 \ \text{ e } \ \overline{x}^2\overline{a}^2\overline{y}^2 = \overline{1} \Rightarrow \overline{x}^2 = \overline{a}^2\overline{y}^2.$$

Segue que $\langle \overline{x}, \overline{ay} \rangle \cong Q_8$ e, por isso, $\langle \overline{x}, \overline{ay} \rangle$ é não abeliano. E, por outro lado, procedendo da mesma forma que nos casos anteriores, obtemos que $\langle \overline{x}, \overline{ay} \rangle$ também não é normal em $\overline{G}$, uma contradição. Por isso, $\overline{a} \notin Z(\overline{G})$.

Se $[\overline{a}, \overline{x}] = \overline{1}$, então $[\overline{a}, \overline{y}] = \overline{x}^2\overline{y}^2$ e novamente obtemos que $\langle \overline{ax}, \overline{y} \rangle$ não é abeliano e não é normal em $\overline{G}$, uma contradição.

Por isso, $[\overline{a}, \overline{x}] = \overline{x}^2\overline{y}^2$. E pelo mesmo motivo, obtemos que $[\overline{ab}, \overline{x}] = \overline{x}^2\overline{y}^2$. Daí segue que $[\overline{b}, \overline{x}] = \overline{1}$. Neste caso, obtemos que $\langle \overline{x}, \overline{b} \rangle$ e $\langle \overline{ax}, \overline{b} \rangle$ não são normais em $\overline{G}$. Mas então, suas imagens inversas também não são normais em G e, portanto:

$$[x, b] = 1 \quad \text{ e } \quad [ax, b] = 1,$$

o que implica em $[a, b] = 1$, uma contradição.

Assim, concluímos que se G é um p-grupo metahamiltoniano finito, então G' está contido em todo subgrupo não abeliano de G e o teorema está demonstrado.

$\square$

Considerações Finais

Destacamos que as propriedades de p-grupos metahamiltonianos finitos aqui trabalhadas e mais algumas em [1] foram essenciais para que L. J. An e X. G. Fang desenvolvessem o teorema de classificação dos p-grupos metahamiltonianos finitos, cujo enunciado veremos abaixo. A classificação completa pode ser vista em [2], um artigo ainda a ser publicado.

Teorema 3.6. *Suponha que G é um p-grupo finito. Então G é metahamiltoniano se, e somente se, G é isomorfo a um dos seguintes grupos não isomorfos:*

(A) G é tal que $|G'| = p$.

(B) $exp(G') = p$ e $cl(G) = 3$. Neste caso, p é ímpar, $d(G) = 2$ e todos subgrupos de índice 2 em G são abelianos.

(Bi) G tem um subgrupo abeliano de índice p.

(B1) $\langle a_1, b \mid a_1^p = a_2^p = a_3^p = b^{p^m} = 1, [a_1, b] = a_2, [a_2, b] = a_3, [a_3, b] = 1, [a_i, a_j] = 1\rangle$, onde $p \geq 5$ para $m = 1$, $p \geq 3$ e $1 \leq i, j \leq 3$.

(B2) $\langle a_1, b \mid a_1^p = a_2^p = b^{p^{m+1}} = 1, [a_1, b] = a_2, [a_2, b] = b^{p^m}, [a_1, a_2] = 1\rangle$, onde $p \geq 3$.

(B3) $\langle a_1, b \mid a_1^{p^2} = a_2^p = b^{p^m} = 1, [a_1, b] = a_2, [a_2, b] = a_1^{\nu p}, [a_1, a_2] = 1\rangle$, onde $p \geq 3$ e $\nu = 1$ ou não é um resíduo quadrático fixo módulo p.

(B4) $\langle a_1, a_2, b \mid a_1^9 = a_2^3 = 1, b^3 = a_1^3, [a_1, b] = a_2, [a_2, b] = a_1^{-3}, [a_2, a_1] = 1\rangle$.

(Bii) G não tem subgrupo abeliano de índice p.

(B5) $\langle a, b \mid a^{p^2} = b^{p^2} = c^p = 1, [a, b] = c, [c, a] = b^{\nu p}, [c, b] = a^p\rangle$, onde $p \geq 5$, ν ou não é um resíduo quadrático fixo módulo p.

(B6) $\langle a, b \mid a^{p^2} = b^{p^2} = c^p = 1, [a, b] = c, [c, a] = a^{-p}b^{-lp}, [c, b] = a^{-p}\rangle$, onde $p \geq 5$, $4l = \rho^{2r+1} - 1$, $r = 1, 2, ..., \frac{1}{2}(p-1)$, ρ é o menor inteiro positivo que é uma raiz primitiva módulo p.

(B7) $\langle a, b \mid a^9 = b^9 = c^3 = 1, [a, b] = c, [c, a] = b^{-3}, [c, b] = a^3\rangle$.

(B8) $\langle a, b \mid a^9 = b^9 = c^3 = 1, [a, b] = c, [c, a] = b^{-3}, [c, b] = a^{-3}\rangle$.

(C) $cl(G) = 2$ *e* $G' \cong C_p^2$.

(C1) $K \times A$, *onde* $K = \langle a_1, a_2, a_3 \mid a_1^{p^{m_1}} = a_2^{p^{m_2+1}} = a_3^{p^{m_3+1}} = 1, [a_1, a_2] = a_3^{p^{m_3}}, [a_1, a_3] = a_2^{p^{m_2}}, [a_2, a_3] = 1\rangle$, $m_1 \geq m_2 = m_3+1$ *e* A *é abeliano tal que* $exp(A) \leq p^{m_3}$.

(C2) $K \times A$, *onde* $K = \langle a_1, a_2, a_3 \mid a_1^{p^{m_1}} = a_2^{p^{m_2+1}} = a_3^{p^{m_3+1}} = 1, [a_1, a_2] = a_3^{p^{m_3}}, [a_1, a_3] = a_2^{\nu p^{m_2}}, [a_2, a_3] = 1\rangle$, $p > 2$, ν *ou é um resíduo quadrático fixo módulo p.*, $m_1 \geq m_2 = m_3 + 1$ *ou* $m_1 \geq m_2 = m_3$ *e* A *é abeliano tal que* $exp(A) \leq p^{m_3}$.

(C3) $K \times A$, *onde* $K = \langle a_1, a_2, a_3 \mid a_1^{p^{m_1}} = a_2^{p^{m_2+1}} = a_3^{p^{m_3+1}} = 1, [a_1, a_2] = a_3^{p^{m_3}}, [a_1, a_3] = a_2^{kp^{m_2}} a_3^{-p^{m_3}}, [a_2, a_3] = 1\rangle$, $1 + 4k$ *não é um resíduo quadrático módulo p para* $p > 2$, $k = 1$ *para* $p = 2$, $m_1 \geq m_2 = m_3$ *e* A *é abeliano tal que* $exp(A) \leq p^{m_3}$.

(C4) $K \times A$, *onde* $K = \langle a_1, a_2, a_3 \mid a_1^{p^{m_1}} = a_2^{p^{m_2+1}} = a_3^{p^{m_3}} = 1, [a_1, a_2] = a_1^{p^{m_1}}, [a_1, a_3] = a_2^{p^{m_2}}, [a_2, a_3] = 1\rangle$, $m_1 > 1$ *para* $p = 2$, *para* $m_1 \geq m_2 \geq m_3$ *e* A *é abeliano tal que* $exp(A) \leq p^{m_2}$.

(C5) $K \times A$, *onde* $K = \langle a_1, a_2, a_3 \mid a_1^{p^{m_1+1}} = a_2^{p^{m_2}} = a_3^{p^{m_3+1}} = 1, [a_1, a_2] = a_3^{p^{m_3}}, [a_1, a_3] = a_1^{p^{m_1}}, [a_2, a_3] = 1\rangle$, $m_1 \geq m_2 = m_3+1$ *e* A *é abeliano tal que* $exp(A) \leq p^{m_2}$.

(C6) $K \times A$, *onde* $K = \langle a_1, a_2, a_3 \mid a_1^{p^{m_1+1}} = a_2^{p^{m_2+1}} = a_3^{p^{m_3}} = 1, [a_1, a_2] = 1, [a_1, a_3] = a_2^{p^{m_2}}, [a_2, a_3] = a_1^{p^{m_1}}\rangle$, $m_1 - 1 = m_2 \geq m_3$ *e* A *é abeliano tal que* $exp(A) \leq p^{m_2}$.

(C7) $K \times A$, *onde* $K = \langle a_1, a_2, a_3 \mid a_1^{p^{m_1+1}} = a_2^{p^{m_2+1}} = a_3^{p^{m_3}} = 1, [a_1, a_2] = 1, [a_1, a_3] = a_2^{p^{m_2}}, [a_2, a_3] = a_1^{\nu p^{m_1}}\rangle$, $p > 2$, ν *é um resíduo quadrático fixo módulo p*, $m_1 - 1 = m_2 \geq m_3$ *ou* $m_1 = m_2 > m_3$ *e* A *é abeliano tal que* $exp(A) \leq p^{m_2}$.

(C8) $K \times A$, *onde* $K = \langle a_1, a_2, a_3 \mid a_1^{p^{m_1+1}} = a_2^{p^{m_2+1}} = a_3^{p^{m_3}} = 1, [a_1, a_2] = 1, [a_1, a_3] = a_2^{p^{m_2}}, [a_2, a_3] = a_1^{kp^{m_1}} a_2^{-p^{m_2}}\rangle$, $1 + 4k$ *não é um resíduo quadrático módulo p para* $p > 2$, $k = 1$ *para* $p = 2$, $m_1 = m_2 > m_3$ *e* A *é abeliano tal que* $exp(A) \leq p^{m_2}$.

(C9) $K \times A$, *onde* $K = \langle a_1, a_2, b \mid a_1^4 = a_2^4 = 1, b^2 = a_1^2, [a_1, a_2] = 1, [a_1, b] = a_2^2, [a_2, b] = a_1^2\rangle$ *e* A *é abeliano tal que* $exp(A) \leq 2$.

(C10) $K \times A$, *onde* $K = \langle a_1, a_2, b, d \mid a_1^4 = a_2^4 = 1, b^2 = a_1^2, d^2 = a_2^2, [a_1, a_2] = 1, [a_1, b] = a_2^2, [a_2, b] = a_1^2, [a_1, d] = a_1^2, [a_2, d] = a_1^2 a_2^2, [b, d] = 1\rangle$ *e* A *é abeliano tal que* $exp(A) \leq 2$.

(D) $cl(G) = 2$ *e* $G' \cong C_p^3$.

(D1) $K \times A$, *onde* $K = \langle a_1, a_2, a_3 \mid a_1^{p^{m_1+1}} = a_2^{p^{m_2+1}} = a_3^{p^{m_3+1}} = 1, [a_1, a_2] = a_3^{p^{m_3}}, [a_1, a_3] = a_2^{\nu p^{m_2}}, [a_2, a_3] = a_1^{p^{m_1}}\rangle$, $p > 2$, ν *é um resíduo quadrático fixo módulo p*,

$m_1 = m_2 = m_3 + 1$ *e* A *é abeliano tal que* $exp(A) \leq p^{m_3}$.

(D2) $K \times A$, *onde* $K = \langle a_1, a_2, a_3 \mid a_1^{p^{m_1+1}} = a_2^{p^{m_2+1}} = a_3^{p^{m_3+1}} = 1, [a_1, a_2] = a_3^{p^{m_3}}, [a_1, a_3] = a_1^{p^{m_1}} a_2^{lp^{m_2}}, [a_2, a_3] = a_1^{p^{m_1}} \rangle$, $1 + 4l$ *não é um resíduo quadrático módulo* p *para* $p > 2$, $l = 1$ *para* $p = 2$, $m_1 = m_2 = m_3 + 1$ *e* A *é abeliano tal que* $exp(A) \leq p^{m_3}$.

(D3) $K \times A$, *onde* $K = \langle a_1, a_2, a_3 \mid a_1^{p^{m_1+1}} = a_2^{p^{m_2+1}} = a_3^{p^{m_3+1}} = 1, [a_1, a_2] = a_3^{p^{m_3}}, [a_1, a_3] = a_2^{\nu p^{m_2}}, [a_2, a_3] = a_1^{p^{m_1}} \rangle$, $p > 2$, ν *é um resíduo quadrático fixo módulo* p, $m_1 = m_2 + 1 = m_3 + 1$ *e* A *é abeliano tal que* $exp(A) \leq p^{m_3}$.

(D4) $K \times A$, *onde* $K = \langle a_1, a_2, a_3 \mid a_1^{p^{m_1+1}} = a_2^{p^{m_2+1}} = a_3^{p^{m_3+1}} = 1, [a_1, a_2] = a_3^{p^{m_3}}, [a_1, a_3] = a_2^{kp^{m_2}} a_3^{-p^{m_3}}, [a_2, a_3] = a_1^{p^{m_1}} \rangle$, $1 + 4k$ *não é um resíduo quadrático módulo* p *para* $p > 2, k = 1$ *para* $p = 2$, $m_1 = m_2 + 1 = m_3 + 1$ *e* A *é abeliano tal que* $exp(A) \leq p^{m_3}$.

(D5) $K \times A$, *onde* $K = \langle a_1, a_2, a_3 \mid a_1^4 = a_2^4 = a_3^4 = 1, [a_1, a_2] = a_3^2, [a_1, a_3] = a_2^2 a_3^2, [a_2, a_3] = a_1^2 a_2^2 \rangle$ *e* A *é abeliano tal que* $exp(A) \leq 2$.

(E) G *é metacíclico.*

(E1) $\langle a, b \mid a^{p^{r+s+u}} = 1, b^{p^{r+s+t}} = a^{p^{r+s}}, a^b = a^{1+p^r} \rangle$, *onde* $r \geq 1$, $u \leq r$ *e* $r + 1 \geq s + u \geq 2$. *Se* $p = 2$, *então* $r \geq 2$.

(E2) $\langle a, b \mid a^{2^3} = b^{2^m} = 1, a^b = a^{-1} \rangle$, *onde* $m \geq 1$.

(E3) $\langle a, b \mid a^{2^3} = 1, b^{2^m} = a^4, a^b = a^{-1} \rangle$, *onde* $m \geq 1$.

(E4) $\langle a, b \mid a^{2^3} = b^{2^m} = 1, a^b = a^3 \rangle$, *onde* $m \geq 1$.

(F) G *não é metacíclico e* G' *é cíclico e* $|G'| \geq p^2$.

(F1) $K \times A$, *onde* $K = \langle a, b \mid a^{p^{r+s+u}} = 1, b^{p^{r+s}} = 1, a^b = a^{1+p^r} \rangle$, $u \leq r$, $r + 1 > s + u \geq 2$ *e* $A \neq 1$ *é abeliano tal que* $exp(A) \leq p^{(r+1)-(s+u)}$.

(F2) $K \times A$, *onde* $K = \langle a, b \mid a^{p^{r+t+u}} = 1, b^{p^r} = 1, a^b = a^{1+p^{r+t}} \rangle$, $t \geq 1$, $r \geq u \geq 2$ *e* $A \neq 1$ *é abeliano tal que* $exp(A) \leq p^{t+(r+1)-u}$.

(F3) $K \times A$, *onde* $K = \langle a, b \mid a^{p^{r+s}} = 1, b^{p^{r+s+t}} = 1, a^b = a^{1+p^r} \rangle$, $t \geq 1$, $r + 1 > s \geq 2$ *e* $A \neq 1$ *é abeliano tal que* $exp(A) \leq p^{(r+1)-s}$.

(F4) $K \times A$, *onde* $K = \langle a, b \mid a^{p^{r+s+u}} = 1, b^{p^{r+s+t}} = a^{p^{r+s}}, a^b = a^{1+p^r} \rangle$, $stu \neq 0$, $r + 1 > s + u \geq 2$ *e* $A \neq 1$ *é abeliano tal que* $exp(A) \leq p^{(r+1)-(s+u)}$.

(F5) $(K \rtimes B) \times A$, *onde* $K = \langle a, b \mid a^{p^{r+t+u}} = 1, b^{p^r} = 1, a^b = a^{1+p^{(r+t)}} \rangle$, $B = \langle b_1 \rangle \times \langle b_2 \rangle \times \cdots \times \langle b_f \rangle$, *tal que* $o(b_i) = p^{r_i}, [a, b_i] = a^{p^{r+t_i}}, [b, b_i] = 1, max\{t, u - 2\} < t_1 < t_2 < \cdots < t_f < t + u$, $r + t > r_1 + t_1 > r_2 + t_2 > \cdots > r_f + t_f \geq t + u \geq t + 2$ *e* A *é abeliano tal que* $exp(A) \leq p^{t+(r+1)-u}$.

(G) $G' \cong C_{p^\alpha} \times C_p$, *onde* $\alpha \geq 2$.

(G1) $\langle a_1, a_2, a_3 \mid a_1^{p^{m_1+1+m_2}} = a_2^{p^{m_2+1}} = a_3^{p} = 1, [a_1, a_2] = a_1^{p^{m_1}}, [a_1, a_3] = a_2^{p^{m_2}}, [a_2, a_3] = 1\rangle$, *onde* $p > 2$ *e* $m_1 > m_2 \geq 1$.

(G2) $K \times A$, *onde* $K = \langle a_1, a_2, a_3 \mid a_1^{p^{m_1+1+k}} = a_2^{p^{m_2+1}} = a_3^{p^{m_3}} = 1, [a_1, a_2] = a_1^{p^{m_1}}, [a_1, a_3] = a_2^{p^{m_2}}, [a_2, a_3] = 1\rangle$, $m_1 \geq m_2 \geq m_3$, $1 \leq k \leq min\{m_1 - m_3, m_2 - m_3 + 1, m_2 - 1\}$ *e* A *é abeliano tal que* $exp(A) \leq p^{m_2-k}$.

Referências Bibliográficas

[1] L. J. An, Q. H. Zhang, *Finite metahamiltonian p-groups,* J. Algebra 442 (2015) 23-55.

[2] L. J. An, X. G. Fang, *A classification of finite metahamiltonian p-groups, preprint.* http://arxiv.org/pdf/1310.5509v1.pdf.

[3] R. Baer, *Situation der Untergruppen und struktur der Gruppen*, S. B. Heidelberg Akad. Mat. Nat., 2(1933), 12-17.

[4] Y. Berkovick, *Groups of prime power order*, vol. 1, Walter de Gruyter, Berlim, 2008.

[5] C. H. Cunha, *Sobre uma classe especial de grupos nilpotentes*, Dissertação (Mestrado em Matemática), Universidade Federal de Minas Gerais, 2015.

[6] R. Dedekind, *Uber Gruppen*, deren samtliche Teiler Normalteiler sind, Math. Ann., 48(1897), 548-561.

[7] D. Gorenstein, *Finite groups*, 2nd edition, Chelsea Publishing Company, 1980.

[8] B. Huppert, *Endliche Gruppen I*, Springer-Verlag, 1967.

[9] C. P. Milies, A. K. Sehgal, *An Introduction to Group Rings*, vol. 1, Kluwer Academic Publishers, 2002.

[10] V.T. Nagrebeckii, *Invariant coverings of subgroups*, Ural. Gos. Univ. Mat. Zap. 5 (1966) 91-100.

[11] V.T. Nagrebeckii, *Finite non-nilpotent groups, any non-abelian subgroup of which is normal*, Ural. Gos. Univ. Mat. Zap. 6 (1967) 80-88.

[12] V.T. Nagrebeckii, *Finite groups in which any non-nilpotent subgroups is invariant*, Ural. Gos. Univ. Mat. Zap. 7 (1968) 45-49.

[13] L. Rédei, *Das schiefe Product in der Gruppentheorie*, Comment.Math.Helvet., 20(1947), 225-267.

[14] D. J. S. Robinson, *A course in the theory of groups*, 2nd ed. United Stades of America, 1995.

[15] G. M. Romalis, N. F. Sesekin, *Metahamiltonian groups*, Ural. Gos. Univ. Mat. Zap., 5 (1966) 101-106.

[16] G. M. Romalis, N. F. Sesekin, *Metahamiltonian groups II*, Ural. Gos. Univ. Mat. Zap., 6 (1968) 52-58.

[17] G. M. Romalis, N. F. Sesekin, *Metahamiltonian groups III*, Ural. Gos. Univ. Mat. Zap., 7 (1969/1970) 195-199.

[18] J. J. Rotman, *An introduction to the theory of groups*, Allyn and Bacon Inc., 1984.

[19] A. R. Teixeira, *O problema do isomorfismo para álgebras de grupos racionais de p-grupos extra-especiais*, Dissertação (Mestrado em Matemática), Universidade Federal de Minas Gerais, 2006.