Universidade de Brasília

Grupos finitos com poucos elementos em órbitas por automorfismos

Maria Luiza Ferrarini Goulart

Advisor: Alex Carrazedo Dantas

Departamento de Matemática
Universidade de Brasília

Dissertação apresentada como requisito parcial para obtenção do grau de
Mestra em Matemática

Instituto de Ciências Exatas

Brasília, 03 de junho de 2022

Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

Grupos finitos com poucos elementos em órbitas por automorfismos

Maria Luiza Ferrarini Goulart*

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

MESTRA EM MATEMÁTICA

Brasília, 03 de junho de 2022.

Comissão Examinadora:

Prof. Dr. Alex Carrazedo Dantas- MAT/UnB (Orientador)

Prof. Dr. Raimundo de Araújo Bastos Júnior – MAT/UnB (Membro)

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

Agradecimentos

Agradeço primeiramente a minha família por todo o apoio e suporte, especialmente a minha mãe, Ione, e ao meu irmão, Dudu. Ao meu pai, que não está mais presente para ver essa conquista, mas que me ensinou muito sobre dedicação, responsabilidade, foco e, principalmente, amor. Sei que está orgulhoso de mim e desde trabalho.

Ao meu namorado, Vinícius, por sempre estar ao meu lado e me fazer acreditar do que sou capaz. A minha querida e melhor amiga Daniella, que está comigo desde o primeiro dia da graduação e assim permanece até hoje. Este trabalho não seria possível sem você. A todos colegas de curso que me ajudaram durante o trajeto, e aos meus amigos pessoais pelo apoio imensurável.

Aos professores do Departamento de Matemática da UnB por todo ensinamento, especialmente ao meu orientador Alex Carrazedo Dantas, por toda a paciência, dedicação e parceria durante a graduação e o mestrado. Aos professores que participaram da banca, Raimundo de Araújo Bastos Júnior, Irene Naomi Nakaoka e Martino Garonzi pelas sugestões e correções.

À CAPES pelo apoio financeiro.

Resumo

Sejam G um grupo finito e $Aut(G)$ o grupo de automorfismos de G. Definimos a órbita por automorfismos do elemento $g \in G$ como o conjunto $O_{Aut(G)}(g) = \{g^{\sigma}; \sigma \in Aut(G)\}$ e chamamos de $Aut(G)$-órbita uma órbita por automorfismos. Determinamos *maol* o tamanho máximo de uma órbita por automorfismos. Essa dissertação tem como objetivo o estudo de grupos finitos cujos tamanhos das órbitas são pequenos. Em particular, estudamos a caracterização de grupos tais que $maol(G) \in \{1,2,3\}$, e mostramos que existe uma família infinita de grupos finitos satisfazendo $maol(G) = 8$. Tais resultados foram estudados tendo como base o artigo *Finite groups with only small automorphism orbits*, de Alexander Bors, publicado em 2020.

Palavras-Chaves: Teoria de grupos, grupo de automorfismos, órbitas.

Abstract

Let G be a finite group and let $Aut(G)$ be the automorphisms group of G. Define the automorphisms orbits of the element $g \in G$ as the set $O_{Aut(G)}(g) = \{g^{\sigma}; \sigma \in Aut(G)\}$ and call $Aut(G)$-orbit as an automorphisms orbits. We determine *maol* the maximum length of an automorphisms orbits. This dissertation aims to study finite groups which the lenght of automorphisms orbits are small. In particular, we study the characterization of groups such that $maol(G) \in \{1,2,3\}$, and we show that there is an infinite family of finite groups satisfying $maol(G) = 8$. Such results were studied based on the article *Finite groups with only small automorphism orbits*, by Alexander Bors, published in 2020.

Key-Words: Group theory, automorphisms groups, orbits.

Notações

$\mathbb{N}$	conjunto dos números naturais
$\mathbb{Z}$, $\mathbb{Z}^+$	conjunto dos números inteiros e dos números inteiros positivos
(m,n)	máximo divisor comum entre m e n
X,Y	conjuntos
G,H	grupos
$g^h = h^{-1}gh$	g conjugado por h
$[g,h] = g^{-1}h^{-1}gh$	comutador de g e h
$o(g)$	ordem do elemento g
$H \leqslant G$, $H \trianglelefteq G$	H subgrupo de G e H subgrupo normal de G
$Z(G)$	centro de G
G'	subgrupo derivado de G
$\Phi(G)$	subgrupo de Frattini de G
$Aut(G)$	grupo de automorfismos de G
$Exp(G)$	expoente de G
$H \times K$, $H \rtimes K$	produto direto de H com K e produto semidireto de H com K
$\lvert G : H \rvert$	índice de H em G
$Im(f)$, $Nuc(f)$	imagem e núcleo da função f
g^f	aplicação da função f em g
$\gamma_i(G)$	termos da série central inferior
$C_G(g)$	centralizador do elemento g
$\mathbb{P}$	conjunto de todos os números primos
π	um conjunto de números primos
π'	$\mathbb{P} \setminus \pi$
$\mathbb{F}$	corpo
$\mathbb{O}^{\varepsilon}_{2^n}(2)$	grupo ortogonal
$Sp(2n,\mathbb{F})$	grupo simplético
$GL(n,\mathbb{F})$	grupo linear geral de grau n
$\mathbb{Z}/m\mathbb{Z}$	grupo cíclico de ordem m
D_{2n}	grupo diedral de ordem $2n$
QD_{2^n}	grupo quasidiedral de ordem 2^n
$Sym(n)$	grupo simétrico de ordem $n!$
A_n	grupo alternado de ordem $n!/2$
Q_n	grupo quatérnio de ordem n

Conteúdo

Lista de Figuras

Lista de Tabelas

Introdução

Sejam G um grupo e g um elemento de G. Denotamos como $Aut(G)$ o grupo de automorfismos do grupo G. Uma vez que $Aut(G)$ age de maneira natural em G, definimos a órbita por automorfismos do elemento g como o conjunto $O_{Aut(G)}(g) = \{g^{\sigma} \mid \sigma \in Aut(G)\}$. Chamaremos de $Aut(G)$-órbita, uma órbita por automorfismos.

Há diversos estudos sobre a caracterização de um grupo finito G com poucas órbitas por automorfismos. De fato, chamando $\omega(G)$ a quantidade de órbitas por automorfismos, temos que se $\omega(G) = 1$, então G é o grupo trivial; se $\omega(G) = 2$, então G é um p-grupo abeliano elementar não trivial; e em [1], [3], [5], [11] de vários autores, encontramos resultados sobre $\omega(G) \in \{3,4,5,6,7\}$.

Também existem trabalhos cujo interesse é o tamanho das órbitas por automorfismos de um grupo finito G, e não a quantidade de órbitas. De fato, um estudo recente com essa temática é o artigo *Finite groups with only small automorphism orbits* [2], de Alexander Bors, publicado em 2020. Estudar alguns dos resultados desenvolvidos por Bors neste artigo é o objetivo principal desse trabalho.

Existe um longo trabalho feito sobre o tamanho das órbitas por automorfismos internos de G, $Inn(G)$-órbitas. Se $x \in G$, é tal que a classe de conjugação que contém x é finita, dizemos que x é um FC-elemento. Um grupo em que todos os elementos são FC-elementos é chamado FC-grupo. Se todas as classes, além de finitas, são limitadas, dizemos que G é um BFC-grupo.

Em 1954 [7], B. H. Neumann provou que BFC-grupos são os grupos cujo subgrupo derivado G' é finito. Após isso, vários outros estudos tentando expressar a ordem do subgrupo derivado foram feitos. Em particular, destaca-se o trabalho realizado por J. Wiegold [12]: *"Se G é um BFC-grupo qualquer, então* $|G'| \leqslant f(n)$*."*, em que n é a constante que limita o tamanho das classes de conjugação do BFC-grupo e $f(n)$ é uma função de n. A saber, Wiegold mostra que $f(n) = n^{\frac{1}{2}n(n-1)log_2 n\{n(n-1)(log_2 n)^2+1\}}$.

Observe que todo grupo finito é um FC-grupo, portanto tal estudo se mostra interessante para grupos infinitos, o que não ocorre no nosso trabalho.

Definindo $maol(G)$ como o tamanho máximo de uma órbita por automorfismos de um

grupo finito G, é simples mostrar que se $maol(G) = 1$, então o único automorfismo de G é a identidade e, portanto, $G \cong \mathbb{Z}/m\mathbb{Z}$, com $m \in \{1,2\}$. Entretanto, o estudo do *maol* aparenta ser um pouco mais complexo, pois mesmo para tamanhos pequenos de *maol*, como 2 e 3, é necessário o estudo de resultados não elementares de teoria de grupos.

Temos que se um grupo finito G é tal que $maol(G) = 2$, então G é um grupo abeliano e mais, $G \cong \mathbb{Z}/m\mathbb{Z}$, com $m = 3,4$ e 6. Para conseguirmos demonstrar esse resultado, são necessárias construções não triviais de homomorfismos e um estudo sobre grupos de Miller, que são grupos não abelianos com grupo de automorfismos abeliano.

Para o caso $maol(G) = 3$, um estudo mais aprofundado sobre a caracterização de grupos cujos elementos têm ordens limitadas se faz necessário para a conclusão de que, se *maol* é igual a 3 com G um grupo abeliano, então $G \cong (\mathbb{Z}/2\mathbb{Z})^2$, e se G é um grupo não abeliano, então $G \cong Sym(3)$, onde $Sym(3)$ denota o grupo de permutações do conjunto $\{1,2,3\}$.

De fato, A. Bors mostra que:

Teorema A. *[2, Página 2] Seja G um grupo finito. São equivalentes:*

1. $maol(G) \leqslant 3$.
2. *O grupo G é isomorfo a um dos seguintes:* $\mathbb{Z}/m\mathbb{Z}$, *com* $m \in \{1,2,3,4,6\}$; $(\mathbb{Z}/2\mathbb{Z})^2$; $Sym(3)$, *com* $Sym(3)$ *denotando o grupo simétrico de ordem* $3! = 6$.

Em particular, segue que existe uma quantidade finita de grupos finitos, não isomorfos dois a dois, com até 3 elementos em suas órbitas por automorfismos.

Em 1984, os matemáticos Robinson e Wiegold já provavam resultados nesse contexto. No trabalho *Groups with boundedly finite automorphism classes* [10], eles caracterizaram a estrutura de grupos (não necessariamente finitos) e forneceram, para cada primo p, o p-grupo infinito $\mathcal{G}_p$, dado pela apresentação

$$\begin{aligned}\mathcal{G}_p = \langle a,b,x_1,x_2,x_3,\ldots \mid\ & [a,x_i] = [b,x_i] = 1,\\ & [x_{2i-1},x_{2i}] = a, [x_{2i},x_{2i+1}] = 1,\\ & [x_i,x_j] = 1, \forall i,j \text{ tal que } |i-j| > 1,\\ & x_1^p = b, x_i^p = 1, \text{ se } i > 1\rangle.\end{aligned}$$

cuja classe de nilpotência é 2 e o expoente é p^2, tal que o grupo de automorfismos de $\mathcal{G}_p$ é infinito não enumerável, mas suas órbitas têm comprimento, no máximo, $p^2(p-1)^2$.

Todavia, grupos finitos e grupos infinitos se comportam de maneiras diferentes em vários aspectos. Em [6], de Ledermann and B. H. Neumann, é demonstrado que se a ordem de um grupo finito G tende ao infinito, então o mesmo acontece com $Aut(G)$. Em outras palavras, esse trabalho diz que grupos finitos grandes possuem muitos automorfismos. Poderíamos

estender essa ideia pensando no comprimento máximo de uma $Aut(G)$-órbita, de modo que: se $|G| \to \infty$, então $maol(G) \to \infty$.

Inspirado na representação por comutadores dos p-grupos infinitos $\mathcal{G}_p$ de Robinson e Wiegold [10], Bors [2] define uma família infinita de 2-grupos finitos, definidos pela apresentação:

$$\begin{aligned}\langle x_1, x_2, \cdots, x_{2^n+1}, a, b \mid\ & [a,b] = [x_i,a] = [x_i,b] = 1, \\ & [x_{2i-1}, x_{2i}] = a, [x_{2i}, x_{2i+1}] = b, \\ & [x_i, x_j] = 1, \text{ se } |i-j| > 1, \\ & x_1^2 = x_{2^n+1}^2 = b, \\ & a^2 = b^2 = x_i^2 = 1, \text{ se } 1 < i < 2^n+1\rangle,\end{aligned}$$

como exemplo de que a suposição feita acima não é válida:

Teorema B. *Existe uma família infinita de 2-grupos finitos, $\{G_n\}_{n\in\mathbb{N}}$, não isomorfos dois a dois, satisfazendo $maol(G_n) = 8$, para todo $n \in \mathbb{N}$.*

Em particular, esse resultado assegura que o limite superior que *maol* pode assumir, de modo a garantir a existência de uma quantidade finita de grupos satisfazendo o valor desse *maol*, é 7.

Nesse sentido, a problemática *"Existe um valor $n \in \mathbb{Z}^+$, tal que $\forall k < n$, há apenas uma quantidade finita de grupos G, satisfazendo $maol(G) = k$?"* se tornou evidente. Com o auxílio da ferramenta GAP, verificamos que existe, pelo menos, 7 grupos com $maol(G) = 4$, 2 grupos com $maol(G) = 5$, 12 grupos $maol(G) = 6$ e 4 satisfazendo $maol(G) = 7$.

Neste trabalho, temos como objetivos principais as demonstrações do Teoremas A e do Teorema B. Para isso, no primeiro capítulo apresentamos alguns conceitos básicos de Teoria de Grupos,;um breve estudo sobre grupos de automorfismos, órbitas, em especial, $Aut(G)$-órbitas; e sobre grupos nilpotentes e solúveis.

O Capítulo 2 tem como objetivo a caracterização de grupos finitos com $Aut(G)$-órbitas de tamanhos, no máximo, 2 ou 3, demonstrando o Teorema A.

No Capítulo 3, aprofundaremos o estudo e a apresentação dos grupos G_i's, nos dando condições para a demonstração do Teorema B.

Por fim, o capítulo de Considerações finais aborda questões para estudos futuros.

Capítulo 1

Preliminares

Neste capítulo iremos abordar alguns resultados e definições de álgebra, especialmente de teoria de grupos, que serão usados posteriormente no restante deste trabalho.

A Seção 1.1 aborda alguns conceitos básicos da teoria de grupos, além de um lema que foi muito importante para a demonstração de resultados futuros que utiliza apenas conceitos básicos da teoria de grupos para sua demonstração. Alguns fatos sobre grupo de automorfismos, órbitas e, em especial, grupos com órbitas por automorfismos limitadas, serão apresentados na Seção 1.2. Por fim, a Seção 1.3 insere definições, caracterizações e resultados sobre nilpotência e solubilidade.

1.1 Alguns Conceitos Básicos de Teoria de Grupos

Neste capítulo, usaremos letras maiúsculas do alfabeto, $A, B, \cdots, G, H, K, \cdots$, para designar grupos quaisquer, enquanto letras minúsculas, $a, b, \cdots, g, h, k$, para elementos de grupos. A cardinalidade de um conjunto X será denotada por $|X|$ e as notações $H \leqslant G$, $H < G$ e $H \lhd G$ serão usada para dizer que H é um subgrupo de G, que H é um subgrupo próprio de G e que H é um subgrupo normal de G, respectivamente.

Para todo elemento $g \in G$, indicaremos por $|g| = n \in \mathbb{Z}^+$ a ordem do elemento g, ou seja, o menor inteiro positivo n, tal que, na notação multiplicativa, $g^n = 1_G$. O *expoente* de G é o menor inteiro positivo m, tal que $g^m = 1_G$, para todo $g \in G$ e indicaremos por $Exp(G)$.

Sejam G um grupo, $g \in G$ e $H \leqslant G$. O conjunto $gH = \{gh \mid h \in H\}$ é a classe lateral à esquerda de H em G contendo g, e definimos $Hg = \{hg \mid h \in H\}$ como a classe lateral à

direita de H. A cardinalidade do conjunto das classes laterais é o *índice* de H em G, denotado por $(G:H)$.

Sabemos que existem conjuntos de índices I,J, de mesmas cardinalidades, e elementos $g_i, g_j \in G$ tais que G pode ser escrito como a união disjunta das classes laterais à esquerda, ou à direita, de H em G se H é subgrupo de G, ou seja,

$$G = \bigcup_{i\in I} g_i H = \bigcup_{j\in J} H g_j.$$

Tomando, para cada $i \in I$, t_i como o representante da classe $g_i H$, definimos o conjunto $T = \{t_i \mid i \in I\}$ como um *transversal à esquerda* de H em G. Analogamente, definimos $T' = \{t_j \mid j \in J\}$ como um *transversal à direita* de H em G.

Definimos o *centro* do grupo G, denotado por $Z(G)$, como o conjunto de elementos que comutam com todos os elementos de G, ou seja,

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

TEOREMA 1.1.1. [9, Página 140] Sejam G um grupo e $Z(G)$ seu centro. Se $G/Z(G)$ é cíclico, então G é abeliano.

Em particular, temos que o índice de $Z(G)$ em G nunca é um número primo, uma vez que todo grupo de ordem prima é cíclico.

O *comutador* de dois elementos x e y de G é dado por $[x,y] = x^{-1}y^{-1}xy$ e x e y comutam se, e somente se, $[x,y] = 1$. O *subgrupo comutador*, ou derivado, de G é o subgrupo gerado por todos os comutadores do grupo, denotado por G'. Dessa forma, segue que $G' = \{1_G\}$ se, e somente se, G é abeliano.

TEOREMA 1.1.2. [9, Página 119] Sejam G um grupo e $x,y,z \in G$. Então valem as seguintes propriedades:

1. $[y,x] = [x,y]^{-1}$
2. $[xy,z] = [x,z]^y[y,z]$
3. $[x,yz] = [x,z][x,y]^z$
4. $[x,y^{-1},z]^y[y,z^{-1},x]^z[z,x^{-1},y]^x = 1$ (Identidade de Hall-Witt)
5. $yx = xy[y,x]$

Indutivamente, uma vez que $[x,y] = x^{-1}y^{-1}xy$, temos que o comutador de $s \geqslant 3$ elementos do grupo G é definido como $[x_1,x_2,\cdots,x_s] = [[x_1,\ldots,x_{s-1}],x_s]$. Se A e B são subconjuntos

de G, definimos como o subgrupo comutador de A e B, denotado por $[A,B]$, o subgrupo $[A,B] = \langle [a,b] \mid a \in A \text{ e } b \in B \rangle$. Analogamente, se $X_1, X_2, \cdots, X_s$ são subconjuntos de G, definimos $[X_1, \cdots, X_s]$ como o subgrupo de G gerado por todos comutadores da forma $[x_1, \cdots, x_s]$, em que $x_i \in X_i$, $1 \leqslant i \leqslant s$.

LEMA 1.1.3. Sejam G grupo, u, v elementos de G e $m \in \mathbb{Z}^+$ um inteiro positivo. A identidade

$$[u^m, v] = [u,v]^{u^{m-1}+u^{m-2}+\cdots+u+1}$$

é válida em qualquer grupo em que $x^{y+z} = x^y x^z$. Além disso, se $[u,v] \in Z(\langle u,v \rangle)$, então $[u^m, v] = [u,v]^m = [u, v^m]$.

Demonstração. Faremos a demonstração da igualdade por indução sobre m. Se $m = 1$, então $[u^1, v] = [u,v]$ e acabou.
Assuma, por hipótese de indução, que

$$[u^{m-1}, v] = [u,v]^{u^{m-2}+u^{m-3}+\cdots+u+1}.$$

Logo,

$$[u^m, v] = [uu^{m-1}, v] = [u,v]^{u^{m-1}}[u^{m-1}, v].$$

Por hipótese de indução, obtemos que

$$\begin{aligned} [u^m, v] &= [u,v]^{u^{m-1}}[u^{m-1}, v] \\ &= [u,v]^{u^{m-1}}[u,v]^{u^{m-2}+u^{m-3}+\cdots+u+1} \\ &= [u,v]^{u^{m-1}+u^{m-2}+\cdots+u+1}, \end{aligned}$$

como queríamos mostrar. Por fim, se $[u^m, v] \in Z(\langle u,v \rangle)$, então $[u^m, v] = [u,v]^m = [u, v^m]$. □

Tais resultados fornecem identidades extremamente úteis que facilitam o entendimento de resultados abordados nos próximos capítulos.

Sabemos que se G é um grupo finito e $|G|$ divisível pelo primo p, então existe $x \in G$ de ordem p. Além disso, G é dito um p-grupo finito quando $|G| = p^n$ para algum primo p e algum inteiro positivo n.

Seja π um conjunto de números primos. O conjunto $\mathbb{P} \setminus \pi$ é denotado por π', em que $\mathbb{P}$ representa o conjunto dos números primos. Um número natural $n \in \mathbb{N}$ é dito π-*número* se para todo primo p, tal que $p \mid n$ temos que $p \in \pi$.

Naturalmente, se $H \leqslant G$ e $|H|$ é um π-número, então H é um π-subgrupo de G. Se, adicionalmente, $|G : H|$ é um π'-número, então H é chamado de π-*subgrupo de Hall de* G. Note que, se G é finito, então os termos p-subgrupo de Sylow e p-subgrupo de Hall são sinônimos em função dos Teoremas de Sylow.

O *subgrupo de Frattini* de um grupo G , denotado por $\Phi(G)$, é a interseção dos subgrupos maximais de G. Note que, como um automorfismo $\sigma \in Aut(G)$ induz uma permutação no conjunto de subgrupos maximais de G, segue que $\Phi(G)$ é caraterístico e, em particular, normal em G.

Definição 1.1. Sejam G um grupo finito e f um homomorfismo $f : G \to Z(G)$. Defina o homomorfismo

$$\begin{aligned} \alpha_f : G &\to G \\ g &\mapsto gg^f. \end{aligned}$$

De fato, $\forall g, h \in G$,

$$(gh)^{\alpha_f} = (gh)(gh)^f,$$

como f é automorfismo, temos que

$$(gh)^{\alpha_f} = ghg^f h^f,$$

uma vez que $g^f \in Z(G)$, então

$$(gh)^{\alpha_f} = gg^f hh^f = g^{\alpha_f} h^{\alpha_f},$$

ou seja, α_f é homomorfismo. Além disso, note que

$$\begin{aligned} Ker(\alpha_f) &= \{g \in G \mid g^{\alpha_f} = 1_G\} \\ &= \{g \in G \mid gg^f = 1_G\} \\ &= \{g \in G \mid g^f = g^{-1}\}. \end{aligned}$$

Ou seja, o núcleo de α_f é trivial se, e somente se, o elemento neutro é o único elemento do centro invertível por f.

Definição 1.2. Um automorfismo $\alpha \in Aut(G)$ é dito automorfismo central quando $\bar{\alpha} = Id_{G/Z(G)}$, em que

$$\begin{aligned} \bar{\alpha} : \frac{G}{Z(G)} &\longrightarrow \frac{G}{Z(G)} \\ gZ(G) &\longmapsto g^{\alpha} Z(G). \end{aligned}$$

Em outras palavras, $\alpha \in Aut(G)$ é central quando $g^{-1}g^{\alpha} \in Z(G)$. Denotamos por $Aut_{cent}(G)$ o subgrupo de $Aut(G)$ formado por todos os automorfismos centrais de G.

Tomando α_f como na Definição 1.1, quando o núcleo $Ker(\alpha_f)$ é trivial e G é finito, α_f é um automorfismo, mais do que isso, α_f é um automorfismo central.

1.2 Órbitas por automorfismos

Sejam G um grupo finito agindo no conjunto X e x um elemento em X. O conjunto $\{gx \mid g \in G\}$ é chamado de *G-órbita* de x e denotado por $O_G(x)$.

Exemplo 1.1. Seja o grupo simétrico $Sym(4)$ de ordem 24:

$$\begin{aligned} Sym(4) = \{&1,(12),(13),(14),(23),(24),(34),(123),(132),\\ &(124),(142),(134),(143),(234),(243),(1234),(1243),\\ &(1324),(1342),(1423),(1432),(12)(34),(13)(24),(14)(23)\}, \end{aligned}$$

e considere a ação dada por conjugação:

$$\begin{aligned} f : Sym(4) \times Sym(4) &\longrightarrow Sym(4)\\ (g,h) &\longmapsto g^h = h^{-1}gh \end{aligned}$$

Observe que as órbitas dessa ação são as classes de conjugação dos elementos de $Sym(4)$. Como a classe de conjugação de um elemento $g \in Sym(n)$ consiste de todos os elementos de $Sym(n)$ com a mesma estrutura cíclica de g, as órbitas da ação por conjugação do $Sym(4)$ são

$$\begin{gathered} \{1\},\\ \{(12),(13),(14),(23),(24),(34)\},\\ \{(123),(132),(124),(142),(134),(143),(234),(243)\},\\ \{(1234),(1243),(1324),(1342),(1423),(1432)\},\\ \{(12)(34),(13)(24),(14)(23)\}. \end{gathered}$$

Portanto, $Sym(4)$ tem 5 órbitas com até 8 elementos quando a ação é por conjugação, como definida anteriormente.

Ao considerarmos o grupo de automorfismos de G, $Aut(G)$, agindo no grupo G, temos que uma $Aut(G)$-órbita, é o conjunto

$$O_{Aut(G)}(g) = \{g^{\sigma} | \sigma \in Aut(G)\}.$$

Uma vez que $Aut(G)$ age no grupo G, segue que G é particionado em $Aut(G)$-órbitas disjuntas. Se $g^{\alpha} = g$, $\forall \alpha \in Aut(G)$, então a órbita de g é unitária.

Seja G um grupo finito cíclico de ordem n, ou seja, $G = \langle g \rangle$ para algum $g \in G$. Segue do *Teorema Fundamental dos Grupos Abelianos Finitos* que todo grupo finito abeliano G é um produto direto de grupos cíclicos. Além disso, se G é um grupo cíclico finito, definindo o endomorfismo $\sigma_k : G \to G$, tal que $\sigma_k(g) = g^k$, temos que [4, Página 26]:

1. O endomorfismo σ_k é um automorfismo de G se, e somente se, $mdc(n,k) = 1$.

2. A função $\varphi : \mathcal{U}(\mathbb{Z}_n) \to G$ definida como $\varphi(\bar{r}) = g^r$ é um isomorfismo de grupos.

Assim, podemos contar a quantidade de automorfismos que um grupo cíclico finito possui através da quantidade de geradores. Note que, nesse caso, $Aut(G)$ é um grupo abeliano, e tomando n como a ordem do grupo G, $|Aut(G)| = \phi(n)$, onde ϕ denota a função de Euler.

LEMA 1.2.1. Sejam G e H dois grupos finitos. Se as ordens $|G|$ e $|H|$ são coprimas, então $Aut(G \times H) \cong Aut(G) \times Aut(H)$.

Demonstração. Seja $\alpha : G \times H \to G \times H$ um automorfismo de $G \times H$. Vamos mostrar que existem automorfismos $\tau \in Aut(G)$ e $\beta \in Aut(H)$, tais que $(g,h)^\alpha = (g^\tau, h^\beta)$, $\forall g \in G$ e $\forall h \in H$. Defina os homomorfismos

$$\begin{aligned} i_G : G &\to G \times H & \qquad \pi_G : G \times H &\to G \\ g &\mapsto (g, 1_H), & (g,h) &\mapsto g, \end{aligned}$$

$$\begin{aligned} i_H : H &\to G \times H & \qquad \pi_H : G \times H &\to H \\ h &\mapsto (1_G, h), & (g,h) &\mapsto h. \end{aligned}$$

Note que a composição $i_G \circ \alpha \circ \pi_H$ é um homomorfismo $\alpha_{GH} : G \to H$, e como $|G|$ e $|H|$ são números coprimos, segue que α_{GH} é o homomorfismo trivial. Analogamente, concluímos que $\alpha_{HG} = i_H \circ \alpha \circ \pi_G$ é o homomorfismo trivial.
Com isso,

$$(g, 1_H)^\alpha = (g^\tau, 1_H); \forall g \in G,$$

em que $\tau = i_G \circ \alpha \circ \pi_G \in Aut(G)$, e

$$(1_G, h)^\alpha = (1_G, h^\beta); \forall h \in H,$$

com $\beta = i_H \circ \alpha \circ \pi_H \in Aut(H)$. Logo, $\forall (g,h) \in G \times H$,

$$(g,h)^\alpha = (g, 1_H)^\alpha (1_G, h)^\alpha = (g^\tau, 1_H)(1_G, h^\beta) = (g^\tau, h^\beta).$$

Assim, $Aut(G \times H)$ imerge em $Aut(G) \times Aut(H)$, pelo monomorfismo

$$\begin{aligned} \varphi : Aut(G \times H) &\longrightarrow Aut(G) \times Aut(H) \\ \alpha &\longmapsto (\tau, \beta). \end{aligned}$$

Claramente, $Aut(G) \times Aut(H)$ imerge em $Aut(G \times H)$ e, uma vez que ambos os grupos $Aut(G \times H)$ e $Aut(G) \times Aut(H)$ são grupos finitos, a primeira imersão é um isomorfismo e o resultado segue. □

O lema anterior se estende por indução para n grupos finitos $G_1, G_2, \cdots, G_n$, cujas ordens são coprimas, garantindo que

$$Aut(G_1, \cdots, G_n) \cong Aut(G_1) \times \cdots \times Aut(G_n).$$

Há diversos estudos e resultados sobre grupos com uma quantidade limitada de órbitas por automorfismos, ou seja, grupos que possuem finitas $Aut(G)$-órbitas. Neste trabalho, porém, o interesse é estudar grupos que possuem órbitas por automorfismos limitadas, ou seja, nosso foco é o estudo do tamanho dessas $Aut(G)$-órbitas, e não em sua quantidade.

Retomando à definição já feita, denotamos por $maol(G)$ como o comprimento máximo de uma órbita por automorfismos do grupo G. Para simplificação da notação, escreveremos alguma vezes apenas *maol*. Mostraremos nos próximos capítulos que existem poucos e finitos grupos finitos tais que $maol(G) \leqslant 3$ e que existem infinitos grupos finitos com *maol* igual a 8.

Segue diretamente da definição de automorfismos que todo grupo terá uma órbita apenas com o elemento neutro. Além disso, claramente uma órbita por automorfismos de um grupo finito G não pode ter mais do que $|G|$ elementos. Portanto, o tamanho de uma órbita por automorfismos de um grupo finito G é, no máximo, $|G| - 1$, ou seja, $maol(G) \leqslant |G| - 1$.

Em particular, se $G = \mathbb{Z}/p\mathbb{Z}^d$, para algum $d \in \mathbb{Z}^+$ e p primo, então $maol(G) = p^d - 1$, pois teremos uma órbita com apenas o elemento neutro e outra órbita com o restante dos elementos. Como esse grupo tem ordem p^d, segue que a segunda, e maior, $Aut(G)$-órbita terá comprimento $p^d - 1$, ou seja, $maol(G) = p^d - 1$. No exemplo abaixo mostraremos o caso em que $p = 3$ e $d = 1$, ou seja, $G = \mathbb{Z}/3\mathbb{Z}$ e que o $maol(G)$ coincide com o *maol* dos grupos $\mathbb{Z}/4\mathbb{Z}$ e $\mathbb{Z}/6\mathbb{Z}$.

Exemplo 1.2. Vamos mostrar que $maol(\mathbb{Z}/3\mathbb{Z}) = maol(\mathbb{Z}/4\mathbb{Z}) = maol(\mathbb{Z}/6\mathbb{Z}) = 2$. De

fato, temos que $Aut(\mathbb{Z}/3\mathbb{Z}) = \{Id, \varphi\}$, $Aut(\mathbb{Z}/4\mathbb{Z}) = \{Id, \alpha\}$ e $Aut(\mathbb{Z}/6\mathbb{Z}) = \{Id, \gamma\}$, com

$$\begin{array}{ccc} \varphi : \mathbb{Z}/3\mathbb{Z} \longrightarrow \mathbb{Z}/3\mathbb{Z} & \alpha : \mathbb{Z}/4\mathbb{Z} \longrightarrow \mathbb{Z}/4\mathbb{Z} & \gamma : \mathbb{Z}/6\mathbb{Z} \longrightarrow \mathbb{Z}/6\mathbb{Z} \\ 0 \longmapsto 0 & 0 \longmapsto 0 & 0 \longmapsto 0 \\ 1 \longmapsto 2 & 1 \longmapsto 3 & 1 \longmapsto 5 \\ 2 \longmapsto 1, & 2 \longmapsto 2 & 2 \longmapsto 4 \\ & 3 \longmapsto 1, & 3 \longmapsto 3 \\ & & 4 \longmapsto 2 \\ & & 5 \longmapsto 1. \end{array}$$

Logo,

$$\begin{cases} O_{Aut(\mathbb{Z}/3\mathbb{Z})}(\mathbb{Z}/3\mathbb{Z}) = \{\{0\}\{1,2\}\}. \\ O_{Aut(\mathbb{Z}/4\mathbb{Z})}(\mathbb{Z}/4\mathbb{Z}) = \{\{0\},\{1,3\},\{2\}\}. \\ O_{Aut(\mathbb{Z}/6\mathbb{Z})}(\mathbb{Z}/6\mathbb{Z}) = \{\{0\},\{1,5\},\{2,4\},\{3\}\}. \end{cases}$$

ou seja,

$$maol(\mathbb{Z}/3\mathbb{Z}) = maol(\mathbb{Z}/4\mathbb{Z}) = maol(\mathbb{Z}/6\mathbb{Z}) = 2,$$

como queríamos mostrar.

1.3 Grupos nilpotentes e solúveis

Definição 1.3. Um grupo G diz-se nilpotente se ele contém uma série de subgrupos

$$\{1_G\} = G_0 \leqslant G_1 \leqslant \cdots \leqslant G_{n-1} \leqslant G_n = G,$$

tal que cada subgrupo G_{i-1} é normal em G e cada quociente G_{i+1}/G_i está contido no centro de G/G_i, $\forall i \in \{0, 1, \cdots, n-1\}$.

Tal série de subgrupos é chamada de *série central* de G. Podemos definir outras duas séries de G, *série central inferior* e *série central superior* de G como a seguir.

Definição 1.4. Seja G um grupo. Tome $Z_0(G) = \{1_G\}$ e $Z_1(G) = Z(G)$ e, para todo $i > 1$, defina $\dfrac{Z_i(G)}{Z_{i-1}(G)} = Z\left(\dfrac{G}{Z_{i-1}(G)}\right)$. Uma vez que $Z_i(G) \leqslant Z_{i+1}(G)$, podemos construir a cadeia

$$\{1_G\} = Z_0(G) \leqslant Z_1(G) \leqslant \cdots \leqslant Z_n(G) \leqslant \cdots.$$

Assim definido, fica claro que se existe n tal que $Z_n(G) = G$, então essa série é uma série central e o grupo G é nilpotente.

Definição 1.5. A séria central inferior de G será

$$G = \gamma_1(G) \geqslant \gamma_2(G) \geqslant \cdots$$

e os termos γ_i são definidos indutivamente como

$$\begin{aligned} \gamma_1(G) &= G \\ \gamma_2(G) &= [\gamma_1(G), G] = [G, G] = G' \\ &\vdots \\ \gamma_{i+1}(G) &= [\gamma_n(G), G] \end{aligned}$$

Naturalmente, G é *nilpotente* quando $\gamma_n(G) = 1_G$, para algum natural n. Nesse caso, dizemos que G é nilpotente de classe n.

Definição 1.6. Seja G um grupo finito não abeliano. Se o grupo de automorfismos de G é abeliano, então G chamado *grupo de Miller*.

PROPOSIÇÃO 1.3.1. Seja G um grupo de Miller. Então:

1. O grupo G é nilpotente de classe 2.
2. Todo subgrupo de Sylow de G tem grupo de automorfismos abeliano.
3. Se G é um p-grupo para algum primo p e $|G'| > 2$, então G' não é cíclico.

Demonstração. (1) Considere a série $\{1_G\} \leqslant Z(G) \leqslant G$. Vamos mostrar que esta é uma série central. De fato,

$$\begin{cases} Z(G)/\{1_G\} = Z(G) \subseteq Z(G). \\ G/Z(G) \cong Inn(G) \leqslant Aut(G). \end{cases}$$

Uma vez que G é um grupo de Miller, segue que $Aut(G)$ é abeliano e, assim, $Inn(G)$ também o é. Ou seja,

$$G/Z(G) \cong Inn(G) \subseteq Z(Inn(G)),$$

e segue que $\{1_G\} \leqslant Z(G) \leqslant G$ é uma série central. Por fim, observe que G é não abeliano, pois é um grupo de Miller e, portanto, G é nilpotente de classe 2.

(2) Uma vez que G é nilpotente, segue que $G = \prod_p G_p$, com p primo e G_p os p-subgrupos de Sylow de G [9, Página 126]. Além disso, tais subgrupos são únicos e suas respectivas ordens são coprimas, ou seja,

$$mdc(|G_{p_i}|, |G_{p_j}|) = 1, \qquad \forall i \neq j.$$

Logo,

$$Aut(G) \cong Aut\left(\prod_p G_p\right) \cong \prod_p Aut(G_p).$$

Uma vez que Aut(G) é, por hipótese, abeliano, o resultado segue.

(3) Suponha que G é um p-grupo para algum p primo e $|G'| > 2$. Vamos mostrar que G' não é cíclico. Se G não tem nenhum fator abeliano não trivial e $|G'| > 2$, então G' tem, pelo menos, 2 fatores cíclicos de ordem máxima na sua decomposição cíclica. Logo, G' não é cíclico se G for puramente não-abeliano.
Porém, note que se G não for puramente não-abeliano, então $G = G_0 \times A$, em que G_0 é puramente não-abeliano e A é abeliano. Desde que $Aut(G_0)$ imerge em $Aut(G)$, temos que G_0 é também um p-grupo de Miller puramente não-abeliano e $|G'| = |G'_0| > 2$. Ou seja, G'_0 não é cíclico. Uma vez que $G' \cong G'_0$, segue o resultado.

□

A nilpotência garante diversas outras propriedades aos grupos. De fato, se G é nilpotente de classe 2, então $G' \leqslant Z(G)$ e se G é um grupo finito nilpotente, então G pode ser escrito como o produto direto dos seus subgrupos de Sylow (que são p-grupos) [9, Página 126]. Além disso, é conhecido o fato de que todo p-grupo finito é nilpotente [9, Página 118]. Com isso, observe que se G é um p-grupo finito nilpotente, então todos os p-subgrupos de Sylow de G são únicos.

O lema a seguir é um resultado para específicos p-grupos não abelianos:

LEMA 1.3.2. Seja G um p-grupo não abeliano tal que:

1. O centro $Z(G)$ é cíclico com $|Z(G)| > p$;
2. O subgrupo G' é não trivial;
3. O grupo quociente G/G' não é um p-grupo abeliano elementar.

Considere a composição

$$f : G \overset{can}{\twoheadrightarrow} G/G' \overset{\pi}{\twoheadrightarrow} \mathbb{Z}/p^2\mathbb{Z} \xrightarrow{\varphi_i} \mathbb{Z}/p^2\mathbb{Z} \hookrightarrow Z(G),$$

em que $\overset{can}{\twoheadrightarrow}$ é o homomorfismo canônico e $\xrightarrow{\varphi_i}$ são os endomorfismos de $\mathbb{Z}/p^2\mathbb{Z}$.
Então, f é homomorfismo e o único elemento do centro invertível por f é o elemento neutro 1_G.

Demonstração. Observe que f é a composição de homomorfismos e, portanto, também é homomorfismo. Vamos mostrar que 1_G é o único elemento de $Z(G)$ invertível por f. De fato,

G é nilpotente, pois é um p-grupo, logo $G' \cap Z(G) \neq \{1_G\}$ e uma vez que $G' = ker(G \overset{can}{\twoheadrightarrow} G/G')$, temos que $G' \subseteq ker(f)$.
Seja $g \in G' \cap Z(G)$ tal que $o(g) = p$ e suponha, por contradição, que exista $z \in Z(G) \setminus 1_G$ tal que $z^f = z^{-1}$ e tome $\langle z \rangle$. Temos que $\langle g \rangle \subseteq \langle z \rangle$, pois $o(z) \geqslant p$. Porém, observe que

$$g \in G' \cap Z(G) \subseteq ker(f)$$

e, portanto, $g \in ker(f)$, donde $f|_{\langle z \rangle}$ é um isomorfismo, pois $z^f = z^{-1}$. Portanto, teríamos que $g^f = g^{-1}$ um absurdo, pois g é não trivial e $g \in ker(f)$, ou seja, $g^f = 1_G$.
Daí, segue que 1_G é o único elemento do centro invertível por f, como queríamos mostrar. □

Definição 1.7. Dizemos que um grupo G é solúvel se existe uma série abeliana que começa em $\{1_G\}$ e termina em G, ou seja, se ele possui subgrupos G_i tais que

$$\{1_G\} = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G,$$

e cada quociente G_{i+1}/G_i é abeliano.

Naturalmente, todo grupo nilpotente é solúvel. Se $H \leqslant G$ e G é um grupo solúvel, então H também é solúvel. Além disso, o grupo G é solúvel se, e somente se, para todo subgrupo normal H de G, G/H e H forem solúveis.

TEOREMA 1.3.3. [9, Página 240] Se p,q são números primos, um grupo de ordem $p^m q^n$, com m,n inteiros positivos, é solúvel.

Esse resultado é conhecido como p-q Teorema de Burnside e será utilizado nos próximos capítulos.

Capítulo 2

Grupos com até 3 elementos nas órbitas por automorfismos

Neste capítulo vamos estudar grupos finitos com $maol \in \{2,3\}$. Para isso, será necessária a introdução de algumas definições e resultados.

2.1 Tamanho máximo de uma órbita por automorfismos $(maol(G))$

LEMA 2.1.1. 1. Sejam $G_1, G_2, ..., G_n$ grupos finitos. Então

$$maol\left(\prod_{k=1}^{n} G_k\right) \geqslant \prod_{k=1}^{n} maol(G_k) \geqslant max\ \{\ maol(G_k) \mid 1 \leqslant k \leqslant n\ \}.$$

2. Para todo grupo abeliano finito G, temos $maol(G) \geqslant \phi(Exp(G))$, com ϕ a função de Euler.

3. Seja G um grupo finito e nilpotente. Então $maol(G) = \prod_{p} maol(G_p)$, com p primo e G_p denotando os p-subgrupos finitos (e únicos) de Sylow de G.

Demonstração. (1) Seja $\alpha = (\alpha_1, \alpha_2, ..., \alpha_n) \in \prod_{k=1}^{n} Aut(G_k)$. Queremos mostrar que existe uma correspondência entre α e um elemento de G_k. Seja

$$\beta_\alpha : \prod_{k=1}^{n} G_k \longrightarrow \prod_{k=1}^{n} G_k$$

$$(g_1,...,g_n) \longmapsto (g_1^{\alpha_1},...,g_n^{\alpha_n})$$

Observe que β_α é um automorfismo, uma vez que α é automorfismo por hipótese. Agora, note que

$$\begin{aligned} \gamma : \prod_{k=1}^{n} Aut(G_k) &\hookrightarrow Aut\left(\prod_{k=1}^{n} G_k\right) \\ \alpha &\longmapsto \beta_\alpha \end{aligned}$$

é uma imersão e segue o resultado.

(2) Como G é abeliano, por hipótese, segue do Teorema Fundamental dos Grupos Abelianos Finitos que G pode ser decomposto em fatores cíclicos G_i's. Mas uma vez que G_i é cíclico, então

$$Exp(G_i) = |G_i|,$$

ou seja,

$$\phi(Exp(G_i)) = \phi(|G_i|),$$

que é exatamente a quantidade de geradores de G_i. Daí,para cada G_i,

$$maol(G_i) = \phi(Exp(G_i)).$$

Como G é o produto direto dos G_i's, temos que $maol(G) \geqslant \phi(Exp(G))$, como queríamos mostrar.

(3) Vamos mostrar que $maol(G) = \prod_p maol(G_p)$, com p primo e G_p os p-subgrupos de Sylow de G. Como G é nilpotente, todos os p-subgrupos de Sylow de G são únicos e, portanto,

$$mdc(|G_{p_i}|,|G_{p_j}|) = 1, \qquad \forall i \neq j.$$

Daí, segue indutivamente do Lema 1.2.1 que

$$Aut\left(\prod_p G_p\right) = \prod_p Aut(G_p)$$

e o resultado segue. □

Agora estamos sob as condições de começar a demonstração do Teorema A.

2.2 Grupos finitos com *maol* igual a 1

LEMA 2.2.1. Seja G um grupo finito. São equivalentes:

1. $maol(G) = 1$.
2. $Aut(G)$ é trivial.
3. $G \cong \mathbb{Z}/m\mathbb{Z}$, com $m \in \{1,2\}$.

Demonstração. Suponha que $maol(G) = 1$ e seja $\alpha \in Aut(G)$. Para cada $g \in G$, uma vez que $maol(G) = 1$, temos que

$$g^{\alpha} \in g^{Aut(G)} = \{g\}$$

e, portanto, $\forall g \in G$, $g^{\alpha} = g$. Logo, α é a identidade e segue da arbitrariedade de $\alpha \in Aut(G)$ que $Aut(G)$ é trivial e, portanto, (1) $\Rightarrow$(2) está feito.
Vamos mostrar que (2) $\Rightarrow$ (3). Suponha que $Aut(G)$ é trivial. Temos que

$$G/Z(G) \cong Inn(G) \leqslant Aut(G) = \{Id_G\}.$$

Concluindo que G é abeliano, pois $G \cong Z(G)$. Assumindo a notação aditiva, temos que $-Id_G$ é um automorfismo e, portanto, $-Id_G = Id_G$, ou seja, G tem expoente 2. Donde segue que $G \cong (\mathbb{Z}/2\mathbb{Z})^d$, com $d \in \mathbb{N}$. Suponha que $d \geqslant 2$. Pelo Lema 2.1.1 (1), temos que

$$maol(G) \geqslant maol((\mathbb{Z}/2\mathbb{Z})^2) = 3 > 1,$$

um absurdo, pois contraria a hipótese que $Aut(G)$ é trivial. Logo, $d < 2$, ou seja, $d \in \{0,1\}$, como queríamos mostrar. Por fim, se $G \cong \{1_G\}$ então $maol(G) = 1$, pois $O_{Aut(g)}(G) = \{\{1_G\}\}$.

Se $G \cong \mathbb{Z}/2\mathbb{Z} = \{0,1\}$, então $Aut(G)$ é trivial e $O_{Aut(G)}(G) = \{\{0\},\{1\}\}$, ou seja, $maol(G) = 1$ e isso conclui nossa demonstração. □

Portanto, existe apenas um grupo não trivial com *maol* igual a 1.

2.3 Grupos finitos com *maol* igual a 2

Nosso objetivo nessa seção é caracterizar um grupo finito com *maol* igual a 2. Observe que se $maol(G) = 2$, então $\alpha^2 = id_G$ para qualquer automorfismos $\alpha \in Aut(G)$. Portanto, temos que o grupo de automorfismos de G tem expoente 2, ou seja, é um 2-grupo abeliano elementar.

Definição 2.1. Seja G um grupo finito tal que G/G' é um 2-grupo abeliano elementar. A d-upla $(g_1, g_2, ..., g_d) \in G^d$ é dita tupla padrão em G quando a tupla se projeta para uma $\mathbb{F}_2$-base de G/G' sob a projeção canônica $G \overset{\pi}{\twoheadrightarrow} G/G'$.

É importante destacar que as nomenclaturas *tupla padrão*, como acabamos de ver, e *tupla potência de comutador*, que veremos a seguir, foram dadas por Bors em [2] e traduzidas e usadas por nós neste trabalho. Essas definições não são usuais em livros e outros trabalhos sobre Teoria de grupos.

Definição 2.2. Para cada tupla padrão $(g_1, g_2, ..., g_d)$ em G, associamos a tupla potência de comutador definida como $\left(d + \binom{d}{2}\right)$-uplas com entradas em G':

$$\begin{aligned}(g_1^2, g_2^2, ..., g_d^2, [g_1, g_2], [g_1, g_3], ..., [g_1, g_d],\\ [g_2, g_3], ..., [g_2, g_d],\\ ..., [g_{d-1}, g_d]).\end{aligned}$$

Exemplo 2.1. Seja G um grupo finito tal que $|G'| = 2$. Então existem

$$2^d \prod_{1=0}^{d-1} (2^d - 2^i) = 2^d (2^d - 2^0)(2^d - 2) \cdots (2^d - 2^{d-1})$$

tuplas padrão em G, pois primeiro temos 2^d opções, já que as entradas são em G' e a ordem desse subgrupo é 2, daí para o primeiro vetor, temos $(2^d - 1)$ opções (todas menos o vetor nulo), para o segundo são $(2^d - 2)$ (todas as opções menos os vetores do subespaço gerado pelo primeiro) e assim em diante.

Definição 2.3. Dizemos que duas tuplas padrão em G são equivalentes se, e somente se, elas têm a mesma tupla potência de comutador.

Considere o conjunto de transformações lineares de um espaço vetorial de dimensão $2n$ sobre o corpo $\mathbb{F}$ que preserva uma forma bilinear simétrica não degenerada. Esse conjunto é um grupo com a multiplicação de matrizes chamado *Grupo Simplético* e denotado por $Sp(2n, F)$. Para a demonstração do próximo resultado, precisamos recorrer ao seguinte teorema de David L. Winter [13, Theorem 1]:

TEOREMA 2.3.1. Seja P um grupo extra-especial de ordem p^{2n+1}, ou seja, P é um p-grupo, para algum primo p, $Z(P)$ é cíclico de ordem prima e $P/Z(P)$ é um p-grupo abeliano elementar não trivial. Seja H o subgrupo normal do grupo de automorfismos $Aut(P)$, consistindo de todos os elementos de $Aut(P)$ que agem trivialmente em $Z(P)$. Então,

$$Aut(P) = \langle \theta \rangle H$$

em que θ tem ordem $p-1$, $H \cap \langle\theta\rangle = \langle 1\rangle$ e $H/Inn(P)$ é isomorfo a um subgrupo do grupo linear especial $Sp(2n,p)$.
Além disso,

i. Se p é ímpar e P tem expoente p, então $\dfrac{H}{Inn(P)} \cong Sp(2n,p)$, em que $Sp(2n,p)$ é o grupo simplético de ordem $p^{n^2}\prod_{i=1}^{n}(p^{2i}-1)$.

ii. Se p é ímpar e P tem expoente p^2, então $\dfrac{H}{Inn(P)}$ é o produto semidireto de $Sp(2n-2,p)$ e um grupo extra-especial normal de ordem p^{2n-1}.

iii. Se $p=2$, então $\dfrac{H}{Inn(P)}$ é isomorfo ao grupo ortogonal $\mathbb{O}^{\varepsilon}_{2^n}(2)$ de ordem $2^{n(n-1)}(2^n-\varepsilon)\prod_{i=1}^{n-1}(2^{2i}-1)$. Aqui, $\varepsilon = 1$ se P é isomorfo ao produto central de n grupos diedrais de ordem 8 e $\varepsilon = -1$ se P é isomorfo ao produto central de $n-1$ grupos diedral de ordem 8 e um grupo quatérnio.

A demonstração desse resultado não coincide com o objetivo principal desse trabalho, e pode ser encontrada em [13].

LEMA 2.3.2. Seja G um grupo finito com $maol(G) = 2$.

1. Se G é abeliano, então $G \cong \mathbb{Z}/m\mathbb{Z}$, com $m \in \{3,4,6\}$.
2. Se G é não abeliano, então
   (a) O grupo G é um 2-grupo de Miller;
   (b) O centro $Z(G)$ de G é cíclico;
   (c) $|G'| = 2$;
   (d) $|Z(G)| > 2$;
   (e) O quociente G/G' é um 2-grupo abeliano elementar.

Demonstração. (1) Suponha que G é abeliano. Logo, G é nilpotente e segue do Lema 2.1.1 (3) que

$$maol(G) = \prod_{p} maol(G_p),$$

com p primo e G_p sendo os p-subgrupos (únicos) de Sylow de G. Além disso, se G_p é não-trivial, então pelo Lema 2.1.1 (2),

$$maol(G_p) \geqslant \phi(Exp(G_p)) \geqslant \phi(p) = p-1.$$

Uma vez que $maol(G) = 2$, G_p é trivial a menos que $p \in \{2,3\}$, ou seja, G é um $\{2,3\}$-grupo abeliano finito de ordem, pelo menos, 3. Consideremos os seguintes casos:
(Caso 1): Suponha que G é um 2-grupo. Pelo Lema 2.1.1 (2),

$$2 = maol(G) \geqslant \phi(Exp(G)).$$

Como $|G| = 2^m$, para algum $m \in \mathbb{N}$, segue que $Exp(G) \leqslant 4$, pois $\phi(8) = 4 \geqslant 2 = maol(G)$. Suponha que $Exp(G) = 2$ e, então, que $G \cong (\mathbb{Z}/2\mathbb{Z})^d$, para algum $d \in \mathbb{Z}^+$. Se $d \in \{0,1\}$, então $maol(G) = 1$ (Lema 2.2.1) um absurdo. Logo, $d \geqslant 2$, e

$$maol(G) \geqslant maol((\mathbb{Z}/2\mathbb{Z})^2) = 3,$$

uma contradição, pois $maol(G) = 2$. Assim, $Exp(G) = 4$ e concluímos que G possui um fator $\mathbb{Z}/4\mathbb{Z}$. Se G tiver mais de um fator $\mathbb{Z}/4\mathbb{Z}$ na sua decomposição cíclica, então

$$maol(G) \geqslant maol((\mathbb{Z}/4\mathbb{Z})^2) \geqslant maol(\mathbb{Z}/4\mathbb{Z}) \cdot maol(\mathbb{Z}/4\mathbb{Z}) = 2 \cdot 2 = 4,$$

um absurdo. Daí, $G \cong (\mathbb{Z}/2\mathbb{Z})^d \times \mathbb{Z}/4\mathbb{Z}$, para algum $d \in \mathbb{N}$. Vamos mostrar que $d = 0$. De fato, se $d \geqslant 1$, então

$$maol(G) \geqslant maol(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}) = 4,$$

outra contradição e segue que $G \cong \mathbb{Z}/4\mathbb{Z}$.

(Caso 2): Suponha que G é um 3-grupo. Novamente,

$$2 = maol(G) \geqslant \phi(Exp(G)).$$

Logo, $Exp(G) = 3$, pois $\phi(9) = 6 > 2$. Daí, $G \cong (\mathbb{Z}/3\mathbb{Z})^d$ com $d \in \mathbb{N}^+$. Se $d \geqslant 2$, então

$$maol(G) \geqslant maol((\mathbb{Z}/3\mathbb{Z})^2) = 4$$

um absurdo. Logo, $d = 1$ e $G \cong \mathbb{Z}/3\mathbb{Z}$.

(Caso 3): Suponha que G é um $\{2,3\}$-grupo. Temos que $G = G_2 \times G_3$, com G_p um p-grupo abeliano não trivial para $p \in \{2,3\}$. Note que G é abeliano, pois G_2 e G_3 o são. Assim, segue do Lema 2.1.1 (3) que

$$2 = maol(G) = maol(G_2) \cdot maol(G_3).$$

Temos os seguintes casos:

$$\begin{cases} maol(G_2) = 2 \text{ e } maol(G_3) = 1, \\ \text{ou} \\ maol(G_2) = 1 \text{ e } maol(G_3) = 2. \end{cases}$$

Se $maol(G_2) = 2$ e $maol(G_3) = 1$, então, pelo Lema 2.2.1, $G_3 \cong \mathbb{Z}/m\mathbb{Z}$, com $m \in \{1,2\}$, o que contradiz o fato de G_3 ser um 3-grupo.
Temos que $maol(G_2) = 1$ e $maol(G_3) = 2$, e segue novamente do Lema 2.2.1 que $G_2 \cong \mathbb{Z}/2\mathbb{Z}$ e concluímos do Caso 2 que $G_3 \cong \mathbb{Z}/3\mathbb{Z}$. Ou seja,

$$G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} = \mathbb{Z}/6\mathbb{Z}.$$

Dessa forma, se G é abeliano, então $G \cong \mathbb{Z}/m\mathbb{Z}$, com $m \in \{3,4,6\}$, como queríamos mostrar.

(2) Suponha que G é não-abeliano.
(a) Vamos mostrar que G é um 2-grupo de Miller. Uma vez que $maol(G) = 2$,

$$\alpha^2 = Id_G, \quad \forall \alpha \in Aut(G),$$

donde $Exp(Aut(G)) = 2$, ou seja, todo elemento, salvo a identidade, de $Aut(G)$ tem ordem 2 e, consequentemente, $Aut(G)$ é abeliano. Como, por hipótese, G é não abeliano, temos que G é um grupo de Miller.
Vamos mostrar que G é um 2-grupo. Segue da Proposição 1.3.1(1) que G é nilpotente e assim $G = \prod_p G_p$, com p primo e G_p denotando os (únicos) p-subgrupos de Sylow de G.
Pelo Lema 2.1.1 (3),

$$2 = maol(G) = \prod_p maol(G_p),$$

ou seja, $maol(G_p) = 2$ para um único primo p e $maol(G_q) = 1$, para todo primo $q \neq p$.
Suponha, por absurdo, que G não é p-grupo. Então, pelo Lema 2.2.1, teríamos que $G_q \cong \mathbb{Z}/2\mathbb{Z}$ e, assim, $|G|$ teria exatamente dois divisores primos distintos $\pi = \{2,p\}$. Desde que G é, por hipótese, não abeliano, segue que G_p é um p-grupo não abeliano.
Daí, $|G_p|/|Z(G_p)| \neq 1$, ou seja, como G_p é um p-grupo, existe um automorfismo de ordem, pelo menos, p, e

$$2 = maol(G) \geqslant maol(G_p) \geqslant p > 2,$$

um absurdo. Logo $G_q = \{1_G\}$ e segue que G é um p-grupo.

Por fim, vamos mostrar que $p = 2$. De fato, como G é grupo de Miller, G é não abeliano e pelo mesmo argumento utilizado para G_p, segue que

$$2 = maol(G) \geqslant p$$

e, dessa forma, $p = 2$, o que conclui nossa demonstração.

(b) Suponha, por absurdo, que $Z(G)$ não é cíclico. Uma vez que G é um 2-grupo de Miller, $Z(G)$ é um 2-grupo. Como estamos supondo que $Z(G)$ não é cíclico, existe a imersão:

$$\gamma : (\mathbb{Z}/2\mathbb{Z})^2 \hookrightarrow Z(G).$$

Além disso, segue da Proposição 1.3.1 (1) que G é nilpotente de classe 2 e, com isso, o quociente central $G/Z(G)$ é um 2-grupo abeliano. Logo, existe a projeção:

$$\pi : G/Z(G) \twoheadrightarrow \mathbb{Z}/2\mathbb{Z}.$$

Note que existem quatro homomorfismos $\varphi : \mathbb{Z}/2\mathbb{Z} \to (\mathbb{Z}/2\mathbb{Z})^2$, são eles:

$$\begin{aligned} \varphi_0 : \mathbb{Z}/2\mathbb{Z} &\longrightarrow (\mathbb{Z}/2\mathbb{Z})^2 \\ 0 &\longmapsto (0,0) \\ 1 &\longmapsto (1,0), \end{aligned} \qquad \begin{aligned} \varphi_1 : \mathbb{Z}/2\mathbb{Z} &\longrightarrow (\mathbb{Z}/2\mathbb{Z})^2 \\ 0 &\longmapsto (0,0) \\ 1 &\longmapsto (0,1), \end{aligned}$$

$$\begin{aligned} \varphi_2 : \mathbb{Z}/2\mathbb{Z} &\longrightarrow (\mathbb{Z}/2\mathbb{Z})^2 \\ 0 &\longmapsto (0,0) \\ 1 &\longmapsto (1,1), \end{aligned} \qquad \begin{aligned} \varphi_3 : \mathbb{Z}/2\mathbb{Z} &\longrightarrow (\mathbb{Z}/2\mathbb{Z})^2 \\ 0 &\longmapsto (0,0) \\ 1 &\longmapsto (0,0). \end{aligned}$$

Por composição, temos quatro diferentes homomorfismos:

$$f_i : G \overset{can}{\twoheadrightarrow} G/Z(G) \overset{\pi}{\twoheadrightarrow} \mathbb{Z}/2\mathbb{Z} \xrightarrow{\varphi_i} (\mathbb{Z}/2\mathbb{Z})^2 \overset{\gamma}{\hookrightarrow} Z(G).$$

Para cada homomorfismo $f_i : G \longrightarrow Z(G)$, temos que $Z(G) \subseteq Ker(f_i)$, pois

$$Z(G) = Ker(G \overset{can}{\twoheadrightarrow} G/Z(G)).$$

Daí, o elemento neutro 1_G é o único elemento de $Z(G)$ invertível por f_i. Seja

$$\begin{aligned} \alpha_{f_i} : G &\longrightarrow G \\ g &\longmapsto g g^{f_i}. \end{aligned}$$

Vamos mostrar que α_{f_i} é um automorfismo central. Ou seja, precisamos mostrar que $Ker(\alpha_{f_i}) = \{1_G\}$. Note que

$$\begin{aligned} Ker(\alpha_{f_i}) &= \{g \in G \mid g^{\alpha_{f_i}} = 1_G\} \\ &= \{g \in G \mid gg^{f_i} = 1_G\} \\ &= \{g \in G \mid g^{f_i} = g^{-1}\}. \end{aligned}$$

Porém, 1_G é o único elemento do centro invertível por f_i e segue que α_{f_i} é um automorfismo central, como queríamos mostrar. Agora, fixe $g \in G$ tal que g não pertença ao núcleo da composição

$$G \overset{can}{\twoheadrightarrow} G/Z(G) \overset{\phi}{\twoheadrightarrow} \mathbb{Z}/2\mathbb{Z}.$$

As imagens de g pelos quatro automorfismos centrais α_{f_i} são todas duas a duas distintas, ou seja, existe uma órbita por automorfismos com, pelo menos, quatro elementos, ou seja, $maol(G) \geqslant 4$. Essa contradição conclui a demonstração.

(c) Queremos mostrar que $|G'| = 2$. Segue do item (1) da Proposição 1.3.1 que G é nilpotente de classe 2. Daí, $G' \leqslant Z(G)$, e temos que G' é cíclico, pois $Z(G)$ o é pelo item anterior (b). Por fim, segue da Proposição 1.3.1 (3) que $|G'| \leqslant 2$. Note que $|G'| = 1$ não acontece, pois, por hipótese, G é não abeliano. Logo, $|G'| = 2$.

(d) Desde que, pela Proposição 1.3.1, G é nilpotente de classe 2, $G' \leqslant Z(G)$. Como $|G'| = 2$, então $Z(G) \geqslant 2$. Suponha, por contradição, que $|Z(G)| = 2$, ou seja, $Z(G)$ é cíclico e $G' = Z(G) \cong \mathbb{Z}/2\mathbb{Z}$.
Do item (a), temos que G é um 2-grupo, portanto, $G/Z(G) \cong Inn(G)$ é um 2-grupo também, e desde que G é um grupo de Miller, $G/Z(G) \cong Inn(G) \leqslant Aut(G)$ é abeliano. Dessa forma, concluímos que G é um 2-grupo extra-especial.
Assim, segue do Teorema 2.3.1, que a ação induzida do grupo de automorfismos $Aut(G)$ em $G/Z(G) \cong (\mathbb{F}_2)^{2^n}$ corresponde a um dos grupos ortogonais $\mathbb{O}^{\varepsilon}_{2^n}(2)$, para algum $\varepsilon \in \{-,+\}$, dependendo do tipo de isomorfismo de G. Em que grupo ortogonal é o conjunto de todas as transformações lineares de um espaço vetorial que preserva formas bilineares.
Em qualquer um dos casos, isso implica que $3 \mid |Aut(G)|$, ou seja, $Aut(G)$ tem, pelo Teorema de Cauchy, pelo menos um elemento de ordem 3 e, portanto, $maol(G) \geqslant 3$, uma contradição. Portanto, $|Z(G)| > 2$.

(e) Suponha, por contradição, que G/G' não é um 2-grupo abeliano elementar. Logo, existe a projeção

$$\pi : G/G' \twoheadrightarrow \mathbb{Z}/4\mathbb{Z}.$$

Também existem quatro endomorfismos do grupo $\mathbb{Z}/4\mathbb{Z}$, são eles: $\{\varphi_0, \varphi_1, \varphi_2, \varphi_3\}$, com $\varphi_0 = Id$ e

$$\begin{array}{ccc} \varphi_1 : \mathbb{Z}/4\mathbb{Z} \longrightarrow \mathbb{Z}/4\mathbb{Z} & \varphi_2 : \mathbb{Z}/4\mathbb{Z} \longrightarrow \mathbb{Z}/4\mathbb{Z} & \varphi_2 : \mathbb{Z}/4\mathbb{Z} \longrightarrow \mathbb{Z}/4\mathbb{Z} \\ 0 \longmapsto 0 & 0 \longmapsto 0 & 0 \longmapsto 0 \\ 1 \longmapsto 3 & 1 \longmapsto 2 & 1 \longmapsto 0 \\ 2 \longmapsto 2 & 2 \longmapsto 0 & 2 \longmapsto 0 \\ 3 \longmapsto 1, & 3 \longmapsto 2, & 3 \longmapsto 0. \end{array}$$

Por composição, obtemos quatro homomorfismos distintos

$$f_i : G \overset{can}{\twoheadrightarrow} G/G' \overset{\pi}{\twoheadrightarrow} \mathbb{Z}/4\mathbb{Z} \overset{\varphi_i}{\longrightarrow} \mathbb{Z}/4\mathbb{Z} \hookrightarrow Z(G).$$

E cada homomorfismo f_i induz o automorfismo

$$\begin{aligned} \alpha_{f_i} : G &\longrightarrow G \\ g &\longmapsto g g^{f_i}. \end{aligned}$$

Vamos mostrar que α_{f_i} é um automorfismo central. De fato,

$$\begin{aligned} Ker(\alpha_{f_i}) &= \{g \in G \mid g^{\alpha_{f_i}} = 1_G\} \\ &= \{g \in G \mid g g^{f_i} = 1_G\} \\ &= \{g \in G \mid g^{f_i} = g^{-1}\}. \end{aligned}$$

E 1_G é o único elemento do centro invertível por f_i, ou seja,o núcleo é trivial, α é automorfismo e o resultado segue. Assim, qualquer elemento $g \in G$ que é mapeado pela composição

$$G \overset{can}{\twoheadrightarrow} G/G' \overset{\pi}{\twoheadrightarrow} \mathbb{Z}/4\mathbb{Z}$$

a um gerador do $\mathbb{Z}/4\mathbb{Z}$, assume quatro imagens distintas pelos automorfismos centrais α_{f_i}. Em outras palavras, existe uma órbita por automorfismos com, pelo menos, quatro elementos, ou seja, $maol(G) \geqslant 4$, uma contradição. Portanto, G/G' é um 2-grupo abeliano elementar.

□

PROPOSIÇÃO 2.3.3. Seja G um grupo finito. São equivalentes:

1. $maol(G) = 2$.
2. $G \cong \mathbb{Z}/m\mathbb{Z}$, com $m \in \{3, 4, 6\}$.

Demonstração. Observe que a implicação $(2) \Rightarrow (1)$ já foi feita no Capítulo 1. Logo, nossa demonstração se resume a mostrar que os grupos $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$ e $\mathbb{Z}/6\mathbb{Z}$ são os únicos cujos

maol é igual a 2, ou seja, a primeira implicação.
Segue do Lema 2.3.2 (1) que é suficiente mostrarmos que G é abeliano. Suponha, por absurdo, que G é não abeliano e assuma a estrutura de G descrita no Lema 2.3.2 (2). Escreva $G/G' = (\mathbb{Z}/2\mathbb{Z})^d$ com $d \in \mathbb{N}^+$. Se $d \leqslant 2$, então

$$|G| = |G'|\frac{|G|}{|G'|} = |G'||G/G'| \leqslant 2 \cdot 4 = 8.$$

Logo, $G \cong \{D_8, Q_8, Sym(3)\}$ e $|Z(G)| \leqslant 2$, contradizendo o Lema 2.3.2 (d). Daí, $d \geqslant 3$ (*). Seja $G' = \{1_G, h\}$. Para cada tupla padrão $(g_1, g_2, ..., g_d) \in G$ a $(d+1)$-upla $(g_1, g_2, ..., g_d, h)$ é uma sequência policíclica geradora de G. Assim, se $(s_1, s_2, ..., s_d)$ é uma tupla padrão em G equivalente a $(g_1, g_2, ..., g_d)$, então as duas sequências policíclicas geradoras $(g_1, g_2, ..., g_d, h)$ e $(s_1, s_2, ..., s_d, h)$ de G induzem a mesma apresentação de potência de comutador, pois h é central em G:

$$[g_i, h] = [s_i, h] = 1_G \text{ , } \forall 1 \leqslant i \leqslant d,$$

uma vez que $h \in G' \subseteq Z(G)$. Daí, existe um automorfismo α de G tal que $g_i^\alpha = s_i$, com $1 \leqslant i \leqslant d$. Isso mostra que as tuplas padrão equivalentes se encontram na mesma órbita da ação coordenada a coordenada de $Aut(G)$ em G^d.
Desde que $|G'| = 2$, o número de tuplas de potência de comutador das tuplas padrão em G é, no máximo, $2^{d+\binom{d}{2}}$, temos que o número de classes de equivalência das tuplas padrão em G é, no máximo, $2^{d+\binom{d}{2}}$. Logo, existe uma classe de equivalência da tupla padrão em G de tamanho no mínimo

$$\frac{2^d \prod_{i=0}^{d-1}(2^d - 2^i)}{2^{d+\binom{d}{2}}} = \frac{2^d \prod_{i=0}^{d-1}(2^d - 2^i)}{2^d 2^{\binom{d}{2}}}$$

$$= \frac{\prod_{i=0}^{d-1}(2^d - 2^i)}{2^0 2^1 \cdots 2^{d-1}} = \frac{2^0 2^1 \cdots 2^{d-1} \prod_{i=0}^{d-1}(2^{d-i} - 2^0)}{2^0 2^1 \cdots 2^{d-1}}$$

$$= \prod_{i=0}^{d-1}(2^{d-i} - 1) = \prod_{j=1}^{d}(2^j - 1).$$

Em particular, a ação coordenada a coordenada de $Aut(G)$ em G^d tem órbita de comprimento, pelo menos, $\prod_{j=1}^{d}(2^j - 1)$. Desde que $maol(G) = 2$, por hipótese, segue que a órbita da ação

de $Aut(G)$ em G^d tem, no máximo, 2^d elementos, ou seja,

$$2^d \geqslant \prod_{j=1}^{d}(2^j-1).$$

Mas, se $d \geqslant 3$ (*), então

$$8 = 2^3 \geqslant \prod_{j=1}^{3}(2^j-1) = (2-1)(4-1)(8-1) = 1\cdot 3\cdot 7 = 21,$$

um absurdo. Portanto, G é abeliano e o resultado segue do Lema 2.3.3 (1). □

2.4 Grupos finitos com *maol* igual a 3

Nosso objetivo nessa seção é caracterizar um grupo finito cujo *maol* é 3. Para isso, serão necessários alguns resultados.

2.4.1 Grupos cujos elementos têm ordens limitadas

Esta seção é focada em caracterizar os grupos finitos que possuem elementos de ordens 1, 2 e 3, resultado feito por B. H. Neumann [8, Theorem 1] em 1937.
Considere o grupo

$$G_1 = (\mathbb{F}_2^2)^{n-1} \rtimes_{\varphi_1} \left\langle \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle,$$

em que $\varphi_1 : \left\langle \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle \to Aut((\mathbb{F}_2^2)^{n-1})$ é o homomorfismo que estende a correspondência $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \mapsto \alpha$, e α é o automorfismo de $(\mathbb{F}_2^2)^{n-1}$ dado por $v^\alpha = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} v$, $\forall v \in (\mathbb{F}_2^2)^{n-1}$, identificando o $\mathbb{F}_2$-espaço vetorial $(\mathbb{F}_2^2)^{n-1}$ com $\left\{ \begin{pmatrix} x_{11} & x_{12} & \cdots & x_{1(n-1)} \\ x_{21} & x_{22} & \cdots & x_{2(n-1)} \end{pmatrix} \mid x_{ij} \in \mathbb{F}_2 \right\}$.

E considere também o grupo

$$G_2 = (\mathbb{Z}/3\mathbb{Z})^{n-1} \rtimes_{\varphi_2} \mathbb{Z}/2\mathbb{Z},$$

em que $\varphi_2 : \mathbb{Z}/2\mathbb{Z} \to Aut((\mathbb{Z}/3\mathbb{Z})^{n-1})$ é o homomorfismo que estende a função $1^\varphi \mapsto \beta$, onde $\beta \in Aut((\mathbb{Z}/3\mathbb{Z})^{n-1})$ é definido por $z^\beta = z^{-1}$, para todo $z \in (\mathbb{Z}/3\mathbb{Z})^{n-1}$.

O seguinte resultado mostra que G_1 e G_2 são os únicos grupos finitos com a propriedade de que o conjunto das ordens de todos os elementos é $\{1,2,3\}$.

TEOREMA 2.4.1. Seja G um grupo n-gerado tal que:

- As ordens de todos os elementos de G pertencem a $\{1,2,3\}$;
- Existem $x,y \in G$ tais que $o(x) = 2$ e $o(y) = 3$.

Então G é um dos seguintes:

i. Um produto direto H de não mais do que $(n-1)$ grupos $(\mathbb{Z}/2\mathbb{Z})^2$, chamados *grupos de Klein* e denotados por K, estendido por um automorfismo de ordem 3 que induz um automorfismo externo em cada um dos K.

ii. Um produto direto V de não mais do que $(n-1)$ grupos de ordem 3, estendido por um automorfismo de ordem 2 que transforma todo elemento no seu inverso.

Para a demonstração desse teorema, precisaremos de alguns outros resultados. A partir de agora, consideraremos $a, a_1, a_2, \ldots$ elementos de ordem 2, e $b, b_1, b_2, \ldots$ elementos de ordem 3, Denotaremos por K o grupo de Klein $(\mathbb{Z}/2\mathbb{Z})^2$ e G um grupo com as propriedades descritas no Teorema 2.4.1.

LEMA 2.4.2. Nenhum elemento de G de ordem 2 comuta com um elemento de ordem 3.

Demonstração. De fato, considere o elemento $ab \in G$ tal que $o(ab) = m$ e suponha, por contradição, que $ab = ba$. Daí,

$$1 = (ab)^m = ababab\cdots ab = a\cdots ab\cdots b = a^m b^m,$$

ou seja, $a^m = b^{-m} \in \langle a\rangle \cap \langle b\rangle = \{1_G\}$. Logo, $o(a) = 2 \mid m$ e $o(b) = 3 \mid m$ e temos que $m \geqslant 6$, um absurdo, pois todos os elementos de G têm ordens 1, 2 ou 3, e o resultado segue. □

LEMA 2.4.3. Sejam $a, a_1, a_2, b \in G$. Então

1. $\langle a_1, a_2\rangle \cong K$ ou $\langle a_1, a_2\rangle \cong Sym(3)$.
2. $\langle a, b\rangle \cong Sym(3)$ ou $\langle a, b\rangle \cong A_4$.

Demonstração. Tome $a_1a_2 \in G$. Então $o(a_1a_2) \in \{2,3\}$. Se $o(a_1a_2) = 2$, então

$$a_1a_2 = a_1a_2a_1a_1 = {a_2}^{a_1}a_1,$$

e

$$a_2a_1 = (a_1a_2)^{-1} = a_2^{-1}a_1,$$

ou seja,

$$\langle a_1, a_2\rangle = \{1_G, a_1, a_2, a_1a_2\} \cong K.$$

Se $o(a_1a_2) = 3$, então $a_1a_2 = b$ e

$$\begin{cases} a_2a_1 = (a_1a_2)^{-1} = b^{-1}; \\ (a_1a_2)^{a_1} = b^{a_1}; \\ (a_1a_2)^{a_1} = a_1a_1a_2a_1 = a_2a_1 = b^{-1}; \\ a_1a_2a_1 = ba_1 \Rightarrow a_2^{a_1} = ba_1; \end{cases}$$

ou seja,

$$\langle b\rangle \trianglelefteq \langle a_1, b\rangle = \langle a_1, a_2\rangle$$

e segue que $\langle a_1, a_2\rangle \cong Sym(3)$. Agora, considere $ab \in G$. Temos que $o(ab) \in \{2,3\}$.
Se $o(ab) = 2$, então $ab = a_1$ e segue que $b = aa_1$, e estamos sob as condições do caso anterior. Logo, $\langle a, b\rangle \cong Sym(3)$.
Se $o(ab) = 3$, tome aa^b. Novamente, se $o(aa^b) = 3$, então $\langle a, a^b\rangle \cong Sym(3)$ e se $o(aa^b) = 2$, então $\langle a, a^b\rangle \cong K$ e

$$\frac{\langle a, b\rangle}{\langle a, a^b\rangle} \cong \langle b\rangle,$$

ou seja,

$$\frac{|\langle a, b\rangle|}{|\langle a, a^b\rangle|} = |\langle b\rangle|,$$

como $|\langle a, a^b\rangle| = 4$, $|\langle a, b\rangle| = 12$. Portanto, $\langle a, b\rangle$ é um grupo de ordem 12, cujos elementos têm ordens 1, 2 e 3 e tem o grupo de Klein como um subgrupo normal, ou seja, $\langle a, b\rangle \cong A_4$. Em outras palavras, temos que se $o(ab) = 3$, então $\langle a, b\rangle \cong A_4$, como queríamos mostrar. □

LEMA 2.4.4. Nenhum elemento de G de ordem 2 pertence a ambos K e $Sym(3)$.

Demonstração. Suponha que $\langle a, a_1\rangle \cong K$ e $\langle a, b\rangle \cong Sym(3)$. Se $\langle a_1, b\rangle \cong Sym(3)$, então

$$b^a = b^{-1} = b^{a_1}.$$

Logo, $aba = a_1ba_1$ e temos que $a_1ab = ba_1a$. Porém, note que $o(aa_1) = 2$, pois $a, a_1 \in K$ por hipótese. Assim, teríamos um elemento de ordem 2, aa_1, comutando com um elemento de ordem 3, b, o que contraria o Lema 2.4.2. Portanto, segue do Lema 2.4.3 que $\langle a_1, b\rangle \cong A_4$.

Tome $b_1 = b^{a_1} = a_1 b a_1$. O comutador de b e b_1 tem ordem 2, pois b e b_1 são elementos de ordem 3 em A_4. Ou seja,

$$b^2 {b_1}^2 b b_1 \neq 1, \qquad (b^2 {b_1}^2 b b_1)^2 = 1.$$

Porém, como $b_1 = b^{a_1}$ e $a, a_1 \in K$, temos que

$$a b_1 a = a a_1 b a_1 a = a_1 a b a a_1 = a_1 b^2 a_1 = {b_1}^2.$$

Daí,

$$a b b_1 a = a b a a b_1 a = a b a {b_1}^2 = b^2 {b_1}^2,$$

ou seja, $(bb_1)^a = b^2 {b_1}^2$. Desde que $a^2 = 1_G$, segue que

$$\begin{aligned} [b, b_1] &= b^2 {b_1}^2 b b_1 \\ &= a b b_1 a b b_1 \\ &= (a b b_1)^2. \end{aligned}$$

Porém, a ordem de $[b, b_1] = (a b b_1)^2$ é 2, ou seja, a ordem do elemento $a b b_1 \in A_4$ é 4, um absurdo, pois todos os elementos de A_4 tem ordens 1, 2 ou 3. Portanto, nenhum elemento de ordem 2 pertence a ambos K e $Sym(3)$, como queríamos mostrar. □

LEMA 2.4.5. Não existem dois subgrupos H_1 e H_2 de G, com $H_1 \cong Sym(3)$ e $H_2 \cong K$.

Demonstração. Segue do Lema 2.4.3 que se $\langle a_1, a_2 \rangle \cong K$ e $\langle a, b \rangle \cong Sym(3)$, então $\langle a, a_1 \rangle \cong K$ ou $\langle a, a_1 \rangle \cong Sym(3)$.
Se $\langle a, a_1 \rangle \cong K$, então $a \in K$ e $a \in Sym(3)$, contrariando o Lema 2.4.4, pois note que $o(a) = 2$.
Se $\langle a, a_1 \rangle \cong Sym(3)$, então a_1 pertenceria a ambos K e $Sym(3)$, também contrariando o Lema 2.4.4. Portanto, nenhum desses casos acontece e o resultado segue. □

LEMA 2.4.6. Se G contém K, todos os elementos de ordem 2 em G comutam.

Demonstração. De fato, se existissem elementos de ordem 2 em G que não comutam entre si, então $Sym(3) \subseteq G$, um absurdo, pois contraria o Lema 2.4.5, uma vez que G contém K por hipótese. □

LEMA 2.4.7. Não existem dois subgrupos H_1 e H_2 de G, tais que $H_1 \cong K$ e $H_2 \cong (\mathbb{Z}/3\mathbb{Z})^2$.

Demonstração. Suponha que $\langle b_1, b_2 \rangle \cong (\mathbb{Z}/3\mathbb{Z})^2$ e que a está em algum K. Portanto, segue dos Lemas 2.4.4 e 2.4.5 que

$$\langle a, b_1 \rangle \cong \langle a, b_2 \rangle \cong \langle {b_1}^2 a b_1, b_2 \rangle \cong A_4.$$

Logo, sabemos que

$$(*)\begin{cases} a^{b_1{}^2} = b_1ab_1{}^2 = ab_1{}^2ab_1, \\ a^{b_2{}^2} = b_2ab_2{}^2 = ab_2{}^2ab_2, \\ a^{b_1b_2{}^2} = b_2b_1{}^2ab_1b_2{}^2 = b_1{}^2ab_1b_2{}^2b_1{}^2ab_1b_2, \\ a^{(b_1b_2)^2} = (b_1b_2)^{-2}a(b_1b_2)^2 = a(b_1b_2)^{-1}ab_1b_2. \end{cases}$$

Por outro lado,

$$\begin{aligned} (b_1b_2)^{-2}a(b_1b_2)^2 &= b_2 \cdot b_1ab_1{}^2 \cdot b_2{}^2 \\ &= b_2ab_1{}^2ab_1b_2{}^2 \\ &= b_2a \cdot b_2{}^2b_2 \cdot b_1{}^2ab_1b_2{}^2 \\ &= b_2ab_2{}^2 \cdot b_2b_1{}^2ab_1b_2{}^2 \\ &= b_2ab_2{}^2b_1{}^2ab_1b_2{}^2b_1{}^2ab_1b_2 \\ &= b_2ab_2{}^2 \cdot b_1{}^2ab_1b_2{}^2b_1{}^2ab_1b_2 \\ &= ab_2{}^2ab_2b_1{}^2ab_1b_2{}^2b_1{}^2ab_1b_2. \end{aligned}$$

Segue disso e da última equação de (*) que

$$\begin{cases} a^{(b_1b_2)^2} = (b_1b_2)^{-2}a(b_1b_2)^2 = ab_2{}^2ab_2b_1{}^2ab_1b_2{}^2b_1{}^2ab_1b_2 \\ a^{(b_1b_2)^2} = (b_1b_2)^{-2}a(b_1b_2)^2 = a(b_1b_2)^{-1}ab_1b_2. \end{cases}$$

Logo,

$$ab_2{}^2ab_2b_1{}^2ab_1b_2{}^2b_1{}^2ab_1b_2 = a(b_1b_2)^{-1}ab_1b_2,$$

e, portanto,

$$b_2{}^2ab_2b_1{}^2ab_1 = 1_G,$$

donde segue

$$b_2{}^2ab_2 = b_1{}^2ab_1$$

e concluímos que

$$b_1b_2{}^2a = ab_1b_2{}^2.$$

Ou seja, temos um elemento de ordem 2, a, comutando com um elemento de ordem 3, $b_1b_2{}^2$, um absurdo, pelo Lema 2.4.2. Daí, G não contém ambos os grupos K e $(\mathbb{Z}/3\mathbb{Z})^2$, como queríamos mostrar. □

Agora estamos sob as condições necessárias para fazermos a demonstração do Teorema 2.4.1 cujo enunciado é *Seja G um grupo n-gerado tal que:*

- *As ordens de todos os elementos de G pertencem a* $\{1,2,3\}$*;*
- *Existem* $x,y \in G$ *tais que* $o(x) = 2$ *e* $o(y) = 3$.

Então G é um dos seguintes:

i. Um produto direto H de não mais do que $(n-1)$ *grupos* $(\mathbb{Z}/2\mathbb{Z})^2$*, chamados grupos de Klein e denotados por K, estendido por um automorfismo de ordem 3 que induz um automorfismo externo em cada um dos K.*

ii. Um produto direto V de não mais do que $(n-1)$ *grupos de ordem 3, estendido por um automorfismo de ordem 2 que transforma todo elemento no seu inverso.*

Demonstração. De fato, se G contém elementos de ordem 2 e de ordem 3, então $K \subseteq G$ e $Sym(3) \nsubseteq G$ ou $K \nsubseteq G$ e $Sym(3) \subseteq G$.
No primeiro caso, os elementos de ordem 2 comutam entre si e existe um subgrupo normal H de G, com índice é 3, pois, caso contrário $(\mathbb{Z}/3\mathbb{Z})^2 \subseteq G$, um absurdo, pois $K \subseteq G$ (Lema 2.4.7). A transformação de H por um elemento fora de H induz um automorfismo de ordem 3, que fixa apenas o elemento neutro em H, uma vez que elementos de ordem 2 não comutam com elementos de ordem 3 (Lema 2.4.2), e dois elementos fora de H dão origem a automorfismos iguais ou recíprocos. Portanto, H está dividido em um número finito de grupos de Klein, K, que é normal em G, ou seja, G é do tipo (i).
No segundo caso, o produto de dois elementos de ordem 3 tem ordem 3, pois, caso contrário, $A_4 \subseteq G$ e, portanto, $K \leqslant A_4 \subseteq G$, o que não ocorre. Assim, os elementos de ordem 3 formam um subgrupo normal V de G, cujo índice é 2, uma vez que $K \nsubseteq G$. Além disso, um elemento de ordem 2 transforma todo elemento de V no seu inverso, ou seja, V é abeliano. Logo, V está dividido em um número finito de $\mathbb{Z}/3\mathbb{Z}$ e segue que G é do tipo (ii).
Por fim, uma vez que G é, por hipótese, n-gerado, os limites superiores para o número de fatores diretos de H e V no teorema são evidentes. □

Vamos classificar os grupos com *maol* igual a 3.

LEMA 2.4.8. Seja G um grupo finito com $maol(G) = 3$.

1. Se G é abeliano, então $G \cong (\mathbb{Z}/2\mathbb{Z})^2$.
2. Se G é não abeliano, então:
   (a) O conjunto das ordens dos elementos de $Aut(G)$ está contido em $\{1,2,3\}$. Em particular, $Aut(G)$ é solúvel.
   (b) G é um $\{2,3\}$-grupo. Em particular, G é solúvel.

Demonstração. (1) Suponha que G é abeliano. Temos que G pode ser escrito como o produto direto dos p-subgrupos de Sylow de G, G_p, com p primo, $G = \prod_p G_p$. Se G_p é não trivial para algum primo $p \geqslant 5$, então segue dos itens (1) e (2) do Lema 2.1.1 que

$$maol(G) \geqslant maol(G_p) \geqslant \phi(p) = p - 1 \geqslant 4 > 3,$$

uma contradição, já que $maol(G) = 3$. Assim, $p \in \{2,3\}$, ou seja, $G = G_2 \times G_3$ e segue do Lema 2.1.1 (3) que

$$3 = maol(G) = maol(G_2) \cdot maol(G_3).$$

Logo,

$$\begin{cases} maol(G_2) = 3 \text{ e } maol(G_3) = 1, \\ \text{ou} \\ maol(G_2) = 1 \text{ e } maol(G_3) = 3. \end{cases}$$

Dividiremos em casos.
(Caso 1): Suponha que $maol(G_2) = 3$ e $maol(G_3) = 1$. Pelo Lema 2.2.1 G_3 é trivial, e $G = G_2$, ou seja, G é um 2-grupo abeliano. Segue do item (2) do Lema 2.1.1 que

$$3 = maol(G) \geqslant \phi(Exp(G)),$$

e temos que $Exp(G) \in \{2,4\}$.
(Subcaso (1. a)): Suponha que $Exp(G) = 2$. Então, $G = \mathbb{Z}/2\mathbb{Z}^d$, para algum $d \in \mathbb{Z}^+$, e

$$3 = maol(G) = 2^d - 1$$
$$3 + 1 = 2^d,$$

donde concluímos que $d = 2$, ou seja, $G = (\mathbb{Z}/2\mathbb{Z})^2$.
(Subcaso (1. b)): Suponha que $Exp(G) = 4$. Logo, $G \cong (\mathbb{Z}/2\mathbb{Z})^{d_1} \times (\mathbb{Z}/4\mathbb{Z})^{d_2}$, para alguns $d_1 \in \mathbb{N}$ e $d_2 \in \mathbb{N}^+$. Se $d_2 \geqslant 2$, então segue do Lema 2.1.1 (1) que

$$maol(G) \geqslant (maol(\mathbb{Z}/4\mathbb{Z}))^2 \geqslant 2^2 = 4,$$

um absurdo, uma vez que $maol(G) = 3$ por hipótese. Daí, $d_2 = 1$. Se $d_1 = 0$, então

$$maol(G) = maol(\mathbb{Z}/4\mathbb{Z}) = 2 \neq 3,$$

outro absurdo. Se $d_1 \geqslant 1$, então segue do Lema 2.1.1 (1) que

$$maol(G) \geqslant maol(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}) = 4 > 3,$$

uma contradição. Dessa forma, se $maol(G_2) = 3$ e $maol(G_3) = 1$, então $G = (\mathbb{Z}/2\mathbb{Z})^2$.

(Caso 2): Suponha que $maol(G_2) = 1$ e $maol(G_3) = 3$. Temos do Lema 2.1.1 (2) que

$$3 = maol(G) = maol(G_2) \cdot maol(G_3) = maol(G_3) \geqslant \phi(Exp(G_3)),$$

e, daí, $Exp(G_3) = 3$, ou seja, $G \cong (\mathbb{Z}/3\mathbb{Z})^d$, com $d \in \mathbb{N}^+$ e, assim,

$$3 = maol(G_3) = 3^d - 1,$$

e $3^d = 4$, um absurdo. Portanto, $maol(G_2) = 3$ e $maol(G_3) = 1$ o que implica que $G \cong (\mathbb{Z}/2\mathbb{Z})^2$, como queríamos mostrar.

(2) Suponha que G é não abeliano.
(a) Vamos mostrar que se $\alpha \in Aut(G)$, então $o(\alpha) \in \{1,2,3\}$. De fato, seja $\alpha \in Aut(G)$. Para cada inteiro positivo $k \in \mathbb{Z}^+$, considere o conjunto dos pontos fixados por α^k:

$$C_G(\alpha^k) = \{g \in G, g^{\alpha^k} = g\}.$$

Afirmação: $C_G(\alpha^k) \leqslant G$.
De fato, ${1_G}^{\alpha^k} = 1_G$ e, assim, $1_G \in C_G(\alpha^k)$. E $\forall g,h \in C_G(\alpha^k)$,

$$(gh^{-1})^{\alpha^k} = g^{\alpha^k}(h^{-1})^{\alpha^k} = g^{\alpha^k}(h^{\alpha^k})^{-1},$$

pois α é automorfismo, e desde que $g,h \in C_G(\alpha^k)$,

$$(gh^{-1})^{\alpha^k} = gh^{-1},$$

e então,

$$gh^{-1} \in C_G(\alpha^k).$$

Daí, $C_G(\alpha^k) \leqslant G$. Como $\alpha \in Aut(G)$, observe que α permuta os elementos de G, ou seja, α pode ser visto como uma permutação. Uma vez que $maol(G) = 3$, todos os ciclos de

$\alpha \in Aut(G)$ em G têm tamanhos 1, 2 ou 3. Equivalentemente,

$$G = C_G(\alpha^2) \cup C_G(\alpha^3).$$

Mas sabemos que $C_G(\alpha^2) \cup C_G(\alpha^3) \leqslant G$ se, e somente se, $C_G(\alpha^2) \subseteq C_G(\alpha^3)$ ou $C_G(\alpha^3) \subseteq C_G(\alpha^2)$, ou seja, como G é um grupo finito, não pode ser a união de dois subgrupos próprios. Em particular, segue que $G \cong C_G(\alpha^2)$ ou $G \cong C_G(\alpha^3)$ e, assim, a ordem de α, o(α), divide 2 ou 3, ou seja, $o(\alpha) \in \{1,2,3\}$, como queríamos mostrar.
Uma vez que $o(\alpha) \in \{1,2,3\}$, $\forall \alpha \in Aut(G)$,

$$|Aut(G)| = 2^m 3^n \mid m,n \in \mathbb{N}^+,$$

e, portanto, segue do *p-q* Teorema de Burnside que $Aut(G)$ é um grupo solúvel, concluindo a prova.

(b) Vamos mostrar que G é um $\{2,3\}$-grupo solúvel. De fato, pelo item anterior (a) $Inn(G) \leqslant Aut(G)$ é solúvel. Uma vez que a extensão de grupos solúveis é solúvel, $Z(G)$ é solúvel, pois é abeliano, e $G/Z(G) \cong Inn(G)$, segue que G é solúvel.
Como $maol(G) = 3$, todas as classes de conjugação em G têm comprimentos iguais a 1, 2 ou 3 e, assim, todos os centralizadores de elementos em G têm índices 1, 2 ou 3 em G.
Uma vez que $\dfrac{G}{Z(G)} \cong \dfrac{G}{\bigcap\limits_{x\in G} C_G(x)}$, temos $\left|\dfrac{G}{Z(G)}\right| = \left|\dfrac{G}{\bigcap\limits_{x\in G} C_G(x)}\right|$, ou seja, $\forall x_i \in G$,

$$\left|\frac{G}{Z(G)}\right| \leqslant |G : C_G(x_1)||G : C_G(x_2)| \cdots |G : C_G(x_n)|.$$

Como $|G : C_G(x_i)| \in \{1,2,3\}$, $\forall x_i \in G$, temos que $\left|\dfrac{G}{Z(G)}\right| = 2^m 3^n$, para alguns $m,n \in \mathbb{N}^+$, ou seja, $G/Z(G)$ é um $\{2,3\}$-grupo.
Desde que G é solúvel, G tem um Hall $\{2,3\}'$-subgrupo, $G_{\{2,3\}'}$, que deve ser central e normal, ou seja, único. Além disso, G tem um Hall $\{2,3\}$-subgrupo, $G_{\{2,3\}}$, que é normal, pois é centralizado por $G_{\{2,3\}'}$. Dessa forma,

$$G = G_{\{2,3\}} \times G_{\{2,3\}'}.$$

Se $G_{\{2,3\}'}$ é não trivial, então segue do Lema 2.1.1 (2) que

$$\begin{aligned} 3 = maol(G) &\geqslant maol(G_{\{2,3\}'}) \\ &\geqslant \phi(Exp(G_{\{2,3\}'})) \end{aligned}$$

$$\geqslant \phi(5) = 4,$$

uma contradição, pois $maol(G) = 3$. Portanto, $G_{\{2,3\}'}$ é trivial e segue que $G = G_{\{2,3\}}$, como queríamos mostrar.

□

LEMA 2.4.9. Seja G um grupo finito não abeliano com $maol(G) = 3$. Então, o conjunto das ordens dos automorfismos internos de G é $\{1,2,3\}$ e, portanto, o conjunto das ordens de todos os automorfismos de G é $\{1,2,3\}$.

Demonstração. Segue do Lema 2.4.8 (2)(a) que o conjunto das ordens dos automorfismos internos de G, $Inn(G)$, está contida em $\{1,2,3\}$, pois $Inn(G) \leqslant Aut(G)$. Dessa forma, é suficiente mostrarmos que $Exp(Inn(G))$ não pode ser 2 ou 3.
De fato, suponha por contradição que $Exp(Inn(G)) \in \{2,3\}$. Daí,

$$|Inn(G)| = |G/Z(G)| = p^m \mid m \in \mathbb{N}^+,$$

com p primo. Logo, $G/Z(G)$ é nilpotente e, consequentemente, G é nilpotente. Além disso, segue do Lema 2.4.8 (2)(b) que $G = G_2 \times G_3$, em que G_p denota o p-subgrupo de Sylow de G, com $p \in \{2,3\}$. Logo, estamos sob as condições do Lema 2.1.1 (3):

$$3 = maol(G) = maol(G_2) \cdot maol(G_3).$$

Assim,

$$\begin{cases} maol(G_2) = 3 \text{ e } maol(G_3) = 1 \\ \text{ ou} \\ maol(G_2) = 1 \text{ e } maol(G_3) = 3. \end{cases}$$

Dividiremos a demonstração em casos.
(Caso 1): Suponha que $maol(G_2) = 3$ e $maol(G_3) = 1$. Segue do Lema 2.2.1 que G_3 é trivial, então G é um 2-grupo não abeliano com $maol(G) = 3$.
Dessa forma, todas as classes de conjugação não centrais em G têm comprimento 2, pois observe que, se $x \in G \setminus Z(G)$, então

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

porém,

$$|x^G| \leqslant |x^{Aut(G)}| \leqslant 3.$$

Logo,

$$3 \geqslant |x^{Aut(G)}| \geqslant |x^G| = |G : C_G(x)|,$$

donde segue que $|x^G| = 2$. Além disso, todas as classes de conjugação não centrais em G são $Aut(G)$-órbitas, pois não podemos ter uma órbita de tamanho 3. De fato, se $x^{Aut(G)} = \{x, x^g, x^\alpha\}$, então $x^{g\alpha} \in x^{Aut(G)}$. Vamos analisar as possibilidades: se $x^{g\alpha} = x$, então

$$(x^\alpha)^{g^\alpha} = (g^\alpha)^{-1}(x^\alpha)(g^\alpha) = (x^g)^\alpha = x^{g\alpha} = x,$$

um absurdo, uma vez que x^α e x não são conjugados. Se $x^{g\alpha} = x^g$ então

$$(x^\alpha)^{g^\alpha} = (g^\alpha)^{-1}(x^\alpha)(g^\alpha) = (x^g)^\alpha = x^{g\alpha} = x^g,$$

ou seja, x^α e x^g são conjugados e, assim, x e x^α também são, um absurdo. Por fim, se $x^{g\alpha} = x^\alpha$, como $\alpha \in Aut(G)$, $x^g = x$, contrariando a hipótese de que a órbita tem 3 elementos. Daí, para qualquer $\alpha \in Aut(G)$, o subgrupo $C_G(\alpha^2) = \{g \in G \mid g^{\alpha^2} = g\}$ contém o conjunto $G \setminus Z(G)$.
Vamos mostrar que $\langle G \setminus Z(G)\rangle = G$. De fato, se $T = \{g_1, g_2, ..., g_n\}$ é um transversal de $Z(G)$ em G e $g_1 \in Z(G)$, então

$$\langle g_2z_2, ..., g_nz_n \mid z_i \in Z(G), 1 \leqslant i \leqslant n\rangle = \langle G \setminus Z(G)\rangle.$$

Além disso, note que ${g_2}^{-1} \in \langle g_2z_2, ..., g_nz_n \mid z_i \in Z(G), 1 \leqslant i \leqslant n\rangle$ e, portanto, $g_2z_2g_2^{-1} = z_2$ também está, para todo $z_2 \in Z(G)$, ou seja, $\langle G \setminus Z(G)\rangle = G$. Assim, $C_G(\alpha^2) = G$.
Portanto, $\alpha^2 = Id_G$ e segue que $Exp(Aut(G)) = 2$, pois as ordens dos automorfismos de G estão contidos em $\{1,2,3\}$. Entretanto, temos por hipótese que $maol(G) = 3$ e segue do princípio da contagem (Orbit-stabilizer theorem), que $3 \mid |Aut(G)|$ e então, pelo Teorema de Cauchy, $Aut(G)$ contém um elemento de ordem 3, uma contradição.

(Caso 2): Suponha que $maol(G_2) = 1$ e $maol(G_3) = 3$. Segue do Lema 2.2.1 que $G_2 \cong \mathbb{Z}/m\mathbb{Z}$, com $m \in \{1,2\}$, ou seja, G_2 é abeliano. Daí, G_3 é um 3-grupo não abeliano com $maol(G_3) = 3$, note que isso ocorre pois G é não abeliano e $maol(G) = 3$.
Observe que, analogamente ao Caso 1, todas as classes de conjugação não centrais em G têm comprimento 3 e são órbitas por automorfismo. Uma vez que o grupo de automorfismos internos age de maneira trivial em todos os elementos do centro de G_3, vamos analisar a ação nos elementos $x \notin Z(G_3)$.

Considere $\{x, x^g, x^h\}$ uma órbita por automorfismos e, portanto, uma classe de conjugação não central. Note que $Inn(G_3)$ é um 3-grupo, pois G_3 o é e que $Inn(G_3)$ age de maneira

transitiva na órbita $\{x, x^g, x^h\}$. Dessa maneira, $Inn(G_3)$ age nessa órbita assim como o A_3 age em $\{1,2,3\}$, já que este é o único 3-subgrupo do $Sym(3)$. Como A_3 é um subgrupo abeliano, o grupo de automorfismos internos também age de maneira abeliana em $\{x, x^g, x^h\}$. Segue da arbitrariedade dessa órbita, que $Inn(G_3)$ comuta com todos os elementos de $G_3 \setminus Z(G_3)$ e, assim, que é um grupo abeliano, implicando que G_3 é um grupo nilpotente de classe 2.
Agora, note que
Afirmação 1: O centro $Z(G_3)$ do grupo G_3 é cíclico.
De fato, se $Z(G_3)$ não é cíclico, então existe a imersão

$$\gamma : (\mathbb{Z}/3\mathbb{Z})^2 \hookrightarrow Z(G_3),$$

pois G_3 é um 3-grupo, logo $Z(G_3) \subseteq G_3$ também o é.
Além disso, como G_3 é nilpotente de classe 2, temos a projeção:

$$\pi : G_3/Z(G_3) \twoheadrightarrow \mathbb{Z}/3\mathbb{Z}.$$

Existem nove homomorfismos $\varphi : \mathbb{Z}/3\mathbb{Z} \to (\mathbb{Z}/3\mathbb{Z})^2$, $\{\varphi_0, \varphi_1, \varphi_2, \varphi_3, \varphi_4, \varphi_5, \varphi_6, \varphi_7, \varphi_8\}$, com $\varphi_0 = Id$ e

$$\begin{array}{cccc}
\varphi_1 : \mathbb{Z}/3\mathbb{Z} \to (\mathbb{Z}/3\mathbb{Z})^2 & \varphi_2 : \mathbb{Z}/3\mathbb{Z} \to (\mathbb{Z}/3\mathbb{Z})^2 & \varphi_3 : \mathbb{Z}/3\mathbb{Z} \to (\mathbb{Z}/3\mathbb{Z})^2 & \varphi_4 : \mathbb{Z}/3\mathbb{Z} \to (\mathbb{Z}/3\mathbb{Z})^2 \\
0 \mapsto (0,0) & 0 \mapsto (0,0) & 0 \mapsto (0,0) & 0 \mapsto (0,0) \\
1 \mapsto (2,2) & 1 \mapsto (1,2) & 1 \mapsto (2,1) & 1 \mapsto (1,0) \\
2 \mapsto (1,1), & 2 \mapsto (2,1), & 2 \mapsto (1,2), & 2 \mapsto (2,0),
\end{array}$$

$$\begin{array}{cccc}
\varphi_5 : \mathbb{Z}/3\mathbb{Z} \mapsto (\mathbb{Z}/3\mathbb{Z})^2 & \varphi_6 : \mathbb{Z}/3\mathbb{Z} \mapsto (\mathbb{Z}/3\mathbb{Z})^2 & \varphi_7 : \mathbb{Z}/3\mathbb{Z} \mapsto (\mathbb{Z}/3\mathbb{Z})^2 & \varphi_8 : \mathbb{Z}/3\mathbb{Z} \mapsto (\mathbb{Z}/3\mathbb{Z})^2 \\
0 \mapsto (0,0) & 0 \mapsto (0,0) & 0 \mapsto (0,0) & 0 \mapsto (0,0) \\
1 \mapsto (0,1) & 1 \mapsto (2,0) & 1 \mapsto (0,2) & 1 \mapsto (0,0) \\
2 \mapsto (0,2), & 2 \mapsto (1,0), & 2 \mapsto (0,1), & 2 \mapsto (0,0).
\end{array}$$

Por composição, temos nove diferentes homomorfismos:

$$f_i : G_3 \overset{can}{\twoheadrightarrow} G_3/Z(G_3) \overset{\pi}{\twoheadrightarrow} \mathbb{Z}/3\mathbb{Z} \xrightarrow{\varphi_i} (\mathbb{Z}/3\mathbb{Z})^2 \overset{\gamma}{\hookrightarrow} Z(G_3).$$

Para cada homomorfismo $f_i : G_3 \longrightarrow Z(G_3)$, temos que $Z(G_3) \leqslant Ker(f_i)$, pois $Z(G_3) = Ker(G_3 \overset{can}{\twoheadrightarrow} G_3/Z(G_3))$. Daí, o elemento neutro 1_{G_3} é o único elemento de $Z(G_3)$ invertível por f_i. Seja

$$\begin{aligned}
\alpha_{f_i} : G_3 &\longrightarrow G_3 \\
g &\longmapsto g g^{f_i}.
\end{aligned}$$

Analogamente ao que foi feito anteriormente no caso $maol(G) = 2$, α_{f_i} é um automorfismo central de G_3. Agora, fixe $g \in G_3$ tal que g não pertença ao núcleo da composição

$$G_3 \overset{can}{\twoheadrightarrow} G_3/Z(G_3) \overset{\phi}{\twoheadrightarrow} \mathbb{Z}/3\mathbb{Z}.$$

As imagens de g pelos nove automorfismos centrais α_{f_i} são todas duas a duas distintas, ou seja, existe uma órbita por automorfismos com, pelo menos, nove elementos. Em outras palavras, $maol(G_3) \geqslant 9$, uma contradição, pois $maol(G_3) = 3$. Portanto, $Z(G_3)$ é cíclico.

Afirmação 2: Temos que $|Z(G_3)| > 3$.
De fato, como G_3 é nilpotente de classe 2, $G_3' \subseteq Z(G_3)$ e, uma vez que G_3 é não abeliano, $G_3' \neq 1$. Logo, $Z(G_3) \geqslant 3$. Suponha, por contradição, que $Z(G_3) = 3$ e, então, G_3 é um 3-grupo extra-especial.
Se $|G_3| = 3^{1+2}$, então

$$\begin{cases} G = \langle a,b,c \mid a^3 = b^3 = c^3 = [a,b] = [a,c] = 1, b^c = ab \rangle, \\ \text{ou} \\ G = \langle a,b \mid a^9 = b^3 = 1, a^b = a^4 \rangle. \end{cases}$$

Se $G = \langle a,b,c \mid a^3 = b^3 = c^3 = [a,b] = [a,c] = 1, b^c = ab \rangle$, então cada uma das correspondências $a \longmapsto a$, $b \longmapsto b$, $c \longmapsto a^{k_1}b^{k_2}c$, com $k_1, k_2 \in \{0,1,2\}$, se estende para um automorfismo de G, pois observe que

$$(a^{k_1}b^{k_2}c)^3 = {a^{k_1}}^3 {b^{k_2}}^3 c^3 = a^{3k_1} b^{3k_2} = 1 = c^3$$

e

$$b^{a^{k_1}b^{k_2}c} = b^{b^{k_2}c} = b^c = ab$$

e, daí, $maol(G) \geqslant 9 > 3$, uma contradição.
Se $G = \langle a,b \mid a^9 = b^3 = 1, a^b = a^4 \rangle$, então cada correspondência $a \longmapsto a^k$, $b \longmapsto b$, com $k \in \{1,2,...,9\}$ e $3 \nmid k$ se estende para um automorfismo de G, pois

$$(a^k)^9 = (a^9)^k = 1$$

e

$$(a^k)^b = (a^b)^k = (a^4)^k = a^{4k} = (a^k)^4$$

e, assim, $maol(G) \geqslant \phi(9) = 6 > 3$, outra contradição.

Segue do Teorema 2.3.1 que $Aut(G_3)/Inn(G_3)$ tem um subgrupo isomorfo ao grupo simplético $Sp(2n,3)$, pois

$$H/Inn(G_3) \cong Sp(2n,3).$$

Uma vez que o grupo simplético $Sp(2n,p) \leqslant GL(2n,p)$ age transitivamente sobre $\mathbb{F}_q^{2n} \setminus \{0\}$, temos que $Aut(G)$ tem uma órbita em G de tamanho, pelo menos,

$$3^{2n-2} - 1 \geqslant 3^{2\cdot 2-2} - 1 = 8 > 3,$$

uma contradição. Portanto, $|Z(G_3)| > 3$.

Afirmação 3: O quociente $G_3/Z(G_3)$ é um 3-grupo abeliano elementar.
De fato, suponha, por contradição, que $G_3/Z(G_3)$ não é um 3-grupo abeliano elementar e existe a projeção

$$\pi : G_3/Z(G_3) \twoheadrightarrow \mathbb{Z}/9\mathbb{Z}.$$

Também existem nove endomorfismos do $\mathbb{Z}/9\mathbb{Z}$, sendo $\phi(9) = 6$ isomorfismos com a identidade, e 3 homomorfismos. São eles:

$$\begin{array}{cccc}
\varphi_1 : \mathbb{Z}/9\mathbb{Z} \longrightarrow \mathbb{Z}/9\mathbb{Z} & \varphi_2 : \mathbb{Z}/9\mathbb{Z} \longrightarrow \mathbb{Z}/9\mathbb{Z} & \varphi_3 : \mathbb{Z}/9\mathbb{Z} \longrightarrow \mathbb{Z}/9\mathbb{Z} & \varphi_4 : \mathbb{Z}/9\mathbb{Z} \longrightarrow \mathbb{Z}/9\mathbb{Z} \\
0 \longmapsto 0 & 0 \longmapsto 0 & 0 \longmapsto 0 & 0 \longmapsto 0 \\
1 \longmapsto 2 & 1 \longmapsto 4 & 1 \longmapsto 5 & 1 \longmapsto 7 \\
2 \longmapsto 4 & 2 \longmapsto 8 & 2 \longmapsto 1 & 2 \longmapsto 5 \\
3 \longmapsto 6 & 3 \longmapsto 3 & 3 \longmapsto 6 & 3 \longmapsto 3 \\
4 \longmapsto 8 & 4 \longmapsto 7 & 4 \longmapsto 2 & 4 \longmapsto 1 \\
5 \longmapsto 1 & 5 \longmapsto 2 & 5 \longmapsto 7 & 5 \longmapsto 8 \\
6 \longmapsto 3 & 6 \longmapsto 6 & 6 \longmapsto 3 & 6 \longmapsto 6 \\
7 \longmapsto 5 & 7 \longmapsto 1 & 7 \longmapsto 8 & 7 \longmapsto 4 \\
8 \longmapsto 7, & 8 \longmapsto 5, & 8 \longmapsto 4, & 8 \longmapsto 2,
\end{array}$$

$$\begin{array}{cccc}
\varphi_5 : \mathbb{Z}/9\mathbb{Z} \longrightarrow \mathbb{Z}/9\mathbb{Z} & \varphi_6 : \mathbb{Z}/9\mathbb{Z} \longrightarrow \mathbb{Z}/9\mathbb{Z} & \varphi_7 : \mathbb{Z}/9\mathbb{Z} \longrightarrow \mathbb{Z}/9\mathbb{Z} & \varphi_8 : \mathbb{Z}/9\mathbb{Z} \longrightarrow \mathbb{Z}/9\mathbb{Z} \\
0 \longmapsto 0 & 0 \longmapsto 0 & 0 \longmapsto 0 & 0 \longmapsto 0 \\
1 \longmapsto 8 & 1 \longmapsto 0 & 1 \longmapsto 3 & 1 \longmapsto 6 \\
2 \longmapsto 7 & 2 \longmapsto 0 & 2 \longmapsto 6 & 2 \longmapsto 3 \\
3 \longmapsto 6 & 3 \longmapsto 0 & 3 \longmapsto 0 & 3 \longmapsto 0 \\
4 \longmapsto 5 & 4 \longmapsto 0 & 4 \longmapsto 3 & 4 \longmapsto 6 \\
5 \longmapsto 4 & 5 \longmapsto 0 & 5 \longmapsto 6 & 5 \longmapsto 3 \\
6 \longmapsto 3 & 6 \longmapsto 0 & 6 \longmapsto 0 & 6 \longmapsto 0 \\
7 \longmapsto 2 & 7 \longmapsto 0 & 7 \longmapsto 3 & 7 \longmapsto 6 \\
8 \longmapsto 1, & 8 \longmapsto 0, & 8 \longmapsto 6, & 8 \longmapsto 3.
\end{array}$$

Daí, por composição, obtemos nove homomorfismos distintos

$$f_i : G_3 \overset{can}{\twoheadrightarrow} G_3/Z(G_3) \overset{\pi}{\twoheadrightarrow} \mathbb{Z}/9\mathbb{Z} \xrightarrow{\varphi_i} \mathbb{Z}/9\mathbb{Z} \hookrightarrow Z(G_3).$$

Analogamente ao que foi feito anteriormente, temos que

$$\begin{aligned} \alpha_{f_i} : G_3 &\longrightarrow G_3 \\ g &\longmapsto g g^{f_i} \end{aligned}$$

é um automorfismo de G_3 e qualquer elemento $g \in G_3 \setminus G_3'$ mapeado pela composição

$$G_3 \overset{can}{\twoheadrightarrow} G_3/Z(G_3) \overset{\phi}{\twoheadrightarrow} \mathbb{Z}/9\mathbb{Z}$$

a um gerador do $\mathbb{Z}/9\mathbb{Z}$ assume nove imagens distintas pelos automorfismos centrais α_{f_i}. Ou seja, existe uma órbita por automorfismos com, pelo menos, nove elementos, contrariando o fato que $maol(G_3) = 3$. Donde, $G_3/Z(G_3)$ é um 3-grupo abeliano elementar, como queríamos mostrar.

Afirmação 4: $G_3' \cong \mathbb{Z}/3\mathbb{Z}$.
De fato, desde que G_3 é nilpotente de classe 2, $G_3' \leqslant Z(G_3)$. Como $Z(G_3)$ é cíclico (Afirmação 1), G_3' é um 3-grupo cíclico. Além disso, uma vez que G_3 é nilpotente de classe 2, então $\forall x, y \in G_3$ e $e, f \in \mathbb{Z}$ que

$$[x^e, y^f] = [x, y]^{ef},$$

e já que $Exp(G_3/Z(G_3)) = 3$, o expoente de G_3' deve ser 3 também e o resultado segue.

Afirmação 5: O grupo quociente G_3/G_3' é um 3-grupo abeliano elementar.

De fato, suponha, por contradição, que G_3/G_3' não é um 3-grupo abeliano elementar e temos a projeção

$$\pi : G_3/G_3' \twoheadrightarrow \mathbb{Z}/9\mathbb{Z}.$$

Também que existem os mesmos (Afirmação 3) nove endomorfismos de $\mathbb{Z}/9\mathbb{Z}$, são eles: $\{\varphi_0, \varphi_1, \varphi_2, \varphi_3, \varphi_4, \varphi_5, \varphi_6, \varphi_7, \varphi_8\}$ e, por composição, obtemos nove homomorfismos distintos

$$f_i : G_3 \overset{can}{\twoheadrightarrow} G_3/G_3' \overset{\pi}{\twoheadrightarrow} \mathbb{Z}/9\mathbb{Z} \overset{\varphi_i}{\longrightarrow} \mathbb{Z}/9\mathbb{Z} \hookrightarrow Z(G_3).$$

Cada homomorfismo f_i induz um automorfismo

$$\begin{aligned} \alpha_{f_i} : G_3 &\longrightarrow G_3 \\ g &\longmapsto g g^{f_i}. \end{aligned}$$

Além disso,

$$\begin{aligned} Ker(\alpha_{f_i}) &= \{g \in G_3 \mid g^{\alpha_{f_i}} = 1_{G_3}\} \\ &= \{g \in G_3 \mid g g^{f_i} = 1_{G_3}\} \\ &= \{g \in G_3 \mid g^{f_i} = g^{-1}\} \end{aligned}$$

Porém, note que 1_{G_3} é o único elemento do centro invertível por f_i. Ou seja, $Ker(\alpha_{f_i}) = \{1_{G_3}\}$ e α_{f_i} é um automorfismo e, assim, um automorfismo central. Qualquer elemento $g \in G_3$ que é mapeado pela composição

$$G \overset{can}{\twoheadrightarrow} G_3/G_3' \overset{\pi}{\twoheadrightarrow} \mathbb{Z}/9\mathbb{Z}$$

a um gerador do $\mathbb{Z}/9\mathbb{Z}$ assume nove imagens distintas pelos automorfismos centrais α_{f_i}.
Em outras palavras, existe uma órbita por automorfismos com, pelo menos, nove elementos, ou seja, $maol(G) \geqslant 9$, uma contradição. Portanto, G_3/G_3' é um 3-grupo abeliano elementar. Agora, repetindo o argumento das tuplas padrões utilizado na Proposição **??**, substituindo 2 por 3, e juntando isso com o fato de que $G_3/G_3' \cong (\mathbb{Z}/3\mathbb{Z})^d$, necessariamente temos que

$$3^d \geqslant \prod_{j=1}^{d} (3^j - 1).$$

Isso implica que $d = 1$ e, então, $|G_3| = 3^2$, contradizendo que G_3 é não abeliano. Daí, $maol(G_2) = 1$ e $maol(G_3) = 3$ também não ocorre.
Portanto, concluímos que $Exp(Inn(G)) \notin \{2,3\}$ e que o conjunto das ordens dos automorfismos internos de G é $\{1,2,3\}$, como queríamos mostrar. Por fim, segue disso e do Lema 2.4.8 (2)(a) que o conjunto das ordens de todos os automorfismos de G é $\{1,2,3\}$. □

Para o melhor entendimento da demonstração do próximo lema, segue a definição de **grupo de Frobenius**:

Definição 2.4. Um grupo finito G é um *grupo de Frobenius* quando em sua representação por permutações G é transitivo, há um subgrupo não-trivial H que fixa um elemento e apenas a identidade fixa mais de um elemento. Tal subgrupo H é chamado *complemento de Frobenius*.

Para maiores resultados sobre esse assunto, consultar [4, Página 140].

LEMA 2.4.10. Seja G um grupo finito. São equivalentes:

1. $maol(G) = 3$.
2. $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ou $G \cong Sym(3)$.

Demonstração. $(1) \Rightarrow (2)$ Suponha que G é um grupo finito com $maol(G) = 3$. Se G é abeliano, então $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ pelo Lema 2.4.8 (1). Vamos assumir que G é não abeliano e mostrar que $G \cong Sym(3)$.
Segue do Teorema 2.4.9 que o conjunto das ordens dos elementos de $Inn(G)$ é $\{1,2,3\}$ e, pelo Teorema 2.4.1, $Inn(G) \cong G/Z(G)$ é um dos seguintes:

- O grupo de Frobenius $(\mathbb{Z}/3\mathbb{Z})^d \rtimes \mathbb{Z}/2\mathbb{Z}$ para algum $d \in \mathbb{N}^+$;
- O grupo de Frobenius $(\mathbb{Z}/2\mathbb{Z})^{2d} \rtimes \mathbb{Z}/3\mathbb{Z}$ para algum $d \in \mathbb{N}^+$.

Note que o tamanho máximo da classe de conjugação em $Inn(G)$ não pode exceder o tamanho máximo da classe de conjugação em G, que é 3. Agora, considere o grupo de Frobenius $(\mathbb{Z}/2\mathbb{Z})^{2d} \rtimes \mathbb{Z}/3\mathbb{Z}$ e sejam $h_1, h_2 \in (\mathbb{Z}/2\mathbb{Z})^{2d}$ e $x \in \mathbb{Z}/3\mathbb{Z}$ um gerador de $\mathbb{Z}/3\mathbb{Z}$. Então

$$\begin{aligned} x^{h_1} &= x^{h_2} \\ x^{h_1 {h_2}^{-1}} &= x, \end{aligned}$$

ou seja,

$$(h_1 {h_2}^{-1})^x = h_1 {h_2}^{-1}.$$

Mas como nenhum elemento de ordem 2 comuta com um de ordem 3 (Lema 2.4.2), $h_1 {h_2}^{-1} = 1$ e, então $h_1 = h_2$. Logo, o comprimento da classe de conjugação de qualquer gerador do Frobenius complementar $\mathbb{Z}/3\mathbb{Z}$ é

$$2^{2d} \geqslant 4 > 3,$$

um absurdo. Assim, $Inn(G) \cong (\mathbb{Z}/3\mathbb{Z})^d \rtimes \mathbb{Z}/2\mathbb{Z}$.
Observe que $(\mathbb{Z}/3\mathbb{Z})^d \rtimes \mathbb{Z}/2\mathbb{Z}$ tem uma classe de conjugação de comprimento 3^d, então temos que $d = 1$, ou seja, $Inn(G) \cong \mathbb{Z}/2\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z}$ e, portanto,

$$G/Z(G) \cong Inn(G) \cong \mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z} \cong Sym(3).$$

Afirmação: $Z(G)$ é um 3-grupo.
De fato, caso contrário, como o Teorema 2.4.8 (2)(b) assegura que G é um $\{2,3\}$-grupo, existe uma imersão

$$\mathbb{Z}/2\mathbb{Z} \overset{l}{\hookrightarrow} Z(G),$$

pois $Z(G) \leqslant G$. Além disso, existe uma sequência finita de homomorfismos de grupos:

$$f : G \overset{can.}{\twoheadrightarrow} G/Z(G) \overset{\cong}{\to} Sym(3) \overset{\pi}{\twoheadrightarrow} \mathbb{Z}/2\mathbb{Z} \overset{l}{\hookrightarrow} Z(G)$$

e, por composição, obtemos um homomorfismo não trivial $G \overset{f}{\to} Z(G)$ com automorfismo central associado α_f. Agora, seja $g \in G$ tal que $g \notin ker(f) \supseteq Z(G)$. O único homomorfismo sobrejetor possível entre os grupos $Sym(3)$ e $\mathbb{Z}/2\mathbb{Z}$ é

$$\begin{gathered}\pi : Sym(3) \longrightarrow \mathbb{Z}/2\mathbb{Z} \\ (1) \longmapsto 0 \\ (12) \longmapsto 1 \\ (13) \longmapsto 1 \\ (23) \longmapsto 1 \\ (123) \longmapsto 0 \\ (132) \longmapsto 0.\end{gathered}$$

Uma vez que

$$ker(\pi) = A_3 = \{(1),(123),(132)\}$$

e $g \notin ker(f) \supseteq ker(\pi)$, segue que $g \notin \ker(\pi)$ e, assim, $g \in \{(12),(13),(23)\}$, que são todos conjugados entre si. Logo, o comprimento da classe de conjugação da imagem de g em $G/Z(G) \cong Sym(3)$ é 3. Como

$$G/Z(G) = \{g_1Z(G), g_2Z(G), g_3Z(G), g_4Z(G), g_5Z(G), g_6Z(G)\},$$

o conjunto g^G intersecta três classes laterais, $g_iZ(G)$ com $1 \leqslant i \leqslant 6$, de $Z(G)$ em G. Além disso, g^{α_f} é um elemento da mesma classe lateral que g, mas diferente do próprio g. Então,

$$|g^{Aut(G)}| \geqslant 2 \cdot 3 = 6 > 3,$$

uma contradição, donde $Z(G)$ é um 3-grupo. Logo, uma vez que $G/Z(G) \cong Sym(3)$ e $|Z(G)| = 3^m$, para algum $m \in \mathbb{N}^+$, G tem um 3-subgrupo de Sylow, G_3, normal, pois tem índice 2. Além disso, G_3 é abeliano, pois o centro $Z(G)$ tem índice 3 em G_3, ou seja, $G_3/Z(G)$ é cíclico. Daí, como $Z(G) \subseteq Z(G_3)$, segue que $G_3/Z(G_3)$ também é cíclico e,

portanto, G_3 é abeliano.
Assim, $G = G_3 \rtimes \mathbb{Z}/2\mathbb{Z}$, em que o gerador h de $\mathbb{Z}/2\mathbb{Z}$ centraliza o subgrupo $Z(G)$ de G_3. Seja $g \in G_3 \setminus Z(G)$. Adotando a notação aditiva em G_3, $(gZ(G))^h = gZ(G)$ ou $(gZ(G))^h = -gZ(G)$, como $g \notin Z(G)$, segue que $(gZ(G))^h = -gZ(G)$ e

$$g^h = -g + z, \qquad z \in Z(G).$$

Note que $3g \in Z(G)$ e

$$\begin{gathered} 3g = (3g)^h = 3g^h = 3(-g+z) = -3g+3z \\ 6g - 3z = 0 \\ 3(2g-z) = 0. \end{gathered}$$

Assim, substituindo $2g - z$ por g, podemos assumir, sem perda de generalidade, que $o(g) = 3$. Uma vez que $g^h = -g + z$ para algum $z \in Z(G)$, observe que $o(z) \mid 3$ pois, caso contrário, g^h teria ordem maior que 3 = $o(g)$. Logo, $o(z) = 3$.
Seja $g' := g + z$. Então

$$\begin{aligned} (g')^h &= g^h + z^h \\ &= (-g+z) + (-h+z+h) \\ &= -g+z+(z-h+h) \\ &= -g+z+z \\ &= -g+2z \\ &= -g-z = -g'. \end{aligned}$$

Daí, novamente substituindo g' por g, podemos assumir, sem perda de generalidade, que $g^h = g^{-1}$. Isso implica que

$$\begin{aligned} G &= G_3 \rtimes \mathbb{Z}/2\mathbb{Z} \\ &= (Z(G) \times \langle g \rangle) \rtimes \mathbb{Z}/2\mathbb{Z} \\ &= Z(G) \times (\langle g \rangle \rtimes \mathbb{Z}/2\mathbb{Z}) \\ &\cong Z(G) \times Sym(3). \end{aligned}$$

Se $Z(G)$ é não trivial, então segue do Lema 2.1.1 (2) que

$$maol(Z(G)) \geqslant \phi(Exp(Z(G))) \geqslant \phi(3) = 2$$

e, pelo Lema 2.1.1 (1),

$$3 = maol(G) \geqslant maol(Z(G)) \cdot maol(Sym(3)) \geqslant 2 \cdot 3 = 6,$$

uma contradição. Portanto, $Z(G)$ é trivial e $G \cong Sym(3)$, como queríamos mostrar.

(2) $\Rightarrow$ (1) Vamos mostrar que $maol(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) = maol(Sym(3)) = 3$. De fato, assumindo $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = K$, existe uma órbita por automorfismos de tamanho 3: $\{(1,1),(1,0),(0,1)\}$, tomando $\varphi_1, \varphi_2, \varphi_3 \in Aut(K)$, com

$$\begin{array}{ccc} \varphi_1 : K \to K & \varphi_2 : K \to K & \varphi_3 : K \to K \\ (0,0) \longmapsto (0,0) & (0,0) \longmapsto (0,0) & (0,0) \longmapsto (0,0) \\ (1,1) \longmapsto (1,1) & (1,1) \longmapsto (0,1) & (1,1) \longmapsto (1,0) \\ (0,1) \longmapsto (1,0) & (0,1) \longmapsto (1,0) & (0,1) \longmapsto (1,1) \\ (1,0) \longmapsto (0,1), & (1,0) \longmapsto (1,1), & (1,0) \longmapsto (0,1). \end{array}$$

Logo, $maol(K) = 3$.
Sabendo que $Aut(Sym(3)) = Inn(Sym(3))$, temos

$$\begin{gathered} (13)(12)(13) = (23) \\ (23)(12)(23) = (13) \\ (123)(12)(132) = (13) \\ (132)(12)(123) = (23). \end{gathered}$$

Portanto, $Cl((12)) = Cl((13)) = Cl((23)) = \{(12),(13),(2,3)\}$.
Além disso,

$$\begin{gathered} (12)(123)(12) = (132) \\ (13)(123)(13) = (132) \\ (23)(123)(23) = (132) \\ (132)(123)(123) = (123). \end{gathered}$$

Portanto, $Cl((123)) = Cl((132)) = \{(123),(132)\}$.
Logo, $O_{Aut(Sym(3))}(Sym(3)) = \{\{(1)\},\{(12),(13),(23)\},\{(123),(132)\}\}$ e
$maol(Sym(3)) = 3$.

□

Capítulo 3

Grupos com *maol* igual a 8

O foco deste capítulo é mostrar que existem infinitos grupos finitos, com *maol* igual a 8. Começaremos introduzindo uma sequência infinita de 2-grupos finitos.

3.1 Uma família infinita de grupos com *maol* igual a 8

Definição 3.1. Seja G_n, com $n \geqslant 1$ um inteiro, o 2-grupo finito definido pela apresentação:

$$\begin{aligned}\langle x_1, x_2, \cdots, x_{2^n+1}, a, b \mid\ & [a,b] = [x_i,a] = [x_i,b] = 1, \\ & [x_{2i-1}, x_{2i}] = a, [x_{2i}, x_{2i+1}] = b, \\ & [x_i, x_j] = 1, \text{ se } |i-j| > 1, \\ & x_1^2 = x_{2^n+1}^2 = b, \\ & a^2 = b^2 = x_i^2 = 1, \text{ se } 1 < i < 2^n+1 \rangle.\end{aligned}$$

Note que G_n é um 2-grupo finito com 2^n+3 geradores e 2^{2^n+3} elementos, $Z(G_n) = \langle a,b \rangle = \{1, a, b, ab\}$ e $G' = Z(G)$, ou seja, $G_n/Z(G_n) \cong (\mathbb{Z}/2\mathbb{Z})^{2^n+1} \cong G/G'$. Donde G_n é nilpotente de classe 2.
Para $n = 1$, temos que

$$\begin{aligned}G_1 = \langle x_1, x_2, x_3, a, b \mid\ & [a,b] = [x_2,a] = [x_2,b] = [x_1,x_3] = 1 \\ & [x_1,x_2] = a, [x_2,x_3] = b, {x_1}^2 = {x_3}^2 = b, \\ & a^2 = b^2 = {x_2}^2 = 1 \rangle.\end{aligned}$$

Com o auxílio da ferramenta GAP, vide imagem a seguir, verificamos que

$$G_1 \cong (\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \rtimes \mathbb{Z}/2\mathbb{Z}$$

e que, de fato, $maol(G_1) = 8$.

```
>f2:=FreeGroup("a", "b", "x_1", "x_2", "x_3");
[ <free group on the generators [ a, b, x_1, x_2, x_3 ]>
>a:=f2.1;; b:=f2.2;; x_1:=f2.3;; x_2:=f2.4;; x_3:=f2.5;;
>G1:=f2/[a^2, b^2, x_2^2, Comm(a, b), Comm(x_1, a), Comm(x_1, x_3),
 Comm(x_1, b), Comm(x_1, x_2)*a, Comm(x_2, x_3)*b, x_1^2*b, x_3^2*b];
[ <fp group on the generators [ a, b, x_1, x_2, x_3 ]>
>StructureDescription(last);
[ "(C4 x C2 x C2) : C2"
>
>
>
>maol:= function (G)
  local  m, n, g, k;
  k:=[];;
   n := AutomorphismGroup(G);
   for g in G do
    m:= Orbit(n, g);
    Add(k, Set(m));
   od;
  return Maximum(List (Set(k), x -> Size(x)));
 end;
[ function( G ) ... end
>maol(G1);
[ 8
```

Figura 3.1 Grupo G_1

Além disso, observe que as correspondências $a \mapsto a$, $b \mapsto b$, $x_i \mapsto x_i$, para $i \neq 2^n$, e $x_{2^n} \mapsto x_{2^n}x_{2^n+1}$, se estendem a um automorfismo não central α_n de G_n. De fato, temos que

$$\begin{aligned}(x_{2^n}x_{2^n+1})^2 &= x_{2^n}x_{2^n+1}x_{2^n}x_{2^n+1}\\ &= x_{2^n}x_{2^n}x_{2^n+1}[x_{2^n+1},x_{2^n}]x_{2^n+1}\\ &= (x_{2^n})^2x_{2^n+1}b^{-1}x_{2^n+1}\\ &= b(x_{2^n+1})^2 = b^2 = 1\end{aligned}$$

Logo, o elemento $x_{2^n}x_{2^n+1}$ tem ordem 2, assim como o elemento x_{2^n}. Segue das relações definidas no Lema 1.1.3 que

$$\begin{aligned}[x_{2^n-1},x_{2^n}x_{2^n+1}] &= [x_{2^n-1},x_{2^n+1}][x_{2^n-1},x_{2^n}]^{x_{2^n+1}}\\ &= 1\cdot(x_{2^n+1})^{-1}[x_{2^n-1},x_{2^n}]x_{2^n+1}\\ &= bx_{2^n+1}ax_{2^n+1}\\ &= b(x_{2^n+1})^2a = b^2a = a\end{aligned}$$

ou seja, $[x_{2^n-1},x_{2^n}] = [x_{2^n-1},x_{2^n}x_{2^n+1}] = a$. E

$$[x_{2^n}x_{2^n+1},x_{2^n+1}] = [x_{2^n},x_{2^n+1}]^{x_{2^n+1}}[x_{2^n+1},x_{2^n+1}]$$

$$= bx_{2^n+1}bx_{2^n+1}$$
$$= b^2(x_{2^n+1})^2 = b$$

ou seja, $[x_{2^n}, x_{2^n+1}] = [x_{2^n}x_{2^n+1}, x_{2^n+1}] = b$.
Portanto, temos que α_n define, de fato, um automorfismo de G_n, o qual não é central, pois $(x_{2^n})^{\alpha_n}(x_{2^n})^{-1} \notin Z(G_n)$.
Nosso objetivo nessa seção será cumprido juntamente com a demonstração da seguinte proposição.

PROPOSIÇÃO 3.1.1. Para todo $n \in \mathbb{N}^+$, temos que $|Aut(G_n) : Aut_{cent}(G_n)| = 2$. Em particular, $maol(G_n) = 8$.

Demostraremos, em etapas divididas por afirmações, que cada automorfismo de G_n age na união $Aut_{cent}(G_n) \cup Aut_{cent}(G_n)\alpha_n$, com α_n o automorfismo não central definido anteriormente e $Aut_{cent}(G_n)$ sendo o grupo dos automorfismos centrais de G_n.
Afirmação 1: *Seja $g \in G_n$ com $o(g) = 4$ e $|G_n : C_{G_n}(g)| = 2$.*

1. *Se não existe $h \in G_n$ tal que $g^2 = [g,h]$, então $g \in x_1 Z(G_n)$.*
2. *Se existe $h \in G_n$ tal que $g^2 = [g,h]$, então $g \in x_{2^n+1}Z(G_n)$.*

Em particular, os dois subgrupos $\langle x_1, Z(G_n)\rangle$ e $\langle x_{2^n+1}, Z(G_n)\rangle$ são característicos em G_n.

De fato, escreva $g \equiv x_1^{u_1} \cdots x_k^{u_k} (\bmod Z(G_n))$, com $u_i \in \mathbb{Z}/2\mathbb{Z}$ e $u_k \neq 0$. Se $k = 1$, então $g \equiv x_1 (\bmod Z(G_n))$. Portanto, a primeira implicação é verdade, pois a condição necessária é satisfeita, e a segunda implicação também, pois

$$g^2 = x_1^2 = b,$$

mas

$$[g, G_n] = [x_1, G_n] = \{1, a\},$$

ou seja, $g^2 = [g,h]$ não ocorre. Daí, assuma $k > 1$. Iremos fazer em dois casos distintos:
(Caso 1): Suponha que $k < 2^n + 1$. Se $y \in C_{G_n}(g)$, então podemos escrever y módulo $C_{G_n}(g)$, como $y = x_1^{v_1}x_2^{v_2}\cdots x_{k+1}^{v_{k+1}}$, em que $v_i \in \mathbb{Z}/2\mathbb{Z}$. Note que aqueles elementos que comutam com g não aparecem na fatoração de y, em vista que estamos escrevendo-o módulo $C_{G_n}(g)$. Lembre que y comuta com g e $[x_i, x_j] = 1$, se $|i-j| > 1$. Logo,

$$[g,y] = 1 = [x_1,x_2]^{u_1v_2+u_2v_1}[x_2,x_3]^{u_2v_3+u_3v_2}$$
$$\cdots$$
$$[x_{k-1},x_k]^{u_{k-1}v_k+u_kv_{k-1}}[x_k,x_{k+1}]^{u_kv_{k+1}}.$$

Agora, observe que se i é par, então $[x_{i-1},x_i]=a$ e $[x_i,x_{i+1}]=b$, e uma vez que $a^2=b^2=1$, a soma dos expoentes dos comutadores do tipo $[x_{i-1},x_i]$ e do tipo $[x_i,x_{i+1}]$ precisa dar um número par, pois $ab\neq 1$. Portanto, escrevendo com notação de álgebra linear, a matriz

$$M=\begin{pmatrix} * & \cdots & * & u_k & u_{k-1} & 0 \\ * & \cdots & * & * & * & u_k \end{pmatrix}$$

induz uma transformação linear $T:(\mathbb{F}_2)^{k+1}\to\mathbb{F}_2^2$, definida por

$$T:\begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_k \\ v_{k+1} \end{pmatrix} \longmapsto \begin{pmatrix} * & \cdots & * & u_k & u_{k-1} & 0 \\ * & \cdots & * & * & * & u_k \end{pmatrix} \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_k \\ v_{k+1} \end{pmatrix}.$$

Como, por hipótese, $u_k\neq 0$, as duas linhas da matriz M são linearmente independentes e temos que M tem posto 2, donde segue que a imagem de T tem dimensão 2. Como $\mathbb{F}_2^2$ também tem dimensão 2, concluímos que T é sobrejetiva e, portanto, que $|Im(T)|=4$. Segue do Teorema do Isomorfismo que

$$Im(T)\cong\frac{V}{Nuc(T)},$$

em que $Im(T)$ é a imagem de T, V é o espaço vetorial $(\mathbb{F}_2)^{k+1}$ e $Nuc(T)$ é o núcleo da transformação linear T. Como $Nuc(T)$ representa os valores $v_1,\cdots,v_{k+1}$ que determinam os elementos que comutam com $g\in G_n$ e $Im(T)$ tem dimensão 2 e ordem 4, segue que

$$|G_n:C_{G_n}(g)|=4,$$

o que contraria a hipótese de que $|G_n:C_{G_n}(g)|=2$, finalizando a demonstração do caso $k<2^n+1$.

(Caso 2): Suponha que $k=2^n+1$. Se $y\in C_{G_n}(g)$, então podemos calcular y módulo $C_{G_n}(g)$, escrevendo-o como $y=x_1^{v_1}x_2^{v_2}\cdots x_{2^n+1}^{v_{2^n+1}}$, com $v_i\in\mathbb{Z}/2\mathbb{Z}$. Novamente, como $[g,y]=1$,

$$1=[x_1,x_2]^{u_1v_2+u_2v_1}[x_2,x_3]^{u_2v_3+u_3v_2}$$
$$\cdots$$
$$[x_{k2^n},x_{2^n+1}]^{u_{2^n}v_{2^n+1}+u_{2^n+1}v_{2^n}}.$$

Usando as relações dos comutadores e sabendo que a e b têm ordem 2, podemos reescrever a expressão acima como o par de equações lineares sobre o corpo $\mathbb{F}_2$ nas variáveis $v_1,\cdots,v_{2^n+1}$:

$$u_2v_1 + u_1v_2 + u_4v_3 + u_3v_4 + \cdots + u_{2^n}v_{2^n-1} + u_{2^n-1}v_{2^n} = 0$$
$$u_3v_2 + u_2v_3 + u_5v_4 + u_4v_5 + \cdots + u_{2^n+1}v_{2^n} + u_{2^n}v_{2^n+1} = 0.$$

Considere os seguintes subcasos:
(Subcaso (a)): Suponha que pelo menos um dos $u_1, u_2, \cdots u_{2^n}$ é diferente de zero.
Desde que, por hipótese, $u_{2^n+1} \neq 0$, ambas as equações são não nulas e como $|G_n : C_{G_n}(g)| = 2$, as equações são $\mathbb{F}_2$-linearmente dependentes, como já vimos no caso anterior. Ou seja,

$$u_2 = u_4 = \cdots = u_{2^n} = 0$$
e
$$u_1 = u_3 = \cdots = u_{2^n+1} = 1.$$

Portanto,

$$g \equiv x_1x_3x_5\cdots x_{2^n+1} (\text{mod } Z(G_n)).$$

Porém, isso implica que

$$g^2 = {x_1}^2{x_3}^2\cdots{x_{2^n+1}}^2 = b\cdot 1\cdots 1\cdot b = b^2 = 1,$$

contradizendo a hipótese de que $o(g) = 4$.
(Subcaso (b)): Suponha que $u_1 = u_2 = \cdots = u_{2^n} = 0$.
Temos que $g \equiv x_{2^n+1}(\text{ mod } Z(G_n))$, portanto, similarmente com o caso $k = 1$, temos que (2) é satisfeita pois a condição necessária é satisfeita e (1) também é válida, pois a condição suficiente é falsa:

$$g^2 = {x_{2^n+1}}^2 = b = [x_{2^n}, x_{2^n+1}] = [x_{2^n}, g].$$

Daí, segue o resultado segue. Por fim, vamos mostrar que $\langle x_1, Z(G_n)\rangle$ e $\langle x_{2^n+1}, Z(G_n)\rangle$ são característicos em G_n. De fato, seja $\alpha \in Aut(G_n)$ e suponha, por absurdo, que existe $h \in G_n$ tal que $[{x_1}^\alpha, h] = ({x_1}^\alpha)^2$. Assim,

$$({x_1}^\alpha)^2 = ({x_1}^2)^\alpha = b^\alpha.$$

Por outro lado,

$$[{x_1}^\alpha, h] = [{x_1}^\alpha, {h_1}^\alpha] = [x_1, h_1]^\alpha \in \{1, a^\alpha\}.$$

Note que $b^\alpha = 1$ não ocorre, pois α é automorfismo, e $b^\alpha = a^\alpha$ também não ocorre, pois α é, em particular, injetivo. Logo, não existe $h \in G_n$ tal que $[{x_1}^\alpha, h] = ({x_1}^\alpha)^2$, donde ${x_1}^\alpha \in \langle x_1, Z(G_n)\rangle$ e concluímos que $\langle x_1, Z(G_n)\rangle$ é característico.
Se $\alpha \in Aut(G_n)$, então

$$({x_{2^n+1}}^\alpha)^2 = ({x_{2^n+1}}^2)^\alpha = b^\alpha$$

$$\begin{aligned} &= [x_{2^n+1}, x_{2^n}]^{\alpha} \\ &= [{x_{2^n+1}}^{\alpha}, {x_{2^n}}^{\alpha}], \end{aligned}$$

ou seja, tomando $h = {x_{2^n}}^{\alpha}$, estamos na condição (2) e temos que ${x_{2^n+1}}^{\alpha} \in \langle x_{2^n+1}, Z(G_n)\rangle$. Uma vez que $Z(G_n)$ já é característico, $\langle x_{2^n+1}, Z(G_n)\rangle$ é característico em G_n, como queríamos mostrar.

Afirmação 2: *Cada um dos três subgrupos de ordem 2,* $\langle a\rangle$, $\langle b\rangle$ *e* $\langle ab\rangle$, *é característico em* G_n.

De fato, temos que

$$\langle a\rangle = \{1, a\} = [\langle x_1, Z(G_n)\rangle, G_n].$$

Portanto, segue da Afirmação 1 que $\langle a\rangle$ é característico em G_n. Além disso,

$$\langle b\rangle = \{1, b\} = [x_{2^n+1}, G_n]$$

e, portanto, $\langle b\rangle$ é característico em G_n. Por fim,

$$\langle ab\rangle = \{1, ab\} = \langle Z(G_n) \setminus (\langle a\rangle \cup \langle b\rangle)\rangle$$

e concluímos que $\langle ab\rangle$ é característico em G_n, como queríamos mostrar.

Afirmação 3: *Para cada* $m \in \{0, 1, \cdots, 2^{n-1}\}$, *o subgrupo* $\langle Z(G_n), x_1, x_3, \cdots, x_{2m+1}\rangle$ *é característico em* G_n.

Faremos a demonstração por indução sobre m. A base de indução, $m = 0$, nos dá $\langle Z(G_n), x_1\rangle$ e está clara pela Afirmação 1. Então, assuma que $m \geqslant 1$ e que $\langle Z(G_n), x_1, x_3, \cdots, x_{2m-1}\rangle$ é característico em G_n. Note que se $m = 2^{n-1}$, então

$$\begin{aligned} \langle Z(G_n), x_1, x_3, \cdots, x_{2m+1}\rangle &= \langle \langle Z(G_n), x_1, x_3, \cdots, x_{2m-1}\rangle, \langle Z(G_n), x_{2m+1}\rangle\rangle \\ &= \langle \langle Z(G_n), x_1, x_3, \cdots, x_{2m-1}\rangle, \langle Z(G_n), x_{2(2^{n-1})+1}\rangle\rangle \\ &= \langle \langle Z(G_n), x_1, x_3, \cdots, x_{2m-1}\rangle, \langle Z(G_n), x_{2^n+1}\rangle\rangle. \end{aligned}$$

Logo, o resultado segue da hipótese de indução e da Afirmação 1. Portanto, vamos assumir que $m < 2^{n-1}$. Seja

$$\begin{aligned} H_m &:= C_{G_n}(\langle Z(G_n), x_1, x_3, \cdots, x_{2m-1}\rangle) \\ &= \langle Z(G_n), x_1, x_3, \cdots, x_{2m-1}, x_{2m+1}, x_{2m+2}, \cdots, x_{2^n+1}\rangle\rangle. \end{aligned}$$

Observe que, por hipótese de indução, H_m é característico em G_n, pois o centralizador de um subgrupo característico é característico, e

$$Z(H_m) = \langle Z(G_n), x_1, x_3, \cdots x_{2m-1}\rangle.$$

Mostraremos a seguinte afirmação: "se $g \in H_m$, $[g,H_m] = \langle a \rangle$ e $|H_m : C_{H_m}(g)| = 2$, então $g \in x_{2m+1}Z(H_m)$". Desde que

$$\langle Z(G_n), x_1, x_3, \cdots, x_{2m+1} \rangle = \langle Z(H_m), x_{2m+1}Z(H_m) \rangle,$$

segue que a demonstração dessa afirmação é suficiente para completar a demonstração da Afirmação 3. Escreva

$$g \equiv x_{2m+1}^{u_{2m+1}} \cdots x_k^{u_k} (\bmod Z(H_m))$$

com $u_i \in \mathbb{Z}/2\mathbb{Z}$ e $u_k \neq 0$. Observe que se $k = 2m+1$, então $g \equiv x_{2m+1}^{u_{2m+1}} (\bmod Z(H_m))$ e acabou. Então vamos assumir $k < 2m+1$. Faremos em casos distintos.
(Caso 1): Suponha que $k < 2^n + 1$.
Se $y \in C_{H_m}(g)$, então, calculando y módulo $C_{H_m}(g)$, podemos escrever $y = x_{2m+1}^{v_{2m+1}} \cdots x_{k+1}^{v_{k+1}}$, com $v_i \in \mathbb{Z}/2\mathbb{Z}$. A hipótese de que $1 = [g,y]$ garante que

$$\begin{gathered} 1 = [x_{2m+1}, x_{2m+2}]^{u_{2m+1}v_{2m+2} + u_{2m+2}v_{2m+1}} \\ \cdots \\ [x_{k-1}, x_k]^{u_{k-1}v_k + u_k v_{k-1}} [x_k, x_{k+1}]^{u_k v_{k+1}}. \end{gathered}$$

Temos que essa expressão pode ser escrita como o par de equações sobre $\mathbb{F}_2$:

$$\begin{gathered} u_{2m+2}v_{2m+1} + u_{2m+1}v_{2m+2} + + u_{2m+4}v_{2m+3} + u_{2m+3}v_{2m+4} + \cdots + u_k v_{k+1} = 0 \\ u_{2m+3}v_{2m+2} + u_{2m+2}v_{2m+3} + u_{2m+5}v_{2m+4} + u_{2m+4}v_{2m+5} + \cdots + u_k v_{k-1} + u_{k-1}v_k = 0 \end{gathered}$$

e analogamente, a menos de índices, ao que foi feito na Afirmação 1, como $u_k \neq 0$, essas duas equações são $\mathbb{F}_2$-linearmente independentes, implicando que $|H_m : C_{H_m}(g)| = 2^2 = 4 > 2$, uma contradição.
(Caso 2): Suponha que $k = 2^n + 1$.
Se $y \in C_{H_m}(g)$, então, analogamente ao que já foi feito, analisamos y módulo $C_{H_m}(g)$, obtendo $y = x_{2m+1}^{v_{2m+1}} \cdots x_{2^n+1}^{v_{2^n+1}}$, com $v_i \in \mathbb{Z}/2\mathbb{Z}$. A hipótese de que $1 = [g,y]$ nos garante que

$$\begin{gathered} 1 = [x_{2m+1}, x_{2m+2}]^{u_{2m+1}v_{2m+2} + u_{2m+2}v_{2m+1}} \\ \cdots \\ [x_{2^n}, x_{2^n+1}]^{u_{2^n}v_{2^n+1} + u_{2^n+1}v_{2^n}}. \end{gathered}$$

Usando as relações de comutador, podemos reescrever essa expressão como o par de equações sobre $\mathbb{F}_2$:

$$\begin{gathered} u_{2m+2}v_{2m+1} + u_{2m+1}v_{2m+2} + u_{2m+4}v_{2m+3} + u_{2m+3}v_{2m+4} + \cdots + u_{2^n}v_{2^n-1} + u_{2^n-1}v_{2^n} = 0 \\ u_{2m+3}v_{2m+2} + u_{2m+2}v_{2m+3} + u_{2m+5}v_{2m+4} + u_{2m+4}v_{2m+5} + \cdots + u_{2^n-2}v_{2^n-1} + u_{2^n+1}v_{2^n} + \\ u_{2^n}v_{2^n+1} = 0. \end{gathered}$$

Faremos em dois subcasos:
(Subcaso (a)): Suponha que pelo menos um de $u_{2m+1},\cdots,u_{2^n}$ é diferente de zero. Portanto, desde que $u_{2^n+1}\neq 0$, por hipótese, ambas as equações são diferentes de zero. Desde que $|H_m : C_{H_m}(g)| = 2$, as equações precisam ser $\mathbb{F}_2$-linearmente dependentes. Isso implica que

$$\begin{cases} u_{2^n+1}v_{2^n} + u_{2^n-1}v_{2^n} = 0 & \Rightarrow u_{2^n+1} = u_{2^n-1} = 1 \\ u_{2^n-1}v_{2^n-2} + u_{2^n-3}v_{2^n-2} = 0 & \Rightarrow u_{2^n+1} = u_{2^n-1} = u_{2^n-3} = 1 \\ u_{2^n-3}v_{2^n-4} + u_{2^n-5}v_{2^n-4} = 0 & \Rightarrow u_{2^n+1} = u_{2^n-1} = u_{2^n-3} = u_{2^n-5} = 1 \\ & \vdots \end{cases}$$

e

$$\begin{cases} u_{2^n}v_{2^n-1} + u_{2^n-2}v_{2^n-1} = 0 & \Rightarrow u_{2^n} = u_{2^n-2} = 0 \\ u_{2^n-2}v_{2^n-3} + u_{2^n-4}v_{2^n-3} = 0 & \Rightarrow u_{2^n} = u_{2^n-2} = u_{2^n-4} = 0 \\ u_{2^n-4}v_{2^n-5} + u_{2^n-6}v_{2^n-5} = 0 & \Rightarrow u_{2^n} = u_{2^n-2} = u_{2^n-4} = u_{2^n-6} = 0 \\ & \vdots \end{cases}$$

ou seja,

$$\begin{aligned} u_{2m+1} = u_{2m+3} = \cdots = u_{2^n+1} = 1 \\ u_{2m+2} = u_{2m+4} = \cdots = u_{2^n} = 0. \end{aligned}$$

Daí, temos que

$$g \equiv x_{2m+1}x_{2m+3}\cdots x_{2^n+1}(\bmod Z(H_m)),$$

e, portanto,

$$\begin{aligned} [g, x_{2m+2}] &= [x_{2m+1}, x_{2m+2}]\cdot[x_{2m+2}, x_{2m+3}] \\ &= a\cdot b = ab. \end{aligned}$$

Um absurdo, pois contraria a hipótese de que $[g,H_m] = \langle a\rangle = \{1,a\}$.
(Subcaso (b)): Suponha que $u_{2m+1} = u_{2m+2} = \cdots = u_{2^n} = 0$. Então

$$g \equiv x_{2^n+1}(\bmod Z(H_m))$$

e, portanto,

$$[g,H_m] = \langle [x_{2^n}, x_{2^n+1}]\rangle = \langle b\rangle,$$

contrariando a hipótese que $[g,H_m] = \langle a\rangle$. Logo, para cada $m \in \{0,1,\cdots,2^{n-1}\}$, o subgrupo $\langle Z(G_n), x_1, x_3, \cdots, x_{2m+1}\rangle$ é característico em G_n, como queríamos provar.

No que segue, considere α um automorfismo arbitrário de G_n. Podemos escrever

$$x_i^{\alpha} \equiv x_1^{\alpha_{i,1}} x_2^{\alpha_{i,2}} \cdots x_{2^n+1}^{\alpha_{i,2^n+1}} (\bmod Z(G_n)),$$

para $i \in \{1,2,\cdots 2^n+1\}$ e com $\alpha_{i,j} \in \mathbb{Z}/2\mathbb{Z}$.

Afirmação 4: *Temos que:*

1. $\alpha_{1,1} = 1$, *e* $\alpha_{1,j} = 0$ *para* $j > 1$.
2. $\alpha_{2^n+1,2^n+1} = 1$ *e* $\alpha_{2^n+1,j} = 0$ *para* $j < 2^n+1$.
3. *Para* $i \in \{1,2,\cdots,2^{n-1}-1\}$ *e* $j \in \{1,2,\cdots 2^{n-1}\}$, *segue que:*
   (a) $\alpha_{2i+1,2j} = 0$;
   (b) *se* $j > i$, *então* $\alpha_{2i+1,2j+1} = 0$;
   (c) $\alpha_{2i+1,1} = 0$, *e* $\alpha_{2i+1,2i+1} = 1$.

Começaremos demonstrando (1): Temos que ${x_1}^{\alpha} \in \langle x_1, Z(G_n)\rangle$ pela Afirmação 1, ou seja,

$${x_1}^{\alpha} \equiv x_1 (\bmod Z(G_n)),$$

donde segue que $\alpha_{1,1} = 1$, e $\alpha_{1,j} = 0$ para $j > 1$.
(2) Temos que ${x_{2^n+1}}^{\alpha} \in \langle x_{2^n+1}, Z(G_n)\rangle$ pela Afirmação 1, ou seja,

$${x_{2^n+1}}^{\alpha} \equiv x_{2^n+1} (\bmod Z(G))$$

donde segue que $\alpha_{2^n+1,2^n+1} = 1$ e $\alpha_{2^n+1,j} = 0$ para $j < 2^n+1$.
(3) Uma vez que para cada $m \in \{0,1,\cdots,2^{n-1}\}$, o subgrupo $\langle Z(G_n), x_1, x_3, \cdots, x_{2m+1}\rangle$ é característico em G_n, pela Afirmação 3, os itens (a) e (b) estão demonstrados. Vamos mostrar que $\alpha_{2i+1,1} = 0$, e $\alpha_{2i+1,2i+1} = 1$.
De fato, se $\alpha_{2i+1,1} = 1$, temos, pelo menos, que

$${x_{2i+1}}^{\alpha} \equiv x_1 (\bmod Z(G_n))$$

e, portanto, $o({x_{2i+1}}^{\alpha}) = 4$, uma contradição, pois $o(x_{2i+1}) = 2$. Por fim, se $\alpha_{2i+1,2i+1} = 0$, então

$${x_{2i+1}}^{\alpha} \in \langle Z(G_n), x_1, x_3, \cdots, x_{2^n-1}\rangle,$$

contradizendo o fato de que $\langle Z(G_n), x_1, x_3, \cdots, x_{2^n-1}\rangle$ é característico (Afirmação 3), e o resultado segue.

Afirmação 5: *Para cada* $i \in \{1, 2, \cdots, 2^{n-1}+1\}$*, temos que:*

1. *O subgrupo* $\langle x_{2i-1}, Z(G_n)\rangle$ *é característico em* G_n*.*
2. *Para* $j = 1, 2, \cdots, i-1$*, segue que:*
   (a) $\alpha_{2j,2j} = 1$,
   (b) ${x_{2j}}^{\alpha} {x_{2j}}^{-1} \equiv {x_1}^{\alpha_{2j,1}} {x_3}^{\alpha_{2j,3}} \cdots {x_{2i-1}}^{\alpha_{2j,2i-1}} {x_{2i}}^{\alpha_{2j,2i}} \cdots {x_{2^n+1}}^{\alpha_{2j,2^n+1}} (\ mod\ Z(G_n))$.

Procederemos por indução sobre i. O caso $i = 1$ está claro pela Afirmação 1. Se $i = 2$, então

$$ {x_3}^{\alpha} \equiv {x_1}^{\alpha_{3,1}} {x_2}^{\alpha_{3,2}} {x_3}^{\alpha_{3,3}} (\ \mathrm{mod}\ (Z(G_n)).$$

Daí, segue da Afirmação 4 (3) que o subgrupo $\langle x_3, Z(G_n)\rangle$ é característico em G_n, pois $\alpha_{3,1} = 0$ (Afirmação 4 item 3 (c)) e $\alpha_{3,2} = 0$ (Afirmação 4 item 3(a)) e o item (1) está feito. Note que, se $i = 22$, então $j = 1$ e

$$ {x_2}^{\alpha} \equiv {x_1}^{\alpha_{2,1}} {x_2}^{\alpha_{2,2}} {x_3}^{\alpha_{2,3}} \cdots {x_{2^n+1}}^{\alpha_{2,2^n+1}}\ (\mathrm{mod} Z(G_n))$$

mas, se $\alpha_{2,2} = 0$, então

$$ {x_2}^{\alpha} \equiv {x_1}^{\alpha_{2,1}} {x_3}^{\alpha_{2,3}} \cdots {x_{2^n+1}}^{\alpha_{2,2^n+1}}\ (\mathrm{mod} Z(G_n)),$$

e teríamos que $x_2^{\alpha} \in C_{G_n}(\langle x_1, Z(G_n)\rangle$, contrariando o fato que $C_{G_n}(\langle x_1, Z(G_n)\rangle$, é característico em G_n.
Logo, vamos assumir que $i \geqslant 2$, e que a afirmação foi provada para i. Seja $j \in \{1, 2, \cdots, i-1\}$. Segue da hipótese de indução que

$$ {x_{2j}}^{\alpha} \equiv x_{2j} {x_1}^{\alpha_{2j,1}} {x_3}^{\alpha_{2j,3}} \cdots {x_{2i-1}}^{\alpha_{2j,2i-1}} {x_{2i}}^{\alpha_{2j,2i}} \cdots {x_{2^n+1}}^{\alpha_{2j,2^n+1}} (\ \mathrm{mod}\ Z(G_n)),$$

e uma vez que $\langle x_{2i-1}, Z(G_n)\rangle$ é característico em G_n, segue que

$$ {x_{2i-1}}^{\alpha} \equiv x_{2i-1} (\ \mathrm{mod}\ Z(G_n)).$$

Se $j < i-1$, então $1 = [x_{2j}, x_{2i-1}]$, pois $|2j - (2i-1)| > 1$ e, portanto,

$$ 1^{\alpha} = 1 = [x_{2i-1}, x_{2j}]^{\alpha} = [{x_{2i-1}}^{\alpha}, {x_{2j}}^{\alpha}].$$

Substituindo pelas expressões acima e sabendo que $[x_i, x_j] = 1$ sempre que $|i-j| > 1$, segue que

$$1 = [x_{2i-1}{}^{\alpha}, x_{2j}{}^{\alpha}] = [x_{2i-1}, x_{2j}]^{\alpha_{2j,2i}}.$$

Note que x_{2i-2} não ocorre uma vez que $j < i-1$. Portanto,

$$1 = [x_{2i-1}, x_{2j}]^{\alpha_{2j,2i}} = a^{\alpha_{2j,2i}},$$

donde segue que $\alpha_{2j,2i} = 0$.
Se $j = i-1$, então aplicando α em

$$b = [x_{2i-2}, x_{2i-1}][x_{2j}, x_{2i-1}],$$

temos que

$$b^{\alpha} = [x_{2i-2}, x_{2i-1}]^{\alpha} = [x_{2i-2}{}^{\alpha}, x_{2i-1}{}^{\alpha}].$$

Como $\langle b \rangle$ é característico (Afirmação 2), $b^{\alpha} = b$ e observe que

$$\begin{cases} x_{2i-2}{}^{\alpha} \equiv x_{2i-2} x_1{}^{\alpha_{2i-2,1}} x_3{}^{\alpha_{2i-2,3}} \cdots x_{2i-1}{}^{\alpha_{2i-2,2i-1}} x_{2i}{}^{\alpha_{2i-2,2i}} \cdots x_{2^n+1}{}^{\alpha_{2i-2,2^n+1}} (\bmod Z(G_n)) \\ x_{2i-1}{}^{\alpha} \equiv x_{2i-1} (\bmod Z(G_n)). \end{cases}$$

Portanto, sabendo que os únicos elementos que não comutam com x_{2i-1} são x_{2i-2} e x_{2i}, temos que

$$[x_{2i-2}{}^{\alpha}, x_{2i-1}{}^{\alpha}] = [x_{2i-2}, x_{2i-1}] = [x_{2i-1}, x_{2i}]^{\alpha_{2i-2,2i}},$$

ou seja,

$$b = [x_{2i-2}, x_{2i-1}][x_{2i-1}, x_{2i}]^{\alpha_{2i-2,2i}} = b \cdot a^{\alpha_{2i-2,2i}},$$

e segue, novamente, que $\alpha_{2j,2i} = 0$. Logo, mostramos que para $j = 1, 2, \cdots, i-1$ temos $\alpha_{2j,2i} = 0$. Donde segue, juntamente com a hipótese de indução e com a Afirmação 3, que

$$\begin{aligned} x_{2j}{}^{\alpha} &\equiv x_{2j} x_1{}^{\alpha_{2j,1}} x_3{}^{\alpha_{2j,3}} \cdots x_{2i-1}{}^{\alpha_{2j,2i-1}} x_{2i+1}{}^{\alpha_{2j,2i+1}} \cdots x_{2^n+1}{}^{\alpha_{2j,2^n+1}} (\bmod Z(G_n)) \\ x_{2i+1}{}^{\alpha} &\equiv x_3{}^{\alpha_{2i+1,3}} x_5{}^{\alpha_{2i+1,5}} \cdots x_{2i+1}{}^{\alpha_{2i+1,2i+1}} (\bmod Z(G_n)). \end{aligned}$$

Além disso, como $1 = [x_{2j}, x_{2i+1}]$ então ao aplicarmos α em ambos os lados da igualdade e procedermos de maneira análoga ao que foi feito anteriormente temos que

$$\begin{aligned} 1 &= [x_{2j-1}, x_{2j}]^{\alpha_{2i+1,2j-1}} [x_{2j}, x_{2j+1}]^{\alpha_{2i+1,2j+1}} [x_{2i+1}, x_{2i+2}]^{\alpha_{2j,2i+2}\alpha_{2i+1,2i+1}} \\ &= a^{\alpha_{2i+1,2j-1}\alpha_{2j,2i+2}\alpha_{2i+1,2i+1}} b^{\alpha_{2i+1,2j+1}}, \end{aligned}$$

o que implica que $\alpha_{2i+1,2j+1} = 0$.
Portanto, mostramos que, para $j = 1, 2, 3, \cdots i-1$, $\alpha_{2i+1,2j+1} = 0$. Donde segue, juntamente

com a Afirmação 4, que $\langle x_{2i+1}, Z(G_n)\rangle$ é característico em G_n.
Por fim, por definição, temos que

$$x_{2i}{}^{\alpha} \equiv x_1{}^{\alpha_{2i,1}} x_2{}^{\alpha_{2i,2}} \cdots x_{2^n+1}{}^{\alpha_{2i,2^n+1}} (\text{mod } Z(G_n))$$

e por hipótese de indução,

$$x_{2j+1}{}^{\alpha} \equiv x_{2j+1}(\text{ mod } Z(G_n)).$$

Se $j < i-1$, então segue de $1 = [x_{2i,2j+1}]$ que

$$\begin{aligned} 1^{\alpha} = 1 &= [x_{2i}, x_{2j+1}]^{\alpha} = [x_{2i}{}^{\alpha}, x_{2j+1}{}^{\alpha}] \\ &= [x_{2j}, x_{2j+1}]^{\alpha_{2i,2j}} [x_{2j+1}, x_{2j+2}]^{\alpha_{2i,2j+2}} \\ &= b^{\alpha_{2i,2j}} a^{\alpha_{2i,2j+2}}, \end{aligned}$$

ou seja, $\alpha_{2i,2j} = \alpha_{2i,2j+2} = 0$. Isso mostra que, para $j = 1, 2, \cdots, i-1$, $\alpha_{2i,2j} = 0$. Assim, para concluirmos a demonstração indutiva, resta apenas mostrar que $\alpha_{2i,2i} = 1$. De fato, suponha o contrário por contradição. Então,

$$x_{2i}{}^{\alpha} \equiv x_1{}^{\alpha_{2i,1}} x_3{}^{\alpha_{2i,3}} \cdots x_{2i-1}{}^{\alpha_{2i,2i-1}} (\text{mod } Z(G_n)),$$

donde segue que $x_{2i}{}^{\alpha} \in C_{G_n}(\langle Z(G_n), x_1, x_3, \cdots, x_{2i-1}\rangle)$, contrariando o fato que o subgrupo $C_{G_n}(\langle Z(G_n), x_1, x_3, \cdots, x_{2i-1}\rangle)$ é característico em G_n. Logo, $\alpha_{2i,2i} = 1$ e o resultado segue.
Afirmação 6: *Para todo* $j \in \{1, 2, \cdots 2^{n-1}\}$, *temos que*

$$\alpha_{2i,2j} = \begin{cases} 1 \textit{ se } i = j, \\ 0 \textit{ caso contrário}. \end{cases}$$

Em outras palavras,

$$x_{2i}{}^{\alpha} \equiv x_{2i} x_1{}^{\alpha_{2i,1}} x_3{}^{\alpha_{2i,3}} \cdots x_{2^n+1}{}^{\alpha_{2i,2^n+1}} (\textit{ mod } Z(G_n)).$$

Esse resultado segue diretamente da Afirmação 5 quando $i = 2^{n-1} + 1$.

Note que pelas Afirmações 5 e 6, sabemos que módulo $Z(G_n)$, α fixa todos os elementos com índices ímpar, ou seja, $x_1, x_3, \cdots, x_{2^n+1}$, e mapeia cada um dos $x_2, x_4, \cdots, x_{2^n}$ nele mesmo vezes algum produto de $x_1, x_3, \cdots, x_{2^n+1}$. A próxima afirmação fará algumas restrições nesses fatores de índices ímpar.
Afirmação 7: *Sejam* $i, j \in \{1, 2, \cdots, 2^{n-1}\}$. *Então:*

1. $\alpha_{2i,2i-1} = 0$.

2. $\alpha_{2j,2i-1} = \alpha_{2i,2j-1}$ *e* $\alpha_{2j,2i+1} = \alpha_{2i,2j+1}$.

De fato, para (1), observe que se $\alpha_{2i,2i-1} = 1$, então

$$x_{2i}{}^{\alpha} \equiv x_{2i} x_1{}^{\alpha_{2i,1}} \cdots x_{2i-3}{}^{\alpha_{2i,2i-3}} x_{2i-1} x_{2+1}{}^{\alpha_{2i,2i+1}} \cdots x_{2^n+1}{}^{\alpha_{2i,2^n+1}} (\text{mod } Z(G_n))$$

e, portanto,

$$\begin{aligned}(x_{2i}{}^{\alpha})^2 &= [x_{2i-1}, x_{2i}] \cdot [x_{2i}, x_{2i+1}]^{\alpha_{2i,2i+1}} \cdot x_{2i}{}^2 \cdot \prod_{k=1}^{2^{n-1}} x_{2k+1}{}^{2\alpha_{2i,2k+1}} \\ &= a \cdot b^{\alpha_{2i,2i+1}} \cdot b^{\alpha_{2i,1}+\alpha_{2i,2^n+1}} \neq 1,\end{aligned}$$

contradizendo o fato que $o(x_{2i}) = 2$.
Para a demonstração de (2), note que

$$\begin{aligned}x_{2i}{}^{\alpha} &\equiv x_{2i} x_1{}^{\alpha_{2i,1}} x_3{}^{\alpha_{2i,3}} \cdots x_{2i-3}{}^{\alpha_{2i,2i-3}} x_{2i+1}{}^{\alpha_{2i,2i+1}} \cdots x_{2^n+1}{}^{\alpha_{2i,2^n+1}} (\text{ mod } Z(G_n)) \\ x_{2j}{}^{\alpha} &\equiv x_{2j} x_1{}^{\alpha_{2j,1}} x_3{}^{\alpha_{2j,3}} \cdots x_{2j-3}{}^{\alpha_{2j,2j-3}} x_{2j+1}{}^{\alpha_{2j,2j+1}} \cdots x_{2^n+1}{}^{\alpha_{2j,2^n+1}} (\text{ mod } Z(G_n)).\end{aligned}$$

Segue de $1 = [x_{2i}, x_{2j}]$ que

$$1^{\alpha} = 1 = [x_{2i}, x_{2j}]^{\alpha} = [x_{2i}{}^{\alpha}, x_{2j}{}^{\alpha}]$$

e, portanto, analogamente ao que foi feito anteriormente, segue que

$$\begin{aligned}1 &= [x_{2i-1}, x_{2i}]^{\alpha_{2j,2i-1}} [x_{2i}, x_{2i+1}]^{\alpha_{2j,2i+1}} [x_{2j-1}, x_{2j}]^{\alpha_{2i,2j-1}} [x_{2j}, x_{2j+1}]^{\alpha_{2i,2j+1}} \\ &= a^{\alpha_{2j,2i-1}+\alpha_{2i,2j-1}} \cdot b^{\alpha_{2j,2i+1}+\alpha_{2i,2j+1}}.\end{aligned}$$

Donde segue que

$$\begin{cases} \alpha_{2j,2i-1} = \alpha_{2i,2j-1} \\ \alpha_{2j,2i+1} = \alpha_{2i,2j+1} \end{cases}$$

como queríamos mostrar.

Afirmação 8: *Temos que:*

1. *Para cada* $i \in \{1, 2, \cdots, 2^{n-1} - 1\}$*, o subgrupo* $\langle x_{2i}, Z(G_n) \rangle$ *é característico em* G_n.

2. *A união das classes laterais* $x_{2^n} Z(G_n) \bigcup x_{2^n} x_{2^n+1} Z(G_n)$ *é um subconjunto característico de* G_n.

Segue da Afirmação 7 (2) que, se $\alpha_{2k,2l-1} = 0$ para alguns $k \in \{1,2,\cdots,2^{n-1}\}$ e $l \in \{1,2,\cdots,2^{n-1}+1\}$, então podemos concluir que $\alpha_{e,o} = 0$ para todos os pares $(e,o) \in \{1,2,\cdots,2^n+1\}^2$ em que e é par, o é ímpar, e $e+o = 2k+2l-1$. Isso ocorre pois, se $2k-2, 2l+1 \in \{1,\cdots,2^n+1\}$, então, segue diretamente da primeira parte da Afirmação 7 (2) que

$$\alpha_{2k,2l-1} = \alpha_{2l,2k-1} = \alpha_{2k-1,2l+1},$$

e se $2l-3, 2k+2 \in \{1,2,\cdots,2^n+1\}$, então segue da segunda parte que

$$\alpha_{2k,2l-1} = \alpha_{2l-2,2k+1} = \alpha_{2k+2,2l-3}.$$

Portanto, pela Afirmação 7 (1), concluímos que $\alpha_{e,o} = 0$, sempre que $e+o \equiv 3 (\text{mod } 4)$, uma vez que

$$(2i) + (2i-1) = 4i - 1 \equiv 3 (\text{mod } 4).$$

Provaremos mais geral, para cada $k = 2,3,\cdots,n+1$, $\alpha_{e,o} = 0$ sempre que $e+o \equiv 1 + 2^{k-1} (\text{mod } 2^k)$.
De fato, mostraremos por indução sobre k, com a base de indução sendo $k = 2$, feito acima. Assuma que $k \leqslant n$, e que $\alpha_{e,o} = 0$, sempre que $e+o \equiv 1 + 2^{k-1} (\text{mod } 2^k)$. Então, em particular, $\alpha_{\varepsilon,1} = \alpha_{\varepsilon,2^n+1} = 0$ sempre que $\varepsilon \in \{1,2,\cdots,2^n+1\}$ e $\varepsilon \equiv 2^{k-1} (\text{mod } 2^k)$.
Se $\alpha_{\varepsilon,\varepsilon+1} = 1$, então uma vez que ε é par, segue das Afirmações 6 e 7(1) que $\alpha_{\varepsilon,\varepsilon-1} = 0$ e, portanto,

$$(x_\varepsilon^\alpha)^2 = [x_\varepsilon, x_{\varepsilon+1}] = b \neq 1$$

uma contradição.
Por isso, $\alpha_{\varepsilon,\varepsilon+1} = 0$ para todo $\varepsilon \in \{1,2,\cdots,2^n+1\}$ com $\varepsilon \equiv 2^{k-1} (\text{mod } 2^k)$, e portanto, $\alpha_{e,o} = 0$ para todos os pares $(e,o) \in \{1,2,\cdots,2^n+1\}^2$, onde e é par, o é ímpar e $e+o \equiv 1 + 2^k (\text{mod } 2^k)$. Isso mostra que $\langle x_{2i}, Z(G_n)\rangle$ é característico em G_n, como queríamos.
Em particular, segue que $\langle x_{2^n}, Z(G_n)\rangle$ é característico em G_n e juntamente com Afirmação 5, temos que a união das classes laterais $x_{2^n}Z(G_n) \bigcup x_{2^n}x_{2^n+1}Z(G_n)$ é um subconjunto característico de G_n e acabou.
Equivalentemente ao que acabamos de fazer por indução sobre k, temos que $\alpha_{e,o} = 0$ para todos os pares $(e,o) \in \{1,2,\cdots,2^n+1\}^2$, onde e é par e o é ímpar a menos que $e+o \equiv 1 + 2^k (\text{mod } 2^{k+1})$, isto é, a menos que $(e,o) = (2^n, 2^n+1)$. Isso com a Afirmação 6, prova a Afirmação 8.

Agora, podemos concluir a demonstração da Proposição 3.1.1: Pelas Afirmações 5 e 8, temos que módulo $Aut_{cent}(G_n)$, todo automorfismo de G_n ou fixa todos os geradores de G_n,

ou mapeia $x_{2^n} \mapsto x_{2^n}x_{2^n+1}$ enquanto fixa todos os outros geradores de G_n.
Em outras palavras, módulo $Aut_{cent}(G_n)$, todo automorfismo de G_n ou fixa os geradores ou é α_n, o automorfismo não central definido anteriormente, ou seja, todo automorfismo de G_n age na união das classes laterais $Aut_{cent}(G_n) \bigcup Aut_{cent}(G_n)\alpha_n$ e daí

$$|Aut(G_n) : Aut_{cent}(G_n)| = 2,$$

como queríamos mostrar.
Por fim, observe que $Aut_{cent}(G_n)$ age transitivamente nas classes laterais não triviais do centro $Z(G_n)$ e, uma vez que $|Z(G_n)| = 4$, segue que $maol(G_n) = 8$, $\forall n \in \mathbb{N}$. Em outras palavras, existem infinitos grupos finitos com *maol* igual a 8.

Capítulo 4

Considerações finais

Este trabalho teve como objetivo principal o estudo de grupos que possuem poucos elementos em suas órbitas por automorfismos. Em particular, caracterizamos todos os grupos G tais que $maol(G) \in \{1,2,3\}$, e mostramos que existe uma família infinita de 2-grupos finitos satisfazendo *maol* igual a8.

O estudo de grupos que satisfazem outros valores de *maol*, assim como a resposta da problemática *"Qual valor $n \in \mathbb{Z}^+$, tal que $\forall k < n$, há apenas uma quantidade finita de grupos G, satisfazendo $maol(G) = k$?"* estão em aberto e ficam como sugestão para trabalhos futuros.

Foi feito um código na ferramenta GAP, vide figura a seguir.

```
>maol:= function (G)
  local  m, n, g, k;
  k:=[];;
   n := AutomorphismGroup(G);
   for g in G do
    m:= Orbit(n, g);
    Add(k, Set(m));
   od;
  return Maximum(List (Set(k), x -> Size(x)));
 end;
[ function( G ) ... end
```

Figura 4.1 Código GAP

Com o auxílio desse código, verificamos que os seguintes grupos possuem *maol* igual a 4: os cíclicos de ordens 5, 8, 10 e 12; $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$; o grupo diedral D_8 com 8 elementos, e o grupo quasidiedral $QD_{2^n} = \langle r,s \; ; \; r^{2^{n-1}} = s^2 = 1 \; , \; srs = r^{2^{n-2}-1} \rangle$, para $n = 4$, com 16 elementos.

O código foi rodado percorrendo os grupos tais que $|G| \leqslant 630$, salve os grupos com ordens 128, 314 e 512, em que o limite de tempo do programa foi excedido (*). Em vista que 16 é a maior ordem dos grupos cujo tamanho máximo de uma órbita por automorfismos é 4, é intuitiva a ideia de que esses podem ser, de fato, os únicos grupos finitos que satisfazem *maol* igual a 4.

A seguir temos uma tabela explicitando todos os grupos encontrados com o auxílio da ferramenta GAP, tais que $maol(G) \in \{4,5,6,7\}$:

Tabela 4.1 Grupos G tais que $maol(G) \in \{4,5,6,7\}$

$maol(G)$	G	$\lvert G\rvert$
	$\mathbb{Z}/m\mathbb{Z}$, com $m \in \{5,8,10,12\}$	{5, 8, 10, 12}
4	$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	8
	D_8	8
	QD_{16}	16
5	D_{10}	10
	$\mathbb{Z}/5\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$	20
	$\mathbb{Z}/7\mathbb{Z}$	7
	Q_8	8
	$\mathbb{Z}/9\mathbb{Z}$	9
	$\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$	12
	D_{12}	12
6	$\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	12
	$\mathbb{Z}/14\mathbb{Z}$	14
	$(\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \rtimes \mathbb{Z}/2\mathbb{Z}$	16
	$\mathbb{Z}/18\mathbb{Z}$	18
	$\mathbb{Z}/3\mathbb{Z} \times Sym(3)$	18
	$\mathbb{Z}/4\mathbb{Z} \times Sym(3)$	24
	$(\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \rtimes \mathbb{Z}/2\mathbb{Z}$	24
	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	8
	D_{14}	14
7	$\mathbb{Z}/7\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z}$	21
	$(\mathbb{Z}/7\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z}) \rtimes \mathbb{Z}/2\mathbb{Z}$	42
	$\mathbb{Z}/2\mathbb{Z}(\mathbb{Z}/7\mathbb{Z}) \rtimes \mathbb{Z}/3\mathbb{Z})$	42

Note que o maior grupo dessa lista tem ordem 42, e o código foi rodado percorrendo grupos tais que $|G| \leqslant 630$, salvo algumas exceções (*).

Neste trabalho, encontramos uma família infinita de 2-grupos finitos cujo *maol* é igual a 8. Ao rodarmos o código restringindo a esse valor, ficou evidente que o grau de liberdade da

estrutura dos grupos, que satisfazem esse comprimento máximos das órbitas por automorfismos, é muito alto. De fato, na tabela a seguir explicitamos os 55 grupos G, encontrados utilizando o algoritmo citado anteriormente, satisfazendo $maol(G) = 8$ e $|G| \leqslant 100$. Note que aparecem diversos grupos que não são 2-grupos. Dada a quantidade dos grupos, eles estão separados pelas suas ordens na tabela.

Tabela 4.2 Grupos G tais que $maol(G) = 8$

G	$\|G\|$
$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$	9
A_4	12
$\mathbb{Z}/15\mathbb{Z}$	15
$\mathbb{Z}/16\mathbb{Z}$; $(\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \rtimes \mathbb{Z}/2\mathbb{Z}$; $\mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$; $\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$; D_{16}; Q_{16} $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$; $\mathbb{Z}/2\mathbb{Z} \times D_8$	16
$\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$	18
$\mathbb{Z}/20\mathbb{Z}$	20
$\mathbb{Z}/24\mathbb{Z}$; $SL(2,3)$; $\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$; $\mathbb{Z}/3\mathbb{Z} \times D_8$; $Sym(4)$; $\mathbb{Z}/2\mathbb{Z} \times A_4$	24
$\mathbb{Z}/30\mathbb{Z}$	30
$(\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \rtimes \mathbb{Z}/2\mathbb{Z}$; $Q_8 \rtimes \mathbb{Z}/4\mathbb{Z}$; $(\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}) \rtimes \mathbb{Z}/2\mathbb{Z}$; QD_{32}; $\mathbb{Z}/4\mathbb{Z} \times D_8$; $(\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \rtimes \mathbb{Z}/2\mathbb{Z}$; $(\mathbb{Z}/2\mathbb{Z} \times Q_8) \rtimes \mathbb{Z}/2\mathbb{Z}$; $(\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \rtimes \mathbb{Z}/2\mathbb{Z}$; $\mathbb{Z}/2\mathbb{Z} \times QD_{16}$; $(\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}) \rtimes \mathbb{Z}/2\mathbb{Z}$; $(\mathbb{Z}/2\mathbb{Z}Q_8) \rtimes \mathbb{Z}/2\mathbb{Z}$; $(\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \rtimes \mathbb{Z}/2\mathbb{Z}$; $(\mathbb{Z}/2\mathbb{Z}D_8) \rtimes \mathbb{Z}/2\mathbb{Z}$	32
$\mathbb{Z}/3\mathbb{Z} \times QD_{16}$	48
$(\mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}) \rtimes \mathbb{Z}/4\mathbb{Z}$; $(\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})\mathbb{Z}/2\mathbb{Z}$; $(\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \rtimes \mathbb{Z}/2\mathbb{Z}$; $(\mathbb{Z}/2\mathbb{Z} \times D_{16}) \rtimes \mathbb{Z}/2\mathbb{Z}$; $(\mathbb{Z}/2\mathbb{Z} \times Q_{16}) \rtimes \mathbb{Z}/2\mathbb{Z}$; $(\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \times \mathbb{Z}/2\mathbb{Z}$; $(\mathbb{Z}/2\mathbb{Z} \times Q_{16}) \rtimes \mathbb{Z}/2\mathbb{Z}$; $(\mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/8\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z})) \rtimes \mathbb{Z}/2\mathbb{Z}$; $(\mathbb{Z}/4\mathbb{Z} \times D_8) \rtimes \mathbb{Z}/2\mathbb{Z}$; $\mathbb{Z}/4\mathbb{Z} \times QD_{16}$; $(\mathbb{Z}/2\mathbb{Z} \times QD_{16}) \rtimes \mathbb{Z}/2\mathbb{Z}$; $(\mathbb{Z}/8\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}) \rtimes \mathbb{Z}/2\mathbb{Z}$; $((\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \rtimes \mathbb{Z}/2\mathbb{Z}) \rtimes \mathbb{Z}/2\mathbb{Z}$; $(\mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/8\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z})) \rtimes \mathbb{Z}/2\mathbb{Z}$; $(\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \rtimes \mathbb{Z}/2\mathbb{Z}$; $((\mathbb{Z}/4\mathbb{Z} \times D_8) \rtimes \mathbb{Z}/2\mathbb{Z}$; $(\mathbb{Z}/4\mathbb{Z}Q_8) \rtimes \mathbb{Z}/2\mathbb{Z}$; $(\mathbb{Z}/4\mathbb{Z} \times D_8) \rtimes \mathbb{Z}/2\mathbb{Z}$; $(\mathbb{Z}/4\mathbb{Z} \times Q_8) \rtimes \mathbb{Z}/2\mathbb{Z}$; $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times D_8) \rtimes \mathbb{Z}/2\mathbb{Z}$;	64

Por fim, o mesmo teste foi feito restringindo os grupos com *maol* igual a 9 ou 10, afim de saber se o grau de liberdade dos grupos que satisfazem esses *maol* também é alto. Entretanto, observa-se que isso não ocorre. Foram encontramos apenas três grupos tais que $maol(G) = 9$

e $|G| \leqslant 630$, salvo algumas exceções (*), e dez grupos com $maol(G) = 10$ e $|G| \leqslant 630$ (*), como podemos ver na tabela a seguir:

Tabela 4.3 Grupos G tais que $maol(G) \in \{9, 10\}$

$maol(G)$	G	|G|
9	D_{18}	18
	$(\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}) \rtimes \mathbb{Z}/2\mathbb{Z}$	18
	$(\mathbb{Z}/9\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z}) \rtimes \mathbb{Z}/2\mathbb{Z}$	54
10	$\mathbb{Z}/11\mathbb{Z}$	11
	$\mathbb{Z}/5\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$	20
	D_{20}	20
	$\mathbb{Z}/22\mathbb{Z}$	22
	$\mathbb{Z}/3\mathbb{Z} \times D_{10}$	30
	$\mathbb{Z}/5\mathbb{Z} \rtimes \mathbb{Z}/8\mathbb{Z}$	40
	$\mathbb{Z}/4\mathbb{Z} \times D_{10}$	40
	$(\mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \rtimes \mathbb{Z}/2\mathbb{Z}$	40
	$\mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/5\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z})$	40
	$\mathbb{Z}/3\mathbb{Z} \times (\mathbb{Z}/5\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z})$	60

Portanto, algumas perguntas seguem em evidência:

Questão 1. Existe $4 \leqslant k \leqslant 7$*, tal que há apenas uma quantidade finita grupos finitos com* $maol \leqslant k$*?*

Questão 2. Para todo k maior do que 8*, existe uma quantidade infinita de grupos finitos com maol igual a k?*

Essas e todas as outras questões abordadas nesse capítulo são temas para pesquisas futuras.

Referências Bibliográficas

[1] R. Bastos and A. C. Dantas, On finite groups with few automorphism orbits, *Comm. Algebra* **44** (2016), no. 7, 2953–2958.

[2] A. Bors, Finite groups with only small automorphism orbits, *J. Group Theory*23 (2020), no. 4, 659-696.

[3] A. C. Dantas, M. Garonzi and R. Bastos, Finite groups with six or seven automorphism orbits, *J. Group Theory* **20** (2017), no. 5, 945–954.

[4] D. Gorenstein, *Finite Groups*, segunda edição, Chelsea Publishing Company, Nova York, (1980).

[5] T. J. Laffey and D. MacHale, Automorphism orbits of finite groups, *J. Aust. Math. Soc. Ser. A* **40** (1986), no. 2, 253–260.

[6] W. Ledermann and B. H. Neumann, On the order of the automorphism group of a finite group. *I, Proc. Roy. Soc. London Ser. A* **233** (1956), 494–506.

[7] B. H. Neumann, Groups covered by permutable subsets. *J. London Math Soc*. **29**, (1954). 236–248.

[8] B. H. Neumann, Groups Whose Elements Have Bounded Orders, *Journal of the London Mathematical Society*, **12** (1937), no. 3, 195–198.

[9] D. J. S. Robinson, *A Course in the Theory of Groups*, 2nd ed., Grad. Texts in Math.80, Springer, New York, (1996).

[10] D. J. S. Robinson and J. Wiegold, Groups with boundedly finite automorphism classes, *Rend. Semin. Mat. Univ. Padova* **71** (1984), 273–286.

[11] M. Stroppel, Locally compact groups with few orbits under automorphisms, *Topol. Proc.* **26** (2002), no. 2, 819–842.

[12] J. Wiegold, Groups with boundedly finite classes of conjugate elements, *Proc. Roy. Soc. London Ser. A* **238** (1957), 389-401.

[13] D. L. Winter, The automorphism group of an extraspecial p-group, *Rocky Mountain J. Math.* **2** (1972), no. 2, 159–168.