Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

Sobre $p\mathcal{E}$-grupos e $p\mathcal{A}$-grupos finitos

Marina Gabriella Ribeiro Bardella

Orientador: Prof. Noraí Romeu Rocco

Brasília, 07 de março de 2012

Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

Sobre *p*E-grupos e *p*A-grupos finitos.

por

Marina Gabriella Ribeiro Bardella*

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

MESTRE EM MATEMÁTICA

Brasília, 07 de março de 2012.

Comissão Examinadora:

Prof. Noraí Romeu Rocco – MAT/UnB (Orientador)

Prof. Ricardo Nunes de Oliveira – IME/UFG

Prof. Marco Antonio Pellegrini – MAT/UnB

*A autora foi bolsista CNPq durante a elaboração desta dissertação.

Resumo

Um grupo G é um E-grupo (respectivamente, A-grupo) se G é tal que seus elementos comutam com suas respectivas imagens endomorfas (respectivamente, automorfas).

Neste trabalho, estudamos algumas propriedades de E-grupos baseadas nos artigos "3-generator groups whose elements commute with their endomorphic images are abelian" e "Minimal number of generators and minimum order of a non-abelian group whose elements commute with their endomorphic images", ambos de A. Abdollahi, A. Faghihi e A. Mohammadi Hassanabadi.

É possível mostrar que qualquer E-grupo e A-grupo possui classe de nilpotência no máximo 3. Em "Finite 3-groups of class 3 whose elements commute with their automorphic images", A. Abdollahi, A. Faghihi, S. A. Linton, e E. A. O'Brien mostraram que esse máximo é atingido; para isso construíram um exemplo de um A-grupo de classe de nilpotência exatamente 3. Baseado nesse artigo, estudamos os aspectos teóricos e certos detalhes dos algoritmos (e suas implementações) usados para a construção de tal grupo.

Palavras-chave: E-grupos, A-grupos, automorfismos, endomorfismos, p-grupos finitos, grupos nilpotentes, condições de Engel, GAP - Groups, Algorithms and Programming.

Abstract

A group G is an E-group (respectively A-group) if G is such that its elements commute with their endomorphic (respectively automorphic) images.

In this work, we study some properties of E-groups based on the papers "3-generator groups whose elements commute with their endomorphic images are abelian" and "Minimal number of generators and minimum order of a non-abelian group whose elements commute with their endomorphic images", both by A. Abdollahi, A. Faghihi and A. Mohammadi Hassanabadi.

It is possible to show that such groups have nilpotency class at most 3. In "Finite 3-groups of class 3 whose elements commute with their automorphic images", A. Abdollahi, A. Faghihi, S. A. Linton, and E. A. O'Brien showed that this maximum is reached. To do so they constructed an A-group having nilpotency class precisely 3. Based on this paper, we study the theorectical aspects and certain details of the algorithms (and their implementations) used for the construction of such group.

Key-words: E-groups, A-groups, automorphisms, endomorphisms, finite p-groups, nilpotent groups, Engel's conditions, GAP - Groups, Algorithms and Programming.

À minha mãe.

Agradecimentos

Se cheguei onde estou é porque muitas pessoas tornaram isso possível. Assim, tenho muito a agradecer.

Primeiramente, agradeço a Deus pelas graças alcançadas e por me carregar no colo nas horas de aflições.

Agradeço ao professor Noraí pela sua orientação, com sua imensa paciência, dedicação e, principalmente, por acreditar que este trabalho fosse possível, mesmo quando nem eu acreditava.

Aos professores da banca examinadora, Marco Antonio Pellegrini e Ricardo Nunes de Oliveira não só pelas valiosas correções e sugestões deste trabalho, mas também pelo auxílio no desenvolvimento desta dissertação.

Agradeço ao professor Theo Zapatta pela disposição em me ajudar e ao professor Eamonn A. O'Brien pela sua atenção.

Agradeço a todos os meus professores, que sempre me incentivaram. Em especial, aos professores Celius Magalhães, João Carlos Pádua e Mauro Rabelo.

Agradeço aos funcionários do Departamento de Matemática - UnB.

Agradeço ao CNPq pelo apoio financeiro.

Agradeço à minha família por todo apoio e compreensão, especialmente à minha mãe, Regina, pelo exemplo de coragem e por seu amor incondicional, estando ao meu lado em todos os momentos da minha vida e aos meus irmãos, Vinicius, Carolina e Arthur, por tornarem minha vida mais divertida.

Agradeço ao meu namorado, Aristóteles, que me ajudou significativamente para que este trabalho fosse possível.

Enfim, agradeço aos meus amigos e colegas que de uma forma ou de outra marcaram minha vida, principalmente aos meus amigos matemáticos que conviveram comigo nos últimos anos.

Sumário

NOTAÇÃO

$\mathbb{N}$, $\mathbb{Z}$:	conjunto dos números naturais e inteiros, respectivamente.
$\hookrightarrow$:	homomorfismo injetor.
$\twoheadrightarrow$:	homomorfismo sobrejetor.
$\cong$:	isomorfismo.
$H \leq G$:	H é subgrupo de G.
$H < G$:	H é subgrupo próprio de G.
$H \trianglelefteq G$:	H é subgrupo normal de G.
$\langle X \rangle$:	grupo gerado pelo conjunto X.
$\|G\|$:	ordem (cardinalidade) de G.
$[x, y] = x^{-1}y^{-1}xy$:	o comutador de x e y.
$[A, B]$:	subgrupo comutador dos conjuntos A e B.
G':	subgrupo derivado de G.
$Z(G)$:	centro de G.
$C_G(H)$:	centralizador de H em G, $C_G(H) = \{g \in G \mid g^{-1}hg = h; h \in H\}$.
$N_G(H)$:	normalizador de H em G, $N_G(H) = \{g \in G \mid g^{-1}Hg = H\}$.
$Aut(G)$:	grupo dos automorfismos de G.
$Inn(G)$:	grupo dos automorfismos internos de G.
$Aut_c(G)$:	grupo dos automorfismos centrais de G.
x^{φ}:	$\varphi(x)$, em que φ é um homomorfismo.
$G \times H$:	produto direto de G por H.
$\Phi(G)$:	subgrupo de Frattini de G.
$cl(G)$:	classe de nilpotência de G.
C_n:	grupo cíclico de ordem n.

Introdução

Um grupo G é dito *nilpotente* se existe uma cadeia finita $G = G_0 \geq G_1 \geq \ldots \geq G_n = 1$ tal que $G_{i+1} \trianglelefteq G_i$ e $G_i/G_{i+1} \leq Z(G/G_{i+1})$, para todo inteiro i com $0 \leq i \leq n-1$, em que $Z(G/G_{i+1})$ é o centro do grupo G/G_{i+1}. Uma tal cadeia é chamada de *série central* de G. Além disso, a *classe de nilpotência* de um grupo nilpotente G, $cl(G)$, é o comprimento da menor série central de G.

Os p-grupos finitos, em que p é um número primo, são exemplos de grupos nilpotentes (Proposição 1.3.11).

Sejam G um grupo, p um número primo e $G^p = \langle g^p \,|\, g \in G \rangle$. Definimos indutivamente, para todo inteiro $i \geq 1$: $\mathcal{P}_0(G) = G$, $\mathcal{P}_i(G) = [\mathcal{P}_{i-1}(G), G]\mathcal{P}_{i-1}^p$. A cadeia $G = \mathcal{P}_0(G) \geq \mathcal{P}_1(G) \geq \ldots \geq \mathcal{P}_i(G) \geq \ldots$ é denominada *série p-central inferior* de G.

Dizemos que um grupo G é *n-Engel* para algum $n \in \mathbb{N}$, se, para quaisquer elementos $x, y \in G$, $[y, \underbrace{x, \ldots, x}_{n}] = 1$. Assim, os grupos nilpotentes de classe no máximo n são exemplos de grupos n-Engel.

Um grupo G é dito ser *E-grupo* (respectivamente, *A-grupo*), se $x^{\varphi}x = xx^{\varphi}$, para todo $x \in G$ e para qualquer endomorfismo (respectivamente, automorfismo), φ de G. Além disso, se G é um p-grupo e é E-grupo (respectivamente, A-grupo), então G é *pE-grupo* (respectivamente, *pA-grupo*). Logo, todo E-grupo é um A-grupo. Podemos ver que os grupos abelianos são exemplos de A-grupos (e de E-grupos).

Sendo ϕ o automorfismo interno induzido por um elemento $g \in G$, $\phi = \gamma_g$, então $[x^g, x] = 1$, ou seja, $[g, x, x] = 1$, para todo elemento $x \in G$. Dessa maneira, segue que todo A-grupo é um grupo 2-Engel e, assim, pelo Teorema de Levi 1.7.3, tal grupo é nilpotente de classe no máximo 3 e pode ser escrito como produto direto de seus subgrupos de Sylow, pela Proposição 1.3.15; além disso, pelo Teorema 3.1.7, qualquer fator direto de um E-grupo é um E-grupo. Logo, para estudarmos E-grupos finitos basta considerarmos os pE-grupos finitos.

R. Faudree [10] demonstrou que a conjectura de que todo E-grupo finito é abeliano é falsa. Para isso, exibiu o primeiro 2E-grupo não abeliano em 1971. De fato, para cada primo p, R. Faudree exibiu um p-grupo de classe de nilpotência 2 como exemplo. Uma condição necessária e suficiente para um p-grupo ser um E-grupo foi dada em 1969 por B. H. Neumann e M. Suzuki e citada por J. J. Malone em [26].

Todos os A-grupos e E-grupos conhecidos, até aquele momento, possuem classe no máximo 2. A. Caranti [31] questionou sobre a existência de um pE-grupo finito ou de um pA-grupo finito possuindo classe 3. O Teorema de Levi 1.7.3, mostra que os grupos 2-Engel sem elementos de ordem 3 tem classe no máximo 2 e, assim, um pA-grupo finito deve ser 3-grupo para ter classe 3.

Em 2008, A. Abdollahi, A. Faghihi e A. Mohammadi Hassanabadi escreveram o artigo "Minimal number of generators and minimum order of non-abelian group whose elements commute with their endomorphic images" [2], no qual mostram que todo E-grupo 3-gerado é nilpotente com classe igual a 2 e que todo 3E-grupo com ordem menor ou igual a 3^{10} é nilpotente com classe igual a 2. Nesse mesmo ano, escreveram o artigo "3-generator groups whose elements commute with their endomorphic images are abelian" [1], no qual mostram que todo E-grupo 3-gerado é abeliano, ou seja, são necessários ao menos 4 geradores para gerar um E-grupo finitamente gerado não abeliano.

Em 2010, A. Abdollahi, A. Faghihi, S. A. Linton, e E. A. O'Brien escreveram um artigo intitulado "Finite 3-groups of class 3 whose elements commute with their automorphic images" [3], no qual respondem uma das questões de A. Caranti construindo um exemplo de um A-grupo G de classe exatamente 3. Mostram que tal máximo é atingido com a demostração do seguinte teorema, em que G é tal como descrito no Capítulo 4 (página 78), e $Aut_c(G)$ denota o grupo de automorfismos centrais de G (um automorfismo $\phi \in Aut(G)$ é dito ser *central* se ϕ comuta com todo automorfismo de $Inn(G)$):

Teorema: *$Aut(G) = Aut_c(G)Inn(G)$. Em particular, G é um A-grupo.*

Este trabalho foi baseado nesses últimos artigos, [1], [3] e em alguns resultados de [2], tendo como objetivo principal construir esse A-grupo G, de classe 3, abordando os detalhes de sua construção e os aspectos teóricos necessários para isso. O teorema anterior está demostrado no Capítulo 4.

Para demonstrar tal teorema foram usados algoritmos implementados no GAP (Groups, Algorithms and Programming) [12]; esta ferramenta proporcionou, inicialmente, a construção do referido grupo para então, obter informações sobre sua estrutura.

Motivado em parte por encontrar tais grupos, G. Traustason [39] desenvolveu uma teoria geral de álgebras alternadas simpléticas e construiu uma família de 3-grupos 2-Engel de classe 3.

No Capítulo 1, incluímos alguns conceitos e resultados da Teoria de Grupos e de Representações que serão usadas no desenvolvimento deste trabalho. Esses resultados, em sua maioria não estão aqui demonstrados, mas o leitor interessado pode encontrar

essas demonstrações em grande parte dos livros de teoria de grupos.

No Capítulo 2, introduzimos os conceitos de grupos livres, grupos policíclicos e apresentações de grupos. O estudo de grupos policíclicos e de apresentações de grupos é importante pois suas características permitem a construção de algoritmos mais eficientes para resolução de problemas. Descrevemos, ainda no Capítulo 2, os aspectos teóricos dos algoritmos envolvidos na demonstração do teorema principal; são eles o algoritmo ANU Nilpotent Quotient, usado para construir uma apresentação para o grupo procurado, o algoritmo de B. Eick, C. R. Leedham-Green e E. A. O'Brien [9], cujas implementações estão disponíveis no GAP [12] e MAGMA [4]; além do algoritmo UNIPOTENTSTABILISER, desenvolvido por E. Costi em sua tese de doutorado [8].

O algoritmo de B. Eick, C. R. Leedham-Green e E. A. O'Brien, descrito em [9] procede por indução sobre o termo da série p-central inferior de um p-grupo finito G. Definindo $P_i = G/\mathcal{P}_i(G)$, é calculado $Aut(P_i(G))$. Como $P_1 = G/\mathcal{P}_1(G)$ é um grupo abeliano elementar, $Aut(P_1) \cong GL(d,p)$ (onde d é o número de geradores de G). Assumimos, por indução, que já conhecemos $Aut(P_i)$, para algum $i \geq 1$. Desejamos encontrar um conjunto de geradores de $Aut(P_{i+1})$, o que será possível tendo em vista os resultados do Capítulo 2.

O algoritmo UNIPOTENTSTABILISER é usado para minimizar e possibilitar o cálculo dos estabilizadores envolvidos.

Dizemos que G é um $p\mathcal{E}$-grupo se G é um grupo 2-Engel finito e existe $r > 0$ tal que $exp(G/G') = p^r$ e $\Omega_r(G) \leq Z(G)$. Assim, se G é um pE-grupo, então G é $p\mathcal{E}$-grupo. O Capítulo 3 é destinado à descrição de algumas propriedades de E-grupos e classificação dos $p\mathcal{E}$-grupos 3-gerados.

No Capítulo 4, aplicamos a teoria desenvolvida nos capítulos anteriores para o grupo mencionado (exemplo de A-grupo de classe 3), a fim de mostrar que de fato é um exemplo, abordando os detalhes de sua construção.

Por fim, o Apêndice A é dedicado aos comandos usados no GAP [12] para a construção desse grupo G e dos grupos envolvidos, bem como aos comandos (e algoritmos) usados para auxiliar na demonstração de que G é um exemplo de pA-grupo, descrita no Capítulo 4.

Capítulo 1

Conceitos Iniciais

Neste capítulo, abordaremos alguns conceitos iniciais da Teoria dos Grupos, a fim de facilitar a leitura, evitando necessidade de recorrer a outras referências com frequência. Mais especificamente, conceituaremos os comutadores, p-grupos e grupos nilpotentes, incluindo as séries centrais e o subgrupo de Frattini, com algumas propriedades. Falaremos um pouco, também, sobre p-grupos regulares e grupos que satisfazem alguma condição de Engel. Além disso, abordaremos alguns conceitos de Teoria de Representações, incluindo formas bilineares.

A maioria das demonstrações deste capítulo não fazem parte do objetivo principal do trabalho; assim muitas dessas demonstrações serão omitidas. O leitor interessado pode consultar [11], [13], [19], [34], [35] e [36].

1.1 Comutadores

Se G é um grupo e $x, y \in G$, então o *conjugado* de x por y é $x^y := y^{-1}xy$ e o *comutador* de x e y é $[x, y] := x^{-1}y^{-1}xy := x^{-1}x^y$; então x comuta com y se, e somente se, $[x, y] = 1$. Definimos ainda, indutivamente, $[x_1, x_2, x_3] := [[x_1, x_2], x_3]$ e para $n \geq 3$:

$$[x_1, \ldots, x_n] := [[x_1, \ldots x_{n-1}], x_n] = [[\ldots [[x_1, x_2], x_3], ..., x_{n-1}], x_n]$$

como sendo o *comutador simples de peso n.*

Definimos, de modo mais geral, o *comutador de dois subgrupos* H *e* K de G como:

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

O subgrupo $[G, G]$ de um grupo G é chamado o *subgrupo derivado* de G, e é denotado por G'. Esse subgrupo tem propriedades importantes (das quais enunciaremos algumas), por isso o interesse em estudá-lo. A proposição seguinte nos mostra que esse subgrupo nos fornece o maior quociente abeliano.

Proposição 1.1.1. *O grupo quociente G/G' é abeliano. Além disso, se $N \trianglelefteq G$ tal que G/N é abeliano, então $G' \subseteq N$.*

Demonstração: Segue da definição de subgrupo derivado. ∎

Proposição 1.1.2. *Sejam G um grupo com $x, y, z \in G$ e um homomorfismo de grupos $\sigma\colon G \to H$. Então:*

i) $[y, x] = [x, y]^{-1}$;

ii) $\sigma([x, y]) = [\sigma x, \sigma y]$;

iii) $[xy, z] = [x, z][x, z, y][y, z]$ *e* $[x, yz] = [x, z][x, y][x, y, z]$;

iv) $[x, y^{-1}, z]^y[y, z^{-1}, x]^z[z, x^{-1}, y]^x = 1$ *(Identidade de Hall-Witt).*

Demonstração: Segue da definição de comutador. ∎

Proposição 1.1.3. *Seja G um grupo e X um conjunto qualquer de geradores de G. Então, G' é gerado por elementos da forma $[x, y]^g$ tais que $x, y \in X$ e $g \in G$.*

Demonstração: Seja N o grupo gerado por elementos da forma $[x, y]^g$ tais que $x, y \in X$ e $g \in G$. Temos que $[x, y]^g = [x^g, y^g] \in G'$. Consequentemente, $N \leq G'$. Além disso, $N \trianglelefteq G$.

Suponha, agora, que $x, y, z \in X$, então, pela Proposição 1.1.2,

$$[xy, z] = [x, z][[x, z], y][y, z] = [x, z][x, z]^{-1}[x, z]^y[y, z] \in N,$$

pois cada fator é um elemento de N. De modo semelhante,

$$[x, yz] = [x, z][x, y][x, y, z] \in N.$$

Como $G = \langle X \rangle$, seguindo esse raciocínio, é possível mostrar que G/N é abeliano, o que significa (pela Proposição 1.1.1) que $G' \subseteq N$. ∎

Definição 1.1.4. *Se G é um grupo e H um subgrupo de G tal que $\alpha(H) = H$, para todo automorfismo $\alpha\colon G \to G$, então dizemos que H é* característico *em G.*

Notação 1.1.5. *Sejam G um grupo, X um conjunto não-vazio de G e $K \leq G$. Denotamos:*

$$\langle X \rangle^K := \langle x^k = k^{-1}xk \,|\, x \in X,\, k \in K \rangle.$$

Proposição 1.1.6. *Sejam G um grupo, $\emptyset \neq X \subseteq G$ e $K \leq G$. Então:*

i) $X \subseteq \langle X \rangle^K \trianglelefteq \langle X, K \rangle$;

ii) $\langle X\rangle^K = \langle X, [X,K]\rangle$;

iii) $[X,K]^K = [X,K]$;

iv) *se* $K = \langle Y\rangle$, *então* $[X,K] = [X,Y]^K$.

Demonstração: Ver [34], 5.1.6. ∎

Proposição 1.1.7. *Seja* G *um grupo com* $H, K \leq G$. *Então:*

i) $[H,K] = [K,H]$;

ii) $[H,K] \trianglelefteq \langle H,K\rangle$;

iii) *se* $H_1 \leq H$ *e* $K_1 \leq K$, *então* $[H_1,K_1] \leq [H,K]$;

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

v) $\alpha([H,K]) = [\alpha H, \alpha K]$, *para qualquer homomorfismo de grupos* $\alpha\colon G \to \tilde{G}$;

vi) *se* H *e* K *são subgrupos normais (respectivamente, característicos) em* G, *então* $[H,K]$ *é um subgrupo normal (respectivamente, característico) em* G.

Demonstração: Ver [35], Proposição 4.5 e Proposição 4.6. ∎

Proposição 1.1.8. *Seja* G *um grupo com* $K \leq H \leq G$ *e* $K \trianglelefteq G$. *Então,* $H/K \leq Z(G/K)$ *se, e somente se,* $[H,G] \leq K$.

Demonstração: Temos que se $h \in H$, então $hK \in Z(G/K)$ se, e somente se, $hKgK = gKhK$, para qualquer $g \in G$, o que acontece se, e somente se, $[h,g] \in K$, para qualquer $g \in G$. ∎

1.2 p-Grupos

Definição 1.2.1. *Sejam* p *um número primo e* G *um grupo. Se a ordem de qualquer elemento de* G *é uma potência de* p, *então* G *é dito um* p-grupo.

Teorema 1.2.2 (Teorema de Cauchy)**.** *Seja* G *um grupo finito e* p *um primo que divide* $|G|$. *Então, existe um elemento em* G *de ordem* p.

Demonstração: Ver [34], 1.6.17. ∎

Do Teorema 1.2.2, se G é um p-grupo finito, então $|G| = p^n$, para algum $n \in \mathbb{N}$.

Definição 1.2.3. *Um* p*-grupo* G *é denominado* p-grupo abeliano elementar *se* G *for abeliano e* $x^p = 1$, *para qualquer elemento* $x \in G$.

Notação 1.2.4. *Se G é um grupo e H um subgrupo próprio de G, então denotamos $H < G$.*

Definição 1.2.5. *Um subgrupo M de G é denominado* subgrupo maximal *de G se $M \neq G$ e não existe $H \leq G$ tal que $M < H < G$.*

Proposição 1.2.6. *Seja G um p-grupo finito. Então:*

i) *se $M \leq G$ é um subgrupo maximal, então $M \trianglelefteq G$ e $|G : M| = p$;*

ii) *se $H < G$, então $H < N_G(H)$.*

Demonstração: Ver [36], Theorem 5.40. ∎

1.3 Grupos Nilpotentes

Definição 1.3.1. *Um grupo G é dito* nilpotente *se existe uma cadeia finita*

$$G = G_0 \geq G_1 \geq \ldots \geq G_n = 1$$

tal que $G_{i+1} \trianglelefteq G_i$ e $G_i/G_{i+1} \leq Z(G/G_{i+1})$, para todo inteiro i com $0 \leq i \leq n-1$. Uma tal cadeia é chamada de série central *de G.*

Note que tal definição implica que $G_{n-1} \leq Z(G)$. Se $G_{n-1} = 1$, então $G_{n-2} \leq Z(G)$, e assim sucessivamente. Isso significa que todo grupo nilpotente possui centro não trivial.

Os grupos abelianos são exemplos de grupos nilpotentes, assim como os p-grupos finitos (conforme será mostrado em 1.3.11). Observe que, pela definição, os grupos nilpotentes são solúveis, mas não vale a recíproca; por exemplo, o grupo simétrico S_3 é solúvel, porém não é nilpotente já que possui centro trivial.

Definição 1.3.2. *Seja $G = G_0 \geq G_1 \geq \ldots \geq G_n = 1$ a menor série central de um grupo nilpotente G. A* classe de nilpotência *de G, $cl(G)$, é o comprimento de tal série, ou seja, $cl(G) = n$.*

Os grupos não triviais de menor classe, quando $cl(G) = 1$, são precisamente os grupos abelianos.

Definição 1.3.3. *Seja G um grupo. Definimos indutivamente:*
$\gamma_1(G) = G$,
$\gamma_2(G) = [\gamma_1(G), G] = [G, G] = G'$,
$\gamma_3(G) = [\gamma_2(G), G]$,
$\vdots$
$\gamma_i(G) = [\gamma_{i-1}(G), G]$.

Lema 1.3.4. *Seja G um grupo, então $\gamma_i(G)$ é subgrupo característico em G, para todo inteiro i com $i \geq 1$. Desse modo, segue que a cadeia*

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

é uma série central e é dita série central inferior *do grupo G.*

Demonstração: Temos que, pela Proposição 1.1.7 v), cada termo $\gamma_i(G)$ é característico em G; em particular, $\gamma_i(G) \trianglelefteq G$, para todo inteiro i. Desse modo, de $\gamma_i(G) = [\gamma_{i-1}(G), G]$ obtemos

$$\left[\frac{\gamma_{i-1}(G)}{\gamma_i(G)}, \frac{G}{\gamma_i(G)}\right] = \{1\}.$$

Logo,

$$\frac{\gamma_{i-1}(G)}{\gamma_i(G)} \leq Z\left(\frac{G}{\gamma_i(G)}\right),$$

para todo inteiro i com $i \geq 1$. ∎

Definição 1.3.5. *Seja G um grupo, e defina indutivamente: $Z_0(G) = \{1\}$, $Z_1(G) = Z(G)$ e Z_i é o único subgrupo de G tal que $Z_i(G)/Z_{i-1}(G) = Z(G/Z_{i-1}(G))$, para todo inteiro i tal que $i \geq 1$.*

Lema 1.3.6. *Seja G um grupo, então $Z_i(G)$ é subgrupo característico em G, para todo i com $i \geq 1$. Assim, segue que a cadeia*

$$\{1\} = Z_0(G) \leq Z_1(G) \leq \ldots \leq Z_i(G) \leq \ldots$$

é uma série central e é dita série central superior *do grupo G.*

Demonstração: De fato, o centro de um grupo é um subgrupo característico; assim, temos que $Z_1(G) = Z(G)$ é característico em G. Suponhamos, por indução, que para algum inteiro $i \geq 1$, $Z_i(G)$ é característico em G. Seja $\alpha \in Aut(G)$, automorfismo qualquer, então α induz um automorfismo $\overline{\alpha}$ em $G/Z_i(G)$, definido por $\overline{\alpha}(xZ_i(G)) = \alpha(x)Z_i(G)$.

Se $xZ_i(G) \in Z(G/Z_i(G))$, então $\alpha(x)Z_i(G) = \overline{\alpha}(xZ_i(G)) \in Z(G/Z_i(G))$, em que $Z(G/Z_i(G)) = Z_{i+1}(G)/Z_i(G)$. Logo, $\alpha(Z_{i+1}(G)) = Z_{i+1}(G)$. O que completa a demonstração. ∎

A seguinte proposição justifica os nomes *inferior* e *superior* das séries centrais definidas anteriormente.

Proposição 1.3.7. *Sejam G um grupo nilpotente e $G = G_0 \geq G_1 \geq \ldots \geq G_n = G$ uma série central de G. Então, $\gamma_{i+1} \leq G_i \leq Z_{n-i}$, para todo i tal que $1 \leq i \leq n$.*

Demonstração: Ver [34], 5.1.9. ∎

Corolário 1.3.8. *Se G é um grupo nilpotente, as séries centrais inferior e superior possuem o mesmo comprimento (finito), que é igual a classe de nilpotência de G.*

Demonstração: Ver [34], 5.1.9. ∎

Proposição 1.3.9. *Sejam G um grupo e i e j inteiros positivos. Então:*

i) $[\gamma_i(G), \gamma_j(G)] \leq \gamma_{i+j}(G)$;

ii) $\gamma_i(\gamma_j(G)) \leq \gamma_{ij}(G)$;

iii) $[\gamma_i(G), Z_j(G)] \leq Z_{j-i}(G)$; $\forall i \leq j$. *Em particular,* $[\gamma_i(G), Z_i(G)] = 1$.

Demonstração: Ver [35], 5.1.11. ∎

Proposição 1.3.10. *Seja G um grupo gerado por um conjunto X. Então, se i e j são inteiros positivos:*

i) $\gamma_i(G) = \langle [x_1, \ldots, x_i]^g \mid x_j \in X$, *para* $1 \leq j \leq i \, e \, g \in G \rangle$;

ii) $\gamma_i(G) = \langle [x_1, \ldots, x_i], \gamma_{i+1}(G) \rangle$, *em que* $x_j \in X$, *para* $1 \leq j \leq i$;

iii) *se* $X = \{x, y\}$, *então* $\gamma_2(G) = \langle [x, y], \gamma_3(G) \rangle$, *logo,* $\gamma_2(G)/\gamma_3(G)$ *é cíclico;*

iv) *se* $X = \{x, y\}$, *então* $G'' := \gamma_2(G') \leq \gamma_5(G)$.

Demonstração: Ver [35], Proposição 5.6. ∎

Proposição 1.3.11. *Todo p-grupo finito é nilpotente.*

Demonstração: Ver [36], Theorem 5.33. ∎

Proposição 1.3.12. *Se G é grupo nilpotente finitamente gerado, então G possui uma série central*

$$G = G_0 > G_1 > \ldots > G_n = 1$$

tal que cada fator G_i/G_{i+1} é cíclico, para todo inteiro i tal que $0 \leq i \leq n-1$.

Demonstração: Ver [35], Teorema 5.8. ∎

Proposição 1.3.13. *Se G é um grupo nilpotente finitamente gerado, então todo subgrupo de G é finitamente gerado.*

Demonstração: Ver [35], Corolário 5.9. ∎

Definição 1.3.14. *Sejam G um grupo e $H \leq G$. Dizemos que H é* subnormal *em G se existe uma cadeia ligando H e G da forma:*

$$H = H_0 \trianglelefteq H_1 \trianglelefteq \ldots \trianglelefteq H_m = G.$$

A proposição a seguir, nos diz que um grupo nilpotente é o produto direto de seus subgrupos de Sylow. Isso é uma justificativa para nos concentrarmos no estudo de p-grupos finitos, pois muitas propriedades de p-grupos podem ser generalizadas para grupos nilpotentes.

Proposição 1.3.15. *Seja G um grupo finito. Então, são equivalentes:*

i) *G é nilpotente.*

ii) *Todo subgrupo de G é subnormal em G.*

iii) *G satisfaz a* condição do normalizador*, ou seja, todo subgrupo próprio de G está contido propriamente em seu normalizador em G ($H < N_G(H)$).*

iv) *Todo subgrupo maximal é normal.*

v) *G é o produto direto de seus subgrupos de Sylow.*

Demonstração: Ver [34], 5.2.4. ∎

Proposição 1.3.16. *Se G é um grupo nilpotente de classe c e $H \leq G$, então:*

i) *H é nilpotente de classe menor ou igual a c;*

ii) *se $H \trianglelefteq G$, então G/H é nilpotente de classe menor ou igual a c.*

Demonstração: Ver [36], Theorem 5.35 e Theorem 5.36. ∎

1.4 Série p-Central Inferior

Definição 1.4.1. *Sejam G um grupo, p um número primo e $G^p = \langle g^p \mid g \in G \rangle$. Definimos indutivamente, para todo inteiro $i \geq 1$:*

$$\mathcal{P}_0(G) = G,\ \mathcal{P}_i(G) = [\mathcal{P}_{i-1}(G), G]\mathcal{P}_{i-1}^p.$$

Definição 1.4.2. *O* expoente *de G é o menor múltiplo comum das ordens dos seus elementos.*

Proposição 1.4.3. *Para cada $i = 1, 2, \ldots$ temos:*

i) $\mathcal{P}_i(G) \trianglelefteq G$;

ii) $\mathcal{P}_i(G)/\mathcal{P}_{i+1}(G) \leq Z(G/\mathcal{P}_{i+1}(G))$;

iii) $\mathcal{P}_i(G)/\mathcal{P}_{i+1}(G)$ *tem expoente* p.

Demonstração:

i) Segue por indução sobre i.

ii) Segue da definição de $\mathcal{P}_{i+1}(G)$ e da Proposição 1.1.8.

iii) Se $x \in \mathcal{P}_i(G)/\mathcal{P}_{i+1}(G)$, então $x = g\mathcal{P}_{i+1}(G)$, para algum $g \in \mathcal{P}_i(G)$. Dessa maneira, pela definição de $\mathcal{P}_{i+1}$, segue que $x^p = g^p\mathcal{P}_{i+1}(G) = \mathcal{P}_{i+1}(G)$.

■

Definição 1.4.4. *A cadeia*

$$G = \mathcal{P}_0(G) \geq \mathcal{P}_1(G) \geq \ldots \geq \mathcal{P}_i(G) \geq \ldots$$

é denominada série p-central inferior *de* G. *E, se* $\mathcal{P}_{k+1}(G) = \{1\}$ *e* $\mathcal{P}_k(G) \neq \{1\}$, *então dizemos que* G *possui* p-classe k.

Proposição 1.4.5. *Se* G *é finitamente gerado, então* $G/\mathcal{P}_i(G)$ *é um* p*-grupo finito, para todo inteiro* i.

Demonstração: A proposição vale se $i = 1$. Suponha então, por indução, que $G/\mathcal{P}_i(G)$ é um p-grupo finito. Como G é finitamente gerado, pela Proposição 1.3.13, $\mathcal{P}_i(G)$ também o é. Assim, segue da Proposição 1.4.3 que $\mathcal{P}_i(G)/\mathcal{P}_{i+1}(G)$ é um p-grupo abeliano elementar finito. Logo, $G/\mathcal{P}_{i+1}(G)$ é p-grupo finito. ■

Proposição 1.4.6. *Seja* G *um grupo.*

i) *Se* φ *é um homomorfismo de* G, *então* $\varphi(\mathcal{P}_i(G)) = \mathcal{P}_i(\varphi(G))$.

ii) *Os termos da série* p*-central inferior,* $\mathcal{P}_i(G)$, *são característicos em* G.

iii) *Se* $N \trianglelefteq G$ *e* G/N *tem* p*-classe* c, *então* $\mathcal{P}_c(G) \leq N$.

Demonstração:

i) Segue da definição de série p-central inferior.

ii) O resultado segue por indução, usando o item anterior.

iii) Segue do item i).

■

1.5 Subgrupo de Frattini

O subgrupo de Frattini tem grande importância no estudo de grupos devido às suas propriedades. Ele é um subgrupo característico de G que consiste de elementos não-geradores do grupo.

Definição 1.5.1. *Sejam G um grupo e x um elemento de G. Se, para qualquer conjunto Y de G tal que $G = \langle x, Y\rangle$, temos que $G = \langle Y\rangle$, então x é dito ser um* não-gerador *de G.*

Definição 1.5.2. *O* subgrupo de Frattini, *$\Phi(G)$, é definido como a interseção de todos os subgrupos maximais de G. Se o grupo G não possui subgrupos maximais, definimos $\Phi(G) := G$.*

Proposição 1.5.3. *$\Phi(G)$ é um subgrupo característico em G.*

Demonstração: Se G não possui maximais, então $\Phi(G) = G$ e não há nada a fazer. Se M é um maximal de G, então $\alpha(M)$ é um maximal em G, para qualquer automorfismo $\alpha \in Aut(G)$. Desse modo, pela definição do Frattini de G, segue o resultado. ∎

Proposição 1.5.4. *Seja G um grupo não-trivial. Então, $\Phi(G)$ é o subgrupo formado por todos os elementos não-geradores de G.*

Demonstração: Ver [34], 5.2.12. ∎

Proposição 1.5.5. *Se G é um grupo finito, então G é nilpotente se, e somente se, $G' \leq \Phi(G)$.*

Demonstração: Ver [34], 5.2.16. ∎

Proposição 1.5.6. *Seja G um p-grupo finito, e denote $G^p = \langle x^p;\, x \in G\rangle$. Então, $\Phi(G) = G'G^p$. Além disso, $\dfrac{G}{\Phi(G)}$ é um espaço vetorial sobre $\mathbb{Z}/p\mathbb{Z}$.*

Demonstração: Como G é nilpotente, $G' \leq \Phi(G)$, pela Proposição 1.5.5. Além disso, a Proposição 1.2.6 diz que se M é um subgrupo maximal em G, então $M \trianglelefteq G$ e $|G/M| = p$, o que mostra que $x^p \in M$, para qualquer elemento $x \in G$. Desse modo, $G^p \leq M$. Pela definição do subgrupo de Frattini, temos que $G^p \leq \Phi(G)$ e, assim, $G^pG' \leq \Phi(G)$.

Por outro lado, temos que $G^pG' \trianglelefteq G$ e que $\dfrac{G}{G^pG'}$ é um grupo abeliano finito de expoente p. Então, $\dfrac{G}{G^pG'} \cong \mathbb{F}_p \times \ldots \times \mathbb{F}_p$, ou seja, $\dfrac{G}{G^pG'}$ é um espaço vetorial sobre $\mathbb{F}_p$.

Agora, observe que $\Phi\Big(\dfrac{G}{G^pG'}\Big) = 1$ e seja $\pi\colon G \to \dfrac{G}{G^pG'}$, o homomorfismo quociente. Assim, se L é um subgrupo maximal qualquer de $\dfrac{G}{G^pG'}$, temos que $\pi^{-1}(L)$ é subgrupo maximal de G. Desse modo, $\Phi(G) \leq \pi^{-1}(L)$ e $\pi(\Phi(G)) \leq \pi(\pi^{-1}(L)) = L$. E, portanto, $\pi(\Phi(G)) \leq \Phi\Big(\dfrac{G}{G^pG'}\Big) = 1$, o que implica que $\Phi(G) \leq G'G^p$. ∎

Definição 1.5.7. *Um* conjunto minimal de geradores *de um grupo G é um subconjunto X de G que gera G tal que nenhum subconjunto próprio de X gera G.*

Teorema 1.5.8 (Teorema da Base de Burnside)**.** *Se G é um p-grupo finito, então quaisquer dois conjuntos minimais de geradores de G possuem o mesmo número de elementos, dado por $dim_{\mathbb{F}_p}\frac{G}{\Phi(G)}$. Além disso, se $x \notin \Phi(G)$, então existe um conjunto minimal de geradores de G que possui x como elemento.*

Demonstração: Seja $X = \{x_1, \ldots, x_n\}$ um conjunto minimal de geradores de G. Dessa forma, sendo $\overline{x_i} = x_i\Phi(G) \in G/\Phi(G)$, então $\overline{X} = \{\overline{x_1}, \ldots, \overline{x_n}\}$ é um conjunto gerador de $G/\Phi(G)$.

Afirmamos que tal conjunto é linearmente independente. De fato, suponhamos que $\overline{X}$ seja linearmente dependente, então podemos assumir, reordenando os elementos se necessário, que $\overline{x_1} \in \langle\overline{x_2}, \ldots, \overline{x_n}\rangle$. Assim, $x_1\Phi(G) \in \langle x_2, \ldots, x_n\rangle\Phi(G)$ e existe $y \in \langle x_2, \ldots, x_n\rangle$ tal que $y^{-1}x_1 \in \Phi(G)$.

Logo, como $X = \{x_1, \ldots, x_n\}$ gera G e $y \in \langle x_2, \ldots, x_n\rangle$, segue que $\{y^{-1}x_1, \ldots, x_n\}$ gera G. Mas, já que $y^{-1}x_1$ é um não-gerador, temos que $\{x_2, \ldots, x_n\}$ gera G. Absurdo, pois X é conjunto minimal de geradores.

Dessa forma, $dim_{\mathbb{F}_p}\frac{G}{\Phi(G)} = n = |X|$, para qualquer conjunto minimal de geradores X.

Agora, se $x \notin \Phi(G)$, então $\overline{x} \neq \overline{1}$, portanto, existe uma base $\{\overline{x}, \overline{x_2} \ldots, \overline{x_n}\}$ de $G/\Phi(G)$ contendo $\overline{x}$. Ou seja, $G/\Phi(G) = \langle\overline{x}, \overline{x_2} \ldots, \overline{x_n}\rangle$ e $G = \langle\Phi(G), x, x_2 \ldots, x_n\rangle$. Observado que $\Phi(G)$ é o conjunto finito dos não-geradores de G, fica provado que $G = \langle x, x_2 \ldots, x_n\rangle$. ∎

1.6 p-Grupos regulares

Introduzimos abaixo duas séries de subgrupos de um p-grupo finito que são importantes no estudo da estrutura de p-grupos.

Definição 1.6.1. *Seja G um p-grupo finito. Para todo inteiro $i \geq 0$, definimos*

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

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

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

Lemos o símbolo $\mho$ como "agemo". Note que agemo é uma palavra formada pela letras da palavra omega em ordem inversa. Podemos observar que Ω_i e $\mho_i$ são subgrupos característicos de G.

Relembrando que o *expoente* de G, denotado de agora em diante por $exp(G)$, é o menor múltiplo comum das ordens dos seus elementos, temos que se G é um p-grupo tal que $exp(G) = p^e$, então $x^{p^e} = 1$, para qualquer elemento x de G e ainda, podemos escrever $\Omega_e(G) = G$. Sendo assim, podemos construir a seguinte série ascendente, denominada Ω-*série* de G:

$$1 = \Omega_0(G) \leq \Omega_1(G) \leq \ldots \leq \Omega_{e-1} \leq \Omega_e(G) = G.$$

De modo semelhante, $\mho_e(G) = 1$ e podemos construir a seguinte série descendente, denominada $\mho$-*série* de G:

$$G = \mho_0(G) \geq \mho_1(G) \geq \ldots \geq \mho_{e-1} \geq \mho_e(G) = 1.$$

Proposição 1.6.2. *Seja G um p-grupo finito.*

i) *Se $exp(G) = p^e$, então $\mho_i(G) \leq \Omega_{e-i}(G)$.*

ii) *Se $N \trianglelefteq G$, então $\mho_i(G/N) = \mho_i(G)N/N$.*

Demonstração:

i) Temos que qualquer gerador x^{p^i} de $\mho_i(G)$ possui ordem no máximo p^{e-i}, pois $exp(G) = p^e$. Logo, segue que $\mho_i(G) \leq \Omega_{e-i}(G)$.

ii) Usaremos a "barra" como notação em $\overline{G} = G/N$. Então,

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

isto é, $\mho_i(G/N) = \mho_i(G)N/N$.

■

1.6.1 Fórmula de coleta de Phillip Hall

Sabemos que $x^n y^n = (xy)^n$ para qualquer grupo abeliano, mas a igualdade não é válida em geral. A fórmula de Phillip Hall, descrita a seguir, relaciona os termos $x^n y^n$ e $(xy)^n$ em qualquer grupo usando comutadores entre x e y. A construção da fórmula se dá indutivamente usando como base a relação $ab = ba[a, b]$.

Teorema 1.6.3 (Fórmula da coleta de Hall)**.** *Sejam G um grupo e $x, y \in G$. Então, para $n \in \mathbb{N}$ e qualquer inteiro i com $2 \leq i \leq n$ existem $c_i = c_i(x, y) \in \gamma_i(\langle x, y \rangle)$ tais que:*

$$x^n y^n = (xy)^n c_2^{\binom{n}{2}} c_3^{\binom{n}{3}} \ldots c_n^{\binom{n}{n}}.$$

Demonstração: Ver [11], Theorem 2.6. ∎

A fórmula da coleta de Hall 1.6.3 tem grande importância quando usamos $n = p$, uma vez que os coeficientes binomiais são divisíveis por p, para $1 \leq i \leq p-1$. Consequentemente, podemos escrever

$$x^p y^p = (xy)^p z c_p,$$

para algum $z \in \mho_1(\langle x, y\rangle')$, o que sugere a definição a seguir.

Definição 1.6.4. *Seja G um p-grupo finito. Dizemos que G é um* p-grupo regular *se, para todo $x, y \in G$, temos que $x^p y^p \equiv (xy)^p (mod\ \mho_1(\langle x, y\rangle'))$. Ou, equivalentemente, se para todo $x, y \in G$, segue que $c_p(x, y) \in \mho_1(\langle x, y\rangle')$.*

A definição de p-grupo regular é local, uma vez que envolve apenas o subgrupo gerado por x e y. Dessa forma, todo subgrupo e grupo quociente de um p-grupo regular são, também, p-grupos regulares. São exemplos de p-grupos regulares: p-grupos abelianos, grupos de expoente p e p-grupos com classe de nilpotência menor que p (em particular, p-grupos de ordem no máximo p^p). Mas, se um 2-grupo é regular, então é abeliano. (Ver [11], Theorem 2.8.)

Alguns grupos descritos nos Capítulos 3 e 4 são regulares e as propriedades aqui apresentadas serão usadas posteriormente.

Lema 1.6.5. *Seja G é um p-grupo regular com $x, y \in G$. Então, $x^p = y^p$ se, e somente se, $(x^{-1}y)^p = 1$.*

Demonstração: A demonstração será feita por indução sobre a ordem de G. Seja $H = \langle x, y\rangle$. Como G é regular podemos escrever $x^{-p}y^p = (x^{-1}y)^p z$, para algum elemento $z \in \mho_1(H')$. Assim, basta provarmos que $\mho_1(H') = 1$ sempre que $x^p = y^p$ ou $(x^{-1}y)^p = 1$. Se H é abeliano, então o lema é verdadeiro; assuma então, que H não é abeliano.

Suponhamos que $x^p = y^p$. Então, y e x^p comutam e $x^p = (x^p)^y = (x^y)^p$. Como H não é cíclico, existe um subgrupo maximal M de H que contém x. Como $M \trianglelefteq H$ (pela Proposição 1.2.6), segue que $x^y \in M$. Aplicando a hipótese de indução sobre M, concluímos que $[x, y]^p = (x^{-1}y)^p = 1$. Pela Proposição 1.1.3, H' é gerado por elementos da forma $[x, y]^h$ possuindo ordem dividindo p, em que $h \in H$. Pela hipótese de indução o lema é válido para H' e, em particular, o produto de dois elementos de H' de ordem dividindo p possui ordem dividindo p, também. Nesse caso, $\mho_1(H') = 1$.

Assuma agora que $(x^{-1}y)^p = 1$, conjugando os membros dessa igualdade por x^{-1}, obtemos que $(yx^{-1})^p = 1$. Então, a implicação já provada fornece que $(xy^{-1}x^{-1}y)^p = 1$, isto é, $[x^{-1}, y]^p = 1$. Como $H = \langle x^{-1}, y\rangle$, segue que $\mho_1(H') = 1$. ∎

Proposição 1.6.6. *Seja G um p-grupo regular. Então, para todo inteiro $i \geq 1$:*

i) $x^{p^i} = y^{p^i}$ *se, e somente se,* $(x^{-1}y)^{p^i} = 1$*, para quaisquer elementos* $x, y \in G$*;*

ii) $\Omega_i(G) = \{x \in G \,|\, x^{p^i} = 1\}$*;*

iii) $\mho_i(G) = \{x^{p^i} \,|\, x \in G\}$*;*

iv) $|G : \Omega_i(G)| = |\mho_i(G)|$ *e* $|G : \mho_i(G)| = |\Omega_i(G)|$.

Demonstração:

ii) Se o item i) é verdadeiro para algum i, então o conjunto $\{x \in G \,|\, x^{p^i} = 1\}$ é um subgrupo de $\Omega_i(G)$ e, portanto, coincide com $\Omega_i(G)$. O que significa que o item ii) segue de i).

i) Seja $\overline{G} = G/\Omega_{i-1}(G)$. Pelo Lema 1.6.5, temos que o resultado já vale para $i = 1$. Usaremos indução sobre i. Supondo que o resultado é válido para $i - 1$ temos que $x^{p^i} = y^{p^i}$ equivale a $(x^{-p}y^p)^{p^{i-1}} = 1$. E, por essa última igualdade, temos que $\overline{x}^p = \overline{y}^p$, o que implica que $(\overline{x}^{-1}\overline{y})^p = \overline{1}$, isto é, $(x^{-1}y)^p \in \Omega_{i-1}(G)$. Mas, como por hipótese o item i) vale para $i-1$, temos que o item ii) também vale para $i-1$. O que significa que todos os elementos de $\Omega_{i-1}(G)$ possuem ordem dividindo p^{i-1} e, assim, $(x^{-1}y)^{p^i} = 1$.

iii) A demonstração será feita por indução sobre i. Veremos que dados $x, y \in G$, existe $z \in G$ tal que $x^p y^p = z^p$. O que equivale a afirmação do item iii), para $i = 1$. Para isso, faremos uma indução sobre $|G|$. Consideremos $H = \langle x, y\rangle$ e $K = \langle xy, \Phi(H)\rangle$. Se $K = H$, então H é cíclico e não há nada para provar. Se $K < H$, como G é regular, temos que $x^p y^p = (xy)^p c$, para algum $c \in \mho_1(H') \leq \mho_1(K)$. De modo que $(xy)^p c$ é um produto de dois elementos em $\mho_1(K)$ que, aplicando a hipótese de indução sobre K, pode ser escrito na forma z^p. Assim, $x^p y^p = z^p$.

Para qualquer inteiro i, temos que

$$\mho_1(\mho_{i-1}(G)) = \{x^p \,|\, x \in \mho_{i-1}(G)\} = \{x^{p^i} \,|\, x \in G\}$$

é um subgrupo de G. E, necessariamente, $\mho_i(G) = \{x^{p^i} \,|\, x \in G\}$.

iv) Dos itens i) e ii) segue que $x^{p^i} = y^{p^i}$ se, e somente se, $x^{-1}y \in \Omega_i(G)$, ou seja, se, e somente se, $x\Omega_i(G) = y\Omega_i(G)$. Assim, a aplicação $\varphi\colon G/\Omega_i(G) \longrightarrow \mho_i(G)$ dada por $\varphi(x\Omega_i(G)) = x^{p^i}$ está bem definida e é injetiva. Pelo item iii), φ é sobrejetiva e, portanto, φ é uma bijeção. O que mostra que $|G : \Omega_i(G)| = |\mho_i(G)|$.

■

Proposição 1.6.7. *Sejam x e y elementos de um grupo G tais que $[x, y]$ comuta com x e y. Então, para todo $n \in \mathbb{Z}$ valem:*

i) $[x, y^n] = [x^n, y] = [x, y]^n$;

ii) $(xy)^n = x^n y^{x^{n-1}} y^{x^{n-2}} \dots y^{x^2} y^x y$;

iii) $(xy)^n = x^n y^n [y, x^{n-1}][y, x^{n-2}] \dots [y, x^2][y, x]$;

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

Demonstração:

i) Segue por indução sobre n, usando a Proposição 1.1.2 iii).

ii) Segue por indução sobre n. Além disso, o resultado vale sem a hipótese de que $[x, y]$ comuta com x e y.

iii) Por hipótese, segue que

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

em que a última igualdade vale pelo item i).

iv) Segue dos itens i) e iii).

■

1.7 Grupos de Engel

Os grupos nilpotentes de classe no máximo n são exemplos de grupos n-Engel. Nessa seção veremos algumas propriedades de grupos n-Engel que serão usadas nos Capítulos 3 e 4.

Definição 1.7.1. *Sejam G um grupo e $n \in \mathbb{N}$. Então, G é dito ser* n-Engel *se, para quaisquer elementos $x, y \in G$, $[y, \underbrace{x, \dots, x}_{n}] = 1$.*

Os grupos nilpotentes de classe no máximo n são exemplos de grupos n-Engel pois, se G é um grupo nilpotente com classe de nilpotência menor ou igual a n, então para quaisquer $x_1, x_2 \dots, x_{n+1} \in G$ segue que $[x_1, \dots, x_{n+1}] = 1$ e tomando $x_2 = y, \dots, x_{n+1} = y$ podemos ver que G satisfaz a definição de n-Engel. Contudo, a recíproca não é verdadeira, conforme em [5].

Proposição 1.7.2. *Todo grupo de expoente* 3 *é* 2*-Engel.*

Demonstração: Seja G um grupo de expoente 3 e sejam x, y elementos de G. Então, $(xy^{-1})^2 = (xy^{-1})^{-1} = yx^{-1}$. Multiplicando o primeiro e o último termo da igualdade por y^2, e usando o fato que, para qualquer $g \in G$, $g^2 = g^{-1}$ segue:

$$xy^{-1}xy = yx^{-1}y^2 = y^{-2}x^{-1}y^{-1} = y^{-1}(y^{-1}x^{-1}y^{-1}) = y^{-1}x(x^{-1}y^{-1})^2.$$

Logo,

$$x(y^{-1}xy) = y^{-1}x(x^{-1}y^{-1})^2 = y^{-1}x(x^{-1}y^{-1})^{-1} = (y^{-1}xy)x,$$

o que mostra que x comuta com x^y. Como $x^{-y}x = [y, x]$, segue que $[y, x, x] = 1$. ∎

Teorema 1.7.3 (Teorema de Levi)**.** *Sejam G um grupo* 2*-Engel e $x, y, z, t \in G$. Então:*

i) $x^G = \{x^g = g^{-1}xg \mid g \in G\}$ *é abeliano;*

ii) $[x, y, z] = [z, x, y]$*;*

iii) $[x, y, z]^3 = 1$*;*

iv) $[x, y, z, t] = 1$*, logo, G é nilpotente de classe no máximo* 3*.*

Demonstração:

i) Observe que $[x, x^y] = [x, x[x, y]] = [x, [x, y]]$. Como G é 2-Engel, x comuta com $[y, x]$; logo, comuta com $[x, y]$ e, portanto, x comuta com x^y. Segue, por conjugação, que quaisquer dois conjugados de x comutam. O que implica que x^G é abeliano.

ii) Seja $A = \langle x^G \rangle$ um grupo abeliano abeliano. A aplicação $\varphi_y \colon A \to A$ definida por $a \mapsto [a, y]$ é um endomorfismo. Temos que os endomorfismos de A formam um anel e denotamos $(\varphi_y + \varphi_z)(a) = \varphi_y(a)\varphi_z(a)$ e 0 como sendo o endomorfismo que associa aos elementos de A à identidade de A $(0(a) = 1)$; denotamos, ainda, $(\varphi_y\varphi_z)(a) = \varphi_y(\varphi_z(a))$.

Como $[a, y, y] = 1$, para todo $a \in A$, temos que $(\varphi_y)^2 = 0$. Da Proposição 1.1.2:

$$\varphi_{yz} = \varphi_y + \varphi_z + \varphi_y\varphi_z; \text{ para cada } a \in A \text{ e} \tag{1.1}$$

$$\varphi_{y^{-1}} = -\varphi_y. \tag{1.2}$$

Como $(yz)^{-1}$ comuta com $[a, yz]$, já que G é 2-Engel, e usando as equações acima, temos, para cada $a \in A$:

$$\begin{aligned} 0 &= \varphi_{yz}\varphi_{z^{-1}y^{-1}} = (\varphi_y + \varphi_z + \varphi_y\varphi_z)(\varphi_z - \varphi_y + \varphi_z\varphi_y) \\ &= -\varphi_y\varphi_z - \varphi_z\varphi_y. \end{aligned}$$

Ou seja,

$$\varphi_y\varphi_z = -\varphi_z\varphi_y; \text{ para cada } a \in A, \tag{1.3}$$

o que significa que, $[a, y, z] = [a, z, y]^{-1}$ e, em particular, $[x, y, z] = [x, z, y]^{-1}$.

Como A é abeliano, $[x, z, y]^{-1} = [[x, z]^{-1}, y] = [z, x, y]$, logo, $[x, y, z] = [z, x, y]$.

iii) Por ii) obtemos que $[x, y^{-1}, z]^y = [x, y^{-1}, z]$. Logo, $[x, y^{-1}, z]^y = [[x, y^{-1}], z] = [x, y, z]^{-1}$ e da Proposição 1.1.2, segue que

$$1 = [x, y, z]^{-1}[y, z, x]^{-1}[z, x, y]^{-1} = [x, y, z]^{-2}[y, z, x]^{-1} = [x, y, z]^{-3}.$$

iv) Da equação 1.3, segue que $\varphi_y\varphi_{zt} + \varphi_{zt}\varphi_y = 0$ e, usando as igualdades 1.1 e 1.3, obtemos:

$$0 = \varphi_y\varphi_z + \varphi_y\varphi_t + \varphi_y\varphi_z\varphi_t + \varphi_z\varphi_y + \varphi_t\varphi_y + \varphi_z\varphi_t\varphi_y = 2\varphi_y\varphi_z\varphi_t.$$

Assim, $[a, y, z, t]^2 = 1$ e, em particular, $[x, y, z, t]^2 = 1$. Mas, de iii) segue que $[x, y, z, t]^3 = 1$, portanto, $[x, y, z, t] = 1$.

■

Lema 1.7.4. *Seja G um p-grupo com $p > 2$ tal que G é 2-Engel finito. Então, G é regular.*

Demonstração: Pela Proposição 1.6.7 iv), para qualquer $m \in \mathbb{N}$,

$$a^{p^m}b^{p^m} = (ab)^{p^m}[a, b]^{\frac{p^m(p^m-1)}{2}},$$

de modo que o resultado segue da definição de p-grupo regular, pois

$$[a, b]^{\frac{p^m(p^m-1)}{2}} \in \mathfrak{V}_1(\langle x, y\rangle').$$

Note que, como já mencionamos anteriormente, se $p = 2$, então G é regular se, e somente se, é abeliano (Ver [11], Theorem 2.8). ■

1.8 Grupo de Automorfismos e Estabilizadores

O grupo dos automorfismos de um grupo, $Aut(G)$, é o conjunto dos automorfismos de G sob a operação de composição.

Definição 1.8.1. *Se g é um elemento de G, então o automorfismo α de G definido por $\alpha(x) = g^{-1}xg$, para todo $x \in G$, é dito ser* automorfismo interno induzido por *g; denotamos α por γ_g. Se $\alpha \in Aut(G)$ não é automorfismo interno, dizemos que é* externo.

Teorema 1.8.2. *Seja G um grupo.*

i) *Se $H \leq G$, então $C_G(H) \trianglelefteq N_G(H)$ e $N_G(H)/C_G(H)$ é isomorfo a um subgrupo de $Aut(H)$.*

ii) *O conjunto dos automorfismos internos de G, $Inn(G) = \{\gamma_g \mid g \in G\}$, é um subgrupo normal de $Aut(G)$ isomorfo a $G/Z(G)$.*

Demonstração: Ver [36], Theorem 7.1. ∎

Definição 1.8.3. *Se ϕ é um automorfismo de G, então ϕ é dito ser* central *se ϕ comuta com todo automorfismo de $Inn(G)$, ou seja, se $\phi(g)g^{-1} \in Z(G)$, para todo $g \in G$.*

Os automorfismos centrais fixam G', o subgrupo comutador de G, ponto a ponto e formam um subgrupo de $Aut(G)$, pois, pela definição, se $\phi \in Aut_c(G)$, então $\phi(g) = gz$ para algum $z \in Z(G)$, logo $\phi([x,y]) = [xz_1, yz_2] = [x,y]$, para alguns $z_1, z_2 \in Z(G)$. Denotaremos $Aut_c(G)$ o subgrupo de $Aut(G)$ gerado por todos os automorfismos centrais de G.

Proposição 1.8.4. *O centralizador de $Inn(G)$ em $Aut(G)$ é Aut_cG.*

Demonstração: Segue da definição de automorfismo central, uma vez que o centralizador de $Inn(G)$ é formado pelos elementos de $Aut(G)$ que comutam com os elementos de $Inn(G)$. ∎

Proposição 1.8.5. *Se G é um grupo tal que $Aut(G)$ é abeliano, então $Aut(G) = Aut_c(G)$.*

Demonstração: Sabemos que $Aut_c(G)$ é o centralizador de $Inn(G)$ em $Aut(G)$, pela Proposição 1.8.4. Como $Aut(G)$ é abeliano, segue o resultado. ∎

Proposição 1.8.6. *Se G é um grupo tal que $Aut(G)$ é abeliano, então a classe de nilpotência de G, $cl(G)$, é no máximo 2.*

Demonstração: Temos que $\dfrac{G}{Z(G)} \cong Inn(G)$ é abeliano, por hipótese, e $Z_2(G)$ é, por definição, o único subgrupo de G tal que $\dfrac{Z_2(G)}{Z(G)} = Z\left(\dfrac{G}{Z(G)}\right) = \dfrac{G}{Z(G)}$, o que mostra que $G = Z_2(G)$. ∎

Definição 1.8.7. *Sejam G um grupo e X um conjunto. Uma ação de G sobre X é definida como sendo um homomorfismo $\varphi\colon G \to Sym(X)$.*

Assim, temos que se φ é uma ação de G sobre X, então φ associa a cada elemento $g \in G$ uma permutação de X. Se estamos falando sobre uma fixada ação φ, denotamos x^g ao invés de $x^{\varphi(g)}$ para a ação de $\varphi(g)$ sobre $x \in X$.

Definindo, agora, uma relação de equivalência, $\sim_G$, no conjunto X por:

$$x \sim_G y \text{ se, e somente se, existe } g \in G \text{ com } y = x^g;$$

dizemos que as classes de equivalências de $\sim_G$ são as *G-órbitas*, ou as *órbitas de G em X*. Denotamos, em particular, a órbita de um elemento x de X por x^G, que é dada por: $x^G = \{x^g \,|\, g \in G\}$.

Definição 1.8.8. *O* estabilizador *de um subconjunto Y de X, denotado $Stab_G(Y)$, é dado por:*

$$Stab_G(Y) = \{g \in G \,|\, y^g = y;\ \forall y \in Y\}.$$

De maneira mais específica, definimos o estabilizador de um único ponto:

Definição 1.8.9. *O* estabilizador *de um elemento $x \in X$, denotado $Stab_G(x)$, é dado por:*

$$Stab_G(x) = \{g \in G \,|\, x^g = x\}.$$

Proposição 1.8.10. *$Stab_G(X) \leq G$.*

Demonstração: Segue direto da definição de estabilizador. ∎

Teorema 1.8.11. *Sejam G um grupo finito que age sobre X e $x \in X$. Então, $|G| = |x^G||Stab_G(x)|$.*

Demonstração: Seja $y \in x^G$. Temos que existe $g \in G$ tal que $x^g = y$. Se $g' \in G$ é tal que $x^{g'} = y$, então $g'g^{-1} \in Stab_G(x)$. Assim, $g' \in Stab_G(x)g$ e podemos ver que os elementos g', com $x^{g'} = y$, são precisamente os elementos da classe lateral $Stab_G(x)g$. Mas $|Stab_G(x)g| = |Stab_G(x)|$, logo, para cada $y \in x^G$, existem exatamente $|Stab_G(x)|$ elementos g' de G com $x^{g'} = y$, e o número total de tais $y \in x^G$ deve ser $\dfrac{|G|}{|Stab_G(x)|}$, o que prova o resultado. ∎

Definição 1.8.12. *Sejam G um grupo e $H \leq G$. Um* transversal à direita (respectivamente, à esquerda) *para H em G é um conjunto completo e irredundante de representantes das classes laterais à direita (respectivamente, à esquerda) de H em G.*

Teorema 1.8.13 (Schreier)**.** *Sejam G um grupo finitamente gerado e H um subgrupo de índice finito de G. Então, H é finitamente gerado.*

Demonstração: Sejam $S = \{s_1, \ldots, s_r\}$, um conjunto de elementos de G tal que $G = \langle S \rangle$, $[G : H] = n$. Seja, ainda, $T = \{1 = t_1, \ldots, t_n\}$ um transversal à direita para H em G. Então, $Y = \{H, Ht_2, \ldots, Ht_n\}$ é o conjunto das classes laterais à direita de H em G.

Consideremos a ação de G em Y dada por: $(Ht_i)g = H(t_i g) = Ht_j$, o que fornece uma permutação em Y e, consequentemente, no conjunto $\{1, \ldots, n\}$ tal que $g(i) = j$.

Assim, para qualquer elemento $g \in G$ e inteiro i tal que $1 \leq i \leq n$, $Ht_i g = Ht_{g(i)}$ e, portanto, temos

$$t_i g = h(t_i, g)t_{g(i)}; \text{ tal que } h(t_i, g) \in H. \tag{1.4}$$

Seja, então, $a \in H$. Já que a é um elemento de G temos que a é um produto de elementos em $S \cup S^{-1}$, digamos $a = u_1 \ldots u_k$, em que $u_i \in S \cup S^{-1}$ e $k \geq 0$. Usando a relação 1.4, temos

$$\begin{aligned}
a &= 1.a = 1_d.u_1 \ldots u_k = (t_1 u_1)u_2 \ldots u_k \\
&= (h(t_1, u_1)t_{u_1(1)})u_2 \ldots u_k \\
&= (h(t_1, u_1)t_{u_1(1)} \cdot u_2)u_3 \ldots u_k \\
&= h(t_1, u_1)h(t_{u_1(1)}, u_2)(t_{u_2 u_1(1)} \cdot u_3)u_4 \ldots u_k \\
&= \ldots \\
&= h(t_1, u_1)h(t_{u_1(1)}, u_2) \ldots h(t_{u_{k-1} \ldots u_1(1)}, u_k)t_{u_k \ldots u_2 u_1(1)} \\
&= h(t_1, u_1)h(t_{u_1(1)}, u_2) \ldots h(t_{u_{k-1} \ldots u_1(1)}, u_k)t_{\alpha(1)}.
\end{aligned}$$

Uma vez que $a, h(t_1, u_1), \ldots, h(t_{u_{k-1} \ldots u_1(1)}, u_k) \in H$, temos que $t_{\alpha(1)} = t_1 = 1$ e, assim,

$$a = h(t_1 u_1)h(t_{u_1(1)}, u_2) \ldots h(t_{u_{k-1} \ldots u_1(1)}, u_k).$$

O que significa que H é gerado pelos elementos da forma $h(t_i, u)$, com $1 \leq i \leq n$, e $u \in S \cup S^{-1}$. Portanto, H é finitamente gerado. ∎

Definição 1.8.14. *Considere a mesma notação do teorema anterior. O conjunto $Z = \{h(t, u) \,|\, t \in T, u \in S \cup S^{-1}\}$ é chamado de* conjunto de geradores de Schreier *para H.*

1.9 Sobre Representações Lineares

1.9.1 Alguns conceitos

Os conceitos e resultados presentes nessa seção podem ser encontrados em [21].

Sejam G um grupo e V um espaço vetorial sobre um corpo F de dimensão finita n. Seja $GL(V)$ o grupo das transformações lineares inversíveis de V, o qual pode ser

identificado com $GL(n, F)$ (o grupo das matrizes $n \times n$ inversíveis com coeficientes em F).

Definição 1.9.1. *Um homomorfismo $\rho\colon G \to GL(V)$ é dito uma* representação linear *de G. O inteiro n é dito ser o* grau da representação *ρ.*

Note que $Ker\,\rho \trianglelefteq G$ assim, $G/Ker\,\rho \cong \rho(G) \leq GL(V)$ e dizemos que a representação é *fiel* se $Ker\,\rho = 1$.

Denotamos a imagem de $g \in G$, $\rho(g)$, por ρ_g. Quando ρ é dado, dizemos que V é uma *representação* de G.

Sejam ρ e ρ' duas representações de um mesmo grupo G em espaços vetoriais V e V'. Dizemos que ρ e ρ' são *equivalentes* se existe um operador linear invertível $T\colon V \to V'$ tal que $T \circ \rho_g = \rho'_g \circ T$, para todo $g \in G$.

Definição 1.9.2. *Uma ação $G \times V \to V$ é dita* linear *se:*

$$x^{(g_1 g_2)} = (x^{g_1})^{g_2},\ x^1 = x;\ \forall x \in V,\ g_1, g_2 \in G \text{ e}$$

$$(x + y)^g = x^g + y^g,\ (\lambda x)^g = \lambda x^g;\ \forall x, y \in V,\ g \in G, \lambda \in F.$$

Dizemos, também, que G age linearmente sobre *V se existe tal ação. Dizemos, ainda, que V é um G-*módulo*, ou um G-*espaço*.*

Definição 1.9.3. *Seja ρ uma representação linear de G. Um subespaço W de V é dito ser G-*invariante *se $\rho_g(W) \subseteq W$, para todo $g \in G$.*

Pela definição anterior, para cada $g \in G$ a restrição de ρ_g a W, denotada por ρ_g^W, em que W é G-invariante, pertence a $GL(W)$ e satisfaz $\rho^W_{g_1 g_2} = \rho^W_{g_1}\rho^W_{g_2}$; para quaisquer $g_1, g_2 \in G$. Portanto, $\rho^W\colon G \to GL(W)$ é uma representação linear de G.

Definição 1.9.4. *Uma representação linear $\rho\colon G \to GL(V)$ é dita ser* irredutível *se V é não-nulo e não há subespaço não-trivial de V que seja G-invariante. Caso contrário, ρ é dita ser* redutível.

Definição 1.9.5. *Sejam A um anel e $(M, +)$ um grupo abeliano. Dizemos que M é um A-*módulo *se existe uma função*

$$\begin{aligned} \cdot :\quad & A \times M \ \to M \\ & (a, m) \ \mapsto a \cdot m \end{aligned}$$

tal que para quaisquer $m, n \in M, a, b \in A$:

$$a(m + m) = am + an;\ (a + b)m = am + bm;\ a(bm) = (ab)m;\ 1_A m = m.$$

Sejam G um grupo finito e F um corpo. Denotamos

$$FG := \left\{ \sum_{g \in G} \alpha_g g; \alpha_g \in F \right\},$$

com as seguintes operações:

- $\sum_{g \in G} \alpha_g g + \sum_{g \in G} \beta_g g = \sum_{g \in G} (\alpha_g + \beta_g) g$
- $\left(\sum_{g \in G} \alpha_g g \right) \left(\sum_{h \in G} \beta_h h \right) = \sum_{g,h \in G} (\alpha_g \beta_h) gh$
- $\lambda \left(\sum_{g \in G} \alpha_g g \right) = \sum_{g \in G} (\lambda \alpha_g) g.$

Temos que FG é uma F-álgebra e G é uma base para FG. Assim, $dim_F FG = |G|$.

Definição 1.9.6. *Dizemos que FG, tal como descrito anteriormente, é a* álgebra de grupo *de G sobre F.*

Definição 1.9.7. *Um FG-*módulo*, M, é um espaço vetorial sobre F, de dimensão finita, que é módulo para o anel FG e verifica:*

$$\alpha(rv) = (\alpha r)v = r(\alpha v); \forall v \in M, r \in FG, \alpha \in F.$$

Assim, um FG-módulo é um G-módulo no sentido da Definição 1.9.2

1.9.2 Formas bilineares

Nesta subseção, definiremos formas bilineares e trataremos de alguns resultados relacionados, os quais serão importantes para simplificar a demonstração do Lema 4.2.2. Esses resultados podem ser encontrados em [19] e [33].

Definição 1.9.8. *Seja V um espaço vetorial sobre um corpo F. Uma* forma bilinear sobre V *é uma função f que atribui a cada par ordenado de vetores x, y de V um escalar $f(x, y) \in F$ que satisfaz:*

$$f(cx_1 + x_2, y) = cf(x_1, y) + f(x_2, y)$$

$$f(x, cy_1 + y_2) = cf(x, y_1) + f(x, y_2).$$

Se denotarmos por $V \times V$ o espaço de todos os pares ordenados de V, podemos dizer que uma forma bilinear sobre V é uma função $f \colon V \times V \to F$ que, se fixada uma coordenada, então a outra pode ser vista como uma função linear.

Note que a função nula, definida de $V \times V$ sobre F, é uma função bilinear, a soma de duas formas bilineares é uma forma bilinear e se f é uma forma bilinear e $\lambda \in F$, então λf é uma forma bilinear; de modo que qualquer combinação de formas bilineares é uma forma bilinear. (Segue da definição.)

Ou seja, o conjunto de todas as formas bilineares sobre V é um espaço vetorial.

É possível associar a uma forma bilinear uma matriz, como descrevemos a seguir. Seja V um espaço vetorial de dimensão finita e seja $\mathcal{B} = \{\alpha_1, \ldots, \alpha_n\}$ uma base ordenada para V. Se f é uma forma bilinear sobre V, *a matriz de f na base ordenada $\mathcal{B}$* é uma matriz $n \times n$, A, com entradas $A_{ij} = f(\alpha_i, \alpha_j)$. Quando for necessário deixar claro qual a base usada, denotarmos essa matriz por $[f]_{\mathcal{B}}$.

Dadas duas bases distintas para o espaço vetorial V, temos duas matrizes associadas a forma f, como já foi descrito. Vejamos como podemos relacionar ambas as matrizes.

Sejam $P = [f]_{\mathcal{B}}$ e $Q = [f]_{\mathcal{B}'}$ matrizes de f nas bases $\mathcal{B} = \{x_1, \ldots, x_n\}$ e $\mathcal{B}' = \{x'_1, \ldots, x'_n\}$, respectivamente. Se $M = (m_{ij})$ é a matriz mudança de base de $\mathcal{B}$ para $\mathcal{B}'$, temos:

$$x'_j = \sum_{l=1}^{n} m_{lj} x_l;$$

logo,

$$f(x'_i, x'_j) = f\left(\sum_{k=1}^{n} m_{ki} x_k, \sum_{l=1}^{n} m_{lj} x_l\right) = \sum_{l,k=1}^{n} m_{ki} f(x_i, x_j) m_{lj}.$$

Ou seja, $Q = M^t P M$.

Observe que, pela relação anterior, duas matrizes que representam a mesma forma, não necessariamente na mesma base ordenada, possuem o mesmo posto. Isso permite uma definição de posto para formas bilineares.

Definição 1.9.9. *Se f é uma forma bilinear sobre um espaço vetorial, o* posto de f *é igual ao posto da matriz de f numa base ordenada.*

Definição 1.9.10. *Uma forma bilinear f de um espaço vetorial V é dita ser* não-degenerada*, ou* não-singular*, se para cada par $\alpha, \beta \in V$ existem $x, y \in V$ tais que $f(\alpha, x) \neq 0$ e $f(y, \beta) \neq 0$.*

Formas Bilineares Simétricas

Definição 1.9.11. *Seja f uma forma bilinear sobre um espaço vetorial V. A forma bilinear f é dita ser* simétrica *se $f(x, y) = f(y, x)$, para quaisquer vetores $x, y \in V$.*

Se V é um espaço de dimensão finita, a forma bilinear, f, é simétrica se, e somente se, sua matriz A em alguma base ordenada é simétrica ($A^t = A$).

Formas Bilineares Anti-Simétricas

Definição 1.9.12. *Seja V um espaço vetorial sobre um corpo F. Uma forma bilinear, f, sobre V é denominada* anti-simétrica *se $f(x,y) = -f(y,x)$, para quaisquer vetores $x, y \in V$; além disso, se F possui característica igual a 2, adicionamos a condição $f(x,x) = 0$, para todo $x \in V$.*

Neste trabalho, apenas consideraremos corpos com característica distinta de 2.

Suponhamos agora que f é uma forma bilinear qualquer sobre V e definamos:

$$g(x,y) = \frac{1}{2}[f(x,y) + f(y,x)],$$

$$h(x,y) = \frac{1}{2}[f(x,y) - f(y,x)].$$

Temos que g é uma forma bilinear simétrica sobre V e h é uma forma bilinear anti-simétrica sobre V, de forma que $f = g + h$. Essa expressão para f como soma de uma forma bilinear simétrica e anti-simétrica é única, logo, o espaço das formas bilineares é uma soma direta do subespaço gerado pelas formas bilineares simétricas com o gerado pelas formas bilineares anti-simétricas.

Se V é um espaço de dimensão finita, a forma bilinear é anti-simétrica se, e somente se, sua matriz A em alguma base ordenada é anti-simétrica ($A^t = -A$).

Se f é anti-simétrica, a matriz de f em qualquer base ordenada possui as entradas da diagonal nulas, já que $f(x,x) = -f(x,x)$, para qualquer $x \in V$, o que significa que $f(x,x) = 0$, para qualquer $x \in V$, já que estamos considerando que a característica de F é distinta de 2. Suponhamos que f é uma forma bilinear anti-simétrica, não-nula, sobre V. Assim, existem $\alpha, \beta \in V$, tais que $f(\alpha,\beta) \neq 0$. Multiplicando α por um escalar conveniente, podemos supor que $f(\alpha,\beta) = 1$.

Teorema 1.9.13. *Seja V é um espaço vetorial de dimensão $n \geq 1$ com uma forma bilinear anti-simétrica, f. Então, f pode ser associada a uma matriz da forma:*

$$\left[\begin{array}{cc|ccc} 0 & 1 & & & \\ -1 & 0 & & & \\ \hline & & \ddots & & \\ & & & \begin{array}{cc} 0 & 1 \\ -1 & 0 \end{array} & \end{array}\right].$$

Demonstração: Ver [33], Theorem 1.1.13. ∎

A base $\mathcal{B}$ de um espaço vetorial anti-simétrico é chamada *hiperbólica* se

$$[f]_{\mathcal{B}} = \left[\begin{array}{cc|ccc} 0 & 1 & & & \\ -1 & 0 & & & \\ \hline & & \ddots & & \\ & & & & \\ \hline & & & 0 & 1 \\ & & & -1 & 0 \end{array}\right]$$

e é chamada *simplética* se

$$[f]_{\mathcal{B}} = \left[\begin{array}{c|c} 0 & I_n \\ \hline -I_n & 0 \end{array}\right],$$

onde I_n é a matriz identidade de $M_n(F)$ (o grupo das matrizes $n \times n$ com coeficientes em F).

Com essa definição, se $\mathcal{B} = \{x_1, y_1, \ldots, x_n, y_n\}$, então $\mathcal{B}' = \{x_1, \ldots, x_n, y_1, \ldots, y_n\}$ é uma base simplética, e vice-versa. Dessa forma, nas condições do Teorema 1.9.13, podemos dizer que V possui base hiperbólica e outra simplética.

1.9.3 Grupos que preservam formas bilineares

Sejam f uma forma bilinear sobre um espaço vetorial V e T um operador linear sobre V. Se definimos $g(\alpha, \beta) := f(T\alpha, T\beta)$, então g é uma forma bilinear.

Definição 1.9.14. *Dizemos que* T preserva f *se* $f(T\alpha, T\beta) = f(\alpha, \beta)$, *para todo par* $\alpha, \beta \in V$.

Note que o conjunto de operadores lineares que preservam uma forma bilinear dada é fechado sob o produto de operadores.

Teorema 1.9.15. *Se* f *é uma forma bilinear não-degenerada sobre um espaço vetorial de dimensão finita* V, *então o conjunto de todos os operadores lineares sobre* V *que preservam* f *é um grupo sob a operação de composição.*

Demonstração: Ver [19], Theorem 7 da página 379. ∎

Sejam M a matriz que representa T, um operador linear, numa base ordenada $\mathcal{B}$ de um espaço vetorial V e A a matriz de f nessa mesma base. Sejam $\alpha, \beta \in V$ tais que X e Y são vetores das coordenadas de α e β, respectivamente. Então, podemos escrever

$$f(\alpha, \beta) = X^t A Y \text{ e}$$

$$f(T\alpha, T\beta) = (MX)^t AMY = X^t (M^t AM) Y.$$

Assim, dizemos que T preserva a forma bilinear f se $M^tAM = A$. Além disso, o conjunto de matrizes M, tal que $M^tAM = A$ é um grupo de matrizes sob a multiplicação.

O grupo simplético

Definição 1.9.16. *Para qualquer número natural n, se F é um corpo, dizemos que o* grupo simplético $Sp(2n, F)$ *(também denotado por $Sp_{2n}(q)$) é o subgrupo de $GL(2n, F)$ que consiste de todas as matrizes $n \times n$, X, sobre F tais que $X^tJX = J$, em que J uma matriz tal que $J^t = -J$ e J^t é a matriz transposta de J.*

Proposição 1.9.17. *A ordem do grupo simplético sobre o corpo F_q é*

$$|Sp(2n, q)| = q^{n^2} \prod_{j=1}^{n} (q^{2j} - 1),$$

em que F_q é o corpo de ordem $q = p^k$, para um primo p.

Demonstração: Ver [33], Theorem 3.1.1. ∎

Proposição 1.9.18. $Sp_{2n}(q) \leq SL_{2n}(q)$.

Demonstração: A demonstração segue da definição anterior. ∎

Definição 1.9.19. *Uma matriz é dita* singular *se seu determinante é nulo; caso contrário é dita* não-singular.

1.9.4 Quadrado simétrico e Quadrado Alternado

Sejam V e W espaços vetoriais de dimensão finita m e n, respectivamente, sobre um mesmo corpo F. Diremos que um espaço vetorial denotado por $V \otimes W$, junto com uma aplicação bilinear

$$\begin{aligned} i\colon \quad V \times W &\to V \otimes W \\ (v, w) &\mapsto v \otimes w \end{aligned}$$

é o *produto tensorial* de V e W se, para qualquer espaço vetorial U sobre o mesmo corpo F e qualquer aplicação bilinear $B\colon V \times W \to U$, existe uma, e apenas uma, transformação *linear* $L\colon V \otimes W \to U$ tal que $B(v, w) = L(v \otimes w)$, isto é, $B = L \circ i$:

$$\begin{array}{ccc} V \otimes W & & \\ {\scriptstyle i}\uparrow & \searrow^{L} & \\ V \times W & \xrightarrow[B]{} & U \end{array}$$

Ou seja, dizemos que a aplicação i é uma aplicação bilinear universal, pois qualquer outra é uma composição de i seguida por uma linear. Esta é a propriedade universal do produto tensorial, também chamada *mapeamento universal* ou *universalidade*.

Pode-se verificar que um produto tensorial $V \otimes W$ existe e que se $\{v_1, \ldots, v_m\}$ e $\{w_1, \ldots, w_n\}$ são bases de V e W, respectivamente, então $V \otimes W$ possui como base o conjunto $\{v_i \otimes w_j \,|\, 1 \leq i \leq m, 1 \leq j \leq n\}$.

Sejam V um FG-módulo com base $\{e_1, \ldots, e_n\}$, em que F é um corpo de característica diferente de 2 e G um grupo finito. Então, podemos definir uma estrutura de FG-módulo sobre $V \otimes V$ por $(w \otimes v)g = wg \otimes vg$; para todo $\in G$ e quaisquer $v, w \in V$.

Definindo $W := V \otimes V$ considere o automorfismo $\vartheta \colon W \to W$ tal que $\vartheta(v \otimes w) = w \otimes v$, logo, $\vartheta^2 = id$. Defina, agora, os subespaços de W:

$$Sym^2(V) := \langle v \otimes w \,|\, \vartheta(v \otimes w) = v \otimes w \rangle$$

chamado o *quadrado simétrico* e

$$Alt^2(V) := \langle v \otimes w \,|\, \vartheta(v \otimes w) = -(v \otimes w) \rangle$$

chamado o *quadrado alternado*, aqui denotado por $\Lambda^2(V)$. Com essa definição, segue que $\{e_i \otimes e_j + e_j \otimes e_i \,|\, 1 \leq i < j \leq n\}$ e $\{e_i \otimes e_j - e_j \otimes e_i \,|\, 1 \leq i < j \leq n\}$ são bases dos subespaços $Sym^2(V)$ e $\Lambda^2(V)$, respectivamente, e, portanto,

$$dim_W Sym^2(V) = \frac{n(n+1)}{2} \text{ e } dim_W \Lambda^2(V) = \frac{n(n-1)}{2}.$$

Note que, para qualquer $\omega \in W$, temos $\omega + \vartheta(\omega) \in Sym^2(V)$ e $\omega - \vartheta(\omega) \in \Lambda^2(V)$; além disso,

$$\omega = \frac{\omega + \vartheta(\omega)}{2} + \frac{\omega - \vartheta(\omega)}{2},$$

o que significa que $W = Sym^2(V) + \Lambda^2(V)$.

E mais, se $\omega = w \otimes v$ tal que $\omega \in Sym^2(V) \cap \Lambda^2(V)$, então $\vartheta(\omega) = \omega = -\vartheta(\omega)$, o que implica que a interseção de tais subespaços é trivial e, portanto, $W = Sym^2(V) \oplus \Lambda^2(V)$.

Capítulo 2

Sobre os Algoritmos

2.1 Grupos Livres

Dizemos que uma relação é livre se é uma relação que aparece em qualquer grupo, como, por exemplo, $xx^{-1} = 1$, em que x é um elemento do grupo. Podemos dizer que um grupo *livre* é um grupo livre de qualquer relação não-trivial entre seus elementos (não é abeliano, não é finito, não é nilpotente, ...). Essa ideia será formalizada por um teorema mais adiante. As demonstrações omitidas nessa seção podem ser encontradas em [22] (Chapters 1, 4) e [36].

Seja X um conjunto. Uma *palavra* em X, denotada por ω é um elemento gerado pelos elementos pertencentes a $X \cup X^{-1}$. Muitas vezes denotaremos ω por $\omega(x_1, \ldots, x_n)$ como sendo a palavra gerada pelos elementos $x_1, \ldots, x_n \in X$. Um exemplo de uma palavra em $X = \{x_1, \ldots, x_7\}$ é $\omega(x_1, \ldots, x_7) = x_1^{-1}x_2x_5x_1x_2^{-1}x_7^{-1}$.

Definição 2.1.1. *Um grupo F é dito* livre sobre um subconjunto X *se, dado um grupo qualquer G e uma função $f\colon X \to G$, existe um único homomorfismo de grupos $\varphi\colon F \to G$ tal que $\varphi_{|X} = f$.*

Assim, se $i\colon X \to F$ é a inclusão de X em F, temos que o diagrama a seguir é comutativo.

$$\begin{array}{ccc} X & \xhookrightarrow{i} & F \\ & \searrow^{f} & \swarrow_{\varphi} \\ & G & \end{array}$$

Proposição 2.1.2. *Se F é livre sobre X, então X gera F.*

Proposição 2.1.3. *Sejam F_1 e F_2 dois grupos livres sobre X_1 e X_2, respectivamente. Então, F_1 e F_2 são isomorfos se e, somente se, $|X_1| = |X_2|$.*

Definição 2.1.4. *Se F é livre sobre X, então dizemos que X é uma* base (livre) *para F; além disso, $|X|$ é dito o* posto *de F.*

O teorema a seguir formaliza a ideia introduzida no início da seção.

Teorema 2.1.5. *Um grupo F é livre sobre X se, e somente se:*

i) *X gera F , e*

ii) *não existe relação não trivial entre os elementos de X.*

Proposição 2.1.6. *Dado um conjunto X, existe um grupo livre F com base X.*

Proposição 2.1.7. *Todo grupo é imagem homomorfa de um grupo livre F sobre X, ou seja, é quociente de um grupo livre.*

Demonstração: Seja G um grupo arbitrário e escolha um elemento $x_g \in X$ para cada $g \in G$, um elemento de G. Defina o conjunto $X = \{x_g \,|\, g \in G\}$, então $f\colon X \to G$, em que $f(x_g) = g$ é uma bijeção. Existe um grupo livre F com base X, pela Proposição 2.1.6. Então, existe um homomorfismo $\varphi\colon F \to G$ estendendo f, de forma que φ é uma função sobrejetora, pois f é sobrejetora. E segue o resultado. ∎

Sejam G um grupo, F um grupo livre, livremente gerado por um conjunto não-vazio X e $\varphi\colon F(X) \to G$ um epimorfismo. Se r é uma palavra pertencente ao núcleo $N = Ker\,\varphi$, então $\varphi(r) = 1$ e dizemos que a palavra $\varphi(r)$ é um *relator*, correspondente a relação $\varphi(r) = 1$. Seja $R \subseteq F$ um conjunto de relatores tal que $N = Ker\,\varphi$ é o fecho normal de R em F. Dizemos que R é o *conjunto definidor de relatores* de G.

Temos que X e R determinam G, a menos de isomorfismo. Desse modo, denotamos $G = \langle X|R\rangle$, em que X é um conjunto não-vazio de geradores e R é o conjunto de relatores, ou seja, um conjunto de palavras em X, ou relações da forma $u = v$ que corresponde ao relator uv^{-1}. O par $\langle X|R\rangle$ é dito ser uma apresentação de $G \cong F/N$.

Exemplos 2.1.8.

$$G = \langle a, b|\, a^4, b^2, a^b = a^{-1}\rangle,$$

$$H = \langle a, b|\, a^4, b^2 = a^2, a^b = a^{-1}\rangle,$$

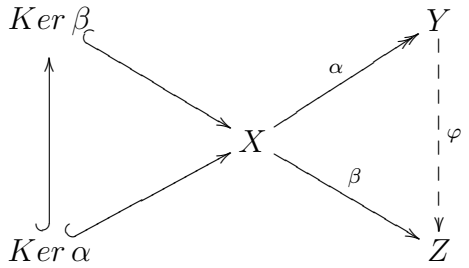
$$A = \langle a, b|\, a^2, b^2, [a, b]\rangle.$$

O que podemos dizer sobre esses grupos? Essas apresentações já nos permite ver algumas relações triviais nos grupos e podemos dizer, por exemplo, que A é um grupo abeliano elementar, ou que H não é abeliano. Mas, podemos decidir imediatamente sobre a finitude desses grupos, por exemplo? É possível criar algoritmos para responder questões sobre a estrutura desses grupos, com uma ajuda computacional. Além disso, as apresentações desses grupos influenciam na eficiência de cálculos computacionais. Podemos calcular uma apresentação mais "vantajosa" para decidir, por exemplo, se possuem ordem prima, se são nilpotentes ou solúveis.

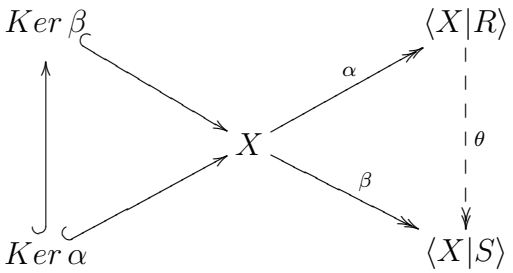
A próxima proposição nos diz que sempre podemos encontrar uma apresentação para qualquer grupo.

Proposição 2.1.9. *Todo grupo possui uma apresentação e todo grupo finito possui uma apresentação finita.*

Lema 2.1.10. *Sejam $\alpha\colon X \to Y$, $\beta\colon X \to Z$ homomorfismos de grupos tais que α é sobrejetor e $Ker\,\alpha \subseteq Ker\,\beta$. Então, existe um homomorfismo $\varphi\colon Y \to Z$ com $\alpha\varphi = \beta$.*



Teorema 2.1.11. ***(Von Dyck)*** *Sejam X um conjunto e F um grupo Livre sobre X. Se R e S são subconjuntos de F tais que $R \subseteq S$, então existe um epimorfismo $\theta\colon \langle X|R\rangle \twoheadrightarrow \langle X|S\rangle$ que fixa X elemento a elemento. Além disso, o núcleo de θ é o fecho normal de $S - R$ em $\langle X|R\rangle$.*



Teorema 2.1.12. ***(Teste de Substituição)*** *Sejam G um grupo com apresentação $\langle X|R\rangle$, H um grupo arbitrário e $\theta\colon X \to H$ uma função. Então, θ se estende a um homomorfismo $\theta'\colon G \to H$ se, e somente se, para todo $x \in X$ e todo $r \in R$, o resultado da substituição de x por $\theta(x)$ em r é a identidade de H.*

2.2 Apresentação por Potências e Comutadores

Uma apresentação de um grupo define uma "maneira" que tal grupo pode ser dado. Assim, em vez de trabalharmos com o grupo, podemos trabalhar com sua apresentação. Como já foi dito, um grupo pode ter uma apresentação mais "vantajosa" que outra no sentido de otimizar cálculos e algoritmos relacionados à estrutura do grupo.

Se tivermos uma apresentação consistente por potências e comutadores para um grupo (ver Definição 2.2.4), podemos, por exemplo, solucionar o problema da palavra

para esse grupo (decidir se duas palavras no mesmo conjunto de geradores representam o mesmo elemento). Além disso, essa apresentação fornece uma série normal para o grupo e muitos algoritmos, desenvolvidos para calcular propriedades de p-grupos, trabalham sobre a série normal do grupo.

A maioria dos conceitos e resultados desse capítulo podem ser encontrados em "The p-group generation algorithm" [32] de E. A. O'Brien.

Definição 2.2.1. *Uma* apresentação por potências e comutadores *para um grupo G consiste em um conjunto finito de geradores $A = \{a_1 \dots a_n\}$ e um conjunto de $\frac{n(n+1)}{2}$ relações descritas por:*

$$a_i^p = \prod_{l=i+1}^{n} a_l^{\alpha(i,l)};\ 1 \leq i \leq n-1 \ e\ a_n^p = 1$$

$$[a_j, a_i] = \prod_{l=j+1}^{n} \alpha_l^{\beta(i,j,l)};\ 1 \leq i < j \leq n-1 \ e\ [a_n, a_i] = 1;\ 1 \leq i \leq n-1,$$

em que p é um número primo e $1 \leq \alpha(i,l), \beta(i,j,l) \leq p-1$; $\alpha(i,l), \beta(i,j,l) \in \mathbb{N}$.

Proposição 2.2.2. *Todo p-grupo finito tem uma apresentação por potências e comutadores.*

Demonstração: Suponhamos que G seja um p-grupo finito de ordem p^n. Então, G é um grupo nilpotente e, pela Proposição 1.3.12, possui uma série central da forma:

$$G = G_1 > G_2 > \ldots > G_{n+1} = 1$$

tal que cada fator G_i/G_{i+1} é cíclico de ordem p, para $1 \leq i \leq n$. Logo,

$$G_n/G_{n+1} = G_n = \langle g_n \,|\, g_n^p = 1 \rangle \leq Z(G) \text{ e} \tag{2.1}$$

$$G_{n-1}/G_n = \langle g_{n-1} \,|\, g_{n-1}^p = 1 \rangle \leq Z(G/G_n). \tag{2.2}$$

O que implica, pela relação de inclusão 2.1, que:

$$G_{n-1} = \langle g_{n-1}, g_n \,|\, g_{n-1}^p = g_n^{\alpha(n-1,n)}, g_n^p = 1, [g_n, g_{n-1}] = 1 \rangle$$

e, pela relação de inclusão 2.2:

$$\begin{aligned} G_{n-2} = \langle g_{n-2}, g_{n-1}, g_n \,|\quad & g_{n-2}^p = g_{n-1}^{\alpha(n-2,n-1)} g_n^{\alpha(n-2,n)}, g_{n-1}^p = g_n^{\alpha(n-1,n)}, g_n^p = 1, \\ & [g_n, g_{n-1}] = [g_n, g_{n-2}] = 1, [g_{n-1}, g_{n-2}] = g_n^{\beta(n-1,n-2,n)} \rangle. \end{aligned}$$

Seguindo um raciocínio análogo, temos que, para todo inteiro k tal que $1 \leq k \leq n$:

$$\begin{aligned} G_k = \langle g_k, g_{k+1}, \ldots, g_{n-1}, g_n \mid \quad & g_i^p = g_{i+1}^{\alpha(i,i+1)} g_{i+2}^{\alpha(i,i+2)} g_n^{\alpha(i,n)}, \\ & k \leq i \leq n-1, 0 \leq \alpha(i,j) < p, g_n^p = 1, \\ & [g_j, g_i] = g_{j+1}^{\beta(i,j,i+1)} g_{j+2}^{\beta(i,j,i+2)} \ldots g_n^{\beta(i,j,n)}, \\ & 1 \leq i < j \leq n-1, 0 \leq \beta(i,j,l) < p, \\ & [g_n, g_j] = 1, 1 \leq j \leq n \rangle. \end{aligned}$$

Portanto, G possui a apresentação por potências e comutadores dada por:

$$\begin{aligned} G = G_1 = \langle g_1, g_2, \ldots, g_{n-1}, g_n \mid \quad & g_i^p = g_{i+1}^{\alpha(i,i+1)} g_{i+2}^{\alpha(i,i+2)} g_n^{\alpha(i,n)}, \\ & 1 \leq i \leq n-1, 0 \leq \alpha(i,j) < p, g_n^p = 1, \\ & [g_j, g_i] = g_{j+1}^{\beta(i,j,i+1)} g_{j+2}^{\beta(i,j,i+2)} \ldots g_n^{\beta(i,j,n)}, \\ & k \leq i < j \leq n-1, 0 \leq \beta(i,j,l) < p, \\ & [g_n, g_j] = 1, k \leq j \leq n \rangle. \end{aligned}$$

■

Observação 2.2.3. *Seja G um grupo finito com a seguinte apresentação por potências e comutadores:*

$$\text{(P)} \qquad \begin{cases} \textit{geradores:} & a_1, \ldots, a_n \\ \textit{relações:} & a_i^p = \prod_{l=i+1}^{n} a_l^{\alpha(i,l)};\ 1 \leq i \leq n-1 \ \textit{e}\ a_n^p = 1 \\ & [a_j, a_i] = \prod_{l=j+1}^{n} \alpha_l^{\beta(i,j,l)};\ 1 \leq i < j \leq n-1 \\ & [a_n, a_i] = 1;\ 1 \leq i \leq n-1 \end{cases}$$

em que p é um número primo, $1 \leq \alpha(i,l)$ e $\beta_(i,j,l) \leq p-1$.

Se $A_i = \langle a_i, \ldots, a_n \rangle$, para todo inteiro i tal que $1 \leq i \leq n$, temos que $A_i \trianglelefteq G$ e ainda que qualquer elemento a de A_i pode ser expresso na sua forma normal*:*

$$a = a_i^{\beta_i} \ldots a_n^{\beta_n} \ \textit{em que}\ 0 \leq \beta_j \leq p-1.$$

Temos ainda que, para cada i, $A_i/A_{i+1} = \langle a_i A_{i+1} \rangle$, tal que $a_i^p \in A_{i+1}$, logo,

$$|A_i/A_{i+1}| = 1 \ \textit{ou}\ |A_i/A_{i+1}| = p.$$

De modo que G é um p-grupo e $|G| \leq p^n$.

Definição 2.2.4. *A apresentação (P), definida anteriormente, é denominada* consistente *se $|G| = p^n$.*

Numa apresentação que não é consistente duas palavras com formas normais dife-

rentes podem representar o mesmo elemento do grupo. Mas, numa apresentação consistente as formas normais são únicas, por isso a importância de uma apresentação ser consistente.

2.2.1 Consistência

O processo de coleta é um método que pode ser usado para determinar a forma normal para um elemento de um grupo dado por uma apresentação consistente por potências e comutadores. Nesta subseção apenas introduziremos o assunto, o leitor interessado em maiores detalhes pode consultar [24].

Sejam p um primo, G um p-grupo finito, d-gerado de ordem no máximo p^n, com apresentação (P), tal como definida na Observação 2.2.3. Os elementos da forma $w = a_1^{\alpha(1)} \dots a_n^{\alpha(n)}$, em que $0 \leq \alpha(i) < p$, são ditos *palavras normais no geradores de G*.

Toda palavra nos geradores de G pode ser transformada numa palavra normal usando o *processo de coleta*, o qual descreveremos a seguir.

- Comece com $w = a_1^{\alpha(1)} \dots a_n^{\alpha(n)}$ uma palavra nos geradores de G.
- Enquanto w não é uma palavra normal faça:

  1. como w não é uma palavra normal, w contém no mínimo uma subpalavra não-normal minimal da forma a_i^p ou $a_j a_i$ com $j > i$. Escolha uma tal subpalavra qualquer, u.
  2. Use alguma relação correspondente em (P) e substitua u por essa nova palavra, obtendo assim uma palavra w', nos geradores de G. (Esse passo é dito ser o *processo de coleta* de u.)
  3. Faça $w := w'$.

Observe que tal processo termina com um número finito de passos.

Se $W = \{a_1^{\alpha(1)} \dots a_n^{\alpha(n)} \mid 0 \leq \alpha(i) < p\}$ é o conjunto de todas as palavras normais de um grupo G tal como descrito no início desta seção, então $|W| = p^n$. Como toda palavra nos geradores de G pode ser transformada numa palavra normal, podemos definir o produto $u.v$ de dois elementos $u, v \in W$ como sendo a palavra normal de uv obtida pelo processo de coleta.

Se W é um grupo, então $W \cong G$, $G = p^n$ e (P) é consistente. Assim, se estabelecermos um critério para que a operação descrita seja associativa, teremos um critério de consistência.

Teorema 2.2.5. *A operação descrita anteriormente (sobre as palavras normais) é associativa se as seguintes identidades são verdadeiras:*

$$\begin{aligned}
&(a_i.a_j).a_k = a_i.(a_j.a_k);\ \textit{para } 1 \leq k < j < i \leq n \\
&(a_j^{p-1}.a_j).a_k = a_j^{p-1}.(a_j.a_k);\ \textit{para } 1 \leq k < j \leq n \\
&(a_i.a_j).a_j^{p-1} = a_i.(a_j.a_j^{p-1});\ \textit{para } 1 \leq j < i \leq n \\
&(a_i.a_i^{p-1}).a_i = a_i.(a_i^{p-1}.a_i);\ \textit{para } 1 \leq i \leq n
\end{aligned} \tag{2.3}$$

Tais identidades com $k \leq d$ são suficientes para garantir a associatividade de W.

Demonstração: Ver [24], Teorema 2.2.5. ∎

As identidades 2.3 são chamadas de *condições* ou *testes de associatividade de Wamsley.*

2.3 Grupos Policíclicos

Um *grupo policíclico* é caracterizado pela existência de uma série normal com fatores cíclicos (ver, por exemplo, a Proposição 1.3.12). Podemos dizer que grupos policíclicos são grupos solúveis em que cada subgrupo é finitamente gerado (ver Teorema 2.3.5). O estudo sobre esses grupos começou com Hirsch em duas publicações [14] e [15], continuando com três artigos futuros [16], [17] e [18]. Nos últimos anos, grupos policíclicos atraiu a atenção de matemáticos por formarem uma grande classe de grupos, na qual muitos problemas a eles relacionados podem ser resolvidos por meio de algoritmos [38].

Nessa classe de grupos estão incluídos os grupos solúveis finitos e os grupos nilpotentes finitamente gerados. Consequentemente, inclui também a classe de p-grupos finitos.

Os conceitos e resultados aqui presentes podem ser encontrados em [20], [29] e [38].

Definição 2.3.1. *Um grupo G é dito ser* policíclico *se, para algum n natural, possui uma sequência de subgrupos:*

$$G = G_1 \geq G_2 \geq \ldots \geq G_n \geq G_{n+1} = 1$$

tal que $G_{i+1} \trianglelefteq G_i$ e G_i/G_{i+1} é cíclico para todo $1 \leq i \leq n$. Tal sequência é chamada de série policíclica de G.

Exemplo 2.3.2. *Seja $G = \langle (1,3)(2,4), (1,2)(3,4), (1,2,3) \rangle$. Observe que G é grupo policíclico. De fato, $V = \langle (1,3)(2,4), (1,2)(3,4) \rangle \trianglelefteq G$ e $C_2 = \langle (1,3)(2,4) \rangle \trianglelefteq V$. Além disso, $G \trianglerighteq V \trianglerighteq C_2$ é série policíclica de G.*

Teorema 2.3.3. i) *Sejam G um grupo e N um subgrupo normal de G. Se N e G/N são policíclicos, então G é policíclico;*

ii) *todo grupo abeliano finitamente gerado é policíclico;*

iii) *todo grupo nilpotente finitamente gerado é policíclico.*

Demonstração: Ver [29], Theorem 2.1.3 e Proposição 1.3.12. ∎

Teorema 2.3.4. *Seja G um grupo policíclico. Então:*

i) *se $N \leq G$, então N é policíclico. Além disso, se $N \trianglelefteq G$ então G/N é policíclico;*

ii) *G é finitamente gerado;*

iii) *G é solúvel.*

Demonstração: Ver [29], Theorem 2.1.1. ∎

Pelo Teorema 2.3.4, todos os grupos policíclicos são solúveis e finitamente gerados, contudo a recíproca não é verdadeira, ou seja, existem grupos solúveis finitamente gerados que não são policíclicos, ver [29], Example 2.1.2. O teorema a seguir determina quando tal recíproca é verdade.

Teorema 2.3.5. *Um grupo G é policíclico se, e somente se, G é solúvel e todo subgrupo de G é finitamente gerado.*

Demonstração: Ver [38], Proposition 4 da página 4. ∎

2.3.1 Sequência policíclica de geradores

Considere G um grupo policíclico. Então, G possui uma série policíclica, digamos $G = G_1 \geq G_2 \geq \ldots \geq G_n \geq G_{n+1} = 1$. Além disso, é possível determinar elementos $\{g_1, \ldots, g_n\}$ em G tais que $\langle g_1, \ldots, g_n \rangle = G$ e $g_i G_{i+1}$ é um gerador de G_i/G_{i+1}, tal gerador existe pois G_i/G_{i+1} é cíclico. Com base nisso, introduziremos o conceito de sequência policíclica de geradores de G.

Definição 2.3.6. *A sequência ordenada $(g_1, \ldots, g_n)$ de elementos de G é dita uma* sequência policíclica de geradores *se os grupos $G_i = \langle g_i, \ldots, g_n \rangle$ formam uma série policíclica de G.*

A sequência policíclica de geradores pode ser usada para expressar cada elemento de G de maneira única. Um elemento $g \in G_i$ pode ser escrito como o produto $g_i^{e_i} g'$ com $g' \in G_{i+1}$. Esse produto é único se G_i/G_{i+1} é infinito ou se G_i/G_{i+1} tem ordem finita m_i, em que $0 \leq e_i \leq m_i$. Por indução, todo $g \in G$ pode ser expresso unicamente como o produto $g_1^{e_1} \ldots g_n^{e_n}$, em que $0 \leq e_j \leq m_j$, se G_i/G_{i+1} é finito de ordem m_j.

A palavra $g_1^{e_1} \ldots g_n^{e_n}$ é chamada de *forma normal de g com respeito à sequência policíclica de geradores* $(g_1, \ldots, g_n)$, e a sequência $exp(g) := (e_1, \ldots, e_n)$ é denominada

vetor expoente de g com respeito à sequência policíclica de geradores $(g_1, \ldots, g_n)$. Se estiver claro no contexto qual é a sequência policíclica de geradores usada, dizemos apenas *forma normal de* g. Uma palavra ω na sequência policíclica de geradores é uma forma normal se, e somente se, $\omega = g_1^{e_1} \ldots g_n^{e_n}$, em que $0 \leq e_i \leq m_i$ se G_i/G_{i+1} é finito de ordem m_i.

Exemplo 2.3.7. *Considere o grupo* $G = \langle (1,3)(2,4), (1,2)(3,4), (1,2,3) \rangle$*, tal como no Exemplo 2.3.2.*

$X := [(1,2,3), (1,2)(3,4), (1,3)(2,4)]$ *é uma sequência policíclica de geradores para* G *tal que* $m_1 = 3, m_2 = 2$ *e* $m_3 = 2$.

Uma *série principal* de um grupo G é uma série normal $G = G_1 \geq G_2 \geq \ldots \geq G_n \geq G_{n+1} = 1$ tal que cada G_{i+1} é o maximal entre os subgrupos normais a G contidos em G_i. Se G é um p-grupo, a série principal de G é uma série policíclica de G, logo, G é policíclico. A correspondente sequência policíclica de geradores para G é denominada *base* para G. Podemos ver que, sendo m_i a ordem de G_i/G_{i+1} (finita ou não), então $g_i^{m_i} \in G_{i+1}$ e $g_k^{m_j} \in G_{j+1}$; para quaisquer inteiros i, j, k tais que $0 \leq i \leq n$ e $0 \leq j \leq k \leq n$.

Assim, a base de um p-grupo determina uma apresentação consistente por potências e comutadores de G, em que as relações definidoras são da forma:

$$g_i^p = g_{i+1}^{\beta(i,i,i+1)} \ldots g_n^{\beta(i,i,n)} \text{ e}$$

$$[g_i, g_j] = g_{j+1}^{\beta(i,j,j+1)} \ldots g_n^{\beta(i,j,n)}$$

para quaisquer inteiros i, j com $1 \leq i < j \leq n$, em que $\beta(i,j,k) \in \{0, \ldots, p-1\}$.

Essa apresentação, denotada por $Pc\langle g_i, \ldots, g_n | R \rangle$, é dita ser *apresentação policíclica* e será usada mais tarde nos grupos definidos no Capítulo 4.

Teorema 2.3.8. *Toda sequência policíclica determina uma única apresentação policíclica. Assim, todo grupo policíclico pode ser definido por uma apresentação policíclica.*

Demonstração: Ver [20], Theorem 8.8. ∎

O teorema a seguir diz que toda apresentação policíclica define um grupo policíclico.

Teorema 2.3.9. *Se G é um grupo definido por uma apresentação policíclica sobre os geradores $x_1, \ldots, x_n$, então G é grupo policíclico com sequência policíclica de geradores $X = (x_1, \ldots, x_n)$.*

Demonstração: Defina $G_i := \langle x_i, \ldots, x_n \rangle \leq G$. As relações em R fornecem que $G_{i+1} \trianglelefteq G_i$; para todo inteiro i tal que $1 \leq i \leq n$. Por construção, G_i/G_{i+1} é cíclico e, assim, G é policíclico. Como $G_i = \langle x_i, G_{i+1} \rangle$, X sequência policíclica de geradores para G. ∎

Exemplo 2.3.10. *Na apresentação*

$$Pc\langle x_1, x_2, x_3 : x_1^2 = x_2,\ x_2^2 = x_3,\ x_3^2 = 1,\ [x_2, x_1] = x_3,\ [x_3, x_1] = 1,\ [x_3, x_2] = 1\rangle$$

temos que $x_1x_2 = x_1x_1^2 = x_1^2x_1 = x_2x_1 = x_1x_2x_3$.

Dessa maneira, vemos que nem todo elemento do grupo com tal apresentação tem uma única forma normal.

2.4 Estabilizadores

Esta seção foi baseada no artigo de B. Eick, C. R. Leedham-Green e E. A. O'Brien [9] e na tese de doutorado de R. Schwingel [37]. Descrevemos aqui algumas técnicas para determinar o estabilizador de um dado grupo.

2.4.1 Estabilizadores de grupos de matrizes

Sejam $G \leq GL(n, q)$ tal que $q = p^s$, p é primo, e $U \leq V$ um subespaço u-dimensional do G-módulo V, n-dimensional. Nesta subseção discutiremos como determinar o $Stab_G(U)$.

Definição 2.4.1. *Um* subgrupo unipotente *de $GL(V)$ é um subgrupo em que qualquer elemento possui todos os autovalores iguais a 1.*

Proposição 2.4.2. *Dado $q = p^s$, um p-subgrupo de Sylow de $GL(n, q)$ tem ordem $p^{s\binom{n}{2}}$ e é isomorfo ao grupo de matrizes unitriangulares inferiores, sendo assim um subgrupo unipotente.*

Demonstração: Temos que a ordem do grupo $GL(n, q)$ é

$$q^{n(n-1)/2} \prod_{1}^{n} (q^i - 1).$$

Uma vez que, para qualquer $i > 0$, $q^i - 1 \equiv -1 \pmod q$ e como $q = p^s$, temos que $q^i - 1 \equiv -1 \pmod p$. O que significa que p é relativamente primo a:

$$\prod_{i=1}^{n} (q^i - 1).$$

Portanto, a ordem do p-subgrupo de Sylow de $GL(n, q)$ é $q^{\binom{n}{2}} = p^{s\binom{n}{2}}$.

O produto de duas matrizes unitriangulares inferiores é ainda uma matriz unitriangular inferior, o conjunto dessas matrizes formam um subgrupo de $GL(n, q)$; além disso, essas matrizes possuem $\binom{n}{2}$ entradas sobre o corpo $GF(q)$ dando um total de $q^{\binom{n}{2}}$ matrizes inferiores, o que demostra o resultado. ∎

Subespaços Invariantes

Consideraremos uma série de composição, $V = V_1 > V_2 > \ldots > V_r > V_{r+1} = 0$, do G-módulo V, isto é, a série de subespaços G-invariantes de V tais que V_i/V_{i+1} é irredutível sob a ação de G. Para $1 \leq j \leq i \leq r+1$, definimos: $U_{i,j} = (U + V_i) \cap V_j$. Como $U_{i,j+1} = U_{i,j} \cap V_{j+1} \leq U_{i,j}$ e $U_{i-1,j} = U_{i,j} + V_{i-1}$, temos que:

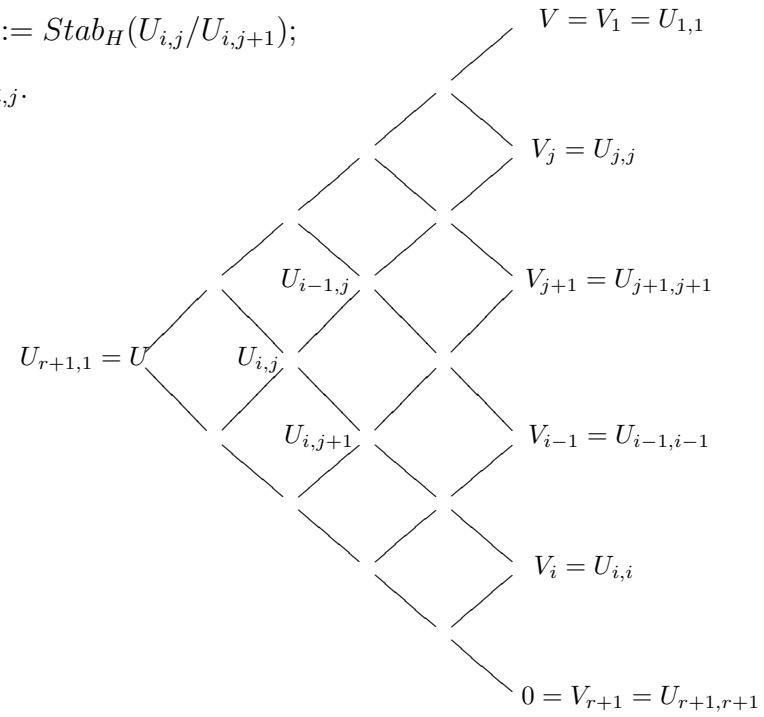
$$Stab_G(U_{i,j}) \leq Stab_G(U_{i-1,j}) \text{ e } Stab_G(U_{i,j}) \leq Stab_G(U_{i,j+1}). \tag{2.4}$$

Lema 2.4.3. *Seja G um grupo agindo sobre Ω e sejam $w, v \in \Omega$ tais que $Stab_G(w) \leq Stab_G(v)$. Então, $Stab_G(w) = Stab_{Stab_{G(v)}}(w)$.*

Demonstração: Segue da definição de estabilizador, já que $Stab_G(w) = \{g \in G, w^g = w\} \subseteq Stab_G(v)$, logo $Stab_G(w) = \{g \in Stab_G(v), w^g = w\}$. ∎

Pelo Lema 2.4.3, podemos dividir o cálculo do estabilizador $Stab_G(U)$ em uma sequência de cálculos de estabilizadores de ordem menor, tal como descrevemos no algoritmo a seguir:

- comece com $H := G$;
- marque $U_{i,i}$; $\forall\, 1 \leq i \leq r+1$;
- enquanto existir algum $U_{i,j}$ desmarcado:
  - escolha um subespaço $U_{i,j}$ tal que $U_{i,j+1}$ e $U_{i-1,j}$ estejam marcados;
  - construa a ação de H sobre $U_{i-1,j}/U_{i,j+1}$;
  - calcule $H := Stab_H(U_{i,j}/U_{i,j+1})$;
  - marque $U_{i,j}$.



Em qualquer estágio do algoritmo, H é um subgrupo de G que estabiliza todos os subespaços marcados. Esse procedimento termina com $H = Stab_G(U)$, já que $Stab_G(U) = \bigcap_{i \geq j} Stab_G(U_{i,j})$, pela relação de inclusão 2.4.

Calculamos $Stab_H(U_{i,j})$ apenas se H já estabiliza $U_{i,j+1}$ e $U_{i-1,j}$ por duas razões. Primeiro, se H não estabiliza $U_{i,j+1}$ ou $U_{i-1,j}$, então podemos encontrar um subgrupo intermediário entre H e $Stab_H(U_{i,j})$, pois pela relação 2.4,

$$Stab_H(U_{i,j}) \leq Stab_H(U_{i-1,j}) < H \text{ ou } Stab_H(U_{i,j}) \leq Stab_H(U_{i,j+1}) < H.$$

Além disso, podemos reduzir a ação de H ao subespaço menor $U_{i-1,j}/U_{i,j+1}$, pois

$$Stab_H(U_{i,j}/U_{i,j+1}) = Stab_H(U_{i,j}).$$

Observe que não existe um único caminho para calcular $Stab_G(U)$.

O estabilizador sob ação de um p-grupo

Se G um p-subgrupo de $GL(n,p)$, então G é unipotente, pelo Lema 2.4.2. R. Schwingel [37] apresentou um algoritmo para construir um representante canônico $\overline{U}$ da G-órbita do subespaço U de V e, ao mesmo tempo, construir um conjunto de geradores para $Stab_G(\overline{U})$ e um elemento $t \in G$ tal que $U^t = \overline{U}$.

O representante canônico é definido por uma relação de ordem sob a órbita de U sob a ação de G. Dessa maneira, podemos decidir se dois subespaços estão na mesma órbita sob G com cálculos e comparações de seus representantes canônicos.

Assumimos que temos $(g_1, \ldots, g_m)$ como uma base para o grupo G, tal como definimos na Seção 2.3. Seja $V = V_1 > V_2 > \ldots > V_n > V_{n+1} = 0$ uma série de composição maximal G-invariante de V. Então, V tem uma base ordenada $(e_1, \ldots, e_n)$ com $e_i \in V_i \setminus V_{i+1}$ para $1 \leq i \leq n$. A forma canônica depende da escolha da base ordenada.

Definição 2.4.4. *Sejam $X, Y \subseteq \{1, \ldots, n\}$. Então, $X < Y$ se ocorre algum dos seguintes casos:*

1. *$X \neq \emptyset$ e $Y = \emptyset$.*
2. *$X \neq \emptyset$, $Y \neq \emptyset$ e $\min X < \min Y$.*
3. *$X \neq \emptyset$, $Y \neq \emptyset$ e se $\min X = \min Y = k$, então $X \setminus \{k\} < Y \setminus \{k\}$.*

Assim, obtemos uma ordem total (ou linear) sobre o conjunto de subconjuntos de $\{1, \ldots, n\}$.

Sejam $v = \sum_{i=1}^{n} a_i e_i \in V$ e $Z_v = \{i : 1 \leq i \leq n \text{ e } a_i = 0\}$. Definimos uma ordem parcial em V: se $Z_v < Z_w$, então $v < w$, para $v, w \in V$.

Definição 2.4.5. *A* forma canônica *de um vetor $v \in V$ em sua órbita sob G é o menor elemento de sua órbita com respeito a esta ordem defina anteriormente.*

R. Schwingel mostrou que a forma canônica de um vetor v é única em sua órbita sob G (ver [37], Theorem 3.2).

Definição 2.4.6. *Sejam dois subespaços m-dimensionais U e W de V com $U = U_1 > U_2 > \ldots > U_m > 0$ e $W = W_1 > W_2 > \ldots > W_m > 0$ as respectivas séries de composição maximal G-invariante de U e W. Dizemos que $U <_s W$ se ocorre algum dos seguintes casos:*

1. *$U_m = \langle u \rangle, W_m = \langle w \rangle$ e $u < w$;*
2. *$i < m$ e $U_{i+1} <_s W_{i+1}$;*
3. *$i < m, U_{i+1} = W_{i+1}$, $U_i = \langle U_{i+1}, u \rangle, W = \langle W_{i+1}, w \rangle$ e se $\overline{u}$ é o menor elemento de $\{u + x \,|\, x \in U_{i+1}\}$ e $\overline{w}$ é o menor elemento de $\{w + x \,|\, x \in W_{i+1}\}$, então $\overline{u} < \overline{w}$.*

A relação $<_s$ define uma ordem parcial sobre os subespaços de V.

Definição 2.4.7. *A* forma canônica *de um subespaço U de V em sua órbita sob G é o menor subespaço em sua órbita com respeito a relação de ordem $<_s$.*

Seja $U \leq V$. A interseção de U com cada V_j resulta numa série maximal em U quando já removido termos duplicados. $Stab_G(U)$ estabiliza cada subespaço dessa série; em particular, estabiliza o subespaço unidimensional, U_1. Determinamos, então, a forma canônica e o estabilizador para U_1, e procedemos recursivamente.

Reduzimos, assim, o caso em que U possui dimensão 1. Seja u um elemento não-nulo de U_1 com coeficiente líder igual a 1. Como G é unipotente, u^g possui, também, coeficiente líder igual a 1. Assim, $Stab_G(U)$ estabiliza u e para encontrar uma forma canônica de U basta encontrar uma forma canônica de u. Descreveremos a seguir como construir essa forma canônica de u. Defina a *altura* de $v \in V$ como sendo o inteiro j tal que $v \in V_j \setminus V_{j+1}$, a altura do vetor nulo é tomada como sendo $n + 1$. Além disso, sendo g um elemento de G, definimos a *altura* $h_v(g)$ com respeito a v como sendo a altura de $v(g - 1)$.

Se $h_u(g) = n+1$ para todo g numa dada base $(g_1, \ldots, g_m)$ para G, então G centraliza u e está terminado. Se não, sejam j o mínimo dessas alturas e k o maior inteiro entre 1 e m tal que $h_u(g_k) = j$ então, defina $g = g_k$. Agora, para algum l tal que $1 \leq l \leq p - 1$ temos $u^{g^l} = \sum_{i=1}^{n} a_i e_i$ com $a_j = 0$ e defina $u_1 = u^{g^l}$. Remova g da base de G.

Para cada $x \neq g$ na base com $h_{u_1}(x) = j$, determine um inteiro l_x em que $0 \leq l_x \leq p - 1$ e tal que $h_{u_1}(xg^{l_x}) > j$ e substitua x por xg^{l_x}.

É possível provar que a sequência resultante é a base para um subgrupo G_1 de G com a propriedade de que $h_{u_1}(x) > j$, para qualquer $x \in G_1$ e, além disso, a forma canônica de u com respeito a G é a forma canônica de u_1 com respeito a G_1.

Exemplo 2.4.8. *Sejam*

$$g_1 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}, g_2 = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \text{ e } g_3 = \begin{bmatrix} 1 & 0 & 2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

elementos em $GL(3,3)$ *e* $X = \{g_1, g_2, g_3\}$. *Sejam, ainda,* $G = \langle X \rangle \leq GL(3,3)$, $V = \mathbb{Z}_3^3$. *Se* $e_1 = (1,0,1), e_2 = (0,1,0)$ *e* $e_3 = (0,0,1)$, *temos que* $\{e_1, e_2, e_3\}$ *é uma base de* V. *Vamos calcular a forma canônica de* $U = \langle u \rangle$, *tal que* $u = (0,1,1)$, *como foi descrito anteriormente.*

Temos que:

$$h_u(g_1) = h(u(g_1 - 1)) = h((0,0,1)) = 3$$
$$h_u(g_2) = h(u(g_2 - 1)) = h((0,0,0)) = 4$$
$$h_u(g_3) = h(u(g_3 - 1)) = h((0,0,0)) = 4.$$

Assim, $j = 3$, $k = 1$ *e* $g = g_1$. *Como* $u^g = ug = (0,1,2)$ *e* $u^{g^2} = ug^2(0,1,0)$, *tomamos* $l = 2$ *e definimos* $u_1 = (0,1,0)$. *Agora, removemos* g *da base,* X, *obtendo* $X = \{g_2, g_3\}$. *Mas,* $h_{u_1}(g_2) = h_{u_1}(g_3) = 4 > 3$. *Logo, a forma canônica de* u *sob* G *é* u_1, X *é uma base para* $Stab_G(u_1)$ *e* g_1 *é um elemento de* G *que transforma* $(0,1,1)$ *em sua forma canônica.*

2.4.2 Estabilizadores em Grupos Híbridos

Explicamos aqui uma técnica geral que usa subgrupos normais do grupo de ação para diminuir os cálculos de órbita e estabilizadores, tal como foi feito em [9]. Uma técnica similar foi introduzida por C. R. Leedham-Green para grupos finitos solúveis e explorada por R. Laue, J. Neubüser e U. Schoenwaelder [23]. Aqui estenderemos a ideia para grupos híbridos (grupos não-solúveis com um subgrupo normal solúvel).

Subgrupos normais e blocos

Definição 2.4.9. *Uma ação de* G *sobre um conjunto* Ω *é dita* transitiva *se existe uma única órbita sob tal ação. Isto é, para quaisquer* $x, y \in \Omega$, *existe* $g \in G$ *tal que* $x^g = y$. *Caso contrário, essa ação é chamada* intransitiva.

Seja $n \in \mathbb{N}$ *com* $n > 0$. *A ação é* n-transitiva *se* $|\Omega| \geq n$, *e, pra quaisquer duas listas ordenadas* $[x_1, x_2, \ldots, x_n]$ *e* $[y_1, y_2, \ldots, y_n]$, *de pontos distintos de* Ω, *existe* $g \in G$ *tal que* $x_i^g = y_i$, *para* $1 \leq i \leq n$.

Note que a condição $|\Omega| \geq n$ para a n-transitividade, assegura que as ações n-transitivas são $(n-1)$-transitivas, para $n > 1$. Quando dissermos "G^Ω é transitivo", queremos dizer que a ação de G sobre Ω é transitiva.

Se G age sobre Ω, então um subconjunto não-vazio Δ de Ω é chamado um *bloco* sob a ação de G se tivermos $\Delta \cap \Delta^g = \emptyset$ ou $\Delta = \Delta^g$, para todo $g \in G$. O bloco é dito *não-trivial* se $|\Delta| > 1$ e $\Delta \neq \Omega$. Note que uma órbita δ de um subgrupo normal N de G é um bloco de G em Ω.

Definição 2.4.10. *Uma ação transitiva de G sobre o conjunto Ω é dita ser* primitiva *se não existe blocos não-triviais sob tal ação.*

Se Δ é um bloco sob um ação, então as distintas translações Δ^g de Δ sob G formam uma partição de Ω. O conjunto das translações é conhecido como um *sistema de blocos*. Assim, uma ação transitiva é primitiva se, e somente se, esta não preserva uma partição não-trivial de Ω. Note também que $|\Delta| = |\Delta^g|$, logo, todos os blocos em tal partição possuem o mesmo tamanho. Assim, se G^Ω é transitivo e $|\Omega|$ é primo, então G^Ω é primitivo.

Lema 2.4.11. i) *Toda ação 2-transitiva é primitiva.*

ii) *Sejam G agindo sobre Ω e $N \trianglelefteq G$. Então, as órbitas de N^Ω são blocos sob a ação de G.*

iii) *Se G^Ω é primitivo e N^Ω é não-trivial, então N^Ω é transitivo.*

Demonstração:

i) Sejam G^Ω 2-transitivo e Δ um bloco com $|\Delta| > 1$. Sejam, também, $x, y \in \Delta$ e $x \neq \gamma \in \Omega$. Então, pela 2-transitividade, temos que existe $g \in G$ tal que $x^g = x$ e $y^g = \gamma$. Logo, $x \in \Delta \cap \Delta^g$ e, assim, $\Delta = \Delta^g$ e $\gamma \in \Delta$. Portanto, $\Delta = \Omega$.

ii) Sejam $\Delta = x^N$ uma órbita de N^Ω, $g \in G$ e suponhamos que $x \in \Delta \cap \Delta^g$. Então, $x = y^g$ para algum $y \in \Delta$. Logo, para qualquer $x^h \in \Delta$ com $h \in N$, como N é normal em G, temos que $gh = h'g$, para algum $h' \in N$, e $x^h = y^{gh} = y^{h'g} \in \Delta^g$. Assim, $\Delta = \Delta^g$ e concluímos a demonstração de ii).

iii) O item iii) segue diretamente de ii).

■

Sejam G um grupo agindo sobre um conjunto Ω e $N \trianglelefteq G$. As órbitas de N sobre Ω são blocos da ação de G sobre Ω, pelo Lema 2.4.11.

Sejam $\omega \in \Omega$ e $\delta = \omega^N$ denotando a órbita de ω sob N. Se $G = \langle N, g \rangle$ e $\left|\frac{G}{N}\right| = p$ é um número primo, então temos uma das seguintes situações:

- $G = NStab_G(\omega)$ e $\left|\frac{Stab_G(\omega)}{Stab_N(\omega)}\right| = p$, ou
- $N = NStab_G(\omega)$ e $Stab_G(\omega) = Stab_N(\omega)$.

Podemos decidir qual desses dois casos ocorre testando se $\omega^g \in \delta$. Se $\omega^g \in \delta$, então $\omega^g = \omega^x$, para algum $x \in N$, e $gx^{-1} \in Stab_G(\omega)$, denotamos $\tilde{g} = gx^{-1}$, o levantamento de g do conjunto estabilizador para o ponto estabilizado. Como $\tilde{g} \notin N$, temos que $G = NStab_G(\omega)$ e $Stab_G(\omega) = \langle Stab_N(\omega), \tilde{g}\rangle$. Se $\omega^g \notin \delta$, então $\delta \cap \delta^g = \emptyset$ e $Stab_G(\omega) \leq Stab_G(\delta) = N$. Assim, a órbita de ω sob G é

$$\delta \dot{\cup} \delta^g \dot{\cup} \ldots \dot{\cup} \delta^{g^{p-1}}.$$

Consideremos, agora, N como sendo um subgrupo normal qualquer de G. O grupo G possui uma ação induzida sobre o conjunto de órbitas de N (pois as órbitas de N sob Ω são blocos da ação de G sobre Ω). Temos que N age trivialmente sobre o conjunto de órbitas e a ação induzida de G é uma ação de G/N. Sejam o conjunto estabilizador $Stab_N(\delta)$ na ação induzida de G/N e $Ng \in Stab_{G/N}(\delta)$. Desse modo, é possível mostrar o seguinte lema:

Lema 2.4.12. *Sejam G um grupo agindo sobre um conjunto Ω e $N \trianglelefteq G$. Para $w \in \Omega$ sejam $\delta = w^N$ e $\{\delta_1, \ldots, \delta_s\}$ a órbita de δ sobre a ação induzida de G/N. Então,*

a) $w^G = \delta_1 \cup \ldots \cup \delta_s$.

b) $Stab_G(w)N/N = Stab_{G/N}(\delta)$ *e* $Stab_N(w) = Stab_G(w) \cap N \trianglelefteq Stab_G(w)$.

c) *Se* $Stab_{G/N}(\delta) = \langle Ng_1, \ldots, Ng_t\rangle$, *então* $Stab_G(w) = \langle \tilde{g_1}, \ldots, \tilde{g_t}\rangle Stab_N(w)$.

Observação 2.4.13. *Fazendo essa mesma análise sobre um série de composição $1 = G_n < G_{n-1} < \ldots < G_0 = G$, em que em a cada passo G_{i-1} e G_i fazem o papel de G e N, podemos escrever um algoritmo, no caso em que G é solúvel, para determinar a órbita de ω sob G e o estabilizador em G de ω, tal algoritmo foi descrito em [23].*

Usando o Lema 2.4.12, dividimos o cálculo de w^G e $Stab_G(w)$ em dois cálculos menores de órbita e estabilizador. Primeiro, determinamos w^N e $Stab_N(w)$. Então, calculamos a órbita e o estabilizador de w^N sob a ação de G/N. Esses dois passos permitem determinar w^G e um conjunto de geradores para $Stab_G(w)$.

Se G possui l geradores, então o conjunto de geradores de Schreier para $Stab_G(w)$ possui cardinalidade $|w^G|(l-1)+1$. Em [9], os autores afirmam que se l_1 e l_2 são os números de geradores de G/N e N, respectivamente, então o Lema 2.4.12 fornece um conjunto de geradores para $Stab_G(w)$ de tamanho $(|w^G| \setminus |w^N|)(l_1-1)+|w^N|(l_2-1)+2$

que, em geral, é muito menor. Além disso, esse conjunto de geradores exibe um conjunto de geradores para o subgrupo normal $Stab_N(w)$ que pode ser usado para iterar essa aproximação. Finalmente, a construção de w^G é, em geral, mais eficiente usando a ação sobre conjuntos como descrito no Lema 2.4.12 a).

Grupos Híbridos possuindo subgrupo normal solúvel

Se o grupo de ação G possui um subgrupo normal solúvel S, podemos aplicar a técnica descrita como no Lema 2.4.12. Assumimos que conhecemos uma série de composição para S, então:

$$G \rhd S = S_1 \rhd S_2 \rhd \ldots \rhd S_l \rhd S_{l+1} = 1,$$

tal que $[S_i : S_{i+1}] = p_i$, um primo, para $1 \leq i \leq l$. Seja $s_i \in S_i \setminus S_{i+1}$ e considere a sequência policíclica de geradores $(s_1, \ldots, s_l)$ de S. Como S_i/S_{i+1} tem ordem prima, temos dois casos:

1. S_i/S_{i+1} fixa $w^{S_{i+1}}$ e $Stab_{S_i}(w) = \langle \tilde{s_i} \rangle Stab_{S_{i+1}}(w)$.
2. S_i/S_{i+1} move $w^{S_{i+1}}$ e $Stab_{S_i}(w) = Stab_{S_{i+1}}(w)$.

Assim, podemos calcular a órbita de w sob S sem "visitar" um elemento de w^S duas vezes e, também, obtemos uma sequência policíclica de geradores para $Stab_S(w)$. O passo indutivo de $Stab_S(w)$ para $Stab_G(w)$ é feito como sugere o Lema 2.4.12.

2.5 Aspectos Teóricos

O algoritmo de B. Eick, C. R. Leedham-Green e E. A. O'Brien, descrito em [9], para calcular o grupo de automorfismos de um p-grupo finito procede por indução sobre os termos da série p-central inferior de um p-grupo finito G. Definindo $P_i = G/\mathcal{P}_i(G)$, em que $\mathcal{P}_i(G)$ é o i-ésimo termo da série p-central inferior de G, é calculado, sucessivamente, $Aut(P_i(G))$.

Salvo quando dito o contrário, nesta seção, G denotará um p-grupo finito, d-gerado, de p-classe c e $G = \mathcal{P}_0(G) \geq \mathcal{P}_1(G) \geq \ldots \geq \mathcal{P}_i(G) \geq \ldots$ sua série p-central inferior. A maioria dos teoremas presentes nesta seção estão demonstrados em [32].

Definição 2.5.1. *Um grupo H é um* descendente *de G se H é d-gerado e o quociente $H/\mathcal{P}_c(H)$ é isomorfo a G. Se H é descendente de G e tem p-classe $c+1$, então H é dito* descendente imediato *de G.*

Proposição 2.5.2. *$P_{i+1} = G/\mathcal{P}_{i+1}(G)$ é descendente imediato de $P_i = G/\mathcal{P}_i(G)$, para qualquer inteiro i tal que $1 \leq i \leq c-1$.*

Demonstração: Note primeiro que a p-classe de P_j é $j-1$, já que pela Proposição 1.4.6:

$$\mathcal{P}_j(P_j) = \mathcal{P}_j(G/\mathcal{P}_j(G)) = \mathcal{P}_j(G)/\mathcal{P}_j(G) = \{1\} \text{ e}$$

$$\mathcal{P}_{j-1}(P_j) = \mathcal{P}_{j-1}(G/\mathcal{P}_j(G)) = \mathcal{P}_{j-1}(G)/\mathcal{P}_j(G) \neq \{1\}.$$

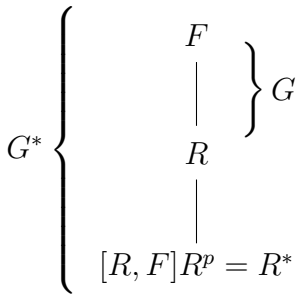
Assim, por definição, precisamos mostrar que ambos são d-gerados e que o quociente $P_{i+1}/\mathcal{P}_i(P_{i+1})$ é isomorfo a $G/\mathcal{P}_i(G)$, uma vez que já sabemos que a p-classe de P_i é $i-1$ e que P_{i+1} possui p-classe igual a i.

De fato, para qualquer inteiro i tal que $1 \leq i \leq$c, $G/\mathcal{P}_j(G)$ é d-gerado pois, por definição, $\mathcal{P}_1(G) = G'G^p$ e, pela Proposição 1.5.6, $\mathcal{P}_1(G) = \Phi(G)$. Temos também que, pela Proposição 1.4.6,

$$\frac{P_{i+1}}{\mathcal{P}_i(P_{i+1})} = \frac{G/\mathcal{P}_{i+1}(G)}{\mathcal{P}_i(G/\mathcal{P}_{i+1}(G))} = \frac{G/\mathcal{P}_{i+1}(G)}{\mathcal{P}_i(G)/\mathcal{P}_{i+1}(G)} \cong G/\mathcal{P}_i(G) = P_i.$$

Portanto, P_{i+1} é descendente imediato de P_i, para $1 \leq i \leq c-1$. ∎

O *p-recobrimento* G^* de um p-grupo $G = F/R$, é a maior extensão elementar abeliana central Frattini de G ($G^* = F/R^*$), isto é, se $\psi\colon G^* \to G$ é o homomorfismo natural da extensão e $M = Ker\,\psi\,(= R/R^*)$, então M é um p-grupo abeliano elementar que é central em G^* tal que $M \leq \Phi(G^*)$ e, além disso, G^* satisfaz as hipóteses do Teorema 2.5.3.



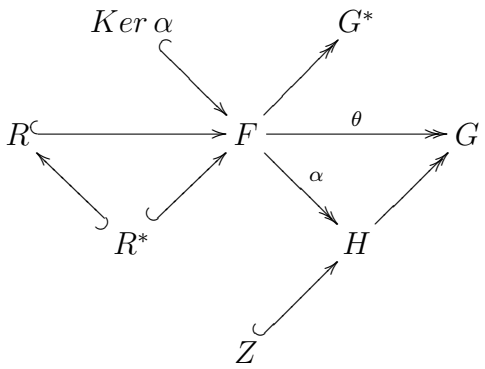
O núcleo M é dito ser o *p-multiplicador* de G. Denominamos, também, $\mathcal{P}_c(G^*) = \dfrac{\mathcal{P}_c(F)R^*}{R^*}$ como sendo o *núcleo* de G.

Na prática, para a construção do p-recobrimento de um grupo, G, usaremos o algoritmo denominado ANU Nilpotent Quotient, um pacote de W. Nickel [30], disponível no GAP [12]. A primeira implementação do algoritmo do quociente nilpotente foi feita por C. C. Sims no software Mathematica ([29]). O ANU Nilpotent Quotient constrói, para um grupo G finitamente apresentado e para um primo p, uma apresentação consistente por potências e comutadores para o maior p-quociente finito de G. Para isso, o algoritmo utiliza a série p-central inferior de G determinando uma apresentação consistente por potências e comutadores para cada $P_i = G/\mathcal{P}_i(G)$. Isso é possível pois P_i é um p-grupo finito, pela Proposição 1.4.5, e se $N \trianglelefteq G$ tal que G/N é p-quociente de G, então o último termo da série p-central inferior de G/N é N, ou seja, existe c' com $N = \mathcal{P}_{c'+1}(G/N) < \mathcal{P}'_c(G/N)$. Assim, pela Proposição 1.4.6, $\mathcal{P}_{c'+1}(G) \leq N$. Logo, $|G/\mathcal{P}_{c'+1}(G)| \leq |G/N|$.

Teorema 2.5.3. *Seja G um p-grupo finito d-gerado. Então, existe um p-grupo G^* d-gerado tal que se H é d-gerado e tem um subgrupo central abeliano elementar Z, tal que $H/Z \cong G$, então H é imagem homomórfica de G^*.*

Demonstração:

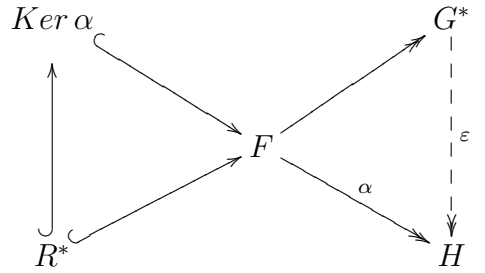
Sejam F o grupo livre de posto d tal que $F = \langle a_1, \ldots, a_d \rangle$ e $R \leq F$ de forma que, se $\theta\colon F \twoheadrightarrow G$ é epimorfismo natural, $F/R \cong G$. Temos que $R^* = R^p[R,F] \leq F^pF'$ e sendo $G^* = F/R^*$, segue que G^* é d-gerado. Além disso, como $R \trianglelefteq F$, temos que $R^* \leq R$.



Sendo H como descrito no teorema, consideremos $\gamma\colon H \twoheadrightarrow G$ e denote $Z := Ker\,\gamma$. Sendo $\alpha\colon F \twoheadrightarrow H$ o epimorfismo natural, α leva R em Z:

$$r \in R = Ker\,\theta \Rightarrow 1 = \theta(r) = \gamma(\alpha(r)) \Rightarrow \alpha(r) \in Ker\,\gamma = Z.$$

Como Z é abeliano elementar, $\alpha(R^p) = (\alpha R)^p = Z^p = 1$. E como Z é subgrupo central de H, então $\alpha([R,F]) = [\alpha R, \alpha F] \leq [Z,H] = \{1_H\}$. Assim, segue que $\alpha(R^*) = \{1_H\}$. Logo, existe uma função injetora de R^* em $Ker\,\alpha$.



Pelo Teorema 2.1.11, segue que existe o epimorfismo $\varepsilon\colon G^* \twoheadrightarrow H$. ∎

Observações 2.5.4. *Segue do Teorema 2.5.3 que:*

i) *todo descendente imediato de G é isomorfo a um quociente de G^*;*

ii) *como a p-classe de G é c, G^* possui p-classe no máximo $c+1$.*

De fato, pela Proposição 1.4.6, e lembrando que não vale, em geral, que $R^* \leq \mathcal{P}_c(F)$, *temos*

$$\mathcal{P}_c(G^*) = \mathcal{P}_c(F/R^*) = \frac{\mathcal{P}_c(F)R^*}{R^*}.$$

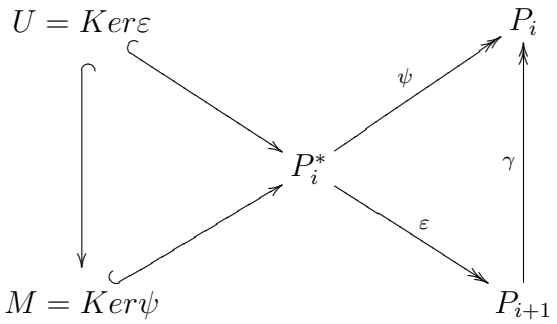
Sendo c *a* p*-classe de* F/R, *pela Proposição 1.4.6,* $\mathcal{P}_c(F) \leq R$, *de modo que* $\mathcal{P}_c(G^*) \leq R/R^*$. *Assim,*

$$\begin{aligned} \mathcal{P}_{c+1}(G^*) = \ (\mathcal{P}_c(G^*))^p[\mathcal{P}_c(G^*), G^*] &\leq (R/R^*)^p[R/R^*, F/R^*] \\ &\leq \frac{R^p[R,F]}{R^*} = 1. \end{aligned}$$

O que significa que a p*-classe de* G^* *é no máximo* $c+1$.

Pela Proposição 2.5.2, $P_{i+1} = G/\mathcal{P}_{i+1}(G)$ é descendente imediato de $P_i = G/\mathcal{P}_i(G)$. Além disso, pelo Teorema 2.5.3, existe o p-recobrimento de $P_i = G/\mathcal{P}_i(G)$, P_i^*, que também é d-gerado. De modo que, pela Observação 2.5.4 i), vale também o seguinte caso particular do Teorema 2.5.3:

Teorema 2.5.5 (Theorem 2.1 de [3])**.** *Sejam* G *um* p*-grupo e* $P_i = G/\mathcal{P}_i(G)$ *com conjunto minimal de geradores dado por* $\{g_1, g_2, \ldots, g_d\}$. *Seja ainda* P_i^* *o* p*-recobrimento de* P_i. *Considere os epimorfismos naturais* $\psi\colon P_i^* \twoheadrightarrow P_i$ *e* $\gamma\colon P_{i+1} \twoheadrightarrow P_i$. *Se* g_j^* *e* $\overline{g_j}$ *são pré-imagens arbitrárias de* ψ *e* γ, *respectivamente, então* $\varepsilon\colon P_i^* \twoheadrightarrow P_{i+1}\colon g_j^* \mapsto \overline{g_j}$ *define um epimorfismo.*



Se G é descrito por uma apresentação consistente por potências e comutadores, então podemos usar o algoritmo descrito em [28] para calcular de modo eficiente uma apresentação por potências e comutadores para G^* e explicitar o homomorfismo $\psi\colon G^* \to G$.

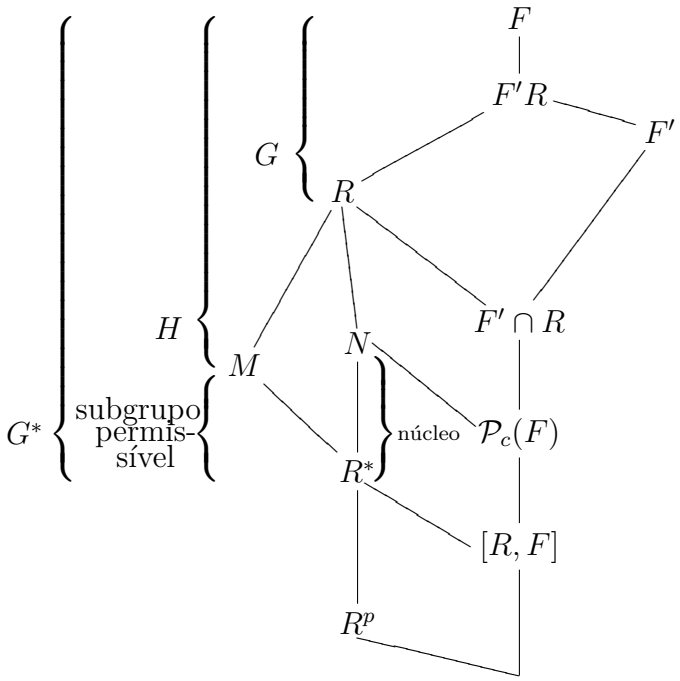
O seguinte lema nos permite concluir que o p-recobrimento de G depende apenas de G e não de sua apresentação. Assim, podemos assumir que $G \cong F/R$ possui uma apresentação por potências e comutadores e, portanto, $R \leq \mathcal{P}_1(F)$.

Lema 2.5.6. *O tipo de isomorfismo de* G^* *depende apenas de* G *e não do subgrupo* $R \leq F$.

Demonstração: Vamos mostrar que dados dois subgrupos $R_1, R_2 \trianglelefteq F$ tais que $F/R_1 = G_1 \cong G_2 = F/R_2$, então os respectivos p-recobrimentos são isomorfos.

Sejam R_1^*, R_2^*, G_1^*, e G_2^* como no Teorema 2.5.3. Se $Z_1 = R_1/R_1^*$, então $G_1^*/Z_1 \cong G_1$, tal que Z_1 é abeliano elementar e central em G_1^*. De modo que, pelo Teorema 2.5.3, G_2^* é imagem homomorfa de G_1^*. Analogamente, G_1^* é imagem homomorfa de G_2^*. ∎

Definição 2.5.7. *Um* subgrupo permissível *é um subgrupo do p-multiplicador que é núcleo de um epimorfismo de G^* sobre um descendente imediato de G.*



Proposição 2.5.8. *M/R^* é permissível se, e somente se, é subgrupo próprio de R/R^* que complementa o núcleo.*

Demonstração: Se $M/R^* \leq R/R^*$ é um subgrupo permissível, então é, por definição, o núcleo de um epimorfismo $\varphi\colon F/R^* \to H$, em que H é um descendente imediato de G. Sendo c a p-classe de G, sabemos que H possui p-classe igual a $c+1$. Isso implica que M é subgrupo próprio de R pois se $M = R$, então $M/R^* = R/R^*$, de modo segue o absurdo:

$$H \cong \frac{G^*}{R/R^*} \cong \frac{F/R^*}{R/R^*} \cong F/R \cong G.$$

Como $R \trianglelefteq F$ e F/R possuem p-classe c, pela Proposição 1.4.6, vale que $\mathcal{P}_c(F) \leq R$ e, portanto, $M\mathcal{P}_c(F) \leq R$.

Pelo Teorema 2.5.3, se $\alpha\colon F \twoheadrightarrow H$ é o epimorfismo natural, $\alpha(R) \leq \mathcal{P}_c(H)$ e, pela Proposição 1.4.6, segue que

$$\mathcal{P}_c(H) = \mathcal{P}_c(\alpha(F)) = \alpha(\mathcal{P}_c(F)) \leq \alpha(R).$$

Logo, $\alpha(R) = \mathcal{P}_c(H)$.

Como φ e α são epimorfismos,

$$\alpha(F) = H \cong \frac{F/R^*}{M/R^*} \cong F/M.$$

Assim,

$$\alpha(R) = R/M$$

e, portanto,

$$\mathcal{P}_c(H) = \mathcal{P}_c(\alpha(F)) = \alpha(\mathcal{P}_c(F)) = \frac{\mathcal{P}_c(F)M}{M}.$$

Desse modo, $R/M = \dfrac{\mathcal{P}_c(F)M}{M}$ e $R = \mathcal{P}_c(F)M$. Então, $\dfrac{\mathcal{P}_c(F)R^*}{R^*}\dfrac{M}{R^*} = \dfrac{R}{R^*}$. Uma vez que $\dfrac{F/R^*}{M/R^*} = \mathcal{P}_c(F/R^*)$, temos que $\mathcal{P}_c(G^*)\dfrac{M}{R^*} = R/R^*$, ou seja, M/R^* complementa o núcleo de G.

Por outro lado, se $M/R^* < R/R^*$ tal que $\mathcal{P}_c(G^*)\dfrac{M}{R^*} = R/R^*$, então $\dfrac{\mathcal{P}_c(F)R^*M}{R^*} = \dfrac{R}{R^*}$. Logo, $R/M = \dfrac{\mathcal{P}_c(F)M}{M}$ e, pela Proposição 1.4.6, $\mathcal{P}_c(F/M) = \dfrac{\mathcal{P}_c(F)M}{M} = R/M$.

Seja $H = F/M$. Sabemos que H é d-gerado, já que (por um comentário sobre o Lema 2.5.6) $M < R \leq \mathcal{P}_1(F)$. Além disso, H é um quociente de F/R^* e

$$\frac{H}{\mathcal{P}_c(H)} = \frac{F/M}{\mathcal{P}_c(F/M)} = \frac{F/M}{R/M} \cong F/R \cong G.$$

Assim, H é descendente de G.

Como $\mathcal{P}_c(F/M) = R/M \neq \{1\}$ (já que $M < R$) e

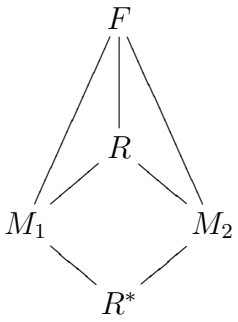
$$\mathcal{P}_{c+1}(F/M) = \left(\frac{R}{M}\right)^p \left[\frac{R}{M}, \frac{F}{M}\right] = \frac{R^p[R,F]M}{M} = \frac{R^*M}{M} = \{1\},$$

temos que a p-classe de F/M é $c+1$.

Logo, H é um descendente imediato de G e M/R^* é um subgrupo permissível. ∎

Teorema 2.5.9. *Sejam dois subgrupos permissíveis de F/R^*, $M_1/R^* \leq R/R^*$ e $M_2/R^* \leq R/R^*$, e um isomorfismo $\varphi\colon F/M_1 \to F/M_2$. Então, existe $\alpha^* \in Aut(G^*)$ tal que*

- *$\alpha^*(M_1/R^*) = M_2/R^*$ e*
- *$\overline{\alpha}\colon F/M_1 \to F/M_2$, a aplicação induzida por α^*, coincide com φ.*



Demonstração: Pela Proposição 2.5.8, M_1/R^* complementa o núcleo e, assim,

$$\frac{\mathcal{P}_c(F)M_1}{M_1} = R/M_1 = \mathcal{P}_c(F/M_1),$$

pela Proposição 1.4.6. O mesmo vale para M_2/R^*. Isso implica que:

$$\varphi(R/M_1) = \varphi[\mathcal{P}_c(F/M_1)] = \mathcal{P}_c[\varphi(F/M_1)] = \mathcal{P}_c(F/M_2) = R/M_2.$$

Como φ é isomorfismo de F/M_1 em F/M_2 tal que $\varphi(R/M_1) = R/M_2$, φ induz um automorfismo α de F/R.

Escolhemos um representante $u_i \in F$ da classe lateral $\alpha(a_iR)$, logo, $\alpha(a_iR) = u_iR$ e definimos α^* como $\alpha^*(\omega(a_1,\ldots,a_d)R^*) = \omega(u_1,\ldots,u_d)R^*$. Temos que α^* está bem definido, pois $\alpha(R) = R$ e $R^* = R^p[R,F]$, uma vez que $\alpha(\omega(a_1,\ldots,a_d)R) = \omega(u_1,\ldots,u_d)R$. O que implica que se $\omega(a_1,\ldots,a_d) \in R$, então $\omega(u_1,\ldots,u_d) \in R$. Logo, podemos concluir que se $\omega(a_1,\ldots,a_d) \in R^*$, então $\omega(u_1,\ldots,u_d) \in R^*$.

Temos que α^* é homomorfismo, e para mostrar que é automorfismo de F/R^* basta então mostrar que é sobrejetor. De fato, sabemos que $\alpha \in Aut(F/R)$ e $\alpha(a_iR) = u_iR$. Logo, $F/R = \langle u_1R,\ldots,u_dR\rangle$ e $F/R^* = \langle u_1R^*,\ldots,u_dR^*, R/R^*\rangle$.

Suponhamos que temos uma apresentação por potências e comutadores de F/R, logo, $R \leq P_1(F)$ e $R/R^* \leq P_1(F/R^*)$. Assim,

$$F/R^* = \langle u_1R^*,\ldots,u_dR^*\rangle = \langle \alpha^*(a_1R^*),\ldots,\alpha^*(a_dR^*)\rangle.$$

Temos que α^* não é univocamente determinado por α, mas α^* restito a R/R^* o é pois, supondo que

$$\alpha(a_iR) = u_iR = u_ir_iR = v_iR; \text{ em que } r_i \neq 1, r_i \in R,$$

temos que α_1^* e α_2^* são dois automorfismos de F/R^* dados por:

$$\alpha_1^*\colon \omega(a_1,\ldots,a_d)R^* \mapsto \omega(u_1,\ldots,u_d)R^*$$
$$\alpha_2^*\colon \omega(a_1,\ldots,a_d)R^* \mapsto \omega(v_1,\ldots,v_d)R^*.$$

Para $i = 1,2$, temos $\alpha_i^*(R/R^*) = R/R^*$. Assim, se $\omega(a_1,\ldots,a_d) \in R$, então $u \in R$ e $v \in R$. Mas, como as palavras em R são produtos de potências p-ésimas com comutadores, e já que

$$[v_j,v_i]R^* = [u_j,u_i]R^* \text{ e } v_i^pR^* = u_i^pR^*,$$

segue que $\omega(u_1,\ldots,u_d)R^* = \omega(v_1,\ldots,v_d)R^*$.

Portanto, α^* restito a R/R^* é univocamente determinado por α.

Denotemos essa restrição por $\overline{\alpha^*}$. Se $\omega(a_1,\ldots,a_d) \in M_1$ e $\varphi(a_iM_1) = b_iM_2$, então $\overline{\alpha^*}(\omega(a_1,\ldots,a_d)R^*) = \omega(b_1,\ldots,b_d)R^*$.

Como $\omega(b_1,\ldots,b_d) \in M_2$, pois:

$$\begin{aligned}\omega(b_1,\ldots,b_d)M_2 &= \omega(b_1M_2,\ldots,b_dM_2) = \omega(\varphi(a_1M_1),\ldots,\varphi(a_dM_1))\\ &= \omega(a_1,\ldots,a_d)\varphi(M_1) = \varphi(M_1) = M_2.\end{aligned}$$

segue que $\overline{\alpha^*}(M_1/R^*) \leq M_2/R^*$.

Agora, já que $F/M_1 \cong F/M_2$, então $\overline{\alpha^*}(M_1/R^*)$ e M_2/R^* possuem o mesmo índice em F/R^* e são isomorfos, ou seja, como $\overline{\alpha^*}(M_1/R^*) \leq M_2/R^*$, temos que $\overline{\alpha^*}(M_1/R^*) = M_2/R^*$.

Portanto, α^* induz um isomorfismo $\overline{\alpha}$ de F/M_1 em F/M_2 com $\overline{\alpha}(a_iM_1) = \varphi(a_iM_1)$, para qualquer i tal que $1 \leq i \leq d$. ∎

Definição 2.5.10. *O automorfismo α^*, tal como descrito no teorema acima, é chamado de* automorfismo estendido.

Lema 2.5.11. *Se $\alpha \in Aut(F/R)$, então α pode ser estendido a um automorfismo $\alpha^* \in Aut(F/R^*)$. Além disso, a restrição de α^* ao p-multiplicador é univocamente determinada por α.*

Demonstração: Segue diretamente do Teorema 2.5.9, escolhendo $M_1 = M_2 = R$. ∎

Em particular, do Teorema 2.5.9 e do Lema 2.5.11, temos o seguinte resultado:

Teorema 2.5.12 (Theorem 2.2 de [3])**.** *Cada automorfismo α de P_i se estende a um automorfismo α^* de P_i^* via um homomorfismo natural $P_i^* \to P_i$. Além disso, α^* deixa M, o p-multiplicador de P_i, invariante e α induz um automorfismo α_M de M, que depende apenas de α.*

Lema 2.5.13. *As extensões de automorfismos internos de G agem trivialmente sobre o p-multiplicador.*

Demonstração: Seja α dado como na última demonstração, em que sendo $a_1,\ldots,a_d$ geradores de F, temos que $\alpha(a_iR) = u_iR$. Então, pela definição de automorfismo estendido, segue que $\alpha^*(a_iR^*) = u_iR^*$, para $1 \leq i \leq d$, e dado a palavra $\omega(a_1,\ldots,a_d)$ segue que $\alpha^*(\omega(a_1,\ldots,a_d)R^*) = \omega(u_1,\ldots,u_d)R^*$.

Supondo que $\alpha \in Inn(G)$, seja a conjugação por um elemento $g \in G$, se $r \in R$, temos que $\alpha^*(rR^*) = r^gR^* = r[r,g]R^*$. Mas então, $\alpha^*(rR^*) = rR^*$, já que $[r,g] \in [R,F]R^p$. O que significa que a ação de α^* é trivial no p-multiplicador. ∎

Definição 2.5.14. *Se M/R^* é um subgrupo permissível, definimos o estabilizador de M/R^* por:*

$$Stab_{Aut(F/R)}(M/R^*) = \langle \alpha \in Aut(F/R) \,|\, \alpha^*(M/R^*) = M/R^* \rangle.$$

Se α^* é uma extensão de um automorfismo α, então α^* fixa M/R^* e a restrição de α^* a F/M pode ser calculada. O grupo de automorfismos de F/M pode ser calculado com o seguinte teorema:

Teorema 2.5.15 (Theorem 2.3 de [3])**.** *Seja ν: $Aut(P_{i+1}) \to Aut(P_i)$ o homomorfismo natural no qual $T = Ker(\nu)$ e $S = im(\nu)$. Então, $Aut(P_{i+1}) = TR$, em que R é uma pré-imagem qualquer de S sob ν.*

Demonstração: Seja F um corpo livre finitamente gerado por $a_1, \ldots, a_d$. Sejam $P_i = F/\mathcal{R}$; $P_{i+1} = F/N$; para algum $N \leq F$, e $P_i^* = F/\mathcal{R}^*$ o p-recobrimento de P_i. Se $\gamma \in Aut(P_{i+1})$, pelo Teorema 2.5.9, sabemos que γ induz um automorfismo $\alpha \in Aut(P_i)$ que se estende a outro automorfismo $\alpha^* \in Aut(F/\mathcal{R}^*)$ tal que $\alpha^*(N/\mathcal{R}^*) = N/\mathcal{R}^*$ *e* $\overline{\alpha}$: $F/N \to F/N$ induzido por α^* coincide com γ. Logo, $\alpha \in Stab_{Aut(P_i)}(N/R^*)$ e $\overline{\alpha} \in R$.

Consideremos que, para uma escolha apropriada de representantes, $\alpha^*(a_iR^*) = u_ir_iR^*$, em que $r_i \in R$ e $1 \leq i \leq d$. Então, $\overline{\alpha}$ é definido por:

$$\overline{\alpha}(a_iN) = u_ir_iN.$$

Temos que $\{u_1, \ldots, u_d\}$ é um conjunto de geradores de $P_{i+1} = F/N$. Definimos o automorfismo $\theta \in Aut(F/N)$ por

$$\theta(u_iN) = u_ir_iN.$$

A restrição de θ a P_i é o automorfismo identidade. Assim, $\theta \in T$ e $\overline{\alpha} = \theta\gamma$. O que mostra o resultado. ∎

Sejam G um grupo, $N \trianglelefteq G$ um subgrupo característico de G e $H \leq Aut(G)$. Consideremos a extensão $\widetilde{G} = G \cdot H$. Então, olhando N e H como subgrupos de $\widetilde{G}$ temos $[N, H] \leq N$, o que implica que H age em G/N. Sejam ainda, $\overline{G} = G/N$ e $\widehat{G} = G/N \cdot H$ uma extensão de $\overline{G}$.

Dizemos que H *centraliza* G/N se $[G/N, H] = 1$ (olhando G/N e H como subgrupos de $\widehat{G}$), ou seja,

$$H \text{ centraliza } G/N \;\Leftrightarrow\; [G, H] \leq N.$$

Lema 2.5.16 (Lemma 2.4 de [3]). *Sejam G um p-grupo com $\mathcal{P}_{c+1}(G) = 1$ e $c \geq 2$. Sejam ainda, $\{g_1, g_2, \ldots, g_d\}$ e $\{x_1, x_2, \ldots, x_l\}$, conjuntos minimais de geradores de G e $\mathcal{P}_c(G)$, respectivamente. Definimos:*

$$\begin{array}{rccll} \beta_{i,j}\colon & G & \longrightarrow & G & \\ & g_i & \mapsto & g_i x_j & \\ & g_k & \mapsto & g_k; & \text{se } k \neq i. \end{array}$$

Então, $\{\beta_{i,j} \,|\, 1 \leq i \leq d,\, 1 \leq j \leq l\}$ é uma sequência policíclica de geradores para o p-grupo abeliano elementar de automorfismos de G que centraliza $G/\mathcal{P}_c(G)$.

Demonstração: Seja $\nu\colon Aut(G) \to Aut(G/\mathcal{P}_c(G))$. Note primeiro que $\mathcal{P}_c(G) \subseteq \Phi(G)$ e que em uma apresentação por potências e comutadores, os geradores de $\mathcal{P}_c(G)$ são produtos de potências e comutadores dos geradores de G e que $\beta_{i,j}(g_i^p) = \beta_{i,j}(g_i)^p = (g_i x_j)^p = g_i^p x_j^p = g_i^p$, uma vez que $\mathcal{P}_{c+1-1}(G) \leq Z_1(G) = Z(G)$ e $\mathcal{P}_c(G)$ é abeliano elementar tal que $exp(\mathcal{P}_c(G)) = p$.

Temos:

$$\begin{array}{lcll} \beta_{i,j}(g_n^p) & = & g_n^p; \quad \forall n \neq i & \\ \beta_{i,j}([g_m, g_k]) & = & [\beta_{i,j}(g_m), \beta_{i,j}([g_k])] & = [g_m, g_k];\ \text{se } m, k \neq i \\ \beta_{i,j}([g_i, g_k]) & = & [\beta_{i,j}(g_i), \beta_{i,j}([g_k])] & = [g_i x_j, g_k] = [g_i, g_k]; \end{array}$$

pois $\mathcal{P}_c(G) \leq Z(G)$ e, portanto, $\beta_{i,j}(x_j) = x_j$.

Como o automorfismo $\beta_{i,j}$ pertence ao núcleo $Ker\,\nu$; para quaisquer i e j tais que $1 \leq i \leq d$ e $1 \leq j \leq l$ e sendo $\gamma \in Ker\,\nu$, então $\gamma \in \langle \beta_{i,j} | 1 \leq i \leq d,\, 1 \leq j \leq l \rangle$. De fato, $\gamma(g_i) = g_i u_i$; para algum $u_i \in \mathcal{P}_c(G)$. Seja $u_i \in \mathcal{P}_c(G)$. Então, $u_i = x_{m_1}^{r_1} \ldots x_{m_n}^{r_n}$, em que $x_{m_1}, \ldots, x_{m_n} \in \{x_1, \ldots, x_l\}$.

Logo, $\gamma(g_i) = g_i u_i = g_i x_{m_1}^{r_1} \ldots x_{m_n}^{r_n} = \beta_{i,m_1}(g_i)^{m_1} . x_{m_2}^{r_2} \ldots x_{m_n}^{r_n}$, de modo que obtemos $\gamma(g_i) = \beta_{i,m_n}(\ldots(\beta_{i,m_1}(g_i)^{m_1}))^{r_n}$, o que implica que $\gamma(g_i) = \prod_{s=1}^{n} \beta_{i,m_s}^{r_s}(g_i)$ e, assim, $\gamma = \prod_{i=1}^{d} \beta_{i,m_1}^{r_1} \ldots \beta_{i,m_n}^{r_n}(g_i)$.

Para mostrar que $T = \langle \beta_{i,j} \,|\, 1 \leq i \leq d,\, 1 \leq j \leq l \rangle$ centraliza $G/\mathcal{P}_c(G)$, precisamos mostrar que $[G, T] \leq \mathcal{P}_c(G)$, isto é, que $[g_m, \beta_{i,j}] \in \mathcal{P}_c(G)$; para todo $1 \leq m \leq d$ e qualquer $\beta_{i,j} \in T$.

Temos que $[g_m, \beta_{i,j}] = g_m^{-1} g_m^{\beta_{i,j}}$. Então,

$$[g_m, \beta_{i,j}] = g_m^{-1} g_m x_j = x_j \in \mathcal{P}_c(G) \text{ se } m = i \text{ e}$$

$$[g_m, \beta_{i,j}] = g_m^{-1} g_m = 1;\ \text{se } m \neq i.$$

Falta apenas mostrar que T é abeliano elementar, de fato:

$$\begin{array}{lll} \beta_{i,j}^{p}(g_i) & = \beta_{i,j}^{p-1}(g_i x_j) & = \ldots = \beta_{i,j}(g_i x_j^{p-1}) = g_i x_j^p = g_i \text{ e} \\ \beta_{i,j}\beta_{i,j'}(g_i) & = \beta_{i,j}(g_i x_{j'}) & = \beta_{i,j}(g_i)\beta_{i,j}(x_{j'}) = g_i x_j x_{j'} = g_i x_{j'} x_j = \beta_{i,j'}\beta_{i,j}(g_i). \end{array}$$

■

Exemplo 2.5.17. *Consideremos o grupo diedral* $D_8 = \langle a, b \,|\, a^8 = b^2 = 1, a^b = a^{-1}\rangle$. *Temos que* $[a,b] = a^{-1}a^b = a^{-2}$ *e* $[a^2, b] = a^{-2}(a^2)^b = a^{-4}$. *Logo, os termos da série 2-central inferior são:* $\mathcal{P}_1(D_8) = D_8^2[D_8, D_8] = \langle a^2\rangle$ *e* $\mathcal{P}_2(D_8) = \mathcal{P}_1(D_8)^2[\mathcal{P}_1(D_8), D_8] = \langle a^2\rangle^2[\langle a^2\rangle, D_8] = \langle a^4\rangle$.

Assim, segue que:

- $P_1 = \dfrac{D_8}{\mathcal{P}_1(D_8)} = \dfrac{D_8}{\langle a^2\rangle}$;
- $P_2 = \dfrac{D_8}{\mathcal{P}_2(D_8)} = \dfrac{D_8}{\langle a^4\rangle} \cong D_4$;
- $P_3 = \dfrac{D_8}{\mathcal{P}_3(D_8)} = \dfrac{D_8}{1} = D_8$.

$$\begin{array}{l} D_8 \\ | \\ \langle a^2\rangle = \mathcal{P}_1(D_8) \\ | \\ \langle a^4\rangle = \mathcal{P}_2(D_8) \\ | \\ 1 = \mathcal{P}_3(D_8) \end{array}$$

Portanto, sabendo que $Aut(P_1) \cong GL(2,2) \cong S_3$ *e que* $Aut(P_2) \cong Aut(D_4) \cong D_4$ *podemos verificar a validade do Teorema 2.5.15 para determinar* $Aut(P_2)$.

Seja $\nu_1 \colon Aut(P_2) \to Aut(P_1)$ *o homomorfismo natural e defina* $\sigma \in Aut(P_2)$ *tal que* $\sigma(a) = a^3$ *e* $\varphi_i \in Aut(P_2)$ *tal que* $\varphi_i(b) = a^i b$, *para* $i \in \{0,1,2,3\}$. *Dessa forma, temos que* $\nu_1(\sigma) = \overline{\sigma} \in Aut(P_1)$ *é tal que* $\overline{\sigma}(a) = \overline{a^3} = \overline{a}$ *e* $\nu_1(\varphi_i) = \overline{\varphi}_i \in Aut(P_1)$ *tal que* $\overline{\varphi}_{2k}(b) = \overline{a^{2k}b} = \overline{b}$, *para* $k \in \{0,1\}$ *e* $\overline{\varphi}_l(b) = \overline{a^l b} = \overline{ab}$, *para* $l \in \{1,3\}$.

Temos que $\nu_1(\varphi_1)^2 = (\overline{\varphi}_1)^2$ *é o automorfismo identidade e* $\overline{\varphi}_1$ *gera* $\nu_1(Aut(P_2))$. *Ou seja,* $\langle\varphi_1\rangle = Im(\nu_1) = S$ *com* $R = \langle\varphi_1\rangle$.

Além disso, sendo os automorfismos internos de P_2*:*

$$\begin{array}{rl} \gamma_a \colon & a \mapsto a \\ & b \mapsto a^{-1}ba = ba^2 = a^2b \\ \gamma_b \colon & a \mapsto b^{-1}ab = a^{-1} \\ & b \mapsto b \\ \gamma_a \circ \gamma_b \colon & a \mapsto a^{-1} \\ & b \mapsto a^2b \end{array}$$

temos que $Inn(P_2) = \{id, \gamma_a, \gamma_b, \gamma_a \circ \gamma_b\} = \langle\gamma_a, \gamma_b\rangle$.

Como $Inn(P_2) = Ker(\nu_1) = T$, *obtemos que* $Aut(P_2) = TR = \langle\gamma_a, \gamma_b\rangle \cdot \langle\varphi_1\rangle$.

Seja agora, $\nu_2 \colon Aut(P_3) \to Aut(P_2)$ *o homomorfismo natural. De maneira seme-*

lhante, $Aut(P_3)$ *é gerado pelos automorfismos* $\tilde{\sigma}_j$ *tais que* $\tilde{\sigma}_j(a) = a^j$ *e* $\tilde{\varphi}_i$ *tal que* $\tilde{\varphi}_i(b) = a^i b$*, para* $j \in \{1, 3, 5, 7\}$ *e* $0 \leq i \leq 7$ *e, dessa maneira,* $\nu_2(Aut(P_3)) = Aut(P_2)$*, que é gerado pelos automorfismos* σ *e* φ_i *descritos anteriormente. Assim, podemos tomar* $R = \langle \tilde{\sigma}_3, \tilde{\varphi}_i \,|\, 0 \leq i \leq 3 \rangle$.

Além disso, de modo análogo, $T = Ker(\nu_2) = \langle \tilde{\sigma}_5, \tilde{\varphi}_4 \rangle$*. Ou então, pelo Lema 2.5.16, como* D_8 *possui classe de nilpotência igual a* 3*, sendo* a *e* b *os geradores de* D_8 *e* a^4 *o gerador de* $\mathcal{P}_2(D_8)$ *obtemos* $\beta_{11} \equiv \tilde{\sigma}_5$ *e* $\beta_{21} \equiv \tilde{\varphi}_4$ *como sendo os geradores de* T*. É possível ver que* $Aut(P_3) = Aut(D_8) = T.R = \langle \tilde{\sigma}_5, \tilde{\varphi}_4 \rangle \langle \tilde{\sigma}_3, \tilde{\varphi}_i \,|\, 0 \leq i \leq 3 \rangle$*. O que mostra que o Teorema 2.5.15 vale para* D_8.

Capítulo 3

E-grupos

O objetivo deste capítulo é fazer um estudo sobre E-grupos. Introduziremos, inicialmente, o conceito de E-grupo, descrevendo algumas de suas propriedades e resultados. Em seguida, classificaremos os $p\mathcal{E}$-grupos 3-gerados. As demonstrações de todos os resultados do capítulo podem ser encontradas em [1], [2] e [26].

3.1 Alguns Conceitos

Definição 3.1.1. *Um grupo G é dito ser* E-grupo *(respectivamente,* A-grupo*), se $x^{\varphi}x = xx^{\varphi}$, para todo $x \in G$ e para qualquer endomorfismo (respectivamente, automorfismo), φ de G.*

Logo, todo E-grupo é um A-grupo. Podemos ver que os grupos abelianos são exemplos de A-grupos. Sendo ϕ o automorfismo interno induzido por um elemento $g \in G$, $\phi = \gamma_g$, então $[x^g, x] = 1$, ou seja, $[g, x, x] = 1$, para todo elemento $x \in G$. Dessa maneira, segue que todo E-grupo e A-grupo, é um grupo 2-Engel e, pelo Teorema de Levi (1.7.3), tal grupo é nilpotente de classe no máximo 3.

Todos os grupos abelianos são exemplos de E-grupos e existem grupos de classe de nilpotência 2 (portanto, não-abelianos) que são E-grupos. O primeiro 2E-grupo não-abeliano foi construído por R. Faudree [10], que definimos a seguir. Todos os A-grupos e E-grupos conhecidos, até aquele momento, classe de nilpotência no máximo 2.

Seja G um grupo com a seguinte apresentação:

$$\begin{aligned} G = \langle a_1, a_2, a_3, a_4 \mid \ & a_i^{p^2} = 1, [a_i, a_j, a_k] = 1, i, j, k \in \{1, 2, 3, 4\}, \\ & [a_1, a_2] = a_1^p, [a_1, a_3] = a_3^p, [a_1, a_4] = a_4^p, \\ & [a_2, a_3] = a_2^p, [a_2, a_4] = 1, [a_3, a_4] = a_3^p \rangle, \end{aligned}$$

em que p é um primo ímpar.

Note que o exemplo é falso se $p = 2$, isso porque se $p = 2$, a aplicação α definida

por

$$a_1^\alpha = a_1^{-1}a_2a_4,\ a_2^\alpha = a_3,\ a_3^\alpha = a_4,\ a_4^\alpha = a_1a_4$$

pode ser estendida a um endomorfismo de G, mas $[a_3^\alpha, a_3] = [a_4, a_3] \neq 1$, então G não é E-grupo.

Definição 3.1.2. *Se G é um p-grupo e é E-grupo (respectivamente, A-grupo), então G é pE-grupo (respectivamente, pA-grupo).*

Uma condição necessária para um p-grupo finito ser um E-grupo foi dada em 1969 por B. H. Neumann e M. Suzuki e citada por J. J. Malone em [26], tal condição está enunciada a seguir. Todos os resultados que seguem, até o fim desta subseção, estão em [26].

Teorema 3.1.3 (Theorem 1 de [26] ou Theorem 1.1 de [3])**.** *Seja G um pE-grupo finito. Se seu quociente derivado G/G' tem expoente p^r, então todos os elementos de G que possuem ordem dividindo p^r são centrais, ou seja, $\Omega_r(G) \leq Z(G)$.*

Demonstração: Sejam $g \in \Omega_r(G)$ e $H = \{h \in G : o(hG') = p^r \text{ em } G/G'\}$. Pelo Teorema Fundamental dos Grupos Abelianos, todo grupo finito abeliano pode ser escrito como produto de fatores cíclicos. Assim, se $h \in H$, temos que $\langle hG'\rangle$ é fator direto de G/G'.

Tome $x \in G$ de ordem p^r. Existem homomorfismos $\alpha\colon G \to \langle x\rangle$ tal que $\alpha(h) = x$ e $\beta\colon \langle x\rangle \to \langle g\rangle$ com $\beta(x) = g$. De forma que, $\gamma := \beta \circ \alpha$; $\gamma\colon G \to G$ com $\gamma(h) = g$ é um endomorfismo, e por hipótese, como G é pE-grupo, $[h, g] = 1$. Logo, já que h é qualquer, $\Omega_r(G) \leq Z(\langle H\rangle)$. Assim, basta mostrar que $G = \langle H\rangle$, ou seja, que dado $a \in G$ qualquer, a pode ser escrito como uma palavra em H. De fato, seja $a \in G$ tal que $a \notin \langle h\rangle$, então $hG'.aG' = h_1G'$, para algum $h_1 \in H$ (pela Fórmula da coleta de Hall 1.6.3). Assim, $a = h^{-1}h_1g'$, para algum $g' \in G'$. Portanto, temos que G é gerado por H e G'.

Como G é nilpotente, temos que $G' \leq \Phi(G)$, pela Proposição 1.5.6, e que $\Phi(G)$ é o conjunto dos não geradores de G, pela Proposição 1.5.4. Logo, H é um conjunto de geradores de G, isto é, $G = \langle H\rangle$. O que completa a demonstração. ∎

Corolário 3.1.4 (Corollary 1.1 de [26])**.** *Seja G um p-grupo finito. Se um elemento de maior ordem em G mantém sua ordem em G/G' (isto é, se $o(g) = n$ então $o(gG') = n$, para $g \in G$) então G não é E-grupo não-abeliano.*

Demonstração: Sejam G um pE-grupo finito e $x \in G$, um elemento de maior ordem em G, que mantém sua ordem em G/G'. Então, $x^{p^r} \in G'$ e como $o(x) \geq o(y)$, para todo $y \in G$, segue que $y^{p^r} \in G'$. Pelo Teorema 3.1.3, concluímos que G é abeliano. ∎

Exemplo 3.1.5. *Considere o maior grupo G gerado por a_1 e a_2 tais que satisfaçam as relações: $a_1^3 = a_2^3 = 1$ e $[a_j, a_j, a_k] = 1$; $i, j, k \in \{1, 2\}$.*

Observe que G não é abeliano, logo $G' = \langle [a_1, a_2] \rangle \neq \{1\}$. Além disso, $a_1 G' \in G/G'$ possui ordem igual a 3, assim como $o(a_1) = 3$ em G. Portanto, pelo Corolário 3.1.4, G não é E-grupo.

De fato, considere φ uma aplicação em G tal que $\varphi(a_1) = a_2$ e $\varphi(a_2) = a_1$. Temos que φ se estende a um endomorfismo, mas $[a_1, \varphi(a_1)] = [a_1, a_2] \neq 1$.

Teorema 3.1.6 (Theorem 6 de [26])**.** *Em um grupo $(G, +)$ um elemento $g \in G$ comuta com sua imagem endomorfa se, e somente se, duas imagens endomorfas de g comutam.*

Demonstração: A demonstração será feita como em [26]. Suponhamos que $g \in G$ comuta com sua imagem endomorfa e sejam α e β endomorfismos de G e id a aplicação identidade de G. Então,

$$\begin{aligned}
\alpha + \beta &= \alpha + \beta + \alpha\beta + id - id - \alpha\beta \\
&= (id + \alpha) + (id + \alpha)\beta - id - \alpha\beta \\
&= (id + \alpha)(id + \beta) - id - \alpha\beta \\
&= (id + \alpha)(\beta + id) - id - \alpha\beta \\
&= (id + \alpha)\beta + (id + \alpha)id - id - \alpha\beta \\
&= \beta + \alpha\beta + id + \alpha - id - \alpha\beta \\
&= \beta + \alpha(\beta + id) - \alpha\beta \\
&= \beta + \alpha(id + \beta) - \alpha\beta \\
&= \beta + \alpha + \alpha\beta - \alpha\beta \\
&= \beta + \alpha.
\end{aligned}$$

A recíproca é direta já que id é um endomorfismo de G. ∎

Teorema 3.1.7 (Theorem 4 de [26])**.** *A imagem endomorfa de um E-grupo é um E-grupo.*

Demonstração: A demonstração será feita como em [26]. Sejam G um E-grupo, H a imagem de G sob um endomorfismo γ e α um endomorfismo de H. Então, $\alpha\gamma$ é um endomorfismo de G com imagem $\alpha(H)$. Sejam β um endomorfismo de H e $h \in H$. Escolhemos $g \in G$ tal que $\gamma(g) = h$. Então,

$$\alpha\gamma(g).\beta\gamma(g) = \beta\gamma(g).\alpha\gamma(g),$$

em que a comutatividade segue do Teorema 3.1.6, e implica que

$$\alpha(h)\beta(h) = \beta(h)\alpha(h).$$

Assim, quaisquer duas imagens endomorfas comutam e o grupo H é um E-grupo. ■

Corolário 3.1.8 (Corollary 4.1 de [26]). *Se G é um E-grupo finito que não possui E-grupo não-abeliano como subgrupo próprio, então toda imagem endomorfa própria de G é abeliana, ou seja, G' é subgrupo do núcleo de cada endomorfismo estrito de G.*

Demonstração: Se a imagem endomorfa própria de G é não-abeliana, então, pelo Teorema 3.1.7, deve ser um E-grupo. ■

3.2 Alguns resultados sobre E-grupos

O objetivo desta seção é mostrar que todo E-grupo finito 3-gerado é nilpotente de classe no máximo 2, Teorema 3.2.14, que se G é um 3E-grupo com $|G| \leq 3^{10}$, então G é nilpotente de classe no máximo 2, Teorema 3.2.15, que todo grupo 2-gerado é abeliano se, e somente se, é um E-grupo, e ainda que todo grupo infinito 3-gerado é abeliano se, e somente se, é um E-grupo, Teorema 3.2.16. Todos os resultados presentes nesta seção estão demonstrados em [2].

Como um E-grupo finito pode ser escrito como produto direto de seus subgrupos de Sylow e, pelo Teorema 3.1.7, qualquer fator direto de um E-grupo é um E-grupo, basta considerarmos os pE-grupos.

Denotaremos $d(G)$ o número mínimo de geradores de um grupo G.

Definição 3.2.1. *Dizemos que G é um $p\mathcal{E}$-*grupo *se G é um grupo 2-Engel finito e existe $r > 0$ tal que $exp(G/G') = p^r$ e $\Omega_r(G) \leq Z(G)$.*

Observação 3.2.2. *Conforme já foi mencionado, temos que os pE-grupos são 2-Engel, assim como os $p\mathcal{E}$-grupos (por definição). Logo, se $p > 2$, os pE-grupos e os $p\mathcal{E}$-grupos são regulares, pela Proposição 1.7.4.*

Observação 3.2.3. *Se G é pE-grupo finito, então G é $p\mathcal{E}$-grupo, pelo Teorema 3.1.3. A recíproca não é verdade em geral. Mostramos isso a seguir conforme foi feito em [2].*

Podemos ver que o grupo dos quatérnios de ordem 8, Q_8, é um $2\mathcal{E}$-grupo contudo, não é 2E-grupo. De fato, Q_8 é 2-Engel, pois

$$[a, b, b] = a^2b^{-1}a^{-2}b = 1 \ e$$

$$[b, a, a] = a^{-1}b^{-1}aba^2 = 1.$$

Pela definição de $p\mathcal{E}$-grupo e sabendo que

$$Q_8 =< a, b | a^b = a^{-1}, a^2 = b^2, a^4 = 1 > \ e \ Q_8' =< a^2 >,$$

temos que Q_8 é um $2\mathcal{E}$-grupo. Mas, Q_8 não é $2A$-grupo uma vez que $[a,b] \neq 1$ e se α é a aplicação tal que $\alpha(a) = b$ e $\alpha(b) = a$, então α pode ser estendido a um automorfismo de Q_8. Assim, Q_8 não é $2E$-grupo.

Lema 3.2.4. *Seja G um $p\mathcal{E}$-grupo tal que $exp(\frac{G}{G'}) = p^r$. Então,*

i) *$exp(G') = exp(G/Z(G))$ e $exp(G) = p^r exp(G')$;*

ii) *se $cl(G) = 2$, então $exp(G') \leq p^r$;*

iii) *se $cl(G) = 3$, então $p = 3$ e $exp(G') = p^{r+1}$.*

Demonstração:

i) Como G é $p\mathcal{E}$-grupo, G é 2-Engel, por definição. Assim, pela Proposição 1.6.7,

$$\begin{aligned} exp(G/Z(G)) \text{ divide } n &\Leftrightarrow a^n \in Z(G); \forall \in G \\ &\Leftrightarrow [a^n, b] = 1; \forall a, b \in G \\ &\Leftrightarrow [a,b]^n = 1; \forall a, b \in G \\ &\Leftrightarrow exp(G') \text{ divide } n. \end{aligned}$$

Isso mostra que $exp(G') = exp(G/Z(G))$.

Agora, como $exp(G/G') = p^r$, temos que $g^{p^r} \in G'$, para qualquer elemento $g \in G$, ou seja, $G^{p^r} \leq G'$. Se $exp(G') = p^t$, então $G^{p^{r+t}} \leq (G^{p^r})^{p^t} \leq (G')^{p^t} = 1$. Além disso, se $G^{p^{r+t-1}} = 1$, então $G^{p^{t-1}} \leq \Omega_r(G) \leq Z(G)$ (pois G é $p\mathcal{E}$-grupo) e $exp(G') \leq p^{t-1}$, o que é absurdo. Portanto, $exp(G) = p^{r+t}$.

ii) Sabemos que $G' \leq Z(G)$, pois $cl(G) = 2$. Assim, por hipótese, $g^{p^r} \in G' \leq Z(G)$, para qualquer elemento $g \in G$, isto é, $exp(G/Z(G)) \leq p^r$. Pelo item i), $exp(G') = exp(G/Z(G))$ e segue o resultado.

iii) Como G é 2-Engel, por definição, então $\gamma_3(G)^3 = 1$, pelo Teorema de Levi 1.7.3. Assim, uma vez que $cl(G) = 3$, temos que $p = 3$ (pois G é p-grupo e existe $g \in G$ com $g^3 = 1$) e podemos escrever, usando a Proposição 1.6.7, que

$$(G')^{3^{r+1}} = [G,G]^{3^{r+1}} = [G^{3^r}, G]^3 \leq [G', G]^3 = \gamma_3(G)^3 = 1,$$

ou seja, $exp(G') \leq 3^{r+1}$. Mas, se $exp(G') \leq 3^r$, então $G' \leq \Omega_r(G) \leq Z(G)$, pois G é $p\mathcal{E}$-grupo, o que contradiz a hipótese $cl(G) = 3$. Portanto, $exp(G') = 3^{r+1}$.

■

Lema 3.2.5. *Seja G um $p\mathcal{E}$-grupo tal que $(G')^{p^k}$ é cíclico, para algum $k \geq 0$. Sejam ainda $a, b \in G$.*

i) *Se $k \geq 1$, então $[a,b]^{p^k} = 1$;*

ii) *se $G = \langle a, b\rangle$, $k = 0$ e $p \neq 2$, então $[a,b] = 1$;*

iii) *se $G = \langle a, b\rangle$, $k = 0$ e $p = 2$, então $[a,b] = 1$ ou $[a,b]^2 = 1$.*

Demonstração: Suponha que $exp(G/G') = p^r$. Temos que $a^{p^r}, b^{p^r} \in G'$ e como $(G')^{p^k}$ é p-grupo cíclico, segue que, se $n = p^{k+r}$, então $\langle a^n, b^n\rangle = \langle a^n\rangle$ ou $\langle a^n, b^n\rangle = \langle b^n\rangle$. Sem perda de generalidade, podemos supor que $b^n = a^{ns}$, para algum inteiro s. Então, pela Proposição 1.6.6, já que G é 2-Engel, segue que

$$(ba^{-s})^n = [b,a]^{sn(n-1)/2}. \tag{3.1}$$

Se $k \geq 1$, então a igualdade 3.1 é trivial, pelo Lema 3.2.4.

Suponhamos que $k = 0$ e $G = \langle a, b\rangle$, temos que $cl(G) \leq 2$, já que G é 2-Engel e, assim, $G' \leq Z(G)$. A igualdade 3.1, pelo Lema 3.2.4, é trivial se p é ímpar ou então, se $p = 2$ e ou $exp(G') \leq 2^{r-1}$ ou $2|s$.

Em qualquer um dos casos anteriores (incluindo o caso $k \geq 1$), como G é $p\mathcal{E}$-grupo, segue que $(ba^{-s})^{p^k} \in \Omega_r(G) \leq Z(G)$. Logo,

$$\begin{aligned} 1 &= [(ba^{-s})^{p^k}, a] = [ba^{-s}, a]^{p^k} = (a^s b^{-1} a^{-1} b a^{-s} a)^{p^k} \\ &= (a^s [b,a] a^{-s})^{p^k} = (a^s a^{-s} [b,a])^{p^k} = [b,a]^{p^k}. \end{aligned}$$

Suponhamos agora que $G = \langle a, b\rangle$ e $p = 2$, s ímpar e $exp(G') = 2^r$. Neste caso, a igualdade 3.1 implica que $(ba^{-s})^{2n} = 1$ e já que G é um $2\mathcal{E}$-grupo, obtemos $(ba^{-s})^2 \in \Omega_r(G) \leq Z(G)$. Logo,

$$1 = [(ba^{-s})^2, a] = [ba^{-s}, a]^2 = [b,a]^2.$$

O que completa a demonstração. ∎

Teorema 3.2.6 (Theorem 2.5 de [2])**.** *Todo $p\mathcal{E}$-grupo 2-gerado é abeliano ou isomorfo a Q_8.*

Demonstração: A demonstração será baseada em [2]. Suponhamos que $G = \langle a, b\rangle$ é um $p\mathcal{E}$-grupo e que $exp(G/G') = p^r$. Então, $G' = \langle [a,b]\rangle$ é p-grupo cíclico e, pelo Lema 3.2.5, segue que $[a,b] = 1$ e G é abeliano ou $p = 2$ e $[b,a]^2 = 1$. Neste último caso, segue que $r \leq 1$. Como G/G' é no máximo 2-gerado, temos que $|\frac{G}{G'}| \leq 4$, o que significa que $|G| = \left|\frac{G}{G'}\right| |G'| \leq 8$.

Logo, G é ou abeliano ou $G \cong Q_8$ ou $G \cong D_4$, o grupo diedral de ordem 8, com apresentação $D_4 = \langle a, b \,|\, a^4 = b^2 = 1, a^b = a^{-1} \rangle$. Mas, D_4 não é $2\mathcal{E}$-grupo, já que existem elementos de ordem 2 em D_4 que não são centrais. Por outro lado, Q_8 é um $2\mathcal{E}$-grupo, conforme foi mostrado na Observação 3.2.3. ∎

Observação 3.2.7. *Se G é um grupo 2-Engel, então $G^3G' \leq Z_2(G)$. De fato, $cl(G) \leq 3$ e $\gamma_3(G)^3 = 1$, pelo Teorema de Levi 1.7.3. Assim, se G é um 3-grupo 2-Engel, então $\Phi(G) \leq Z_2(G)$.*

Lema 3.2.8. *Sejam G um $p\mathcal{E}$-grupo e $exp(G/G') = p^r$. Então, $Z_2(G)^{p^r} = Z(G) \cap G^{p^r}$. Em particular, se $cl(G) = 3$, então $exp\big(\frac{Z_2(G)}{Z(G)}\big) = 3^r$.*

Demonstração: Pelo Teorema de Levi 1.7.3, podemos assumir que $p = 3$. Seja $x \in Z_2(G)^{3^r}$. Pelo Lema 1.7.4, G é regular e pela Proposição 1.6.6, $x = y^{3^r}$, para algum $y \in Z_2(G)$. Como $G^{3^r} \leq G' \leq Z_2(G)$, usando as Proposições 1.6.7 e 1.3.9, temos que

$$[x, g] = [y^{3^r}, g] = [y, g^{3^r}] = 1; \, \forall g \in G.$$

Isso implica que $x \in Z(G)$.

Agora, assuma que $x \in G^{3^r} \cap Z(G)$. Então, $x = y^{3^r}$, para algum $y \in G$ e, então

$$1 = [x, g] = [y^{3^r}, g] = [y, g]^{3^r}; \, \forall g \in G.$$

Logo, $[y, g] \in \Omega_r(G) \leq Z(G)$, o que implica que $y \in Z_2(G)$. Consequentemente, $x \in Z_2(G)^{3^r}$. O que mostra a primeira parte do lema.

Suponha, por contradição, que $cl(G) = 3$ e $Z_2(G)^{3^{r-1}} \leq Z(G)$, então obtemos que $G^3 \leq Z_2(G)$, pela Observação 3.2.7, e

$$G^{3^r} = (G^3)^{3^{r-1}} \leq Z_2(G)^{3^{r-1}} \leq Z(G).$$

Assim, $G^{3^r} \leq Z(G)$, o que contradiz o Lema 3.2.4 iii). Portanto, $exp\big(\frac{Z_2(G)}{Z(G)}\big) = 3^r$. ∎

Lema 3.2.9. *Seja G um grupo 2-Engel. Se $\frac{G}{Z_2(G)}$ é 2-gerado, então $cl(G) \leq 2$.*

Demonstração: Se $\frac{G}{Z_2(G)} = \langle aZ_2(G), bZ_2(G) \rangle$, então $G = \langle a, b, Z_2(G) \rangle$. Assim,

$$G' = \langle [x, y], \gamma_3(G) \,|\, x, y \in \{a, b\} \cup Z_2(G) \rangle.$$

Como G é 2-Engel, obtemos que $G' \leq Z(G)$, o que completa a demonstração. ∎

Teorema 3.2.10 (Theorem 2.9 de [2])**.** *Todo $p\mathcal{E}$-grupo 3-gerado é nilpotente de classe no máximo 2.*

Demonstração: A demonstração será feita por contradição e baseada em [2]. Suponhamos que $G = \langle x, y, z\rangle$ é um $p\mathcal{E}$-grupo de classe 3 e que $exp(G/G') = 3^r$. Seja $H = (G')^3\gamma_3(G)$. Como $cl(G) = 3$, pelo Lema 3.2.4, $[H, G] = 1 = H^{3^r}$.

Temos, para alguns inteiros $\alpha, \beta, \gamma, \alpha', \beta', \gamma', t_1, t_2, t_3 \in \{-1, 0, 1\}$:

$$x^{3^r} \equiv [x, y]^{\alpha}[y, z]^{t_1}[z, x]^{\beta}(mod\, H);\ y^{3^r} \equiv [x, y]^{\gamma}[y, z]^{\beta'}[z, x]^{t_2}(mod\, H) \text{ e}$$

$$z^{3^r} \equiv [x, y]^{t_3}[y, z]^{\alpha'}[z, x]^{\gamma'}(mod\, H).$$

Uma vez que $[x, x^{3^r}] = 1$ e $[x, y, z] \neq 1$, segue que $t_1 = t_2 = t_3 = 0$. Como $[x^{3^r}, y] = [x, y^{3^r}]$, segue que

$$[x^{3^r}, y] \equiv [[x, y]^{\alpha}, y][[z, x]^{\beta}, y] \equiv [x, y, y]^{\alpha}[z, x, y]^{\beta} \equiv [z, x, y]^{\beta} \text{ e}$$

$$[y^{3^r}, x] \equiv [[x, y]^{\gamma}, x][[y, z]^{\beta'}, x] \equiv [x, y, x]^{\gamma}[y, z, x]^{\beta'} \equiv [y, z, x]^{\beta'} \equiv [z, x, y]^{\beta'}.$$

Logo, $\beta' = -\beta$ e, de modo semelhante, temos que $\alpha' = -\alpha$ e $\gamma' = -\gamma$. Assim, para certos $h_1, h_2, h_3 \in H$, temos

$$x^{3^r} = [x, y]^{\alpha}[z, x]^{\beta}h_1;\ \ y^{3^r} = [x, y]^{\gamma}[y, z]^{-\beta}h_2 \ \text{ e } \ z^{3^r} = [y, z]^{-\alpha}[z, x]^{-\gamma}h_3. \tag{3.2}$$

O que implica, já que $[H, G] = 1$:

$$[x, y]^{3^r} = [x, y, z]^{\beta}, [z, x]^{3^r} = [x, y, z]^{-\alpha}, [y, z]^{3^r} = [x, y, z]^{\gamma}. \tag{3.3}$$

Então, como $H^{3^r} = 1$ e usando as igualdades 3.2 e 3.3 podemos ver que $x^{3^{2r}} = y^{3^{2r}} = z^{3^{2r}} = 1$. Como G é regular, concluímos que $G^{3^{2r}} = 1$, o que contradiz o Lema 3.2.4. ∎

Observação 3.2.11. *Suponhamos que G é um p-grupo finito tal que $\Omega_1(G) \leq Z(G)$. Se G não possui um fator direto não-trivial, então $\Omega_1(G) \leq \Phi(G)$. De fato, seja $x \in G$ um elemento de ordem p tal que $x \notin \Phi(G)$. Então, existe um subgrupo maximal M de tal forma que $x \notin M$. Uma vez que $x \in Z(G)$, por hipótese, temos que $\langle x\rangle \trianglelefteq G$. Então, $G = M \times \langle x\rangle$, um absurdo.*

Lema 3.2.12. *Sejam G um E-grupo e $a \in G$ tal que $\langle aG'\rangle$ é um somando direto infinito de $\dfrac{G}{G'}$. Então, $a \in Z(G)$.*

Demonstração: Por hipótese, temos, para algum $X \subseteq G$,

$$\frac{G}{G'} = \langle aG'\rangle \oplus \langle XG'\rangle.$$

Como G é nilpotente, $G' \leq \Phi(G)$ e então, $G = \langle a, X\rangle$. Assim, é suficiente mostrar que $[a, x] = 1$, para todo $x \in X$.

Sejam $\pi\colon G \longrightarrow \frac{G}{G'}$ o epimorfismo natural e $\psi\colon \langle aG'\rangle \oplus \langle XG'\rangle \longrightarrow \langle aG'\rangle$ a aplicação projeção da primeira componente. Agora, para cada $x \in X$, defina a aplicação $\phi_x\colon \langle aG'\rangle \longrightarrow \langle x\rangle$ tal que $\phi_x(a^iG') = x^i$, para todo $i \in \mathbb{Z}$. Temos que $\langle aG'\rangle \cong \mathbb{Z}$ e ϕ_x é um homomorfismo de grupos associando aG' a x. Logo, $\phi_x\psi\pi$ é um endomorfismo de G que associa a a x ($\phi_x\psi\pi(a) = x$). Como G é um E-grupo, concluímos que $[a, x] = 1$; completando a demonstração. ∎

Lema 3.2.13. *Seja G um p-grupo finito com $cl(G) = 3$. Se $|G' : G' \cap Z(G)| = p$, então $|G : Z_2(G)| = p^2$.*

Demonstração: Suponhamos que $G = \langle a, b, c_1, \ldots, c_r\rangle$ tal que $G'Z(G) = \langle [a, b]\rangle Z(G)$. Substituindo c_i por um adequado $c_i a^{\alpha_i} b^{\beta_i}$, podemos assumir que $[c_i, a], [c_i, b] \in Z(G)$, para $i = 1, \ldots, r$.

Afirmamos que $c_1, \ldots, c_r \in Z_2(G)$. Para mostrar essa afirmação, é suficiente mostrar que $[c_i, c_j] \in Z(G)$, para $1 \leq i < j \leq r$. Suponha que $[c_i, c_j] = [a, b]^l z$, com $z \in Z(G)$. Já que $[c_k, a], [c_k, b] \in Z(G)$, $[b, c_k, a] = 1$ e sabendo que

$$[c_k^{-1}, b^{-1}] = c_k b c_k^{-1} b^{-1} c_k b b^{-1} c_k^{-1} = c_k b [c_k, b] b^{-1} c_k^{-1} = [c_k, b],$$

temos que

$$\begin{aligned}
[a, b, c_k] &= [a, b, c_k][b, c_k, a] \\
&= [a, b]^{-1} c_k^{-1} a^{-1} b^{-1} a c_k b a^{-1} [b, c_k] a \\
&= b^{-1} a^{-1} b a a^{-1} c_k^{-1} [c_k^{-1}, a^{-1}] b^{-1} a c_k b a^{-1} [b, c_k] a \\
&= b^{-1} a^{-1} b c_k^{-1} b^{-1} [c_k^{-1}, a^{-1}] c_k a [a, c_k] b a^{-1} [b, c_k] a \\
&= b^{-1} a^{-1} b b^{-1} c_k^{-1} c_k a b [c_k, b] [c_k, a] [a, c_k] a^{-1} [b, c_k] a \\
&= 1,
\end{aligned}$$

de modo que segue a afirmação. Consequentemente, $G/Z_2(G) = \langle a, b\rangle Z(G)/Z_2(G)$ possui ordem igual a p^2. ∎

O teorema a seguir diz que se G é um E-grupo finito 3-gerado, então $cl(G) \leq 2$. Na verdade, pelo Teorema 3.3.15, não existe tal G com $cl(G) = 2$.

Teorema 3.2.14 (Theorem 1.1 de [2])**.** *Todo E-grupo finito 3-gerado é nilpotente de classe no máximo 2.*

Demonstração: A demonstração segue como em [2]. Seja G um E-grupo 3-gerado. Se $\frac{G}{G'}$ é finito, como G é nilpotente, $G' \leq \Phi(G)$, G é finito e G é o produto direto

de seus subgrupos de Sylow. Todo subgrupo de Sylow de G pré-imagem endomorfa de G e então, pelo Teorema 3.1.7, eles são no máximo E-grupos 3-gerados. Neste caso, o Teorema 3.2.10 completa a demonstração.

Se $\frac{G}{G'}$ é infinito, então, pelo Teorema Fundamental de Grupos Abelianos Finitamente Gerados, temos, para alguns $a, b, c \in G$ tais que aG' tem ordem infinita,

$$\frac{G}{G'} = \langle aG' \rangle \oplus \langle bG', cG' \rangle.$$

Assim, pelo Lema 3.2.12, $a \in Z(G)$ e, como G é 2-Engel (pois é E-grupo), segue que $G' = \langle [b, c] \rangle$ e que $\gamma_3(G) = \gamma_3(\langle b, c \rangle) = 1$. Isto completa a demonstração. ∎

Logo, pelos Teoremas 3.2.6 e 3.2.14, se $d \leq 3$, todo $p\mathcal{E}$-grupo d-gerado possui classe de nilpotência menor ou igual a 2.

Teorema 3.2.15 (Theorem 1.2 de [2]). *Seja G um 3E-grupo. Se $|G| \leq 3^{10}$, então G é nilpotente de classe no máximo 2.*

Demonstração: A demonstração será feita por contradição, tal como em [2]. Seja G um 3E-grupo finito de menor ordem sujeito às propriedades $cl(G) = 3$ e $|G| \leq 3^{10}$. Então, G não possui um fator direto não-trivial e $\Omega_1(G) \leq \Phi(G)$, pela Observação 3.2.11. Assim, $\Omega_1(G) \leq \Phi(G) \cap Z(G)$. Se $d(G) \geq 5$, então $\left|\frac{G}{\Phi(G)}\right| \geq 3^5$. Como G é regular e

$$\Phi(G) = G^3G', \ |\Phi(G) \cap Z(G)| \geq |\Omega_1(G)| = |G : G^3| \geq 3^5 \text{ e } cl(G) = 3,$$

temos $\Phi(G) \cap Z(G) < \Phi(G)$. Segue que $|G| \geq 3^{11}$, uma contradição. Logo, o Teorema 3.2.14 implica que $d(G) = 4$.

Se $|G' : G' \cap Z(G)| = 3$, então, pelo Lema 3.2.13, temos $|G : Z_2(G)| = 9$. Assim, $\frac{G}{Z_2(G)}$ é um grupo 2-gerado e, pelo Lema 3.2.9, $cl(G) \leq 2$, uma contradição. Logo,

$$|G' : G' \cap Z(G)| \geq 9.$$

Uma vez que

$$|G| = |G : \Phi(G)||\Phi(G) : \Phi(G) \cap Z(G)||\Phi(G) \cap Z(G)| \text{ e}$$

$$\begin{aligned} |\Phi(G) : \Phi(G) \cap Z(G)| &= |G'G^3 : G'G^3 \cap Z(G)| \\ &= |Z(G)G'G^3 : Z(G)| \\ &= \frac{|Z(G)G'||G^3|}{|Z(G)G' \cap G^3||Z(G)|}, \end{aligned}$$

obtemos

$$|G| = |G : \Phi(G)||G' : G' \cap Z(G)||G^3 : G'Z(G) \cap G^3||\Phi(G) \cap Z(G)| \geq 3^4.3^2.1.3^4 = 3^{10}.$$

Assim,

$$|G| = 3^{10},\ |\Omega_1(G)| = |\Phi(G) \cap Z(G)| = 3^4,\ |G' : Z(G) \cap G'| = 9 \text{ e } G^3 \leq G'Z(G).$$

Além disso, temos que $|G : G^3| = |\Omega_1(G)|, G^3 = \Phi(G) \leq Z_2(G)$ e

$$G'^9 = [G^3, G]^3 \leq (\gamma_3(G))^3 = 1, \tag{3.4}$$

de modo que segue que $\Phi(G)$ é um grupo abeliano de ordem 3^6 e $d(\Phi(G)) = 4$. Dessa forma,

$$\Phi(G) \cong C_{27} \times C_3 \times C_3 \times C_3 \text{ ou } C_9 \times C_9 \times C_3 \times C_3.$$

Pela relação de inclusão 3.4 e pelo Lema 3.2.4 iii), temos que $exp\left(\frac{G}{G'}\right) = 3$. Portanto, pelo Lema 3.2.8, segue $Z_2(G)^3 = \Phi(G) \cap Z(G)$.

Agora, o Lema 3.2.9 implica que

$$d\left(\frac{G}{Z_2(G)}\right) = 3 \text{ ou } 4.$$

Então, $|Z_2(G)| = 3^6$ ou 3^7, implicando que $Z_2(G) = \Phi(G)$ ou $|Z_2(G) : \Phi(G)| = 3$. Se $Z_2(G) = \Phi(G)$, então $|Z_2(G)^3| = |\Phi(G) \cap Z(G)| = 9$, absurdo. Logo,

$$|Z_2(G) : \Phi(G)| = 3.$$

Como $exp(G/G') = 3$, temos que $G^3 \leq G'$ e $\Phi(G) = G'$. Assim, $[Z_2(G), \Phi(G)] = 1$, pela Proposição 1.3.9. Portanto, temos que $\Phi(G) \leq Z(Z_2(G))$ e $Z_2(G)$ é um grupo abeliano com $d(Z_2(G)) = 4$. De fato, se $d(Z_2(G)) \geq 5$, então existe $x \in G$, um gerador de $Z_2(G)$, tal que $x \notin \Phi(G)$. Dessa forma, x é um gerador de G e existe $H \subseteq G$ tal que $G = \langle H, x\rangle$ e $x \notin H$, isto é, $G = H \times \langle x\rangle$. Mas, pelo Teorema 3.1.7, temos que H é um 3E-grupo e $|H| \leq 3^{10}$, o que contradiz a minimalidade da ordem de G.

Assim,

$$Z_2(G) \cong C_{81} \times C_3 \times C_3 \times C_3 \text{ ou } C_{27} \times C_9 \times C_3 \times C_3 \text{ ou } C_9 \times C_9 \times C_9 \times C_3.$$

De modo que, $|Z_2(G)^3| = |\Phi(G) \cap Z(G)| = 27$, o que é uma contradição. ∎

Teorema 3.2.16 (Theorem 1.3 de [2])**. i)** *Um grupo 2-gerado é abeliano se, e somente*

se, é um E-grupo.

ii) *Um grupo infinito 3-gerado é abeliano se, e somente se, é um E-grupo.*

Demonstração: A demonstração será feita como em [2].

i) Seja G um E-grupo 2-gerado. Suponhamos primeiro que $\frac{G}{G'}$ é finito. Como G é nilpotente, $G' \leq \Phi(G)$ e então, G é finito; além disso, G é produto direto de seus subgrupos de Sylow. Todo subgrupo de Sylow de G é, também, no máximo 2-gerado e é um E-grupo, pelo Teorema 3.1.7. Pelo Teorema 3.2.6 e pela Observação 3.2.3, temos que todo subgrupo de Sylow de G é abeliano e assim, G é abeliano.

Suponhamos agora que $\frac{G}{G'}$ é infinito. Pelo Teorema Fundamental dos Grupos Abelianos Finitamente Gerados, para alguns $a, b \in G$, tal que $\langle aG' \rangle$ é infinito, temos que

$$\frac{G}{G'} = \langle aG' \rangle \oplus \langle bG' \rangle.$$

Já que $G' \leq \Phi(G)$, $G = \langle a, b \rangle$, o resultado do item segue pelo Lema 3.2.12.

ii) Seja G um E-grupo infinito 3-gerado. Como G é infinito e nilpotente, segue que $\frac{G}{G'}$ é um grupo infinito 3-gerado. Assim,

$$\frac{G}{G'} = \langle aG' \rangle \oplus \langle bG' \rangle \oplus \langle cG' \rangle,$$

para alguns $a, b, c \in G$, tal que $\langle aG' \rangle$ é infinito e $G = \langle a, b, c \rangle$. Pelo Lema 3.2.12, $a \in Z(G)$. Se ou $\langle bG' \rangle$ ou $\langle cG' \rangle$ é infinito, então o Lema 3.2.12 garante que G é abeliano. Suponhamos que $\langle bG' \rangle$ e $\langle cG' \rangle$ são finitos. Temos que $G' = \langle [b, c] \rangle \leq H = \langle b, c \rangle$ é finito. Portanto, $G = \langle a \rangle \times H$, já que $a \in Z(G)$ possui ordem infinita e H é um grupo finito. Logo, H é um E-grupo 2-gerado, pelo Teorema 3.1.7 e uma vez que é fator direto de G. O resultado segue do item i).

■

3.3 Classificação dos $p\mathcal{E}$-grupos 3-gerados

O principal objetivo desta seção é mostrar que 4 é o número mínimo de geradores necessários para construir um E-grupo não-abeliano, o que pode ser concluído usando os Teoremas 3.2.16 e 3.3.15. Observe que o exemplo de R. Faudree [10] é 4-gerado. Classificaremos os $2\mathcal{E}$-grupos 3-gerados e determinaremos todos os $p\mathcal{E}$-grupos tais que seus subgrupos derivados são cíclico. Todos os resultados contidos nesta seção estão demonstrados em [1], exceto quando dito o contrário.

Notação 3.3.1. *Para um primo p, inteiros $1 \leq t \leq r$ e $[m_{ij}] \in GL(3, \mathbb{Z}_{p^t})$ escrevemos $G(p, r, t, [m_{ij}])$ para denotar o grupo G com a seguinte apresentação:*

$$\begin{aligned}\langle x, y, z \mid \quad & x^{p^{r+t}} = y^{p^{r+t}} = z^{p^{r+t}} = 1 \\ & [x^{p^t}, y] = [x^{p^t}, z] = [y^{p^t}, x] = [y^{p^t}, z] = [z^{p^t}, x] = [z^{p^t}, y] = 1, \\ & [x, y] = x^{p^r m_{11}} y^{p^r m_{12}} z^{p^r m_{13}}, \\ & [x, z] = x^{p^r m_{21}} y^{p^r m_{22}} z^{p^r m_{23}}, \\ & [y, z] = x^{p^r m_{31}} y^{p^r m_{32}} z^{p^r m_{33}} \rangle,\end{aligned}$$

em que $1 \leq t \leq r$ e $[m_{ij}] \in GL(3, \mathbb{Z}_{p^t})$.

Teorema 3.3.2 (Theorem 2.2 de [1])**.** *Seja G um $p\mathcal{E}$-grupo não-abeliano 3-gerado tal que $exp(G/G') = p^r$, $exp(G') = p^t$ e ($p > 2$ ou ($p = 2$ e $exp(G') \neq 2^r$)). Então, $|G| = p^{3(r+t)}$ e $G = G(p, r, t, [m_{ij}])$. Além disso, $G(p, r, t, [m_{ij}])$ é $p\mathcal{E}$-grupo.*

Demonstração: Pelo Teorema 3.2.10, temos que $cl(G) = 2$. Como G é 3-gerado, existem elementos $a, b, c \in G$ tais que

$$\frac{G}{Z(G)} = \langle aZ(G) \rangle \times \langle bZ(G) \rangle \times \langle cZ(G) \rangle.$$

Já que $exp(G/Z(G)) = exp(G') = p^t$, temos que $|aZ(G)| = |bZ(G)| = p^t$ e $|cZ(G)| = p^s$, para algum s tal que $0 \leq s \leq t$. Então, $G' = \langle [a, b], [a, c], [b, c] \rangle$, pois $cl(G) = 2$ e $G = \langle a, b, c, Z(G) \rangle$ e ainda, $|[a, b]| \leq p^t$, $|[a, c]| \leq p^s$ e $|[b, c]| \leq p^s$, pois $|aZ(G)| = p^t$ e $|cZ(G)| = p^s$. Assim, $|G'| \leq p^{t+2s}$.

Como G é regular, temos que $|G : \Omega_r(G)| = |G^{p^r}|$, pela Proposição 1.6.6. E, uma vez que $\Omega_r(G) \leq Z(G)$ e $G^{p^r} \leq G'$,

$$|G| = |\Omega_r(G)||G^{p^r}| \leq |Z(G)||G'|;$$

e obtemos que $|G : Z(G)| \leq |G'|$. Portanto, $p^{2t+s} \leq p^{t+2s}$ e $t \leq s$, o que implica que

$$s = t,\ |G'| = \left|\frac{G}{Z(G)}\right| = p^{3t} \text{ e } G' = \langle [a, b] \rangle \times \langle [a, c] \rangle \times \langle [b, c] \rangle.$$

Concluímos, assim, de $\dfrac{G}{G^p Z(G)} \cong C_p \times C_p \times C_p$ (o que vale pois, já que G não é abeliano, temos que $t \geq 1$) que $Z(G) \leq \Phi(G)$ e $G = \langle a, b, c \rangle$.

Agora, como

$$G^{p^r} \leq G' \text{ e } |G'| = |G : Z(G)| \leq |G : \Omega_r(G)| = |G^{p^r}|,$$

e já que $t \leq r$, segue que $G' = G^{p^r}$ e $G^{p^r} = \langle a^{p^r}, b^{p^r}, c^{p^r} \rangle$. Pelo Lema 3.2.4, $exp(G) = p^{r+t}$. Mas, já que $G' = G^{p^r}$ é um grupo abeliano de ordem p^{3t}, segue que

$$G^{p^r} = \langle a^{p^r}, b^{p^r}, c^{p^r} \rangle = \langle a^{p^r} \rangle \times \langle b^{p^r} \rangle \times \langle c^{p^r} \rangle \text{ e } |a| = |b| = |c| = p^{r+t}.$$

Além disso, como $G^{p^r} = \langle a^{p^r} \rangle \times \langle b^{p^r} \rangle \times \langle c^{p^r} \rangle \leq \langle a^{p^t}, b^{p^t}, c^{p^t} \rangle$, temos que $\langle a^{p^t}, b^{p^t}, c^{p^t} \rangle = \langle a^{p^t} \rangle \times \langle b^{p^t} \rangle \times \langle c^{p^t} \rangle$, e então,

$$p^{3r} = |\langle a^{p^t}, b^{p^t}, c^{p^t} \rangle| \leq |G^{p^t}| \leq |\Omega_r(G)| \leq |Z(G)| = |G : G'| \leq p^{3r}.$$

Dessa forma,

$$G^{p^t} = \Omega_r(G) = Z(G) \text{ e } |G| = p^{3(r+t)}.$$

Já que $G' = G^{p^r}$, existe uma matriz 3×3, $M = [m_{ij}] \in GL(3, \mathbb{Z}_{p^t})$ tal que

$$[a,b] = a^{p^r m_{11}} b^{p^r m_{12}} c^{p^r m_{13}}, [a,c] = a^{p^r m_{21}} b^{p^r m_{22}} c^{p^r m_{23}}, [b,c] = a^{p^r m_{31}} b^{p^r m_{32}} c^{p^r m_{33}},$$

e todo elemento de G pode ser escrito como $a^i b^j c^k$, para $i, j, k \in \mathbb{Z}$, e

$$\begin{aligned}(a^i b^j c^k)(a^{i'} b^{j'} c^{k'}) = \quad & a^{i+i'-i'jp^r m_{11} - i'kp^r m_{21} - j'kp^r m_{31}} \\ & b^{j+j'-i'jp^r m_{12} - i'kp^r m_{22} - j'kp^r m_{32}} c^{k+k'-i'jp^r m_{13} - i'kp^r m_{23} - j'kp^r m_{33}}.\end{aligned}$$

Consideremos, agora, $\tilde{G} = \mathbb{Z}_{p^{r+t}} \times \mathbb{Z}_{p^{r+t}} \times \mathbb{Z}_{p^{r+t}}$ e definimos a operação binária sobre $\tilde{G}$:

$$\begin{aligned}(i,j,k)(i',j',k') = \quad & (i + i' - i'jp^r m_{11} - i'kp^r m_{21} - j'kp^r m_{31}, \\ & j + j' - i'jp^r m_{12} - i'kp^r m_{22} - j'kp^r m_{32}, \\ & k + k' - i'jp^r m_{13} - i'kp^r m_{23} - j'kp^r m_{33}).\end{aligned}$$

Com essa operação binária, $\tilde{G}$ é grupo e $\tilde{G} \cong G$. Concluímos, então, que G possui a apresentação desejada. ∎

Lema 3.3.3. *Seja G um grupo nilpotente finito de classe 2. Se G é 2-gerado, então $|G| = |G'|^2 |Z(G)|$.*

Demonstração: Sejam $G = \langle a, b \rangle$, $H = \langle a \rangle Z(G)$ e $K = \langle b \rangle Z(G)$. Então, $H \trianglelefteq G$ e $K \trianglelefteq G$ com $G = HK$ e $H \cap K = Z(G)$. Se $|aZ(G)| = n$, então $[a^n, b] = 1$ e $[a,b]^n = 1$. Segue, assim, que $|G'|$ divide n pois $G' = \langle [a,b] \rangle$. Logo, G' divide $\left| \frac{H}{Z(G)} \right|$ e, de modo semelhante, divide $\left| \frac{K}{Z(G)} \right|$. Dessa maneira, $|G'|^2 |Z(G)|$ divide $|G|$.

Por outro lado, suponhamos que b^i não comuta com a, então $1 \neq [a, b^i] = [a,b]^i$. Logo, para cada b^i pertencente ao transversal de $C_G(a)$ em G temos um elemento não-

trivial correspondente em G'. Assim, $|G : C_G(a)| \leq |G'|$. De modo semelhante obtemos que $|G : C_G(b)| \leq |G'|$. Consequentemente, segue que

$$|G : Z(G)| = |G : C_G(a) \cap C_G(b)| \leq |G : C_G(a)||G : C_G(b)| \leq |G'|^2.$$

Portanto, $|G| = |G'|^2|Z(G)|$. ∎

Teorema 3.3.4 (Theorem 2.4 de [1]). *Seja G um $p\mathcal{E}$-grupo não-abeliano com subgrupo derivado cíclico. Então, $G \cong Q_8 \times C_2^n$, para algum $n \in \mathbb{Z}$ não-negativo.*

Demonstração: Como G é p-grupo e G' é cíclico, temos que existem $a, b \in G$ tais que $G' = \langle [a, b] \rangle$. Sejam $H = \langle a, b \rangle$, $exp(G/G') = p^r$ e $|G'| = p^t$. Pelo Lema 3.3.3,

$$|G'|^2 \leq |H'|^2 = |H : Z(H)| \leq |H : Z(G) \cap H| = |HZ(G) : Z(G)| \leq |G : Z(G)|.$$

Logo, $|G| \geq |G'|^2|Z(G)|$. Se $p > 2$, então, por regularidade,

$$|G| = |G^{p^r}||\Omega_r(G)| \leq |G'||Z(G)|,$$

o que implica que G é abeliano, um absurdo. Então, $p = 2$.

Como G' é um 2-grupo cíclico e $a^{2^r}, b^{2^r} \in G'$, usando as mesmas ideias da demonstração do Lema 3.2.5, podemos assumir que $a^{2^r} = b^{2^r s}$, para algum $s \in \mathbb{Z}$, de modo que podemos concluir que $(ab^{-s})^{2^{r+1}} = 1$, $(ab^{-s})^2 \in Z(G)$ e $[a, b]^2 = 1$. Logo, $t = 1$.

Se $r \geq 2$, então $(ab^{-s})^{2^r} = 1$ (pois $|G'| = 2$) e $ab^{-s} \in Z(G)$, o que implica que $[a, b] = 1$, uma contradição. Portanto, $r = 1$ e $G^2 = G'$, de modo que obtemos $a^2 = b^2 = [a, b]$ e então, $H \cong Q_8$.

Agora, afirmamos que $G = HC_G(H)$ e que $C_G(H)$ é um 2-grupo abeliano elementar. De fato, se $G < HC_G(H)$, existe um elemento $g \in G$ tal que $g \notin HC_G(H)$ e então, $g^2 \neq 1$ (pelo Teorema 3.1.3) e $g^2 = a^2 = b^2$ (pois $G^2 = G'$), de modo que $(ga)^2 = [g, a]$. Se $[g, a] = 1$, então $ga \in Z(G) \leq C_G(H)$ e $g \in HC_G(H)$, um absurdo. Logo, $[g, a] \neq 1$ e $[g, a] = [a, b]$. Analogamente, $[g, b] = [a, b]$. Assim, gab comuta com a e b, ou seja, $g \in HC_G(H)$, absurdo. Portanto, $G = HC_G(H)$. Suponhamos, agora, que existe $x \in C_G(H)$ tal que $x^2 \neq 1$. Logo, $x^2 = a^2$ e $(xa)^2 = 1$. Então, $xa \in Z(G)$ e $1 = [xa, b] = [a, b]$, um absurdo.

Portanto, a afirmação é verdadeira e temos, também, que $H \cap C_G(H) = Z(H) = \langle a^2 \rangle$ e assim, $C_G(H) = \langle a^2 \rangle \times E$, para algum 2-grupo E abeliano elementar. Como $G \cong H \times E$, vale o resultado. ∎

A demonstração de alguns lemas desta seção foram feitas computacionalmente, usando o GAP [12]. Usamos o símbolo `gap>` para denotar o início de uma linha de comando usual dentro do programa GAP.

Lema 3.3.5. *Seja G um $2\mathcal{E}$-grupo não-abeliano 3-gerado tal que $exp(G/G') = exp(G') = 2$ e $|G| = 32$. Então, G é isomorfo a um dos seguintes grupos:*

i) $\langle x, y, z \,|\, x^4 = y^4 = [y, z] = 1, x^2 = z^2 = [x, y], (xz)^2 = y^2 \rangle$.

ii) $\langle x, y, z \,|\, x^4 = z^4 = [y, z] = 1, x^2 = y^2 = [x, y], [x, z] = z^2 \rangle$.

Demonstração: A demonstração será feita computacionalmente, usando o GAP [12]. Definimos as seguintes funções:

```
gap> 2Engel:= G -> ForAll(Cartesian(G,G), a -> LeftNormedComm([a[1], a[2], a[2]])
> =One(G));
gap> 3gerado:= G -> Length(MinimalGeneratingSet(G)) = 3;
```

Definimos agora a seguinte lista de grupos de ordem 32:

```
gap> C:=AllSmallGroups(32, 2Engel, 3gerado, g->Exponent(DerivedSubgroup(g)) = 2,
                 g->Exponent(g/DerivedSubgroup(g)) = 2);
```

Nos comandos a seguir, `G` é a lista de todos os grupos com as propriedades descritas no lema.

```
gap> G:=[];; i:=1;;
gap> while i<=Length(C) do
>       j:=1;;Omegar:=[];;
>       e:=Elements(C[i]);;
>       while j<=32 do
>               if e[j]^2 = Identity(C[i]) then Add(Omegar, e[j]); fi;
>               j:=j+1;
>       od;
> if  IsSubset(Centre(C[i]),Omegar)=true then
>       Add(G,C[i]); fi;
> i:=i+1;
> od;
gap> G;
[ <pc group of size 32 with 5 generators>, <pc group of size 32 with 5 generators> ]
```

Agora, comparamos os dois grupos fornecidos anteriormente com os grupos descritos no lema:

```
gap> F:=FreeGroup(3);;
gap> R:=[F.1^4, F.2^4, Comm(F.2,F.3), F.1^-2*Comm(F.1,F.2), F.3^-2*Comm(F.1,F.2),
>        F.2^-2*(F.1*F.3)^2];;
gap> R2:=[F.1^4, F.3^4, Comm(F.2,F.3), F.1^-2*Comm(F.1,F.2), F.2^-2*Comm(F.1,F.2),
>       F.3^-2*Comm(F.1,F.3)];;
gap> J:=F/R;; j:=GeneratorsOfGroup(J);;
gap> J2:=F/R2;; j2:=GeneratorsOfGroup(J2);;
gap> g:=MinimalGeneratingSet(G[1]);;
```

```
gap> iso:=IsomorphismFpGroupByGenerators(G[1],g);;
gap> H:=Image(iso);;
gap> phi:= GroupHomomorphismByImages(H, J, GeneratorsOfGroup(H), j);;
gap> Size(Image(phi)) = 32;
true
gap> g2:=MinimalGeneratingSet(G[2]);;
gap> iso2:=IsomorphismFpGroupByGenerators(G[2],g2);;
gap> H2:=Image(iso2);;
gap> psi:=  GroupHomomorphismByImages(H2, J2 , GeneratorsOfGroup(H2), j2);;
gap> Size(Image(psi)) = 32;
true
```

O que mostra o lema. ∎

Lema 3.3.6. *Existem exatamente quatro $2\mathcal{E}$-grupos G de ordem 2^6 tais que $|G'| = 2^3$ $exp(G/G') = exp(G') = 2$, satisfazendo $G^2 = G'$.*

Demonstração: A demonstração será feita computacionalmente, usando o GAP [12]. Defina as seguintes funções:

```
gap> 2Engel:= G -> ForAll(Cartesian(G,G), a -> LeftNormedComm([a[1], a[2], a[2]])
> =One(G));
gap> G2igualDerivado:= G-> GroupWithGenerators(List(Elements(G),x->x^2))
>                      = DerivedSubgroup(G);
```

A funções `2Engel` e `G2igualDerivado` determinam se o grupo é 2-Engel e se $G^2 = G'$, respectivamente.

Defina agora a seguinte lista de grupos, `G` de ordem 64, satisfazendo as condições do teorema:

```
gap> C:=AllSmallGroups(64, 2Engel,G2igualDerivado, g-> Order(DerivedSubgroup(g))=8,
>     g -> Exponent(g/DerivedSubgroup(g))=2, g -> Exponent(DerivedSubgroup(g))=2);;
gap> G:=[];; i:=1;;
gap> while i<=Length(C) do
>     j:=1;;Omegar:=[];;
>     e:=Elements(C[i]);;
>     while j<=64 do
>      if e[j]^Exponent(C[i]/DerivedSubgroup(C[i])) = Identity(C[i])
>        then Add(Omegar, e[j]); fi;
>      j:=j+1;
>     od;
>    if  IsSubset(Centre(C[i]),Omegar)=true then
>     Add(G,C[i]); fi;
>    i:=i+1;
>  od;
gap> G;
[ <pc group of size 64 with 6 generators>, <pc group of size 64 with 6 generators>,
<pc group of size 64 with 6 generators>, <pc group of size 64 with 6 generators>  ]
```

O GAP retorna exatamente quatro grupos, o que mostra o lema. ∎

Teorema 3.3.7 (Theorem 2.5 de [1]). *Seja G um $2\mathcal{E}$-grupo não-abeliano 3-gerado tal que $exp(G/G') = exp(G') = 2^r$. Então, G é isomorfo a um dos seguintes grupos:*

i) $Q_8 \times C_2$.

ii) $\langle x, y, z \,|\, x^4 = y^4 = [y, z] = 1, x^2 = z^2 = [x, y], (xz)^2 = y^2\rangle$.

iii) $\langle x, y, z \,|\, x^4 = z^4 = [y, z] = 1, x^2 = y^2 = [x, y], [x, z] = z^2\rangle$.

iv) $G(2, r, r, [m_{ij}])$; *tal que* $[m_{ij}] \in GL(3, \mathbb{Z}_{p^r})$.

Demonstração: Suponhamos que $\frac{G}{Z(G)} = \langle aZ(G)\rangle \times \langle bZ(G)\rangle \times \langle cZ(G)\rangle$, para alguns $a, b, c \in G$ tais que $|aZ(G)| = |bZ(G)| = 2^r$, $|cZ(G)| = 2^s$ com $0 \leq s \leq r$.

Se $s = 0$, então G' é cíclico e então, pelo Teorema 3.3.4, $G \cong Q_8 \times C_2$.

Suponhamos, então, que $s \geq 1$. Temos que $G' = \langle [a, b], [a, c], [b, c]\rangle$. Uma vez que $(G')^{2^s}$ é um 2-grupo cíclico, pelo Lema 3.2.5, temos que $[a, b]^{2^s} = 1$. Logo, $exp(G') \leq 2^s$ e $r = s$. Dessa maneira,

$$|\frac{G}{Z(G)}| = 2^{3r} \text{ e } |a| = |b| = |c| = 2^{2r}.$$

De modo que, como $2^{3r} = |G : Z(G)| \leq |G : \Omega_r(G)| \leq |G : G'| \leq 2^{3r}$, temos que

$$G' = Z(G) = \Omega_r(G).$$

Assim, por regularidade, e pelo Teorema 1.6.2 segue que:

$$|G| = |\Omega_{r+1}||G^{2^{r+1}}| \leq |\Omega_{r+1}(G) : \Omega_r(G)||\Omega_r(G)||(G')^2| \leq 8|Z(G)||(G')^2|.$$

Então, $|(G')^2| \geq 2^{3r-3}$. Suponhamos que $G' \cong C_{2^r} \times C_{2^u} \times C_{2^v}$ tal que $0 \leq v \leq u \leq r$. Se $v = 0$, temos que $|(G'^2)| = 2^{r+u-2} \leq 2^{2r-2}$. Logo, nesse caso, $r = 1$, $|G| = 2^5$ e, pelo Lema 3.3.5, G possui apresentação como no item ii) ou iii).

Se $v \geq 1$ e $|(G')^2| = 2^{r+u+v-3}$, temos que $u = v = r$, $|G'| = 2^{3r}$ e $|G| = 2^{6r}$. Portanto, $G' = \langle [a, b]\rangle \times \langle [a, c]\rangle \times \langle [b, c]\rangle$.

Agora, afirmamos que $G^{2r} = G'$. Se $r = 1$, então $|G| = 64$ e, pelo Lema 3.3.6, existem exatamente quatro $2\mathcal{E}$-grupos G de ordem 2^6 tais que $|G'| = 2^3$ $exp(G/G') = exp(G') = 2$, satisfazendo $G^2 = G'$. Suponhamos, agora, que $r > 1$. Provamos que $\langle a^{2^r}, b^{2^r}, c^{2^r}\rangle = \langle a^{2^r}\rangle \times \langle b^{2^r}\rangle \times \langle c^{2^r}\rangle$. Se $a^{2^r m} b^{2^r n} c^{2^r l} = 1$, então $(a^{2m} b^{2n} c^{2l})^{2^r} = 1$ e, assim, $a^{2m} b^{2n} c^{2l} \in Z(G)$. Isso implica que 2^r divide $2m, 2n$ e $2l$, o que implica que, m, n, l são

pares e $a^m b^n c^l \in \Omega_r(G) = Z(G)$. Logo, $a^{2^r m} = b^{2^r n} = c^{2^r l} = 1$. Consequentemente,

$$\langle a^{2^r}, b^{2^r}, c^{2^r} \rangle = \langle a^{2^r} \rangle \times \langle b^{2^r} \rangle \times \langle c^{2^r} \rangle \cong C_{2^r} \times C_{2^r} \times C_{2^r} \text{ e } G^{2^r} = G'.$$

Uma demonstração semelhante ao final da demonstração do Teorema 3.3.2 fornece que $G \cong G(2, r, r, [m_{ij}])$; tal que $[m_{ij}] \in GL(3, \mathbb{Z}_{p^r})$. ∎

Observação 3.3.8. *Os grupos descritos nos itens i), ii) e iii) do Teorema 3.3.7 não são E-grupos. De fato, basta considerar o endomorfismo $\varphi\colon G \longrightarrow G$ tal que $G = \langle x, y, z \rangle$ é tal como em i), ii) ou iii) e ainda, $\varphi(y) = x$; $\varphi(x) = x$ e $\varphi(z) = z$.*

Lema 3.3.9. *Sejam G um pE-grupo finito 3-gerado e $\alpha \in End(G)$.*

i) *Se $\alpha \in Aut(G)$, então α é um automorfismo central.*

ii) *Se $\alpha \notin Aut(G)$, então $Im(\alpha) \leq Z(G)$, em que $Im(\alpha)$ denota a imagem de α.*

Demonstração: Suponhamos que G não é abeliano, $exp(G') = p^t$ e $exp(G/G') = p^r$. Pelos Teoremas 3.3.2, 3.3.7 e pela Observação 3.3.8, existem elementos $a, b, c \in G$ tais que $G = \langle a, b, c \rangle$, $|a| = |b| = |c| = p^{r+t}, G^{p^t} = Z(G) = \Omega_r(G)$, e

$$G^{p^r} = G' = \langle [a, b] \rangle \times \langle [a, c] \rangle \times \langle [b, c] \rangle, |[a, b]| = |[a, c]| = |[b, c]| = p^t.$$

Agora, afirmamos que $C_G(g) = \langle g \rangle Z(G)$, para cada $g \in \{a, b, c\}$. Por simetria entre a, b e c, é suficiente mostrar essa afirmação para $g = a$. Seja $x \in C_G(a)$. Então, existem inteiros i, n, m e um elemento $w \in Z(G)$ tais que $x = a^i b^n c^m w$. Como $[x, a] = 1$, obtemos $[b, a]^n [c, a]^m = 1$ e então, $n \equiv m \equiv 0 \, (mod\, p^t)$. Portanto, $x = a^i w_a$, para algum $w_a \in Z(G)$, como desejado. Logo, $a^\alpha = a^i w_a, b^\alpha = b^j w_b$ e $c^\alpha = c^k w_c$, em que $0 \leq i, j, k \leq p^t - 1$ e $w_a, w_b, w_c \in Z(G)$.

De $[(ab)^\alpha, ab] = 1$ e $[(ac)^\alpha, ac] = 1$, concluímos, respectivamente, que $i = j$ e $i = k$. Como $G^{p^r} = G'$, temos $a^{p^r} = [a, b]^s [b, c]^k [a, c]^l$ em que s, k e l são inteiros. Portanto,

$$(a^\alpha)^{p^r} = [a^\alpha, b^\alpha]^s [b^\alpha, c^\alpha]^k [a^\alpha, c^\alpha]^l,$$

de modo que $a^{p^r i} = a^{p^r i^2}$. Assim, $i^2 \equiv i \, (mod\, p^t)$ e então, $i = 1$ ou $i = 0$.

Se $i = 1$, então α é um automorfismo central de G. Se $i = 0$, então a imagem de α está no centro de G. ∎

Notação 3.3.10. *Dada a matriz* $A = \begin{pmatrix} i_1 & j_1 & k_1 \\ i_2 & j_2 & k_2 \\ i_3 & j_3 & k_3 \end{pmatrix}$ *denotamos* $\begin{pmatrix} k_3 & -k_2 & k_1 \\ -j_3 & j_2 & -j_1 \\ i_3 & -i_2 & i_1 \end{pmatrix}$ *por $\overline{A}$. Além disso, denotamos $adj(B)$ a matriz quadrada adjunta de B.*

Lema 3.3.11. *Sejam* $G = G(p, r, t, [m_{ij}]) = \langle a, b, c\rangle$, *tal que* $p > 2$ *ou* $(p = 2$ *e* $t \neq r)$, $M = [m_{ij}] \in GL(3, \mathbb{Z}_{p^t})$ *e* $A = \begin{pmatrix} i_1 & j_1 & k_1 \\ i_2 & j_2 & k_2 \\ i_3 & j_3 & k_3 \end{pmatrix}$. *Então, a aplicação* α, *definida por*

$$a^\alpha = a^{i_1} b^{j_1} c^{k_1} z_1, b^\alpha = a^{i_2} b^{j_2} c^{k_2} z_2, c^{i_3} b^{j_3} c^{k_3} z_3,$$

tal que $i_1, j_1, \ldots, k_3 \in \mathbb{Z}$ *e* $z_1, z_2, z_3 \in Z(G)$, *pode ser estendida a um endomorfismo de* G *se, e somente se, a igualdade* $MA = adj(\overline{A})M$ *é verdadeira no anel das matrizes sobre* $\mathbb{Z}_{p^t}$.

Demonstração: Já que $exp(G) = p^{r+t}$ e $exp(G') = p^t$, temos $x^{p^{r+t}} = [x^{p^t}, y] = 1$; para todo $x, y \in G$, pelo Teorema 3.3.2. Então, α pode ser estendido a um endomorfismo de G se, e somente se,

$$[a^\alpha, b^\alpha] = (a^\alpha)^{p^r m_{11}} (b^\alpha)^{p^r m_{12}} (c^\alpha)^{p^r m_{13}}, [a^\alpha, c^\alpha] = (a^\alpha)^{p^r m_{21}} (b^\alpha)^{p^r m_{22}} (c^\alpha)^{p^r m_{23}},$$

$$[b^\alpha, c^\alpha] = (a^\alpha)^{p^r m_{31}} (b^\alpha)^{p^r m_{32}} (c^\alpha)^{p^r m_{33}}.$$

Como $(xy)^{p^r} = x^{p^r} y^{p^r} [y, x]^{\binom{p^r}{2}} = x^{p^r} y^{p^r}$ (já que $t \leq r$), para todo $x, y \in G$ e $G^{p^r} = \langle a^{p^r}\rangle \times \langle b^{p^r}\rangle \times \langle c^{p^r}\rangle \cong C_{p^t} \times C_{p^t} \times C_{p^t}$, segue que a seguinte igualdade no anel das matrizes sobre $\mathbb{Z}_{p^t}$ vale se, e somente se, α pode ser estendido a um endomorfismo de G:

$$\begin{pmatrix} i_1 & j_1 & k_1 \\ i_2 & j_2 & k_2 \\ i_3 & j_3 & k_3 \end{pmatrix} \begin{pmatrix} m_{11} & m_{21} & m_{31} \\ m_{12} & m_{22} & m_{32} \\ m_{13} & m_{23} & m_{33} \end{pmatrix} =$$

$$\begin{pmatrix} m_{11} & m_{21} & m_{31} \\ m_{12} & m_{22} & m_{32} \\ m_{13} & m_{23} & m_{33} \end{pmatrix} \begin{pmatrix} i_1 j_2 - j_1 i_2 & i_1 j_3 - j_1 i_3 & i_2 j_3 - j_2 i_3 \\ i_1 k_2 - k_1 i_2 & i_1 k_3 - k_1 i_3 & i_2 k_3 - k_2 i_3 \\ j_1 k_2 - k_1 j_2 & j_1 k_3 - k_1 j_3 & j_2 k_3 - k_2 j_3 \end{pmatrix},$$

o que completa a demonstração. ∎

O teorema a seguir foi demonstrado, em 1995, por M. Morigi, [27]. A demonstração foi feita por contradição. Supondo que G é um p-grupo finito 3-gerado tal que $Aut(G)$ é abeliano, é possível deduzir alguma informação sobre sua estrutura. Então, pode-se mostrar que todo grupo com tal estrutura não possui nenhum automorfismo central. O que contradiz a Proposição 1.8.4.

Teorema 3.3.12 (Principal resultado de [27])**.** *Não existe um p-grupo finito não-abeliano 3-gerado que possua um grupo de automorfismos abeliano, para qualquer primo p ímpar.*

Demonstração: Ver [27]. ∎

O Teorema 3.3.12 é falso para $p = 2$, contudo é verdadeiro para certos 2-grupos, conforme diz a proposição a seguir.

Proposição 3.3.13 (Proposition 4.2 de [1]). *Não existe um 2-grupo finito G não-abeliano 3-gerado que possua um grupo de automorfismos abeliano tal que $exp(G') = 2^t$, $exp(G) = 2^{2t}$ e $t \geq 1$.*

Demonstração: A demonstração é semelhante a do Teorema 3.3.12. ∎

Lema 3.3.14. *Não existe $2\mathcal{E}$-grupo não-abeliano de ordem 64 possuindo um grupo de automorfismos abeliano.*

Demonstração: A demonstração será feita computacionalmente. Usando o GAP [12], definimos as funções:

```
gap> 2Engel:= G -> ForAll(Cartesian(G,G), a -> LeftNormedComm([a[1], a[2], a[2]])
> =One(G));
gap> AutGAbeliano:= G -> IsAbelian(AutomorphismGroup(G))=true;
gap> naoabeliano:=  G -> IsAbelian(G)=false;
```

Nos comandos que seguem, `G` é uma lista de $2\mathcal{E}$-grupos não-abelianos de ordem 64 possuindo um grupo de automorfismos abeliano.

```
gap> C:=AllSmallGroups(64, 2Engel,naoabeliano,AutGAbeliano);;
gap> i:=1;; G:=[];;
gap> while i<=Length(C) do
> j:=1;;Omegar:=[];;e:=Elements(C[i]);;
>   while j<=32 do
>     if e[j]^Exponent(C[i]/DerivedSubgroup(C[i])) = Identity(C[i]) then
>        Add(Omegar, e[j]); fi;
> j:=j+1; od;
> if  IsSubset(Centre(C[i]),Omegar)=true then
>  Add(G,C[i]);fi;
> i:=i+1;od;
```

O GAP retorna que a lista `G` é vazia. O que completa a demonstração. ∎

Teorema 3.3.15 (Theorem 1.1 de [1]). *Todo E-grupo 3-gerado é abeliano.*

Demonstração: O Teorema 3.2.14 diz que um E-grupo finito 3-gerado é nilpotente de classe no máximo 2 e o Teorema 3.2.16 diz que um E-grupo infinito 3-gerado é abeliano. Assim, para demonstrar o teorema basta mostrar que todo pE-grupo finito 3-gerado é abeliano, pelo Teorema 3.1.7.

Suponhamos, por contradição, que G é um pE-grupo não-abeliano 3-gerado. Pelos Teoremas 3.3.2 e 3.3.7 e Observação 3.3.8, existem $a, b, c \in G$ tal que $G = G(p, r, t, [m_{ij}])$; em que $M = [m_{ij}] \in GL(3, \mathbb{Z}_{p^t})$. Separamos a demonstração em dois casos

Suponhamos, inicialmente, que $p > 2$ ou $p = 2$ e $t \neq r$. Seja $H = G(p, t, t, [m_{ij}]) = \langle x, y, z\rangle$. Afirmamos que todo automorfismo de H é central. De fato, se $\beta \in Aut(H)$, então

$$x^\beta = x^{i_1}y^{j_1}z^{k_1}z_1, y^\beta = x^{i_2}y^{j_2}z^{k_2}z_2, z^\beta = x^{i_3}y^{j_3}z^{k_3}z_3$$

em que $z_1, z_2, z_3 \in Z(H)$ e $i_1, j_1, \ldots, k_3 \in \{0, \ldots, p^t - 1\}$. Se $A = \begin{pmatrix} i_1 & j_1 & k_1 \\ i_2 & j_2 & k_2 \\ i_3 & j_3 & k_3 \end{pmatrix}$, pelo Lema 3.3.11, segue que $MA = (adj\overline{A})M$. Agora, definimos α uma aplicação sobre G por

$$a^\alpha = a^{i_1}b^{j_1}c^{k_1}, b\alpha = a^{i_2}b^{j_2}c^{k_2}, c\alpha = a^{i_3}b^{j_3}c^{k_3}.$$

Pelo Lema 3.3.11, α pode ser estendido a um endomorfismo de G e pelo Lema 3.3.9, α é um automorfismo central ou $Im(\alpha) \leq Z(G)$.

Se $\alpha \in Aut_c(G)$, então $a^{-1}a^\alpha \in Z(G)$ e assim, $a^{i_1-1}b^{j_1}c^{k_1}Z(G) = Z(G)$. Como

$$\frac{G}{Z(G)} = \langle aZ(G)\rangle \times \langle bZ(G)\rangle \times \langle cZ(G)\rangle \text{ e } |aZ(G)| = |bZ(G)| = |cZ(G)| = p^t,$$

segue que $i_1 = 1, j_1 = 0, k_1 = 0$. De modo semelhante, $b^{-1}b^\alpha \in Z(G)$ e $c^{-1}c^\alpha \in Z(G)$. Consequentemente, A é a matriz identidade e $\beta \in Aut_c(H)$.

Se $Im(\alpha) \leq Z(G)$, de modo análogo, obtemos que A é a matriz nula e então, $Im(\beta) \leq Z(G)$, um absurdo. Portanto, $Aut(H) = Aut_c(H)$ e todo automorfismo de H fixa os elementos de $H' = Z(H)$.

Se φ e $\psi \in Aut(H)$ são automorfismos quaisquer, então $h^{\varphi\psi} = h^{\psi\varphi}$, para todo $h \in \{x, y, z\}$, já que $Aut(H) = Aut_c(H)$. Consequentemente, $Aut(H)$ é abeliano, o que contradiz o Teorema 3.3.12 ou a Proposição 3.3.13, exceto quando $p = 2$ e $t = 1$. Nesse caso, $|H| = 64$ e pelo Lema 3.3.14 temos uma contradição.

Suponhamos, agora, que $p = 2$ e $t = r$. Pelo Lema 3.3.9, todo automorfismo de G é central, assim $Aut(G)$ é abeliano (pois $G' = Z(G)$). Assim como no primeiro caso, isso é uma contradição. ∎

Agora, provamos uma generalização do Teorema 3.2.10.

Teorema 3.3.16 (Theorem 4.3 de [1]). *Não existe um $p\mathcal{E}$-grupo G de classe 3 tal que $G = \langle x_1, \ldots, x_n\rangle$, para $n \geq 3$, e tal que para qualquer $i \in \{1, \ldots, n\}$ o conjunto $\{[x_i, x_j, x_k] \,|\, 1 \leq j < k \leq n,\ j \neq i \neq k\}$ é um subconjunto linearmente independente do 3-grupo abeliano elementar $\gamma_3(G)$.*

Demonstração: Suponhamos por contradição que G é um $p\mathcal{E}$-grupo de classe 3. Sejam $exp(G/G') = p^r$ e $H = (G')^3\gamma_3(G)$. Pelo Lema 3.2.4, $[H, G] = \mho_r(H) = 1$. Módulo H temos que:

$$x_1^{3^r} = [x_1, x_2]^{m_2}[x_1, x_3]^{m_3} \dots [x_1, x_n]^{m_n} \prod_{2\leq i<j\leq n} [x_i, x_j]^{t_{ij}},$$

para $m_2, \dots, m_n, m_{ij} \in \{-1, 0, 1\}$. Como $[x_1, x_1^{3^r}] = 1$, temos que

$$\prod_{2\leq i<j\leq n} [x_1, x_i, x_j]^{t_{ij}} = 1.$$

Segue da hipótese que $t_{ij} = 0$, para todo i, j. De modo semelhante, módulo H, temos que, para $m_1, k_3, \dots, k_n \in \{-1, 0, 1\}$:

$$x_2^{3^r} = [x_2, x_1]^{m_1}[x_2, x_3]^{k_3} \dots [x_2, x_n]^{k_n} \prod_{2\leq i<j\leq n} [x_i, x_j]^{t_{ij}}.$$

Como $[x_1^{3^r}, x_2] = [x_2^{3^r}, x_1]^{-1}$, obtemos que $k_3 = m_3, \dots, k_n = m_n$.

Analogamente, módulo H,

$$x_i^{3^r} = \prod_{j=1}^{n} [x_i, x_j]^{m_j};\ , \forall i \in \{1, 2, \dots, n\}.$$

Assim, $[x_i, x_j]^{3^r} = \prod_{k=1}^{n} [x_i, x_k, x_j]^{m_k}$; para todo $i, j \in \{1, 2, \dots, n\}$. De modo que:

$$x_i^{3^{2r}} = (x_i^{3^r})^{3^r} = \prod_{j=1}^{n} [x_i, x_j]^{3^r m_j} = \prod_{j=1}^{n}\prod_{k=1}^{n} [x_i, x_k, x_j]^{m_j m_k} = 1\ , \forall i \in \{1, 2, \dots, n\}.$$

Portanto, $\mho_{2r}(G) = 1$, o que contradiz o Lema 3.2.4. ∎

Capítulo 4

Um A-grupo de classe 3

O objetivo principal deste capítulo, e de fato de toda a dissertação, é construir um p-grupo finito, G, para $p = 3$, de classe 3 tal que seus elementos comutem com suas respectivas imagens automorfas. Para isso, usamos o algoritmo de B. Eick, C. R. Leedham-Green e E. A. O'Brien descrito em [9].

4.1 Construção de um $3\mathcal{E}$-grupo de classe 3

Pelo Teorema de Levi 1.7.3, todo grupo 2-Engel sem elementos de ordem 3 é nilpotente de classe no máximo 2. Assim, um pA-grupo finito deve ser 3-grupo para ter classe 3. A. Caranti [31] questionou sobre a existência de um pE-grupo finito ou de um pA-grupo finito possuindo classe 3.

No Capítulo 3, vimos que se G é um pE-grupo de classe 3, então G deve possuir ao menos 4 geradores. Além disso, já foi mostrado que todo 3E-grupo com ordem menor ou igual a 3^{10} é nilpotente com classe igual a 2. Nesta seção, construiremos um $3\mathcal{E}$-grupo de classe 3, já que pelo Teorema 3.1.3 um pA-grupo deve ser um $p\mathcal{E}$-grupo.

De agora em diante, G denotará o grupo tal como descrito a seguir, a menos que seja explicitado o contrário. Consideraremos o maior grupo 2-Engel, G, de expoente 27 gerado por $x_1, \ldots, x_9$ tais que satisfaçam as seguintes relações definidoras:

$$
\begin{aligned}
x_1^3 &= [x_2, x_3][x_4, x_5][x_6, x_7][x_8, x_9] & \qquad x_6^3 &= [x_1, x_7][x_2, x_9][x_3, x_5][x_4, x_8] \\
x_2^3 &= [x_1, x_3][x_4, x_6][x_5, x_8][x_7, x_9] & x_7^3 &= [x_1, x_8][x_4, x_9][x_3, x_6][x_2, x_5] \\
x_3^3 &= [x_1, x_2][x_4, x_7][x_5, x_9][x_6, x_8] & x_8^3 &= [x_1, x_9][x_3, x_4][x_2, x_7][x_5, x_6] \\
x_4^3 &= [x_1, x_5][x_2, x_6][x_3, x_9][x_7, x_8] & x_9^3 &= [x_1, x_6][x_3, x_8][x_2, x_4][x_5, x_7], \\
x_5^3 &= [x_1, x_4][x_2, x_8][x_3, x_7][x_6, x_9]
\end{aligned}
$$

esse grupo foi construído por A. Abdollahi, A. Faghihi e A. Mohammadi Hassanabadi em [2].

Nosso propósito é mostrar que o grupo descrito anteriormente é um A-grupo de classe de nilpotência 3. Usando o ANU Nilpotent Quotient, um pacote de W. Nickel

[30], disponível no GAP [12], podemos construir uma apresentação por potências e conjugados, conforme descrito em A.1.

Com isso, obtemos:

$$|G| = 3^{84}; |G'| = 3^{75}; |Z(G)| = 3^{39};\ \text{e}\ exp(G/G') = 3;$$

tal que $G' = Z_2(G) \cong C_9^{39} \times C_3^3$; $\Omega_1(G') = \gamma_3(G) = Z(G) \cong C_3^{39}$.

Como todo comutador $[x_i, x_j]$ aparece uma única vez nas relações definidoras acima, segue que:

$$\langle x_1^3, \ldots, x_9^3 \rangle = \langle x_1^3 \rangle \ldots \langle x_9^3 \rangle.$$

Além disso, segue pelo Lema 1.7.4, que $G^3 = \langle x_1^3, \ldots, x_9^3 \rangle (G')^3$ e que G é regular, portanto, $|G^3| = 3^{45}$.

Pela regularidade de G, e pela Proposição 1.6.6, temos que

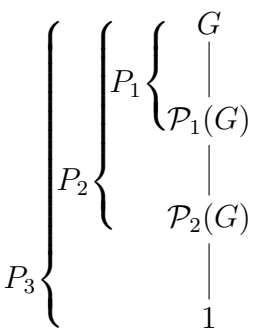
$$|\Omega_1(G)| = |G : G^3| = 3^{39}.$$

Como $\Omega_1(G) = \gamma_3(G) = Z(G)$, segue que G é 3$\mathcal{E}$-grupo de classe 3.

Teorema 4.1.1 (Theorem 1.2 de [3]). *$Aut(G) = Aut_c(G)Inn(G)$. Em particular, G é um A-grupo.*

Para demonstrar o Teorema 4.1.1, usamos o algoritmo de B. Eick, C. R. Leedham-Green e E. A. O'Brien [9], cuja implementação está disponível no GAP [12] e MAGMA [4].

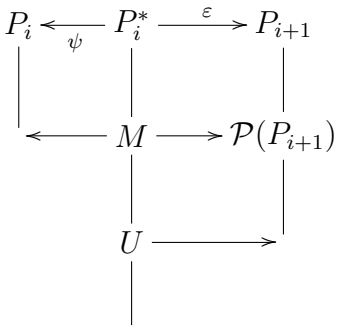
O algoritmo descrito em [9] procede por indução sobre os termos da série p-central inferior de um p-grupo finito G. Definindo $P_i = G/\mathcal{P}_i(G)$, é calculado $Aut(P_i(G))$. Como $P_1 = G/\mathcal{P}_1(G)$ é um grupo abeliano elementar, $Aut(P_1) \cong GL(d, p)$ (onde d é o número de geradores de G). Assumimos, por indução, que já conhecemos $Aut(P_i)$, para algum $i \geq 1$. Desejamos encontrar um conjunto de geradores de $Aut(P_{i+1})$, o que será possível tendo em vista os resultados do Capítulo 2, em particular o Lema 2.5.16.



Do Teorema 2.5.5, como $M \leq \Phi(P_i^*)$, segue que $P_i^* = \langle g_i^*, \ldots, g_d^* \rangle$. Se tivermos uma sequência policíclica de geradores para P_i^* e P_{i+1}, podemos determinar $U := Ker(\varepsilon)$, em que $\varepsilon \colon P_i^* \twoheadrightarrow P_{i+1}$ é o epimorfismo fornecido pelo Teorema 2.5.5 . Por construção, $U \leq M$.

Descrevemos, inicialmente, a ação de $Aut(P_i)$ sobre M. Seja $m \in M$, como $M \leq \Phi(G)$, podemos escrever $m = \omega(g_1^*, \ldots, g_d^*)$, para alguma palavra ω no conjunto dos

geradores $\{g_1^*, \ldots, g_d^*\}$ de P_i^*. Seja ainda $h_i = \alpha(\psi(g_i^*)) \in P_i$. Escolhemos a pré-imagem $h_i^* \in P_i^*$ sob o epimorfismo natural $\psi\colon P_i^* \to P_i$ e definimos $\alpha_M(m) = \omega(h_1^*, \ldots, h_d^*)$.



Usando a ação de $Aut(P_i)$ sobre M, já descrita, podemos definir o estabilizador de U sob $Aut(P_i)$, $S := Stab_{Aut(P_i)}(U)$. Pelo Lema 2.5.13, as extensões dos automorfismos internos de G agem trivialmente sobre o p-multiplicador, logo, $Inn(P_i)$ estabiliza U.

Agora, pelo Teorema 2.5.15 precisamos determinar os subgrupos T e S, em que T é o núcleo do homomorfismo natural $\nu\colon Aut(P_{i+1}) \to Aut(P_i)$. Como o Lema 2.5.16 fornece uma sequência policíclica de geradores para T, a maior tarefa é construir um conjunto de geradores para S.

A técnica padrão para construir o estabilizador S de um subespaço U é listar as órbitas de U e, simultaneamente, calcular os geradores de Schreier para S, tal como é descrito em [20]. Se o tamanho da órbita é pequeno, então essa técnica é muito eficiente, o que não é o caso. Em [9] vários refinamentos são descritos para diminuir a dificuldade do cálculo do estabilizador.

Em resumo, segue o procedimento para que possamos demonstrar o Teorema 4.1.1.

Explore a estrutura do p-multiplicador M de P_i, que é um $Aut(P_i)-$módulo, pois M é um grupo abeliano elementar. Use a série de composição de M para diminuir o comprimento das órbitas construídas.

Observe do Lema 2.5.16 que $Aut(P_i)$ possui um p-subgrupo normal N, o centralizador de $V \cong G/\mathcal{P}_1(G)$ em $Aut(P_i)$ e $Aut(P_i)/N$ é isomorfo a um subgrupo de $GL(V)$, pelo Teorema 1.8.2. Em particular, a ação de N sobre M é como um subgrupo unipotente de GL(M), pelo Lema 2.4.2. E. Costi [8] descreveu um algoritmo chamado UnipotentStabiliser para descrever um representante canônico $\overline{U}$ da N-órbita do subespaço U de M, tal algoritmo foi descrito também em [9] e explicado na Seção 2.4.1. Simultaneamente, constrói-se um conjunto de geradores para o estabilizador de $\overline{U}$ em N e $t \in N$, tal que $U^t = \overline{U}$. Use o algoritmo para construir o estabilizador de U em N sem explicitar a construção de suas órbitas.

Se possível, substitua a ação de $Aut(P_i)$ pela ação de um subgrupo próprio de $Aut(P_i)$ que contém o estabilizador de U.

Se o grupo que age sobre M é solúvel, então sua série de composição ascendente determina órbitas sob os sucessivos termos da série. Em cada passo, use a propriedade que a órbita sob um subgrupo normal é um bloco da ação por permutação (pelo Lema 2.4.11).

4.2 O grupo de automorfismos de G

Lembre que G é um grupo de ordem 3^{84} e classe de nilpotência igual a 3 tal que os termos de sua série p-central inferior e série inferior coincidem. Além disso, $P_1 = G/\mathcal{P}_1(G)$ possui ordem 3^9 e $P_2 = G/\mathcal{P}_2(G)$ tem ordem 3^{45} com centro possuindo ordem igual a 3^{36}. Na Tabela 4.1, descrevemos $log_3(|P_i|)$ e os postos dos respectivos p-multiplicador M de P_i e do núcleo U do epimorfismo de P_i^* a P_{i+1}, identificando U como sendo subespaço do correspondente espaço vetorial M.

i	P_i	M	U
1	9	45	9
2	45	204	165
3	84		

Tabela 4.1: Informações sobre G

Lema 4.2.1. *Sejam $G = \mathbb{Z}_p^d$ e $A := Aut(G)$. O p-multiplicador de G, M, pode ser visto como um A-módulo de dimensão $d + \binom{d}{2}$ e pode ser escrito como $M = M_1 \oplus M_2$. Em que:*
$G = \langle x_1, \ldots, x_d | x_i^p = 1, [x_i, x_j] = 1; \forall\, 1 \leq i, j \leq d \rangle$,
$M = \langle h_j, w_{kl} \,|\, h_i = x_i^p, w_{kl} = [x_k, x_l], [x_i, h_k] = 1, [x_i, w_{kl}] = 1; \forall\, 1 \leq i, j, k, l \leq d \,\rangle$,
$M_1 = \langle w_{kl} \,|\, w_{kl} \in M; \forall\, 1 \leq k < l \leq d \,\rangle$ *e*
$M_2 = \langle h_j \,|\, h_j \in M; \forall\, 1 \leq j \leq d \,\rangle$.

Além disso, M_1 e M_2 são submódulos invariantes e irredutíveis de dimensões $\binom{d}{2}$ e d, respectivamente.

Demonstração: Temos que M possui dimensão $d + \binom{d}{2}$, pois é núcleo do epimorfismo $\psi\colon G^* \to G$, em que G^* é o p-recobrimento de G,.

Os automorfismos de G podem ser estendidos a G^* e então, podemos restringí-los a M. Desse modo, podemos definir uma ação de $Aut(G)$ sobre M.

Sabemos que M_1 e M_2 são invariantes pois, se $\phi \in Aut(G)$, então, para quaisquer inteiros j, k, l tais que $1 \leq k < l \leq d$ e $1 \leq j \leq d$:

$$\phi^*(w_{kl}) = \phi([x_k, x_l]) = [\phi(x_k), \phi(x_l)] \quad \text{e} \quad \phi^*(h_j) = \phi(x_i^p) = (\phi(x_i))^p.$$

A demonstração do lema consistirá em mostrar inicialmente que os módulos M_1

e M_2 são cíclicos e, então, mostrar que qualquer elemento de M_1 e M_2 (diferente do elemento neutro) gera o módulo todo.

Temos que M_1 e M_2 são grupos abelianos elementares de expoente p, pois M o é. Definimos $K := w_{12}A$ um módulo cíclico, mostraremos que $K = M_1$.

Definimos $\sigma_i \in Sym(d)$ tal que $\sigma_i = (12\ldots i-1\ldots i+1\ldots d)$, para qualquer $1 \leq i \leq d$ e ainda, $\phi_i \colon G \to G$ tal que $\phi_i(x_j) = x_{\sigma_i(j)}$, para todo j com $\leq j \leq d$. Temos que ϕ_i é automorfismo de G; para todo i tal que $1 \leq i \leq d$.

Como M_1 é A-módulo, para todo $f \in Aut(G)$ e $m \in M_1$ temos que $f(m) \in M_1$. Em particular, para todo $\sigma_i \in Aut(G)$ e $m \in M_1$, $\phi_i^*(m) \in M_1$. Com isso, segue que:

$$\left.\begin{array}{r} \phi_1^*(w_{12}) = \phi_1[x_1,x_2] = [x_1,x_3] = w_{13} \in K \\ \phi_1^*(w_{13}) = \phi_1[x_1,x_3] = [x_1,x_4] = w_{14} \in K \\ \phi_1^*(w_{14}) = \phi_1[x_1,x_4] = [x_1,x_5] = w_{15} \in K \\ \vdots \\ \phi_1^*(w_{1(d-1)}) = \phi_1[x_1,x_{d-1}] = [x_1,x_d] = w_{1d} \in K \end{array}\right\} \begin{array}{l}\text{temos } d-1 \text{ geradores} \\ \text{em comum com } M_1\end{array}$$

como $w_{12} = [x_1,x_2] \in K$ então, $w_{12}^{-1} = w_{21} = [x_2,x_1] \in K$:

$$\left.\begin{array}{r} \phi_1^*(w_{21}) = \phi_2[x_2,x_1] = [x_2,x_3] = w_{23} \in K \\ \phi_1^*(w_{23}) = \phi_2[x_2,x_3] = [x_2,x_4] = w_{24} \in K \\ \phi_1^*(w_{24}) = \phi_2[x_2,x_4] = [x_2,x_5] = w_{25} \in K \\ \vdots \\ \phi_1^*(w_{2(d-1)}) = \phi_2[x_2,x_{d-1}] = [x_2,x_d] = w_{2d} \in K \end{array}\right\} \begin{array}{l}\text{temos mais } d-2 \text{ geradores} \\ \text{em comum com } M_1\end{array}$$

$$\vdots \qquad \text{(continuamos o processo recursivamente)}$$

$$\left.\begin{array}{rll} \phi_1^*(w_{(d-2)(d-3)}) & = \phi_{d-2}[x_{d-2},x_{d-3}] = [x_{d-2},x_{d-1}] & = w_{(d-2)(d-1)} \in K \\ \phi_1^*(w_{(d-2)d}) & = \phi_{d-2}[x_{d-2},x_{d-1}] = [x_{d-2},x_d] & = w_{(d-2)d} \in K \end{array}\right\} \begin{array}{l}\text{temos mais 2} \\ \text{geradores em} \\ \text{comum com } M_1\end{array}$$

temos mais 1 gerador em comum com M_1:

$$\phi_1^*(w_{(d-1)(d-2)}) = \phi_{d-1}[x_{d-1},x_{d-2}] = [x_{d-1},x_d] = w_{(d-1)d} \in K$$

no total, temos $(d-1)+(d-2)+\ldots+\ldots+1 = \binom{d}{2}$ geradores em comum com os geradores de M_1. Logo, $K = M_1$ pois K é submódulo de M_1.

Seja agora, $m \in K$. Mostraremos que $mA = M_1$. Temos, para $\epsilon_{ij} \in \{0,1,\ldots,p-1\}$:

$$\begin{aligned} m &= w_{12}^{\epsilon_{12}} \ldots w_{13}^{\epsilon_{13}} w_{23}^{\epsilon_{23}} \ldots w_{2d}^{\epsilon_{2d}} \ldots w_{(d-1)d}^{\epsilon_{(d-1)d}}; \\ &= [x_1,x_2]^{\epsilon_{12}} \ldots [x_1,x_d]^{\epsilon_{1d}} [x_2,x_3]^{\epsilon_{23}} \ldots [x_2,x_d]^{\epsilon_{2d}} \ldots [x_{d-1},x_d]^{\epsilon_{(d-1)d}}. \end{aligned}$$

Sem perda de generalidade, suponhamos $\epsilon_{12} \neq 0$ e definimos $\psi_i, \in Aut(G)$ para

todo i tal que $1 \leq i \leq d$ por: $\psi_i(x_i) = x_i$ e $\psi_i(x_j) = x_j^{-1}$; $i \neq j$.

Desse modo, como $m \in mA$, seque que $\psi_1^*(m) \in K$ e $n := \psi_1^*(m).m \in K$, em que:

$$\begin{aligned} n &:= \psi_1^*(m).m = ([x_1, x_2^{-1}][x_1, x_2])^{\epsilon_{12}} \dots ([x_1, x_d^{-1}][x_1, x_d])^{\epsilon_{1d}} \\ &= [x_2, x_1]^{\epsilon_{12}} \dots [x_d, x_1]^{\epsilon_{1d}}. \end{aligned}$$

Isso pois, pela Proposição 1.1.2 e já que G^* possui classe de nilpotência 2:

$$\begin{aligned} [x_i, x_j^{-1}][x_i, x_j] &= [x_i x_j, x_j^{-1}][x_i, x_j, x_j^{-1}]^{-1} \\ &= [x_i x_j, x_j^{-1}] \\ &= x_j^{-1} x_i^{-1} x_j x_i x_j x_j^{-1} \\ &= [x_j, x_i]. \end{aligned}$$

Além disso, $\psi_2^*(n) \in K$ e $\psi_2^*(n).n = ([x_2, x_1][x_2, x_1^{-1}])^{\epsilon_{12}} = [x_1, x_2]^{\epsilon_{12}} \in mA$.

Como $\epsilon_{12} \in \{1, \dots, p-1\}$, segue que $w_{12} = [x_1, x_2] \in mA$ pois ϵ_{12} e p são coprimos. Portanto, $ma = K$ e M_1 é irredutível.

Definimos, agora, $\alpha \in Aut(G)$ com $\alpha(x_i) = x_{i+1}$, para todo i tal que $1 \leq i \leq d-1$ e $\alpha(x_d) = x_1$. Mostraremos que $L := h_1 A = M_2$.

Temos:

$$\alpha^*(h_1) = h_2 \in L;$$

$$\alpha^*(h_2) = h_3 \in L;$$

$$\vdots$$

$$\alpha^*(h_{d-1}) = h_d \in L.$$

Logo, todos os geradores de M_2 pertencem a L, que é submódulo de M_2. Segue que $L := h_1 A = M_2$ e M_2 é cíclico.

Agora, seja $l \in L$ elemento qualquer. Para mostrar que M_2 é irredutível basta mostrar que $lA = M_2$. Temos que:

$$l = h_1^{\epsilon_1} \dots h_d^{\epsilon_d} \text{ tal que } 1 \leq \epsilon_i \leq p; \forall 1 \leq i \leq d.$$

Sem perda de generalidade, suponhamos $\epsilon_1 \neq 0$ e definimos $\gamma \in Aut(G)$ tal que $\gamma(x_1) = x_1$ e $\gamma(x_i) = x_i$; para todo i tal que $2 \leq i \leq d$.

Assim, como $l \in lA, \gamma^*(l) \in lA$ temos que, $\gamma^*(l).l = h_1^{2\epsilon_1} \in lA$. Mas, $\epsilon_1 \in \{1, \dots, p-1\}$, o que mostra que $h_1 \in lA$, pois ϵ_1 e p são coprimos. Portanto, $lA = L = M_2$ e M_2 é irredutível.

Logo, M_1 e M_2 são submódulos irredutíveis de M tal que todo elemento de M pode ser escrito como um elemento de M_1 mais um elemento de M_2, ou seja, $M = M_1 + M_2$.

Falta mostrar que $M_1 \cap M_2 = \{1\}$.

Suponhamos que $M_1 \cap M_2 \neq \{1\}$, então:

$$p^{d+\binom{d}{2}} = |M| = |M_1 + M_2| = \frac{|M_1||M_2|}{|M_1 \cap M_2|} = \frac{p^{\binom{d}{2}}.p^d}{|M_1 \cap M_2|} < p^{d+\binom{d}{2}}.$$

O que é absurdo. Segue assim, que $M = M_1 \oplus M_2$. ∎

Lema 4.2.2 (Lemma 3.1 de [3]). *$Aut(P_2) = Aut_c(P_2)$.*

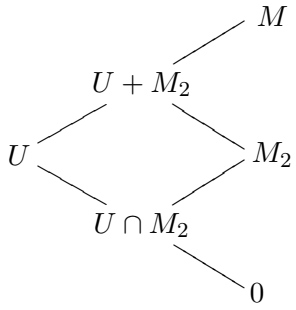
Demonstração: Temos que $A = Aut(P_1) \cong GL(9,3)$, pois P_1 é abeliano elementar, além disso, $M = M_1 \oplus M_2$, conforme o Lema 4.2.1. Como M_1 é gerado por comutadores, e já que $[x,y] = -[y,x]$, segue que a ação de A sobre M_1 é a representação do quadrado alternado $\Lambda^2(V)$, em que $V = GF(3)^9$. E ainda, podemos dizer que a ação de A restrita M_2 é como $GL(V)$.

O GAP fornece que os geradores de U (ver A.2) são $u_1, \ldots, u_9$ tais que:

$$\begin{aligned}
u_1 &:= x_1^{-3}[x_2,x_3]^2[x_4,x_5]^2[x_6,x_7]^2[x_8,x_9]^2 & u_6 &:= x_6^{-3}[x_1,x_7]^2[x_2,x_9]^2[x_3,x_5]^2[x_4,x_8]^2\\
u_2 &:= x_2^{-3}[x_1,x_3]^2[x_4,x_6]^2[x_5,x_8]^2[x_7,x_9]^2 & u_7 &:= x_7^{-3}[x_1,x_8]^2[x_4,x_9]^2[x_3,x_6]^2[x_2,x_5]^2\\
u_3 &:= x_3^{-3}[x_1,x_2]^2[x_4,x_7]^2[x_5,x_9]^2[x_6,x_8]^2 & u_8 &:= x_8^{-3}[x_1,x_9]^2[x_3,x_4]^2[x_2,x_7]^2[x_5,x_6]^2\\
u_4 &:= x_4^{-3}[x_1,x_5]^2[x_2,x_6]^2[x_3,x_9]^2[x_7,x_8]^2 & u_9 &:= x_9^{-3}[x_1,x_6]^2[x_3,x_8]^2[x_2,x_4]^2[x_5,x_7]^2.\\
u_5 &:= x_5^{-3}[x_1,x_4]^2[x_2,x_8]^2[x_3,x_7]^2[x_6,x_9]^2
\end{aligned}$$

E, sendo:

$$\begin{aligned}
w_1 &:= [x_2,x_3]^2[x_4,x_5]^2[x_6,x_7]^2[x_8,x_9]^2 & w_6 &:= [x_1,x_7]^2[x_2,x_9]^2[x_3,x_5]^2[x_4,x_8]^2\\
w_2 &:= [x_1,x_3]^2[x_4,x_6]^2[x_5,x_8]^2[x_7,x_9]^2 & w_7 &:= [x_1,x_8]^2[x_4,x_9]^2[x_3,x_6]^2[x_2,x_5]^2\\
w_3 &:= [x_1,x_2]^2[x_4,x_7]^2[x_5,x_9]^2[x_6,x_8]^2 & w_8 &:= [x_1,x_9]^2[x_3,x_4]^2[x_2,x_7]^2[x_5,x_6]^2\\
w_4 &:= [x_1,x_5]^2[x_2,x_6]^2[x_3,x_9]^2[x_7,x_8]^2 & w_9 &:= [x_1,x_6]^2[x_3,x_8]^2[x_2,x_4]^2[x_5,x_7]^2,\\
w_5 &:= [x_1,x_4]^2[x_2,x_8]^2[x_3,x_7]^2[x_6,x_9]^2
\end{aligned}$$



temos que o estabilizador em A do 18- dimensional A-módulo $U + M_2 = \langle u_1, \ldots, u_9, h_1, \ldots h_9\rangle = \langle w_1, \ldots, w_9, h_1, \ldots h_9\rangle$ contém o estabilizador de U em A.
Do mesmo modo, $W = \dfrac{U+M_2}{M_2} = \langle w_1 + M_2, \ldots, w_9 + M_2\rangle$ é 9- dimensional A- módulo e temos que seu estabilizador em A possui o estabilizador de U em A.

Vamos então determinar o estabilizador de W em A, $Stab_A(W)$.

Como a ação de A sobre M_1 é a representação do quadrado alternado $\Lambda^2(V)$, para cada elemento não-nulo em W, $w + M_2$, podemos determinar uma forma bilinear anti-simétrica 9×9 da seguinte forma: associamos $w + M_2$ ao vetor de expoentes de w sob os

geradores de M_1, digamos $\epsilon_w := [\epsilon_1, \ldots, \epsilon_{36}]$. A matriz que representa a forma bilinear mencionada é dada por:

$$E_w = \begin{bmatrix} 0 & \epsilon_1 & \epsilon_2 & \epsilon_3 & \epsilon_4 & \epsilon_5 & \epsilon_6 & \epsilon_7 & \epsilon_8 \\ -\epsilon_1 & 0 & \epsilon_9 & \epsilon_{10} & \epsilon_{11} & \epsilon_{12} & \epsilon_{13} & \epsilon_{14} & \epsilon_{15} \\ -\epsilon_2 & -\epsilon_9 & 0 & \epsilon_{16} & \epsilon_{17} & \epsilon_{18} & \epsilon_{19} & \epsilon_{20} & \epsilon_{21} \\ -\epsilon_3 & -\epsilon_{10} & -\epsilon_{16} & 0 & \epsilon_{22} & \epsilon_{23} & \epsilon_{24} & \epsilon_{25} & \epsilon_{26} \\ -\epsilon_4 & -\epsilon_{11} & -\epsilon_{17} & -\epsilon_{22} & 0 & \epsilon_{27} & \epsilon_{28} & \epsilon_{29} & \epsilon_{30} \\ -\epsilon_5 & -\epsilon_{12} & -\epsilon_{18} & -\epsilon_{23} & -\epsilon_{27} & 0 & \epsilon_{31} & \epsilon_{32} & \epsilon_{33} \\ -\epsilon_6 & -\epsilon_{13} & -\epsilon_{19} & -\epsilon_{24} & -\epsilon_{28} & -\epsilon_{31} & 0 & \epsilon_{34} & \epsilon_{35} \\ -\epsilon_7 & -\epsilon_{14} & -\epsilon_{20} & -\epsilon_{25} & -\epsilon_{29} & -\epsilon_{32} & -\epsilon_{34} & 0 & \epsilon_{36} \\ -\epsilon_8 & -\epsilon_{15} & -\epsilon_{21} & -\epsilon_{26} & -\epsilon_{30} & -\epsilon_{33} & -\epsilon_{35} & -\epsilon_{36} & 0 \end{bmatrix} \in \Lambda^2(V).$$

Construímos, assim, um algoritmo no GAP para determinar os postos dessas formas como descrito em A.3. Desse modo, podemos ver que precisamente 4 dessas formas possuem posto 4, 956 dessas formas possuem posto 6 e 18.722 possuem posto 8.

Essas quatro formas de posto 4 ocorrem em pares, $\{\gamma, -\gamma\}$ e $\{\zeta, -\zeta\}$. Além disso, as matrizes que representam γ e ζ são, respectivamente:

$$[\gamma] = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ -1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ -1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & 0 & 0 & 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & 0 & 0 & 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 & -1 & 0 & 0 & 1 & 1 \\ -1 & -1 & -1 & -1 & -1 & 0 & 0 & 1 & 1 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 & 0 & 0 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 & 0 & 0 \end{bmatrix}$$

e

$$[\zeta] = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ -1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 \\ -1 & -1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ -1 & -1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 & 0 & 0 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 & 0 & 0 & 1 & 1 & 1 \\ -1 & 0 & -1 & -1 & -1 & -1 & 0 & 1 & 1 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 & 0 & 1 \\ 0 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & 0 \end{bmatrix}.$$

Note que se $C = Stab_A(\gamma) \cap Stab_A(\zeta)$, então $Stab_A(W) \leq C$ e, assim,

$$Stab_A(W) \subseteq Stab_C(W).$$

Mudamos, então, a base dessas formas para que a matriz que representa tais formas seja da forma

$$J = \begin{bmatrix} \tilde{J} & 0 \\ 0 & 0 \end{bmatrix} \quad \text{tal que, } \tilde{J} = \begin{bmatrix} 0 & I_2 \\ -I_2 & 0 \end{bmatrix}.$$

Temos que J é uma forma bilinear anti-simétrica. Como já foi visto, uma matriz A respeita essa forma anti-simétrica se $A^T JA = J$. Assim, escrevendo

$$A = \begin{bmatrix} B & C \\ D & E \end{bmatrix}$$

em que, $B \in Mat_{(4\times4,3)}$, $C \in Mat_{(4\times5,3)}$, $D \in Mat_{(5\times4,3)}$, e $E \in Mat_{(5\times5,3)}$, temos que devem valer as igualdades sobre A:

$$B^T\tilde{J}B = \tilde{J},\ C^T\tilde{J}B = 0,\ B^T\tilde{J}C = 0 \text{ e } C^T\tilde{J}C = 0.$$

Logo, B deve ser uma matriz simplética que, pela Proposição 1.9.18, possui determinante 1 e uma vez que $\tilde{J}$ é não-singular, temos que $C = 0$. Como a matriz A procurada é não-singular, precisamos que E também seja não-singular. Dessa maneira, devemos ter que $B \in Sp(4,3)$, $C = 0, E \in GL(5,3)$ e $D \in Mat_{(5\times4,3)}$, o que significa que o estabilizador de J é da forma

$$\begin{bmatrix} Sp(4,3) & 0 \\ * & GL(5,3) \end{bmatrix},$$

em que sua ordem é $3^{20}|Sp(4,3)||GL(5,3)|$.

Além disso, o subgrupo das matrizes da forma

$$\begin{bmatrix} I_4 & 0 \\ * & I_5 \end{bmatrix}$$

é normal a esse estabilizador e o quociente é isomorfo ao produto direto $Sp(4,3) \times GL(5,3)$.

Portanto, podemos escrever os estabilizadores de γ e ζ como um subgrupo de $GL(V)$ da forma $3^{20} \cdot (Sp(4,3) \times GL(5,3))$, voltando essa matriz para a base canônica (inicial) de γ e de ζ. Essa transformação foi justificada na Seção 1.9 e os cálculos feitos no GAP estão descritos em A.4.

Na prática, calculamos esses estabilizadores com a ajuda do GAP, observando que o grupo simplético $Sp(4,3)$ contido no GAP não possui os geradores que queremos e, por isso esse grupo foi construído a partir dos seguintes geradores:

$$\begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \quad \text{e} \quad \begin{bmatrix} 0 & 1 & 1 & 0 \\ -1 & -1 & 1 & -1 \\ 1 & 1 & 1 & -1 \\ 0 & -1 & 1 & 0 \end{bmatrix}.$$

Para determinar a interseção, C, dos dois estabilizadores, o qual fixa γ e ζ, foi usado uma representação por permutação desses grupos (ver A.5), já que por a ordem dos grupos ser muito grande e por se tratarem de grupos de matrizes, o GAP é pouco eficiente nesse cálculo. Pode-se, também, usar o algoritmo de P. A. Brooksbank e E. A. O'Brien descrito em [6].

Essa interseção possui ordem $2^{11} \times 3^{23}$ e contém o estabilizador de U em A. Assim, basta mostrar que o estabilizador de U em C é trivial, pois nesse caso temos que, pelo Teorema 2.5.15, $Aut(P_2) = T$, onde T é definido como no Lema 2.5.16.

Os autores de [3] sugerem o cálculo do estabilizador de U em A a partir do normalizador de C, N (que, consequentemente, contém o estabilizador de U em A). Isso porque N é normal em A, o que possibilita o uso do algoritmo descrito em [9], o qual foi explicado na Seção 2.4.2, para mostrar que $Stab_N(U)$ é trivial, a partir do Lema 2.4.12. Esse normalizador também pode ser calculado via representação permutacional e possui ordem $2^{14} \times 3^{23}$.

Da mesma forma, usando a representação permutacional e com um pouco mais de cálculos no GAP (ver A.6), segue que $Stab_N(U)$ é trivial, e segue o resultado. ∎

Agora, para determinar $Aut(P_3) = Aut(G)$ procedemos de maneira análoga a descrita para determinamos $Aut(P2)$. Assim, precisamos construir $Stab_A(U)$, em que $U = Ker\,\varepsilon$ tal que $\varepsilon\colon P_2^* \longrightarrow G$ é o epimorfismo natural.

Lema 4.2.3. *Seja $U = Ker\,\varepsilon$ tal que $\varepsilon\colon P_2^* \longrightarrow G$ é o epimorfismo natural. Então, $Stab_A(U) = Inn(P_2)$.*

Demonstração: Sabemos que $Inn(P_2) \subseteq Stab_A(U)$, pois, pelo Lema 2.5.13, as extensões dos automorfismos internos de G agem trivialmente sobre o p-multiplicador, logo $Inn(P_2)$ estabiliza U.

Seja $A = Aut(P_2)$. Temos que P_2 é um 3-grupo 9-gerado cujo centro possui ordem 3^{36}. Portanto, segue que, pelo Lema 4.2.2, $|A| = |Aut_c(P_2)| = 3^{324}$ (pois $324 = 9 \times 36$). A age sobre M, o p-multiplicador de P_2, como um subgrupo unipotente de $GL(204,3)$, pela Proposição 2.4.2, já que A é um 3-grupo.

Os autores de [3] sugerem o uso do algoritmo UnipotentStabiliser, tal como foi descrito na subseção 2.4.1, para construir $Stab_A(U)$ e dessa maneira, mostraram que não existe nenhum automorfismo externo em A que estabiliza U.

Devido as ordens elevadas dos grupos em questão, é necessário o uso computacional (como o GAP [12] ou Magma [4]) para construir o estabilizador de U em A. Contudo, não conseguimos implementar tal algoritmo computacionalmente.

De qualquer forma, consideramos que este lema é verdadeiro, uma vez que já foi mostrado em [3]. ∎

Demonstração do Teorema 4.1.1:

Pelo Lema 4.2.3, $Stab_A(U) = Inn(P_2)$, em que $U = Ker\,\varepsilon$ tal que $\varepsilon\colon P_2^* \longrightarrow G$ é o epimorfismo natural.

Agora, observando que $P_3 = G$, pelo Teorema 2.5.15, se $\nu\colon Aut(G) \to Aut(P_2)$ é o homomorfismo natural em que $T = Ker(\nu)$ e $S = im(\nu)$ então, $Aut(G) = TR$, tal que R é uma pré-imagem qualquer de S sob ν. Mas, $S = Stab_A(U) = Inn(P_2)$ e, assim, $R = Inn(G)$. Pelo Lema 2.5.16 e lembrando que $\mathcal{P}_2(G) = Z(G)$, segue que $T = Aut_c(G)$. Assim, $Aut(G) = Aut_c(G)Inn(G)$.

Em particular, o grupo G, descrito anteriormente, é um exemplo de 3-grupo com classe 3 que é A-grupo.

Seja $x \in G$. Se $\alpha \in Aut(G)$, então existem $\sigma \in Aut_c(G), \gamma_g \in Inn(G)$ tais que $\alpha = \sigma\gamma_g$, logo, $\alpha(x) = \sigma\gamma_g(x) = \sigma(\gamma_g(x)) = \gamma_g(x).z$; para algum $z \in Z(G)$.

Dessa forma, $[x, \alpha(x)] = [x, \gamma_g(x).z] = [x, \gamma_g(x)] = [x, x^g] = [x, x[x, g]] = [x, [x, g]]$. Como G é 2-Engel, x comuta com $[g, x]$. Logo, comuta com $[x, g]$ e, assim, x comuta com x^g. Portanto, $[x, \alpha(x)] = 1$. ∎

4.3 Sobre o problema de A. Caranti

A questão inicial de A. Caranti foi publicada em seu artigo "Finite p-groups of exponent p^2 in which each element commutes with its endomorphic images" [7] e foi dividida em três itens:

a) Existe um 3E-grupo finito G com $cl(G) = 3$?

b) Existe um p-grupo finito G com $cl(G) > 2$ e $Aut(G) = Aut_c(G)Inn(G)$?

c) Existe um grupo 2-Engel G satisfazendo b)?

I. Malinowska respondeu o item b) em seu artigo "On automorphism groups of finite p-groups" [25] de forma afirmativa mostrando que o p-grupo G de menor ordem tal que $Aut(G) = Aut_c(G)Inn(G)$ possui ordem p^6 e classe de nilpotência igual a 3. Além disso, mostrou que para cada primo $p > 2$ e para todo inteiro $n \geq 7$ existe um p-grupo

G de ordem p^n com $Aut(G) = Aut_c(G)Inn(G)$ e seu grupo de automorfismo é um p-grupo de classe de nilpotência menor do que a classe de nilpotência de G.

Segue um dos exemplos dados por I. Malinowska nesse artigo [25] que responde afirmativamente o item b) do problema de A. Caranti:

Exemplo 4.3.1. *Considere o grupo G com a seguinte apresentação:*

$$G = \langle a, b, c, d \,|\, \begin{array}{l} a^{p^2} = b^{p^2} = c^p = d^p = 1,\ [a,b] = a^p,\ [a,c] = b^p \\ [b,c] = 1,\ [a,d] = c,\ [b,d] = a^{pm}b^{pk},\ [c,d] = a^{pl}\rangle, \end{array}$$

em que $p > 3$ e $k, l, m \neq 0\,(mod\, p)$ ou $p = 3, l = 1$ e $k, m \neq 0\,(mod 3)$. Então, G possui ordem p^6, classe de nilpotência 3 e satisfaz $Aut(G) = Aut_c(G)Inn(G)$.

Vamos verificar computacionalmente apenas dois casos desse exemplo:
Caso 1: p=3 Nos comando abaixo, `F` é um grupo livre gerado pelos 4 elementos `a,b,c,d`.

```
gap>    ###  CONSTRUINDO O GRUPO G  ###
gap> R:=[a^9, b^9, c^3, d^3,
>     a^-1*b^-1*a*b*a^-3, a^-1*c^-1*a*c*b^-3, b^-1*c^-1*b*c,
>     a^-1*d^-1*a*d*c^-1, b^-1*d^-1*b*d*b^-3*a^-3,  c^-1*d^-1*c*d*a^-3];;
gap>
gap> H:=F/R;;
gap> Size(H);;
gap> G:=Image(IsomorphismPcGroup(H));;
gap> g:=GeneratorsOfGroup(G);;
gap> NilpotencyClassOfGroup(G);
3
gap> A:=AutomorphismGroup(G);;
gap> I:=InnerAutomorphismsAutomorphismGroup(A);;
gap>
gap> i:=1;; e:=Elements(A);;
gap> Autc:=[];; #lista de automorfismos centrais de G
gap> for j in [1 .. Length(e)] do
>  if  ForAll([1..4], i->Inverse(g[i])*Image(e[j],g[i]) in Center(G))
>      then Add(Autc, e[j]);
>  fi;
> od;
gap>
gap> AutC:= GroupWithGenerators(Autc);;
gap> In:=Intersection(AutC, I);;
gap>
gap> Size(AutC)*Size(I)/Size(In) = Size(A);
true
```

Caso 2: p=5 Nos comando que seguem, `F` é um grupo livre gerado pelos 4 elementos `a,b,c,d`.

```
gap>    ###  CONSTRUINDO O GRUPO G  ###
gap> R:=[a^(5^2), b^(5^2), c^5, d^5,
>     a^-1*b^-1*a*b*a^-5, a^-1*c^-1*a*c*b^-5, b^-1*c^-1*b*c,
>     a^-1*d^-1*a*d*c^-1, b^-1*d^-1*b*d*b^-5*a^-5,  c^-1*d^-1*c*d*a^-5];;
gap> H:=F/R;;
gap> Size(H);
15625
gap> G:=Image(IsomorphismPcGroup(H));;
gap> g:=GeneratorsOfGroup(G);;
gap> NilpotencyClassOfGroup(G);
3
gap> A:=AutomorphismGroup(G);;
gap> I:=InnerAutomorphismsAutomorphismGroup(A);;
gap>
gap> i:=1;; e:=Elements(A);;
gap> Autc:=[];; #lista de automorfismos centrais de G
gap> for j in [1 .. Length(e)] do
>  if  ForAll([1..4], i->Inverse(g[i])*Image(e[j],g[i]) in Center(G))
>      then Add(Autc, e[j]);
>  fi;
> od;
gap> AutC:= GroupWithGenerators(Autc);;
gap> In:=Intersection(AutC, I);;
gap> Size(AutC)*Size(I)/Size(In) = Size(A);
true
```

I. Malinowska não exigiu que seus grupos apresentados em [25] fossem 2-Engel. Assim, ela não respondeu os outros itens do problema de A. Caranti.

A. Abdollahi, A. Faghihi e A. Mohammadi Hassanabadi [2] apresentaram o grupo descrito no Capítulo 4 e mostraram que é um $p\mathcal{E}$-grupo. A. Abdollahi, A. Faghihi, S. A. Linton, e E. A. O'Brien foram os primeiros a exibir um exemplo de um pA-grupo de classe de nilpotência 3 no artigo "Finite 3-groups of class 3 whose elements commute with their automorphic images" [3], usando para isso o grupo descrito em [2], respondendo, assim, o item c) do problema de A. Caranti, com o Teorema 4.1.1.

Como explicamos anteriormente, mostrar que um grupo é um pA-grupo não mostra, necessariamente, que tal grupo é pE-grupo. Assim, o primeiro item ainda não foi respondido. Contudo, com base nas propriedades de E-grupos e nas propriedades do grupo descrito no Capítulo 4 (estudas por esses autores e descritas nos Capítulos 3 e 4) podemos ver que tal grupo é um "candidato" a ser um pE-grupo.

Apêndice
A

O Grupo G no GAP

A.1 Construção do grupo e suas propriedades

Para a construção do grupo usamos o pacote ANU Nilpotent Quotient, um pacote de W. Nickel [30], com o comando `LoadPackage("anupq")`. Segue os comandos usado para gerar o grupo.

Iniciamos criando um grupo livre `F` e definindo algumas das relações desejadas `R`:

```
gap> F:= FreeGroup(9);; # grupo livre com 9 geradores
gap> R := [
>  F.1^(-3)*Comm(F.2,F.3)*Comm(F.4,F.5)*Comm(F.6,F.7)*Comm(F.8,F.9),
>  F.2^(-3)*Comm(F.1,F.3)*Comm(F.4,F.6)*Comm(F.5,F.8)*Comm(F.7,F.9),
>  F.3^(-3)*Comm(F.1,F.2)*Comm(F.4,F.7)*Comm(F.5,F.9)*Comm(F.6,F.8),
>  F.4^(-3)*Comm(F.1,F.5)*Comm(F.2,F.6)*Comm(F.3,F.9)*Comm(F.7,F.8),
>  F.5^(-3)*Comm(F.1,F.4)*Comm(F.2,F.8)*Comm(F.3,F.7)*Comm(F.6,F.9),
>  F.6^(-3)*Comm(F.1,F.7)*Comm(F.2,F.9)*Comm(F.3,F.5)*Comm(F.4,F.8),
>  F.7^(-3)*Comm(F.1,F.8)*Comm(F.4,F.9)*Comm(F.3,F.6)*Comm(F.2,F.5),
>  F.8^(-3)*Comm(F.1,F.9)*Comm(F.3,F.4)*Comm(F.2,F.7)*Comm(F.5,F.6),
>  F.9^(-3)*Comm(F.1,F.6)*Comm(F.3,F.8)*Comm(F.2,F.4)*Comm(F.5,F.7)];;
gap> H:= F/ R;;
```

mas, `H` não é o grupo procurado. Definimos, então, uma função, a qual denominamos nos comandos que seguem por `2Engel`, que é identidade no grupo e geramos o maior grupo 2-Engel `G` de expoente 27 com os geradores já descritos.

```
gap> 2Engel:= function(x,y) return PqLeftNormComm([x,y,y]); end;;
gap>
gap> G:= Pq( H : Prime := 3, Exponent:=27, Identities := [2Engel] );;
#I  Class 1 with 9 generators.
#I  Class 2 with 45 generators.
#I  Class 3 with 84 generators.
#I  Class 3 with 84 generators.
```

O comando `Pq( H:Prime:= 3, Exponent:=27, Identities:= [2Engel])` descreve a propriedades do grupo tais como mencionadas no Capítulo 3, além disso a resposta do GAP mostra que tal grupo possui ordem 3^{84}.

A seguir descrevemos como é possível obter uma apresentação para o grupo G. Para o GAP, um grupo policíclico é diferente de um grupo finitamente gerado, assim como é diferente da sua apresentação. Logo, para obter uma apresentação para `G` precisamos, inicialmente, de um grupo finitamente gerado isomorfo a `G`, `GFp`, o que pode ser obtido com os comandos `isofp:=IsomorphismFpGroup(G)` e `GFp:=Image(isosp)`. O comando `P:=PresentationFpGroup(GFp)` retorna um registro de apresentação contendo uma cópia da apresentação de `GFp` no mesmo conjunto de geradores. `TzGoGo(P)` pode ser usado para, usando transformações de Tietze, simplificar a apresentação `P`, reduzindo o número de geradores e relatores sem aumentar muito a soma total dos comprimentos dos relatores (`length`). Assim, temos:

```
gap> P;
<presentation with 9 gens and 1653 rels of total length 60807>
```

Nos comandos que seguem, notamos as propriedades já afirmadas no Capítulo 3.

```
gap> NilpotencyClassOfGroup(G);
3
gap> DerivedSubgroup(G); # o subgrupo derivado de G
<pc group of size 608266787713357709119683992618861307 with 75 generators>
gap> Frat:=FrattiniSubgroup(G);; # o subgrupo de Frattini de G
gap> Size(Frat) = 3^75;
true
gap> StructureDescription(Frat);
"C9 x C9 x C9 x C9 x C9 x C9 x C9 x C9 x C9 x C9 x C9 x C9 x C9 x C9 x C\
9 x C9 x C9 x C9 x C9 x C9 x C9 x C9 x C9 x C9 x C9 x C9 x C9 x C9 x C9 \
x C9 x C9 x C9 x C9 x C9 x C3 x C3 x C3"
gap>
gap> GFrat:=  G/Frat;;
gap> Exponent(GFrat);
3
gap> Size (GFrat) = 3^9;
true
gap> IsElementaryAbelian(GFrat);
true
gap> ZG:= Center(G);;
gap> Size(ZG) = 3^39;
true
gap> IsElementaryAbelian(ZG);
true
```

Finalmente, o GAP nos mostra as relações entre as séries centrais inferior, superior e p-central inferior:

```
gap> P:= PCentralSeries( G, 3 );; # serie p-central inferior
gap> P1:= G / P[2];;
gap> P2:= G / P[3];;
gap> P3:= G / P[4];;
gap> Size(P1) = 3^9; Size(P2) = 3^45; Size(P3) = 3^84;
true
true
true
gap> gamma := LowerCentralSeries( G );; # serie central inferior
gap>
gap> gamma[1]=P[1;; gamma[2]=P[2]; gamma[3]=P[3]; gamma[4]=P[4];
true
true
true
true
gap> z:=UpperCentralSeriesOfGroup(G);; # serie central superior
gap>
gap> z[1]=P[1]; z[2]=P[2]; z[3]=P[3]; z[4]=P[4];
true
true
true
true
```

A.2 p-recobrimento de P_1

Nos comandos abaixo, `PCover1` define o p-recobrimento de P_1, ou seja, é o grupo P_1^*. Além disso, como P_1, P_2 e P_1^* são 9-gerados podemos considerar apenas os 9 primeiros geradores fornecidos pelo GAP para gerar cada um desses grupos.

```
gap> PCover1:= PqPCover( P1 : Prime := 3 );;
gap>
gap> allgenP1:= GeneratorsOfGroup(P1);;
gap> allgenPCover1:=GeneratorsOfGroup(PCover1);;
gap> allgenP2:=GeneratorsOfGroup(P2);;
gap>
gap> genP1:=List([1..9], i -> allgenP1[i]);;
gap> genPCover1:=List([1..9], i -> allgenPCover1[i]);;
gap> genP2:=List([1..9], i -> allgenP2[i]);;
```

Os Teoremas 2.5.3 e 2.5.5 garantem a existência de um epimorfismo entre P_1^* e P_1, definido a seguir como `psi`, bem como entre P_1^* e P_2, definido como `epsilon`. Além disso, o p-multiplicador `M`, o núcleo do epimorfismo `psi`, é decomposto em dois

submódulos `M1` e `M2`, como descrito no Lema 4.2.1. E ainda, definimos o núcleo do epimorfismo `epsilon` como sendo `U`.

```
gap> psi:=GroupHomomorphismByImages(PCover1, P1, genPCover1, genP1);;
gap> M:=Kernel(psi);;   # p-multiplicador
gap> genM:=GeneratorsOfGroup(M);;
gap> genM1:=List([1..36], i -> genM[i]);;
gap> genM2:=List([37..45], i -> genM[i]);;
gap> M1:= GroupWithGenerators(genM1);;
gap> M2:= GroupWithGenerators(genM2);;
gap>
gap> epsilon:=GroupHomomorphismByImages(PCover1, P2, genPCover1, genP2);;
gap> U:=Kernel(epsilon);;
gap> allgenU:=GeneratorsOfGroup(U);;
```

Feito isso, podemos descrever os geradores de `U` em função do conjunto minimal de geradores de `PCover1` (P_1^*).

```
gap> f9:=FreeGroup("a", "b", "c", "d", "e", "f", "g", "h", "i");;
gap> phi:=GroupHomomorphismByImages(f9, PCover1, GeneratorsOfGroup(f9),
> genPCover1);;
gap>
gap> genU:= List( allgenU, u -> PreImagesRepresentative(phi, u));; # geradores de U
```

Como já sabemos quais são os geradores dos grupos W e M_1, apenas definimos eles para o GAP. Para cálculos futuros, definimos, a partir dos geradores de `PCover1`, `geradoresdeM1`, os geradores de `M1` (agora visto como grupo finitamente apresentado). Para simplificar os comandos usados, definimos `TW`, o conjunto dos representantes das classes laterais de $U + M_2$ em M_2.

A.3 Algoritmo que associa aos elementos de W uma forma bilinear

Para contar, agora, as formas descritas na demonstração do Lema 4.2.2 criamos um algoritmo, como feito a seguir, em que foi preciso usar a propriedade de que `W` é um grupo finitamente apresentado, e explicitar isso para o GAP com um isomorfismo.

O algoritmo determina o vetor expoente de cada elemento do grupo `W` e constrói a matriz correspondente para assim, calcular o posto dessa matriz e determinar quantas são as formas de posto 4. Além disso, foi pedido que o GAP "imprimisse" os elementos cujo as suas matrizes correspondentes possuem posto 4 e adicionasse essas matrizes à lista `mat4`.

```
gap> MM1:=GroupWithGenerators(geradoresdeM1);;
gap> f36:=FreeGroup(36);;
gap> phim1:=GroupHomomorphismByImages(f36, MM1, GeneratorsOfGroup(f36),
> geradoresdeM1);;
gap> genm1:= List( geradoresdeM1, m -> PreImagesRepresentative(phim1, m));;
gap> w:=List( TW, t -> PreImagesRepresentative(phim1, t));;
gap> genf36:=GeneratorsOfGroup(f36);;
gap>
gap> expoentew:=function(i,x) return ExponentSumWord(x,genf36[i]);  end;;
gap>
gap>
gap> posto4:=0;; elementos4:=[];; mat4:=[];;
gap> posto6:=0;; elementos6:=[];; posto8:=0;;
gap>
gap> for e1 in [0..2] do
>     for e2 in [0..2] do
>       for e3 in [0..2] do
>          for e4 in [0..2] do
>             for e5 in [0..2] do
>                for e6 in [0..2] do
>                   for e7 in [0..2] do
>                      for e8 in [0..2] do
>                         for e9 in [0..2] do
>   omega:=w[1]^e1*w[2]^e2*w[3]^e3*w[4]^e4*w[5]^e5*w[6]^e6*w[7]^e7*w[8]^e8*w[9]^e9;
>   e:=[];;  #vetor expoente
>   for i in [1..36] do
>   exp:= expoentew(i,omega);
>     Add(e, exp);
>    od;
>  e:=Z(3)*e;  ### convertendo o vetor expoente a um vetor sobre GF(3)
>  mat:=[
>  [Z(3)*0, e[1],   e[2],    e[3],   e[4],   e[5],   e[6],   e[7],   e[8]],
>  [-e[1], Z(3)*0,  e[9],    e[10],  e[11],  e[12],  e[13],  e[14],  e[15]],
>  [-e[2], -e[9],  Z(3)*0,   e[16],  e[17],  e[18],  e[19],  e[20],  e[21]],
>  [-e[3], -e[10], -e[16],  Z(3)*0,  e[22],  e[23],  e[24],  e[25],  e[26]],
>  [-e[4], -e[11], -e[17],  -e[22], Z(3)*0,  e[27],  e[28],  e[29],  e[30]],
>  [-e[5], -e[12], -e[18],  -e[23], -e[27], Z(3)*0,  e[31],  e[32],  e[33]],
>  [-e[6], -e[13], -e[19],  -e[24], -e[28], -e[31], Z(3)*0,  e[34],  e[35]],
>  [-e[7], -e[14], -e[20],  -e[25], -e[29], -e[32], -e[34], Z(3)*0,  e[36]],
>  [-e[8], -e[15], -e[21],  -e[26], -e[30], -e[33], -e[35], -e[36], Z(3)*0]];
>  postomat:= RankMat(mat);
>  if postomat = 4 then posto4:= posto4 +1;
>  Print("omega = "); Print(omega); Print(" \n");
>  Add(elementos4, omega);
>  Add(mat4, mat);
```

```
>       fi;
>  if postomat = 6 then posto6:= posto6 +1; fi;
>  if postomat = 8 then posto8:= posto8 +1; fi;
>                         od;
>                      od;
>                   od;
>                od;
>             od;
>          od;
>       od;
>    od;
> od;

omega = f1*f24*f32*f30*f2*f23*f29*f35*f3*f19*f14*f33*f10*f5*f28*f20*f16*f27*f13*f8\
*f4*f12*f34*f21*f11*f18*f7*f26*f17*f6*f25*f15

omega = f1*f24*f32*f30*f2*f23*f29*f35*f9*f22*f31*f36*f3*f19*f14*f33*f10*f5*f28*f20\
*f4*f12*f34*f21*f11*f18*f7*f26*f17*f6*f25*f15

omega = f1*f24*f32*f30*f1*f24*f32*f30*f2*f23*f29*f35*f2*f23*f29*f35*f3*f19*f14*f33\
*f3*f19*f14*f33*f10*f5*f28*f20*f10*f5*f28*f20*f16*f27*f13*f8*f16*f27*f13*f8*f4*f12\
*f34*f21*f4*f12*f34*f21*f11*f18*f7*f26*f11*f18*f7*f26*f17*f6*f25*f15*f17*f6*f25*f15

omega = f1*f24*f32*f30*f1*f24*f32*f30*f2*f23*f29*f35*f2*f23*f29*f35*f9*f22*f31*f36\
*f9*f22*f31*f36*f3*f19*f14*f33*f3*f19*f14*f33*f10*f5*f28*f20*f10*f5*f28*f20*f4*f12\
*f34*f21*f4*f12*f34*f21*f11*f18*f7*f26*f11*f18*f7*f26*f17*f6*f25*f15*f17*f6*f25*f15

gap> posto4;
4
gap> posto6;
956
gap> posto8;
18722
```

Veja que essas quatro formas de posto 4 ocorrem em pares, $\{\gamma, -\gamma\}$ e $\{\zeta, -\zeta\}$.

A.4 O estabilizador das formas γ e ζ

Para determinar o estabilizador dessas formas, primeiro construímos o grupo simplético com os geradores que desejamos, para em seguida, definir o grupo que estabiliza tais formas na base anti-simétrica.

```
gap> gensp1:=[[1,0,1,1],[0,1,1,1],[0,0,1,0],[0,0,0,1]]*Z(3)^0;;
gap> gensp2:=[[0,1,1,0],[2,2,1,2],[1,1,1,2],[0,2,1,0]]*Z(3)^0;;
gap> Symp:=GroupWithGenerators([gensp1,gensp2]);
<matrix group with 2 generators>
```

```
gap> Size(Symp) = Size(Sp(4,3));
true
gap> gengl:=GeneratorsOfGroup(GL(5,3));
[ [ [ Z(3), 0*Z(3), 0*Z(3), 0*Z(3), 0*Z(3) ],
      [ 0*Z(3), Z(3)^0, 0*Z(3), 0*Z(3), 0*Z(3) ],
      [ 0*Z(3), 0*Z(3), Z(3)^0, 0*Z(3), 0*Z(3) ],
      [ 0*Z(3), 0*Z(3), 0*Z(3), Z(3)^0, 0*Z(3) ],
      [ 0*Z(3), 0*Z(3), 0*Z(3), 0*Z(3), Z(3)^0 ] ],
  [ [ Z(3), 0*Z(3), 0*Z(3), 0*Z(3), Z(3)^0 ],
      [ Z(3), 0*Z(3), 0*Z(3), 0*Z(3), 0*Z(3) ],
      [ 0*Z(3), Z(3), 0*Z(3), 0*Z(3), 0*Z(3) ],
      [ 0*Z(3), 0*Z(3), Z(3), 0*Z(3), 0*Z(3) ],
      [ 0*Z(3), 0*Z(3), 0*Z(3), Z(3), 0*Z(3) ] ] ]
gap> gengl1:=gengl[1];;
gap> gengl2:=gengl[2];;
gap> genstab1:=
> [ [  1,  0,  1,  1,    0,  0,  0,  0,  0 ],
>   [  0,  1,  1,  1,    0,  0,  0,  0,  0 ],
>   [  0,  0,  1,  0,    0,  0,  0,  0,  0 ],
>   [  0,  0,  0,  1,    0,  0,  0,  0,  0 ],
>   [  0,  0,  0,  0,    1,  0,  0,  0,  0 ],
>   [  0,  0,  0,  0,    0,  1,  0,  0,  0 ],
>   [  0,  0,  0,  0,    0,  0,  1,  0,  0 ],
>   [  0,  0,  0,  0,    0,  0,  0,  1,  0 ],
>   [  0,  0,  0,  0,    0,  0,  0,  0,  1 ] ]*Z(3)^0;;
gap> genstab2:=
> [ [  0,  1,  1,  0,    0,  0,  0,  0,  0 ],
>   [  2,  2,  1,  2,    0,  0,  0,  0,  0 ],
>   [  1,  1,  1,  2,    0,  0,  0,  0,  0 ],
>   [  0,  2,  1,  0,    0,  0,  0,  0,  0 ],
>   [  0,  0,  0,  0,    1,  0,  0,  0,  0 ],
>   [  0,  0,  0,  0,    0,  1,  0,  0,  0 ],
>   [  0,  0,  0,  0,    0,  0,  1,  0,  0 ],
>   [  0,  0,  0,  0,    0,  0,  0,  1,  0 ],
>   [  0,  0,  0,  0,    0,  0,  0,  0,  1 ] ]*Z(3)^0;;
gap> genstab3:=
> [ [  1,  0,  0,  0,    0,  0,  0,  0,  0 ],
>   [  0,  1,  0,  0,    0,  0,  0,  0,  0 ],
>   [  0,  0,  1,  0,    0,  0,  0,  0,  0 ],
>   [  0,  0,  0,  1,    0,  0,  0,  0,  0 ],
>   [  0,  0,  0,  0,    2,  0,  0,  0,  0 ],
>   [  0,  0,  0,  0,    0,  1,  0,  0,  0 ],
>   [  0,  0,  0,  0,    0,  0,  1,  0,  0 ],
>   [  0,  0,  0,  0,    0,  0,  0,  1,  0 ],
>   [  0,  0,  0,  0,    0,  0,  0,  0,  1 ] ]*Z(3)^0;;
```

```
gap> genstab4:=
> [ [  1,  0,  0,  0,    0,  0,  0,  0,  0 ],
>   [  0,  1,  0,  0,    0,  0,  0,  0,  0 ],
>   [  0,  0,  1,  0,    0,  0,  0,  0,  0 ],
>   [  0,  0,  0,  1,    0,  0,  0,  0,  0 ],
>   [  0,  0,  0,  0,    2,  0,  0,  0,  1 ],
>   [  0,  0,  0,  0,    2,  0,  0,  0,  0 ],
>   [  0,  0,  0,  0,    0,  2,  0,  0,  0 ],
>   [  0,  0,  0,  0,    0,  0,  2,  0,  0 ],
>   [  0,  0,  0,  0,    0,  0,  0,  2,  0 ] ]*Z(3)^0;;
gap> genstab:=[genstab1*genstab3, genstab2*genstab4];;
> #Geradores do "GL(5,4) x Sp(4,3)"
gap>
gap> ###### construindo os outros geradores
gap> for i in [1.. 5] do
> for j in [1..4] do
> k:=[
> [1,0,0,0,0,0,0,0,0],
> [0,1,0,0,0,0,0,0,0],
> [0,0,1,0,0,0,0,0,0],
> [0,0,0,1,0,0,0,0,0],
> [0,0,0,0,1,0,0,0,0],
> [0,0,0,0,0,1,0,0,0],
> [0,0,0,0,0,0,1,0,0],
> [0,0,0,0,0,0,0,1,0],
> [0,0,0,0,0,0,0,0,1]];;
> k[i+4][j]:=1;
> Add(genstab, k*Z(3)^0);
> od;
> od;
gap> Stab:=GroupWithGenerators(genstab);; ##Estabiliza matgamma e matzeta
```

Agora, fazemos uma mudança de base para achar o estabilizador dessas formas mencionadas na mesma base.

```
gap> matgamma:=[
>  [ 0, 2, 2, 2, 2, 2, 2, 2, 2],
>  [ 1, 0, 0, 2, 2, 2, 2, 2, 2 ],
>  [ 1, 0, 0, 2, 2, 2, 2, 2, 2 ],
>  [ 1, 1, 1, 0, 0, 2, 2, 2, 2 ],
>  [ 1, 1, 1, 0, 0, 2, 2, 2, 2 ],
>  [ 1, 1, 1, 1, 1, 0, 0, 2, 2 ],
>  [ 1, 1, 1, 1, 1, 0, 0, 2, 2 ],
>  [ 1, 1, 1, 1, 1, 1, 1, 0, 0 ],
>  [ 1, 1, 1, 1, 1, 1, 1, 0, 0 ]]*Z(3);;
```

```
gap> Mgamma:=[
> [ 2, 1, 2, 0, 1, 0, 0, 0, 0],
> [ 1, 0, 1, 1, 2, 2, 0, 0, 0],
> [ 0, 0, 0, 0, 0, 1, 0, 0, 0],
> [ 2, 0, 0, 0, 1, 0, 2, 0, 0],
> [ 0, 0, 0, 0, 0, 0, 1, 0, 0],
> [ 0, 0, 2, 0, 2, 0, 0, 2, 0],
> [ 0, 0, 0, 0, 0, 0, 0, 1, 0],
> [ 0, 0, 0, 0, 1, 0, 0, 0, 2],
> [ 0, 0, 0, 0, 0, 0, 0, 0, 1]]*Z(3)^0 ;;  #####matriz mudança de base para gamma
gap> teste:= TransposedMat(Mgamma)*matgamma*Mgamma;;    Display(last);
 . . 1 . . . . . .
 . . . 1 . . . . .
 2 . . . . . . . .
 . 2 . . . . . . .
 . . . . . . . . .
 . . . . . . . . .
 . . . . . . . . .
 . . . . . . . . .
 . . . . . . . . .
```

Assim, podemos converter os geradores dos estabilizadores calculados para a base canônica, como segue.

```
gap> genStabgamma:= Mgamma*genstab*Inverse(Mgamma);;
gap> Stabgamma:=GroupWithGenerators(genStabgamma);
<matrix group with 22 generators>
gap> matzeta:=[
>  [0, 1, 1, 1, 1, 1, 1, 1, 0],
>  [2, 0, 1, 1, 1, 1, 0, 1, 1],
>  [2, 2, 0, 0, 1, 1, 1, 1, 1],
>  [2, 2, 0, 0, 1, 1, 1, 1, 1],
>  [2, 2, 2, 2, 0, 0, 1, 1, 1],
>  [2, 2, 2, 2, 0, 0, 1, 1, 1],
>  [2, 0, 2, 2, 2, 2, 0, 1, 1],
>  [2, 2, 2, 2, 2, 2, 2, 0, 1],
>  [0, 2, 2, 2 ,2, 2, 2, 2, 0]]*Z(3)^0;;
```

Da mesma maneira fazemos para o estabilizador da forma ζ.

```
gap> Mzeta:=[
>  [2, 0, 2, 1, 0, 1, 1, 0, 0],
>  [1, 1, 1, 0, 2, 1, 0, 0, 0],
>  [0, 0, 2, 0, 2, 0, 0, 2, 0],
>  [0, 0, 0, 0, 0, 0, 0, 1, 0],
>  [2, 0, 0, 0, 1, 0, 0, 0, 2],
```

```
>  [0, 0, 0, 0, 0, 0, 0, 0, 1],
>  [0, 0, 0, 0, 1, 1, 0, 0, 0],
>  [0, 0, 0, 0, 0, 1, 0, 0, 0],
>  [0, 0, 0, 0, 0, 0, 1, 0, 0]]*Z(3)^0;;
gap> ####matriz mudança de base para zeta
gap> teste:= TransposedMat(Mzeta)*matzeta*Mzeta;;    Display(last);
 . . 2 . . . . . .
 . . . 2 . . . . .
 1 . . . . . . . .
 . 1 . . . . . . .
 . . . . . . . . .
 . . . . . . . . .
 . . . . . . . . .
 . . . . . . . . .
 . . . . . . . . .
```

De forma que podemos converter os geradores do estabilizador para a base canônica.

```
gap> genStabzeta:= Mzeta*genstab*Inverse(Mzeta);;
gap> Stabzeta:=GroupWithGenerators(genStabzeta);;
<matrix group with 22 generators>
```

O GAP é capaz de calcular um grupo permutacional isomorfo a um grupo dado, usando uma representação permutacional. Nos comandos que seguem, `V` é um espaço sob o corpo `GF(3)` e `A` é um grupo permutacional isomorfo a `a`, o grupo das matrizes invertíveis lineares $GL(9,3)$. Da mesma forma, `StabgammaPerm` e `StabzetaPerm` são grupos de permutação isomorfos a `Stabgamma` e `Stabzeta`, respectivamente.

```
gap> a:=GL(9,3);;
gap> V:=FullRowSpace(GF(3),9);;
gap> L:=Elements(V);;
gap> L:=Difference(L,[Zero(V)]);;
gap> Length(L);
19682
gap> A:=Action(a,L,OnPoints);
<permutation group with 2 generators>
gap>
gap> StabgammaPerm:=Action(Stabgamma,L,OnPoints);  ### representacao permutacional
<permutation group with 22 generators>
gap> Collected(Factors(Size(StabgammaPerm)));
[ [ 2, 17 ], [ 3, 34 ], [ 5, 2 ], [ 11, 2 ], [ 13, 1 ] ]
gap> StabzetaPerm:=Action(Stabzeta,L,OnPoints);  ### representacao permutacional
<permutation group with 22 generators>
gap> Collected(Factors(Size(StabzetaPerm)));
[ [ 2, 17 ], [ 3, 34 ], [ 5, 2 ], [ 11, 2 ], [ 13, 1 ] ]
```

A.5 O cálculo da interseção e do normalizador

A interseção, C, dos estabilizadores e o seu normalizador, N, podem ser calculados como segue.

```
gap> C:= Intersection(StabgammaPerm,StabzetaPerm);
<permutation group with 16 generators>
gap> Collected(Factors(Size(C)));
[ [ 2, 11 ], [ 3, 23 ] ]
gap> #### Calculando o Normalizador
gap> N:=Normalizer(A,C);
<permutation group with 19 generators>
gap> Collected(Factors(Size(N)));
[ [ 2, 14 ], [ 3, 23 ] ]
```

A.6 O cálculo do estabilizador de U em N

Segue os comandos usado para determinar que $Stab_N(U)$ é trivial. Observe que, na verdade, apenas determinamos o estabilizador dos geradores de U. Contudo, $Stab_N(U)$ deve ser um subgrupo do estabilizador que foi determinado, o que implica que $Stab_N(U)$ é trivial. Lembre que N é um grupo permutacional que age sobre L, que é um espaço vetorial sob o corpo $GF(3)$, portanto isomorfo a U. Nos comandos que seguem determinamos as posições dos geradores de U no espaço L e então, calculamos o estabilizador desejado.

```
gap> geradoresdeu:=[
> [1,0,0,0,0,0,0,0,0],
> [0,1,0,0,0,0,0,0,0],
> [0,0,1,0,0,0,0,0,0],
> [0,0,0,1,0,0,0,0,0],
> [0,0,0,0,1,0,0,0,0],
> [0,0,0,0,0,1,0,0,0],
> [0,0,0,0,0,0,1,0,0],
> [0,0,0,0,0,0,0,1,0],
> [0,0,0,0,0,0,0,0,1]]*Z(3);;
gap>
gap> u:=[];;
gap> for i in [1..9] do
> Add(u, Position(L, vetoru[i]));
> od;
gap> EstabilizadordeUemN:= Intersection(List( [1..9], i ->
>                            Stabilizer(N, u[i], OnPoints)));
Group(())
```

A.7 p-recobrimento de P_2

Nesta seção mostraremos como construir o p-recobrimento de P_2, de modo análogo à construção feita na Seção A.2. Nos comandos abaixo, `PCover2` define o p-recobrimento de P_2, ou seja, é o grupo P_2^*. Além disso, como P_2, P_3 e P_2^* são 9-gerados podemos considerar apenas os 9 primeiros geradores fornecidos pelo GAP para gerar cada um desses grupos.

```
gap> PCover2:= PqPCover( P2 : Prime := 3 );;
gap> Size(PCover2)= 3^249;
true
gap> allgenP2:= GeneratorsOfGroup(P2);;
gap> allgenPCover2:=GeneratorsOfGroup(PCover2);;
gap> allgenP3:=GeneratorsOfGroup(P3);;
gap>
gap> genP2:=List([1..9], i -> allgenP2[i]);;
gap> genPCover2:=List([1..9], i -> allgenPCover2[i]);;
gap> genP3:=List([1..9], i -> allgenP3[i]);;
```

Agora, definimos os epimorfismos `psi`, entre P_2^* e P_2, e `epsilon`, entre P_1^* e P_2. Além disso, definimos o p-multiplicador `M` como sendo o núcleo do epimorfismo `psi` e `U` como sendo o núcleo do epimorfismo `epsilon`. Observe que $|M| = 3^{204}$ e $|U| = 3^{165}$.

```
gap> psi:=GroupHomomorphismByImages(PCover2, P2, genPCover2, genP2);;
gap>
gap> M:=Kernel(psi);   # p-multiplicador
<pc group with 204 generators>
gap>
gap> epsilon:=GroupHomomorphismByImages(PCover2, P3, genPCover2, genP3);;
gap>
gap> U:=Kernel(epsilon);
<pc group with 165 generators>
```

De forma semelhante feita para P_1 na Seção A.2, podemos, a partir dos comandos anteriores, descrever os geradores de `U` e de `M` em função do conjunto minimal de geradores de `PCover2` (P_2^*).

Referências Bibliográficas

[1] A. ABDOLLAHI, A. FAGHIHI, and A. MOHAMMADI HASSANABADI. 3-generator groups whose elements commute with their endomorphic images are abelian. *Comm. Algebra*, (36):3783–3791, 2008.

[2] A. ABDOLLAHI, A. FAGHIHI, and A. MOHAMMADI HASSANABADI. Minimal number of generators and minimum order of a non-abelian group whose elements commute with their endomorphic images. *Comm. Algebra*, (36):1976–1987, 2008.

[3] A. ABDOLLAHI, A. FAGHIHI, S. A. LINTON, and E. A. O'BRIEN. Finite 3-groups of class 3 whose elements commute with their automorphic images. *Archiv der Mathematik*, 95:1–7, 2010.

[4] W. BOSMA, J. CANNON, and C. PLAYOUST. The MAGMA algebra system I: The user language. *J. Symbolic Computation*, (24):235–265, 1997.

[5] S. BRAZIL JÚNIOR. Condição de Engel em teoria dos grupos. Master's thesis, Universidade de Brasília, 1997.

[6] P. A. BROOKSBANK and E. A. O'BRIEN. Constructing the group preserving a system of forms. *J. Symbolic Computation*, (18):227–241, 2008.

[7] A. CARANTI. Finite p-groups of exponent p^2 in which each element commutes with its endomorphic images. *J. Algebra*, (97):1–13, 1985.

[8] E. COSTI. *Constructive Membership Testing in Classical Groups*. PhD thesis, Queen Mary, University of London, 2009.

[9] B. EICK, C. R. LEEDHAM-GREEN, and E. A. O'BRIEN. Constructing the automorphism group of a p-group. *Comm. Algebra*, (30):2271–2295, 2002.

[10] R. FAUDREE. Groups in which each element commutes with its endomorphic images. *Proc. Amer. Math. Soc.*, (27):236–240, 1971.

[11] G. A. FERNÁNDEZ-ALCOBER. An introduction to finite p-groups: Regular p-groups and groups of maximal class. *Matemática Contemporânea: Atas da XVI Escola de Álgebra*, 20, 2001.

[12] The GAP Group. *GAP - Groups, Algorithms and Programming, Version 4.4.12*, 2008.

[13] M. HALL. *The Theory of groups*. New York, 1959.

[14] K. A. HIRSH. On infinite soluble groups (i). *Proceedings of the London Mathematical Society*, 44(2):53–60, 1938.

[15] K. A. HIRSH. On infinite soluble groups (ii). *Proceedings of the London Mathematical Society*, 44(2):336–414, 1938.

[16] K. A. HIRSH. On infinite soluble groups (iii). *Journal of the London Mathematical Society*, 49(2):184–94, 1946.

[17] K. A. HIRSH. On infinite soluble groups (iv). *Journal of the London Mathematical Society*, 27:81–85, 1952.

[18] K. A. HIRSH. On infinite soluble groups (v). *Journal of the London Mathematical Society*, 29:250–251, 1954.

[19] K. HOFFMAN and R. KUNZE. *Linear Algebra*. Prentice-Hall, 1961.

[20] D. F. HOLT, B. EICK, and E. A. O'BRIEN. *Handbook of Computational Group Theory*. Chapman and Hall/CRC London, 2005.

[21] B. HUPPERT. *Character theory of finite groups*. De Gruyter expositions in mathematics. Walter de Gruyter, 1998.

[22] D. L. JOHNSON. *Topics in the Theory of Group Presentations*. Cambridge University Press, 1980.

[23] R. LAUE, J. NEUBÜSER, and U. SCHOENWAELDER. Algorithms for finite soluble groups and the SOGOS system. In *Computational Group Theory*, pages 105–135, London, New York, 1984. (Durham, 1982).

[24] A. MALDONADO. Sobre o algoritmo de Newman-O'Brien para geração de p-grupos. Master's thesis, Universidade Estadual de Campinas, 1994.

[25] I. MALINOWSKA. On automorphism groups of finite p-groups. *Rend. Sem. Mat. Univ. Padova*, (91):265–271, 1994.

[26] J. J. MALONE. More in groups in which each element commutes with its endomorphic images. *Proc. Amer. Math. Soc.*, (65):209–214, 1977.

[27] M. MORIGI. On the minimal number of generators of finite non-abelian p-groups having an abelian automorphism group. *Comm. Algebra*, (23):2045–2065, 1995.

[28] M. F. NEWMAN and E. A. O'BRIEN. Application of computers to questions like those of burnside. *J. Algebra Comput.*, II(6):593–605, 1996.

[29] W. NICKEL. *Central Extensions of Polycyclic Groups*. PhD thesis, Australian National University, 1993.

[30] W. NICKEL. Computation of nilpotent Engel groups. *J. Austral. Math. Soc. Ser. A*, (67):214–222, 1999.

[31] The Kourovka Notebook. *Unsolved Problems in Group Theory*. Novosibirsk, 16 edition, 2006.

[32] E. A. O'BRIEN. The p-group generation algorithm. *J. Symbolic Computation*, pages 667–698, 1990.

[33] O. T. O'MEARA. *Symplectic Groups*. American Mathematical Society, Province, Rhode Island, 1978.

[34] D. J. S. ROBINSON. *A Course in the Theory of Groups*. Springer Verlag, New York, 2ª edition, 1995.

[35] N. R. ROCCO. Metódos de lie em teoria dos grupos. *Atas da 9ª Escola de Álgebra*, pages 129–213, 1987.

[36] J. J. ROTMAN. *An Introduction to the Theory of Groups*. Allyn and Bacon Inc., 1984.

[37] R. SCHWINGEL. *Two matrix group algorithms with applications to computing the automorphism group of a finite p-group*. PhD thesis, Queen Mary and Westfield College, University of London, 2000.

[38] D. SEGAL. *Polycyclic Groups*. Cambridge Tracts in Mathematics. Cambridge University Press, 2005.

[39] G. TRAUSTASON. Symplectic altenating algebras. *J. Algebra Comput.*, (18):719–757, 2008.