Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

Subgrupo comutador em p-grupos finitos

Débora de Faria Pereira Senise

Brasília

2024

Débora de Faria Pereira Senise

Subgrupo comutador em p-grupos finitos

Dissertação apresentada ao Departamento de Matemática da Universidade de Brasíia, como parte dos requisitos para obtenção do grau de MESTRE em Matemática.

Orientador:
Prof. Dr. Emerson Ferreira de Melo

Brasília

2024

Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

Subgrupo comutador em p-grupos finitos

por

Débora de Faria Pereira Senise

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

MESTRE EM MATEMÁTICA

Brasília, 25 de Janeiro de 2024

Comissão Examinadora:

Prof. Dr. Emerson Ferreira de Melo (UnB)

Prof. Dr. Raimundo de Araújo Bastos Júnior (UnB)

Prof. Dr. Iker de las Heras (UPV/EHU)

Resumo

Essa dissertação estuda uma condição para que, em p-grupos finitos, o subgrupo comutador coincida com o conjunto de comutadores. Baseado no artigo *"Commutators in finite p-groups with 2-generator derived subgroup"*, o foco desse trabalho é mostrar que, em um p-grupos finito G cujo subgrupo comutador G' pode ser gerado por 2 elementos, todo elemento do subgrupo comutador é um comutador. Ademais, existe $x \in G$ tal que $G' = \{[x, g] \mid g \in G\}$.

Palavras-Chaves: p-Grupos Finitos, Subgrupo Comutador, Comutadores.

Abstract

This dissertation studies a condition so that, in finite p-groups, the derived subgroup coincides with the set of commutators. Based on the article *"Commutators in finite p-groups with 2-generator derived subgroup"*, the focus of this work is to prove that, in a finite p-group G whose derived subgroup G' can be generated by 2 elements, every element of the derived subgroup is a commutator and, more than that, there exists $x \in G$ such that $G' = \{[x, g] \mid g \in G\}$.

Key-Words: Finite p-Groups, Commutator Subgroup, Commutators.

Notações

$p, q, ...$	números primos
S	conjunto
$\mathbb{N}, \mathbb{R}, \mathbb{C}$	conjunto dos naturais, reais e complexos
G, H, L, N	grupos, subgrupos
$g, h, ...$	elementos de um grupo
$\|G : H\|$	índice de H em G
$\varphi, \rho, \sigma, \phi...$	homomorfismos de grupos
$g^h = h^{-1}gh$	g conjugado por h
x^φ	φ aplicado em x, $\varphi(x)$
$[g, h] = g^{-1}h^{-1}gh$	comutador de g e h
$H^g = g^{-1}Hg$	H conjugado por g
H^φ	φ aplicado em H, $\varphi(H)$
$H \trianglelefteq G$, $H \triangleleft G$	H é normal em G, H é normal próprio de G
$[H, N] = \langle [h, n] \mid h \in H, n \in N \rangle$	comutador dos subgrupos H por N
$H \times N$	produto direto de H por N
$N \rtimes H$	produto semidireto de H por N
$N \wr H$	produto entrelaçado de N e H
H max G	H maximal em G
H max$_G$ N	H é maximal entre os subgrupos próprios de N que são normais em G
$K(G) = \{[g, h] \mid g, h \in G\}$	conjunto dos comutadores de G
$K_x(H) = \{[x, h] \mid h \in H\}$	
$[x, H] = \langle K_x(H) \rangle$	
$d(G)$	número mínimo de geradores de G
$exp(G)$	expoente de G
$Z(G)$	centro do grupo G
$C_G(x)$	centralizador de um elemento x em G
$C_G(H)$	centralizador de um subgrupo H em G
$N_G(H)$	normalizador de H em G
G'	subgrupo comutador
$\gamma_i(G)$	termos da séries central inferior

$\Phi(G)$	subgrupo de Frattini
$G^{p^i} = \langle \{x^{p^i} \mid x \in G\} \rangle$	subgrupo gerado pelas p^i-ésimas potências dos elementos de G
C_n	grupo cíclico de ordem $n \in \mathbb{N}$
$N \trianglelefteq_o G$	N é um subgrupo aberto normal de G
$\overline{H}$	fecho de H
$x \equiv y \pmod{H}$	x é congruente a y módulo H
$H \cong K$	H é isomorfo a K

Sumário

Introdução

Sejam G um grupo, G' o subgrupo comutador e $K(G) = \{[x, y] = x^{-1}y^{-1}xy \mid x, y \in G\}$ o conjunto dos comutadores de G. Logo depois da introdução de comutadores na teoria de grupos na véspera do século XX, foi observado que o conjunto $K(G)$ pode não ser um subgrupo, ou seja, o subgrupo comutador $G' = \langle K(G)\rangle$ pode ser estritamente maior que $K(G)$. Um dos primeiros exemplos foi dado por Fite ([8]) em 1902, quando ele construiu um grupo G de ordem 256 em que G' tem ordem 16 e $K(G)$ tem 15 comutadores. Então é natural perguntar-se: quando que $G' = K(G)$ e quando que $K(G) \subsetneq G'$?

Tal pergunta foi deixada de lado, até que:

"In a group the product of two commutators need not be a commutator, consequently the commutator group of a given group cannot be defined as the set of all commutators, but only as the group generated by these. There seems to exist very little in the way of criteria or investigations on the question when all elements of the commutator group are commutators." [21]

Ore fez esse comentário na introdução de [21] em 1951, desde então, muitos resultados foram feitos nessa direção.

Em 1977, Guralnick obteve na sua tese de doutorado ([11]) avanços significativos, mostrando que se (i) $|G| < 96$ ou (ii) $|G'| < 16$, então $G' = K(G)$. Assim, o exemplo de Fite possui o menor G' possível, e Guralnick também apresenta um exemplo de um grupo G de ordem 96 em que $G' \neq K(G)$, ou seja, a cota de (i) não pode ser melhorada. Em 1982, Guralnick mostra em [12] que, dado G um grupo finito e P um p-Sylow de G, se $P^* = P \cap G'$ é abeliano e $d(P^*) \leq 2$ então $P^* \subseteq K(G)$.

Esses são resultados para grupos finitos em geral, agora mais especificamente para p-grupos, ainda no artigo [12], Guralnick mostra que se G' é um p-grupo abeliano com $p > 3$ e $d(G') \leq 3$ então $G' = K(G)$. No mesmo artigo ele apresenta contra-exemplos

com $p = 2$ ou 3 e $d(G') = 3$ (Exemplos 3.5 e 3.6), mostrando que a condição falha nesses casos.

Posteriormente, outro resultado notável é o de Lieback, O'Brien, Shalev e Tiep ([17]) (The LOST Theorem - o "teorema perdido"), que em 2010 provaram a Conjectura de Ore, de que todo grupo simples G satisfaz a condição $G' = K(G)$. Claramente, isso também é verdade para grupos no outro extremo do expectro, os grupos abelianos. Mas os grupos abelianos são um exemplo trivial em que $G' = K(G)$. Uma família de grupos mais interessante que satisfaz essa condição é encontrada por Rodney, em 1974, que mostra em [23] que, em um grupo nilpotente G com G' cíclico, G' consiste de comutadores. Tal propriedade não ocorre se tirarmos a hipótese de nilpotência, como mostrado por Macdonald em 1963, em [19]. O interessante dessa coleção de resultados é ver que esse fenômeno ocorre para grupos abelianos, ocorre para os grupos "menos abelianos possíveis", os grupos simples, ocorre para algumas famílias no meio desse espectro mas para outras não, como por exemplo os grupos de Macdonald ([20]) . Uma coleção de resultados tanto da igualdade quanto da desigualdade podem ser encontrados em [13].

No artigo [6] de De Las Heras e Fernández-Alcober, que será estudado nesse trabalho, os autores generalizam o resultado de Guralnick já citado acima, mostrando que a hipótese de G' abeliano não é necessária. Portanto, o principal teorema desse trabalho é o seguinte:

Teorema A. *Seja G um p-grupo finito. Se G' pode ser gerado por 2 elementos, então exsite $x \in G$ tal que $G' = \{[x, g] \mid g \in G\}$.*

A demonstração desse teorema baseia-se em perceber que G' é necessariamente *powerful* se G é um p-grupo finito e $d(G') \leq 2$.

Como uma consequência imediata do Teorema A, obtemos o resultado abaixo sobre grupos pro-p com subgrupo comutador 2-gerado.

Teorema B. *Seja G um pro-p grupo. Se G' pode ser topologicamente gerado por 2 elementos, então existe $x \in G$ tal que $G' = \{[x, g] \mid g \in G\}$.*

Esse trabalho está dividido em três partes principais.

No Capítulo 1 serão apresentados alguns conceitos e resultados preliminares de grupos, comutadores, grupos nilpotentes, p-grupos finitos e grupos profinitos, abordando o que será necessário para os resultados posteriores. Também demonstraremos nesse capítulo a Fórmula de Compilação de Hall-Petresco, que vale para grupos em geral, não só p-grupos. Essa será muito utilizada nas demonstrações dos resultados de grupos *powerful*, no Capítulo 2, e nas demonstrações dos resultados principais, no Capítulo 3.

No Capítulo 2 é feito um estudo de grupos *powerful*, cujos resultados são feitos em

[18] por Lubotzki e Mann. As demonstrações são baseadas nos livros [16] de Khukhro e [5] de Dixon, Sautoy, Mann e Segal. Entretanto, as demonstrações foram reescritas utilizando-se a Fórmula de Compilação de Hall-Petresco demonstrada no Capítulo 2.

Por fim, utilizaremos os resultados apresentados no Capítulo 2 para, no Capítulo 3, demonstrarmos os resultados principais de De las Heras e Fernandes-Alcober.

Capítulo

1

Preliminares

Nesse capítulo abordamos a teoria que é a base para o estudo do tema principal. Veremos então o básico de comutadores e subgrupos comutadores, grupos nilpotentes, p-grupos finitos e grupos profinitos. Por serem resultados muito conhecidos em qualquer estudo introdutório desses temas, as demonstrações serão omitidas.

1.1 Definições e Resultados Básicos

Essa seção tem como objetivo estabelecer definições básicas que serão muito utilizadas ao longo de todo o trabalho.

Definição 1.1.1. *Dado um grupo G e um subconjunto S de G, o subgrupo de G gerado por S é a interseção de todas os subgrupos de G contendo S. Será denotado por $\langle S \rangle$.*

Em outras palavras, $\langle S \rangle$ é o menor subgrupo de G que contém S. É mais claro pensar que $\langle S \rangle$ contém S, os inversos dos elementos de S, e todos os produtos possíveis entre eles.

Se existir $S \subseteq G$ tal que $\langle S \rangle = G$ dizemos que S é um conjunto gerador de G, e $d(G) = min\{|S| \mid \langle S \rangle = G\}$, ou seja, $d(G)$ é o número mínimo de elementos necessário para gerar G. Se $d(G) = d$, dizemos que G é d-gerado. No caso de grupos finitos, tal subconjunto S sempre existe.

Definição 1.1.2. *Sejam G um grupo e H um subgrupo de G, então:*

- $Z(G) = \{z \in G \mid zg = gz \ \forall g \in G\}$ *é chamado* ***centro*** *de G. É o subgrupo formado pelos elementos de G que comutam com todos os elementos de G.*

- $C_G(H) = \{c \in G \mid ch = hc \ \forall h \in H\}$ *é chamado* ***centralizador*** *de* H *em* G. *É o subgrupo formado pelos elementos de* G *que comutam com todos os elementos de* H.
- $N_G(H) = \{n \in G \mid nH = Hn\}$ *é chamado* ***normalizador*** *de* G. *É o subgrupo formado pelos elementos de* G *que normalizam* H.

Definição 1.1.3. *Sejam* G *um grupo e* N *um subgrupo de* G. *O subgrupo* N *é dito* ***característico*** *em* G *se* $N^\phi = N$ *para qualquer* $\phi \in Aut(G)$.

Lema 1.1.4. *Sejam* G *um grupo, e* $N \leq H$ *subgrupos de* G. *Se* N *é característico em* H *e* H *é característico em* G, *então* N *é característico em* G. *Além disso, se* N *é característico em* H *e* H *é normal em* G, *então* N *é normal em* G

1.2 Comutadores e subgrupos comutadores

Essa seção tem como objetivo estabelecer definições e resultados básicos de comutadores que serão utilizados ao longo de todo o trabalho. Muitos resultados serão apresentados sem demonstração, para mais detalhes confira o capítulo 1 de [7]. Também veremos exemplos de quando o grupo comutador coincide com o conjunto de comutadores e exemplos de quando não coincide.

Definição 1.2.1. *O **comutador** de dois elementos x, y de um grupo G é definido por*

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

Definição 1.2.2. *Definimos composição de comutadores de um subconjunto X indutivamente pelo seu peso: os elementos de X são comutadores de peso 1; se c_1 e c_2 são comutadores de peso r_1 e r_2, então $[c_1, c_2]$ é um comutador de peso $r_1 + r_2$ de elementos de X.*

Para comutadores de peso maior que 1, normamos à esquerda:

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

Definição 1.2.3. *Definimos o **subgrupo comutador** de dois subgrupos H e K de G por:*

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

e de maneira similar definimos $[H_1, H_2, ..., H_n] = [...[H_1, H_2]..., H_n]$.

No resultado seguinte, coletamos as principais propriedades de comutadores e subgrupos comutadores.

Teorema 1.2.4 ([7], Teorema 1.7)**.** *Seja G um grupo, $x, y, z \in G$ e $H, K, L \leq G$. Então:*

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

(ii) $[x, y]^{\sigma} = [x^{\sigma}, y^{\sigma}]$ *para qualquer homomorfismo* $\sigma : G \to G \setminus \{1\}$

(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 Witt.)*

(v) $[H, K] = [K, H]$.

(vi) *K normaliza H se, e somente se, $[H,K] \leq H$, e K centraliza H se, e somente se, $[H,K] = 1$. Em particular, N é um subgrupo normal de G se, e somente se, $[N,G] \leq N$.*

(vii) *$[H,K]^\sigma = [H^\sigma, K^\sigma]$ para qualquer homomorfismo $\sigma : G \to G^*$. Em particular, o subgrupo comutador de dois subgrupos característicos (normais) de G é também característico (normal).*

(viii) *Se N é um subgrupo normal de G então $[HN/N, KN/N] = [H,K]N/N$.*

(ix) *Se HK é um subgrupo de G e H normaliza L então $[HK,L] = [H,L][K,L]$.*

Demonstraremos apenas o item (vi), que explica uma ideia essencial nesse trabalho.

Demonstração. **(vi)** Temos que K normaliza H se, e somente se, para todos $h \in H$ e $k \in K$ existe $h_1 \in H$ tal que $h^k = h_1$, equivalentemente, $h^{-1}h^k = h^{-1}h_1$, ou seja, $[h,k] \in H$ e portanto $[H,K] \in H$. E K centraliza H se, e somente se, para todos $h \in H$ e $k \in K$, $h^k = h$, equivalentemente, $h^{-1}h^k = 1$, ou seja, $[h,k] = 1$ e portanto $[H,K] = 1$.

□

Teorema 1.2.5 (Lema dos três subgrupos, [16])**.** *Sejam H, K e L subgrupos de G e N um subgrupo normal de G. Se $[H,K,L]$, $[K,L,H] \leq N$, então $[L,H,K] \leq N$.*

A próxima definição é a de um subgrupo comutador particularmente especial para toda a Teoria de Grupos e que será o personagem principal desse trabalho.

Definição 1.2.6. *Seja G um grupo, definimos o **subgrupo comutador** de G, denotado por G', como sendo*

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

Também denotamos por $G'' = [G',G']$ o subgrupo comutador de G'.

Veja que, dados $a,b \in G$, $ab = ba \cdot a^{-1}b^{-1}ab = ba[a,b]$. Logo, o comutador de a e b é o "preço" que se tem que pagar para trocar a e b de lugar.

Pela propriedade (vii) do Teorema 1.2.4, G' é característico em G. Então podemos olhar para o grupo quociente G/G' e, nesse grupo, $abG' = ba[a,b]G' = baG'$, ou seja, G/G' é abeliano. Por isso G' é também chamado de *abelianizador* de G. Além disso:

Proposição 1.2.7. *Sejam G um grupo e N um subgrupo normal de G. Se G/N é abeliano, então $G' \leq N$.*

Em outras palavras, G' é o "menor" subgrupo normal de G cujo quociente é abeliano, no sentido de que G' está dentro de qualquer outro subgrupo com a mesma propriedade.

Exemplo 1.2.8. *$S_3 = \langle (12), (123) \rangle$. Então $S_3' = \langle (123) \rangle$ e $S_3/S_3' = \langle (12)S_3' \rangle$, que é abeliano.*

Entretanto, G' é o grupo **gerado** pelos comutadores, mas não necessariamente um elemento qualquer de G' é um comutador, ou seja, G' não precisa coincidir com o conjunto de comutadores de G, como no exemplo a seguir.

Exemplo 1.2.9. *Em sua tese de doutorado Guralnick encontrou os grupos de menor ordem tais que G' não coincide com o conjunto de comutadores. Tais grupos tem ordem 96 e são isomorfos à $((C_4 \times C_2) \rtimes C_4) \rtimes C_3$ e $(C_2 \times C_2 \times Q_8) \rtimes C_3$. Veja [11] ou [10] para mais detalhes.*

Exemplo 1.2.10. *Com o objetivo de apresentar exemplos elementares de grupos em que G' não coincide com o conjunto de comutadores, em [20] Macdonald construiu, para cada n natural, grupo de matrizes n-gerados ($n \geq 3$) e provou que para $n \geq 6$ esses grupos possuem, de fato, tal propriedade.*

Mas quando que $G' = \{[x, y] \mid x, y \in G\}$ ocorre?

Exemplo 1.2.11. *Como em [11] Guralnick mostrou que um grupo G de ordem 96 é o grupo de menor ordem que satisfaz $\{[x, y] \mid x, y \in G\} \subsetneq G'$, então qualquer grupo de ordem menor que 96 satisfaz $G' = \{[x, y] \mid x, y \in G\}$.*

Exemplo 1.2.12. *Todo grupo abeliano satisfaz essa propriedade, afinal, todo comutador é trivial e $G' = 1$.*

Exemplo 1.2.13. *Temos também o LOST Theorem [17] (Teorema "Perdido"), em que Liebeck, O'Brien, Shalev e Tiep (por isso "LOST") mostraram, em 2010, que em um grupo simples não abeliano todo elemento é um comutador, provando assim a conjectura de Ore. Como em um grupo simples não abeliano temos $G = G'$, isso significa que G' coincide com o conjunto dos comutadores.*

Definição 1.2.14. *A **série central inferior** de um grupo G é definida indutivamente por meio de $\gamma_1(G) = G$ e $\gamma_{i+1} = [\gamma_i(G), G]$.*

Outra forma de escrever é $\gamma_i(G) = [G, ..., G]$, onde G se repete i vezes. Então a série central inferior é o mesmo que

$$... \leq [G, G, G] \leq [G, G] \leq G$$

Segue de (vii) do Teorema 1.2.4 que $\gamma_i(G)$ é característico em G para todo i. O próximo resultado é uma propriedade importante dessa série.

Teorema 1.2.15 ([7], Teorema 1.9)**.** *Para qualquer grupo G, $[\gamma_i(G), \gamma_j(G)] \leq \gamma_{i+j}(G)$*

Corolário 1.2.16. *Seja G um grupo. Então qualquer comutadorde peso i está no subgrupo $\gamma_i(G)$.*

Teorema 1.2.17 ([7], Teorema 1.11)**.** *Sejam G um grupo e N um subgrupo normal de G. Então $\gamma_i(G/N) = \gamma_i(G)N/N$ para todo $i \geq 1$.*

Lema 1.2.18 ([7], Seção 3.4)**.** *Se G é um grupo, $N \trianglelefteq G$, e G/N é cíclico, então $G' = [G, N]$.*

O próximo lema apresenta uma das inclusões mais utilizadas nas contas do capítulo 3, e sua demonstração utiliza a Fórmula de Compilação de Hall, que ainda será apresentada na seção 1.6 desse capítulo, mas seu enunciado diz respeito tão somente à comutadores. Considere que, dado L um grupo, $L^n = \langle x^n \mid x \in L \rangle$.

Lema 1.2.19. *Sejam G um grupo, L e N subgrupos normais de G. Então, para $n \in \mathbb{N}$, temos:*

$$[L^n, N] \leq [L, N]^n [L, N, L] \tag{1.1}$$

Demonstração. Os geradores de $[L^n, N]$ são da forma $[x, u]$, para $x \in L^n$ e $u \in N$. Se $x \in L^n$, então x é um produto de n-ésimas potências de elementos de L. Mas veja que, dados $l_1, l_2 \in L$, pela propriedade (iii) do Teorema 1.2.4,

$$[l_1^n l_2^n, u] = [l_1^n, u][l_1^n, u, l_2^n][l_2^n, u] = [l_1^n, u][l_2^n, u][l_1^n, u, l_2^n][[l_1^n, u, l_2^n], [l_2^n, u]]$$

pertence à $[L^n, N][L, N, L]$. Logo, basta mostrar que elementos da forma $[l^n, u]$, $l \in L$ e $u \in N$, estão em $[L, N]^n[L, N, L]$. De fato, pela Fórmula de Compilação de Hall-Petresco, (1.6.3):

$$[l^n, u] = l^{-n} u^{-1} l^n u = l^{-n} (u^{-1} l u)^n = (l^{-1} u^{-1} l u)^n q = [l, u]^n q$$

sendo que q é o produto de comutadores em $\gamma_2(\langle l, u \rangle)$ que aparece na Fórmula de Compilação Hall-Petresco, que será, para quaisquer l e u, um elemento de $[L, N, L]$.

□

1.3 Grupos nilpotentes

O conceito de grupos nilpotentes é importante nesse trabalho pelo fato de ser uma propriedade nata dos p-grupos. Essa seção também se baseia no capítulo 1 de [7].

Definição 1.3.1. *Um grupo G é chamado **nilpotente** se $\gamma_{c+1}(G) = 1$ para algum c. O menor c que satisfaz isso é chamado de classe de nilpotência de G.*

Veja que os grupos nilpotentes de classe 1 são precisamente os grupos abelianos. Da definição de série central inferior, fica claro que quanto maior a classe de nilpotência de um grupo, mais distante um grupo está de ser abeliano.

Observação 1.3.2. *Seja G um grupo nilpotente e N um subgrupo normal de G, então $[N, G] < N$. Afinal, se tivéssemos $[N, G] = N$, como $[N, G] \leq [G, G]$, isso implicaria que $N \leq [G, G]$ e daí $[N, G] \leq [[G, G], G]$, então $N \leq [[G, G], G]$. Seguindo assim teríamos $N = 1$. Logo, se $N \neq 1$, temos que $[N, G] < N$. Então, se G é nilpotente, a série central inferior é estritamente decresce enquanto não estabilizar no $\{1\}$:*

$$\{1\} = \gamma_{c+1}(G) \lhd \gamma_c(G) \lhd ... \lhd \gamma_2(G) \lhd \gamma_1(G) = G$$

e o mesmo ocorre com outras séries da forma:

$$\{1\} \lhd ... \lhd [N, G, G] \lhd [N, G] \lhd N$$

Em p-grupos, isso implica que $|N : [N, G]| \geq p$.

A seguir veremos que a propriedade de ser nilpotente pode ser caracterizada por uma outra série de G.

Definição 1.3.3. *Seja G um grupo. A **série central superior** de G é definida recursivamente por $Z_0(G) = 1$ e $Z_{i+1}(G)/Z_i(G) = Z(G/Z_i(G))$.*

Observe que, se H é subgrupo de G, $[H, G] \leq Z_i(G)$ se, e somente se, $H \leq Z_{i+1}(G)$. Afinal, $[H, G] \leq Z_i(G)$ significa que a imagem dos elementos de H comutam com todos os elementos de $G/Z_i(G)$. Por outro lado, se $H \leq Z_{i+1}(G)$ então $H/Z_i(G) \leq Z(G/Z_i(G))$, logo, $[H/Z_i(G), G/Z_i(G)] = Z_i(G)$, então $[H, G] \leq Z_i(G)$.

Lema 1.3.4 ([7], Lema 1.12)**.** *Seja G um grupo nilpotente de classe c. Então $\gamma_{c+1-i}(G) \leq Z_i(G)$ para todo $0 \leq i \leq c$.*

Teorema 1.3.5 ([7], Teorema 1.13)**.** *Um grupo G é nilpotente de classe c se, e somente se, $Z_c(G) = G$ e $Z_{c-1} \neq G$.*

Por isso, a classe de nilpotência de um grupo é o comprimento tanto da série central superior quanto da série central inferior.

A série central superior não é particularmente importante para esse trabalho, mas o próximo resultado sim, e ele é o motivo pelo qual vale a pena introduzi-la. No Teorema 1.4.1 vemos que $Z(G) \neq 1$ em qualquer p-grupo finito G não trivial. Dessa forma, como cada $G/Z_i(G)$ é um p-grupo, $Z(G/Z_i(G)) = Z_{i+1}(G)/Z_i(G)$ não é trivial enquanto $G/Z_i(G)$ não for trivial. Logo, a série central superior é estritamente crescente até que, para algum $c \in \mathbb{N}$, $Z_c(G) = G$. Com isso, temos o seguinte corolário:

Corolário 1.3.6 ([7], Corolário 1.14)**.** *Qualquer p-grupo finito é nilpotente.*

1.4 p-Grupos finitos

Nessa seção vamos estabelecer resultados envolvendo p-grupos, que serão o nosso principal objeto de estudo. Durante quase todo o trabalho estaremos no mundo dos p-grupos finitos, portanto as propriedades aqui enunciadas serão frequentemente utilizadas. Essa seção se baseia em [7].

Teorema 1.4.1 ([7], Teorema 1.1)**.** *Seja G um p-grupo finito e N um subgrupo normal não trivial de G. Então $N \cap Z(G) \neq 1$. Em particular, o centro de um p-grupo não trivial é não trivial.*

Corolário 1.4.2. *Seja G um p-grupo finito. Então:*

(i) *Qualquer subgrupo normal de G de ordem p é central em G.*

(ii) *Se $G/Z(G)$ é cíclico, então G é abeliano.*

(iii) *Todo p-grupo de ordem p^2 é abeliano.*

Teorema 1.4.3 ([7], Teorema 1.3)**.** *Seja G um p-grupo finito.*

(i) *Se $H < G$ então $H < N_G(H)$.*

(ii) *Se M é um subgrupo maximal de G então M é normal em G e $|G : M| = p$.*

Teorema 1.4.4 ([7], Teorema 1.4)**.** *Seja G um p-grupo finito de ordem p^m.*

(i) *Se N é um subgrupo normal de G de ordem p^k, então existe uma série*

$$1 = G_0 \leq G_1 \leq ... \leq G_k = N \leq ... \leq G_m = G \tag{1.2}$$

tal que $G_i \trianglelefteq G$ e $|G_{i+1} : G_i| = p$ para todo i. Em particular, um p-grupo possui subgrupos normais de todas as ordens possíveis.

(ii) *Se H é um subgrupo de G de ordem p^k, então existe uma série*

$$1 = G_0 \leq G_1 \leq ... \leq G_k = H \leq ... \leq G_m = G \tag{1.3}$$

tal que $G_i \trianglelefteq G_{i+1}$ e $|G_{i+1} : G_i| = p$ para todo i. Então todo subgrupo de um p-grupo é subnormal.

Definição 1.4.5. *O **expoente** de um grupo G é o menor múltiplo comum das ordens dos elementos de G. Escrevemos $exp(G)$. Em outras palavras, se $exp(G) = e$ então e é o menor número tal que $x^e = 1$ para todo $x \in G$.*

No caso de um p-grupo, o expoente é simplesmente a maior ordem entre os elementos de G.

Definição 1.4.6. *Um p-grupo G é **abeliano elementar** se é abeliano e se todos os elementos de G diferentes da unidade tem ordem p, ou seja, $exp(G) = p$.*

Pelo Teorema Fundamental dos Grupos Abelianos Finitos, se G é abeliano elementar então $G = C_p \times ... \times C_p$.

Definição 1.4.7. *Seja G um grupo, o **subgrupo de Frattini** de G é a interseção dos seus subgrupos maximais, e é denotado por $\Phi(G)$.*

Como a imagem de um subgrupo maximal de G sobre um automorfismo de G é ainda um subgrupo maximal, $\Phi(G)$ será invariante por automorfismos de G, portanto é característico. Um dos motivos pelos quais esse grupo possui um papel importante é pelo seguinte resultado:

Teorema 1.4.8 ([7], Teorema 1.5)**.** *Seja G um grupo finito e $x_1, ..., x_n \in G$. Então temos que $G = \langle x_1, ..., x_n \rangle$ se, e somente se, $G/\Phi(G) = \langle x_1\Phi(G), ..., x_n\Phi(G) \rangle$.*

Esse teorema deixa claro que os elementos fora de $\Phi(G)$ serão elementos geradores. Mais precisamente, temos:

Definição 1.4.9. *Um elemento $x \in G$ é chamado **não gerador** se, dado $S \subseteq G$, $\langle S, x \rangle = G$ implica que $\langle S \rangle = G$, ou seja, x pode ser omitido de qualquer subconjunto gerador dado.*

Lema 1.4.10. *O subgrupo de Frattini de um grupo finito coincide com o conjunto de não geradores de G.*

Demonstração. Seja $S \subseteq G$ tal que $\langle S, x \rangle = G$. Pelo Teorema 1.4.8, $\langle S, x \rangle = \langle S \rangle = G$ se, e somente se, $\langle S\Phi(G), x\Phi(G) \rangle = \langle S\Phi(G) \rangle = G/\Phi(G)$. Ou seja, x é não gerador se, e somente se, $x \in \Phi(G)$. □

No caso de p-grupos, o resultado é ainda mais forte pois o índice de $\Phi(G)$ determina o número mínimo de geradores de G.

Teorema 1.4.11 (Teorema da Base de Burnside, [7], Teorema 1.6)**.** *Seja G um p-grupo finito. Então:*

(i) *$G/\Phi(G)$ é um p-grupo abeliano elementar e consequentemente pode ser visto como espaço vetorial sobre $\mathbb{F}_p$*

(ii) *O conjunto* $\{x_1, ..., x_d\}$ *é um conjunto de geradores minimal de* G *se, e somente se,* $\{x_1\Phi(G), ..., x_d\Phi(G)\}$ *é uma base de* $G/\Phi(G)$.

(iii) *O número minimal* d *de geradores do grupo* G *coincide com a dimensão de* $G/\Phi(G)$ *como um* $\mathbb{F}_p$*-espaço vetorial. Em outras palavras,* $|G : \Phi(G)| = p^d$.

Ilustraremos a importância desse teorema com um corolário simples, mas que será usado na demonstração da Proposição 3.17.

Corolário 1.4.12. *Seja* G *um* p*-grupo finito e* $d(G) = 2$*, então* G *tem* $p + 1$ *maximais.*

Demonstração. Pelo Teorema 1.4.11, $G/\Phi(G) \cong C_p \times C_p$. Cada elemento $(a, b) \in C_p \times C_p$, não ambos triviais, gera um maximal. Cada maximal possuí $p-1$ elementos distintos dos outros maximais, e existem $p^2 - 1 = (p + 1)(p - 1)$ elementos não triviais de $C_p \times C_p$. Logo, $C_p \times C_p$ possuí $p+1$ maximais. Como todos esses maximais são cíclicos, em $G/\Phi(G)$ todos serão da forma $\langle a\Phi(G)\rangle$, $a \in G$. Logo, G tem $p + 1$ maximais.

□

A seguir, introduziremos os subgrupos que serão a base desse trabalho, pois olharemos para a estrutura dos p-grupos a partir deles e de seus quocientes.

Definição 1.4.13. *Seja* G *um* p*-grupo. Para cada* $i \geq 1$ *definimos:*

$$G^{p^i} = \langle x^{p^i} \mid x \in G\rangle$$

isto é, o subgrupo gerado pelas p^i*-ésimas potências dos elementos de* G.

Exemplo 1.4.14. *Considere o grupo* $G = \langle a, b \mid a^{27} = b^9 = 1,\ a^b = a^4\rangle \cong C_{27} \rtimes C_9$. *Então:*

- $G^3 = \langle a^3, b^3\rangle \cong C_9 \times C_3$
- $G^9 = \langle a^9\rangle \cong C_3$
- $G^{27} = 1$

Os subgrupos G^{p^i} são característicos, pois, dado φ um homomorfismo de G e $x \in G$, $(x^{p^i})^\varphi = (x^\varphi)^{p^i} \in G^{p^i}$, então φ leva geradores de G^{p^i} em geradores de G^{p^i}, logo, $(G^{p^i})^\varphi = G^{p^i}$.

Observe que G^{p^i} é o subgrupo **gerado** pelas p^i-ésimas potências, mas não necessariamente um elemento de G^{p^i} é uma p^i-ésima potência, ou seja, não necessariamente G^{p^i} coincide com $\{x^{p^i} \mid x \in G\}$, como mostrado no seguinte exemplo:

Exemplo 1.4.15. *Seja* $G = \langle a, b \mid a^4 = b^4 = 1,\ a^b = a^{-1} \rangle$. *O conjunto dos quadrados dos elementos de* G *é* $\{1, a^2, b^2\}$, *que não é um subgrupo.*

No caso em que G é abeliano, conseguimos $G^{p^i} = \{x^{p^i} \mid x \in G\}$. Isso decorre do fato de que $f : G \to G$ definido por $x \mapsto x^{p^i}$ é um homomorfismo, já que G é abeliano, e a imagem de f é um grupo e coincide com $\{x^{p^i} \mid x \in G\}$.

Introduziremos mais adiante os grupos *powerful*, uma classe de grupos que possui um papel central na demonstração dos resultados principais e nos quais a igualdade $G^{p^i} = \{x^{p^i} \mid x \in G\}$ também se verifica.

Não ter essa igualdade no caso geral pode parecer desanimador a princípio, mas os grupos G^{p^i} carregam por natureza uma propriedade interessante: a de limitar o expoente do grupo. O quociente G/G^{p^i} possui expoente no máximo p^i, pois por definição $x^{p^i} \in G^{p^i}$.

No caso de G^p, G/G^p é um grupo de expoente p, que é uma das condições necessárias para que um quociente seja abeliano elementar. Por isso G^p está relacionado com $\Phi(G)$, como mostra o próximo resultado.

Teorema 1.4.16 ([7], Teorema 2.2)**.** *Seja* G *um* p*-grupo finito. Então:*

(i) *Se* $N \trianglelefteq G$ *e* G/N *é abeliano elementar, então* $\Phi(G) \leq N$.

(ii) $\Phi(G) = G'G^p$.

Seja G um p-grupo e $exp(G) = p^e$. Então $G^{p^e} = 1$, e temos a seguinte série descendente

$$G \geq G^p \geq ... \geq G^{p^{e-1}} \geq G^{p^e} = 1$$

Essa série em um p-grupo é estritamente decrescente, uma vez que

$$G^{p^{i+1}} \leq (G^{p^i})^p \leq \Phi(G^{p^i}) < G^{p^i}$$

desde que $G^{p^i} \neq 1$. Então essa série terá exatamente e passos. No exemplo 1.4.14, veja que $exp(G) = 3^3$ e:

$$1 = G^27 \leq G^9 \leq G^3 \leq G$$

Teorema 1.4.17 ([7], Teorema 2.4)**.** *Seja* G *um* p*-grupo finito e* $N \trianglelefteq G$. *Então* $(G/N)^{p^i} = G^{p^i}N/N$.

O próximo lema é utilizado na demonstração do item (ii) do Lema 3.12 e possui uma notação própria, que será utilizada apenas em seu enunciado:

- $k(G)$ é o número de caracteres irredutíveis de G, ou, equivalentemente, o número de classes de conjugação de G.
- $mc(G) = \frac{k(G)}{|G|}$ é a medida de comutatividade de G, ou seja, a probabilidade de dois elementos de G comutarem.
- $b_G(x) = log_p(|G : C_G(x)|) = log_p(|Cl_G(x)|)$ e $b_G(G) = max\{b_G(x) \mid x \in G\}$ (o expoente da potência de p da maior classe de conjugação) é a largura de x e G, respectivamente.

Lema 1.4.18 ([1], Lema 2.12)**.** *Seja G um p-grupo de ordem p^n. Então:*

(a) $b_G(G) \leq 1 \iff |G'| \leq p \iff k(G) \geq p^{n-1} + p - 1$.

(b) $b_G(G) \geq 2 \iff |G'| \geq p^2 \iff mc(G) \leq \frac{2}{p^2} - \frac{1}{p^4}$.

1.5 Conceitos básicos de grupos profinitos

Nessa secção veremos a base teórica para compreender o enunciado e a demonstração do Teorema B. Essa seção se baseia principalmente nas notas de aula da matéria de Grupos Profinitos ministrada na Universidade de Brasília em 2023 por Pavel Zalesski e Sheila Chagas ([26]). Também utiliza [25] e [9]. Não será feita uma abordagem ampla de grupos profinitos, apenas o necessário para escrever e provar a versão profinita do Teorema A.

1.5.1 Prelúdio topológico

Vamos começar estabelecendo algumas definições.

Definição 1.5.1. *Um **espaço topológico** é um conjunto X com uma família de subconjuntos de X (chamados conjuntos abertos) de tal forma que:*

(a) *O conjunto vazio e X são conjuntos abertos;*

(b) *A interseção de dois conjuntos abertos quaisquer é um conjunto aberto;*

(c) *Uma união arbitrária de conjuntos abertos é um conjunto aberto.*

A coleção de subconjuntos abertos é uma topologia em X. Um subconjunto é chamado fechado se o complementar dele é aberto.

Se Y é um subconjunto de X, o fecho $\overline{Y}$ de Y é a interseção de todos os subconjuntos fechados que contém Y. Um subconjunto Y de X é chamado denso em X se $\overline{Y} = X$.

Uma vizinhança aberta de um elemento $x \in X$ é um conjunto aberto que contém x.

Uma base para uma topologia em X é uma coleção $\{U_\lambda \mid \lambda \in \Lambda\}$ de conjuntos abertos tal que cada conjunto aberto é a união de alguns conjuntos U_λ.

A topologia de X que consiste de todos os subconjuntos de X é chamada topologia discreta.

Se Y é um subconjunto de X, a topologia de X induz a topologia em Y que consiste em todos os subconjuntos da forma $Y \cap U$, onde U é um subconjunto aberto em X. Esta topologia é chamada topologia induzida.

Um espaço topológico é chamado compacto se, para cada família dada $\{U_\lambda \mid \lambda \in \Lambda\}$ de subconjuntos abertos tal que $X = \bigcup_{\lambda\in\Lambda} U_\lambda$, existe uma subfamília finita $\{U_{\lambda_1}, ..., U_{\lambda_n}\}$ tal que $X = \bigcup_{i=1}^{n} U_{\lambda_i}$.

Lema 1.5.2. *Um espaço topológico X é compacto se, e somente se, para cada família $\{C_\lambda \mid \lambda \in \Lambda\}$ de subconjuntos fechados onde cada interseção de um número finito de conjuntos C_λ não é vazio, temos $\bigcap_{\lambda\in\Lambda} C_\lambda \neq \emptyset$.*

Demonstração. ($\Longrightarrow$) Suponha, por contradição, que existe uma família $\{C_\lambda \mid \lambda \in \Lambda\}$ de subconjuntos fechados onde cada interseção de um número finito de conjuntos C_λ não é vazio, mas $\bigcap_{\lambda\in\Lambda} C_\lambda = \emptyset$

Temos que cada $(X \setminus C_\lambda)$ é aberto (complementar de fechado). Então

$$\bigcup_{\lambda\in\Lambda}(X \setminus C_\lambda) = X \setminus \underbrace{\bigcap_{\lambda\in\Lambda} C_\lambda}_{=\emptyset} = X$$

ou seja, $\{X \setminus C_\lambda\}_{\lambda\in\Lambda}$ é uma cobertura aberta de X, logo, pela compacidade de X, existe uma subfamília finita $\{C_{\lambda_i}\}_{i=1}^n$, $n \in \mathbb{N}$, tal que:

$$\bigcup_{i=1}^{n}(X \setminus C_{\lambda_i}) = X \setminus \bigcap_{i=1}^{n} C_{\lambda_i} = X$$

Mas isso significa que $\bigcap_{i=1}^n C_{\lambda_i} = \emptyset$, o que não pode ocorrer. Logo $\bigcap_{\lambda\in\Lambda} C_\lambda \neq \emptyset$.

($\Longleftarrow$) Suponha que para cada família $\{C_\lambda \mid \lambda \in \Lambda\}$ de subconjuntos fechados onde cada interseção de um número finito de conjuntos C_λ não é vazio, temos $\bigcap_{\lambda\in\Lambda} C_\lambda \neq \emptyset$. Suponha também, por contradição, que X não é compacto. Então existe uma cobertura $\{A_\lambda\}_{\lambda\in\Lambda}$ de X que não admite subcobertura finita. Logo, para qualquer coleção finita $\{A_{\lambda_i}\}_{i=1}^n$, $n \in \mathbb{N}$, temos:

$$(X \setminus \bigcup_{i=1}^{n} A_{\lambda_i} \neq \emptyset)$$

ou seja,

$$\bigcap_{i=1}^{n}(X \setminus A_{\lambda_i}) \neq \emptyset$$

Como os A_λ são abertos, cada $X \setminus A_\lambda$ é fechado, então $\{X \setminus A_\lambda\}_{\lambda\in\Lambda}$ é uma família de fechados onde cada interseção finita é não vazia, logo, por hipótese,

$$\bigcap_{\lambda\in\Lambda}(X \setminus A_\lambda) \neq \emptyset$$

Mas isso significa que:

$$(X \setminus \bigcup_{\lambda \in \Lambda} A_\lambda) \neq \emptyset$$

o que é uma contradição pois $\bigcup_{\lambda \in \Lambda} A_\lambda = X$.

□

Um espaço topológico X é conexo se X não pode ser representado como uma união disjunta de subconjuntos abertos. X é totalmente desconexo se cada subespaço conexo tem no máximo um elemento.

Lema 1.5.3. *Seja X um espaço compacto e Hausdorff.*

(a) *Logo X é normal, isto é, para cada par de subconjuntos fechados C, D tal que $C \cap D = \emptyset$ existem subconjuntos abertos U, V tais que $C \subseteq U$, $D \subseteq V$ e $U \cap V = \emptyset$.*

(b) *Seja $x \in X$ e A a interseção de todos os subconjuntos de X que contém x e são abertos e fechados simultaneamente, então A será uma componente conexa de x.*

(c) *Se X é totalmente desconexo, cada subconjunto aberto é uma união de subconjuntos abertos-fechados.*

Corolário 1.5.4. *Seja X um espaço compacto e totalmente desconexo, logo $\{x\}$ é fechado para cada $x \in X$.*

Sejam X e Y espaços topológicos. Uma aplicação $f : X \to Y$ é contínua se, para cada conjunto aberto $U \subseteq Y$, a imagem inversa $f^{-1}(U)$ é aberta em X.

Dizemos que f é um homeomorfismo se f é bijetora e f e f^{-1} são contínuas. Nesse caso, f leva abertos em abertos.

Lema 1.5.5. *Sejam X e Y espaços topológicos. Temos que:*

(a) *Todo subconjunto fechado de um espaço compacto é compacto.*

(b) *Todo subconjunto compacto de espaço Hausdorff é fechado.*

(c) *Se $f : X \to Y$ é contínua e X é compacto, então $f(X)$ é compacto.*

Demonstração. **(a)** Seja X um espaço compacto e V um subconjunto fechado de X. Seja $\{A_\lambda\}_{\lambda \in \Lambda}$ uma cobertura aberta de V. Então:

$$X = (X \setminus V) \cup (\bigcup_{\lambda \in \Lambda} A_\lambda)$$

ou seja, $\{A_\lambda\}_{\lambda\in\Lambda} \cup (X \setminus V)$ é uma cobertura aberta de X. Pela compacidade de X, existe uma subcobertura finita $\{A_{\lambda_i}\}_{i=1}^n$ tal que:

$$X = (X \setminus V) \cup (\bigcup_{i=1}^{n} A_{\lambda_i})$$

Como $V \cap (X \setminus V) = \emptyset$, é preciso que $V \subseteq \bigcup_{i=1}^n A_{\lambda_i}$, então $\{A_{\lambda_i}\}_{i=1}^n$ é uma subcobertura finita de V, logo V é compacto.

(b) Seja X Hausdorff e $F \subseteq X$ compacto. Seja $x \in F$ e $y \in X \setminus F$. Então existem abertos B_x e A_y que contém x e y, respectivamente, tais que $B_x \cap A_y = \emptyset$. Percorrendo x por F temos que $F \subseteq \bigcup_{x\in F} B_x$, ou seja, $\{B_x\}_{x\in F}$ é uma cobertura aberta de F, logo, pela compacidade de F, admite subcobertura finita $\{B_{x_i}\}_{i=1}^n$.

Considere $y \in X \setminus F$ fixo e A_{x_i} um aberto que contém y tal que $A_{x_i} \cap B_{x_i} = \emptyset$, $i = 1, ..., n$. Então $y \in \bigcap_{i=1}^n A_{x_i}$. Mas

$$(\bigcap_{i=1}^{n} A_{x_i}) \cap (\bigcup_{j=1}^{n} B_{x_j}) = \bigcup_{j=1}^{n} ((\bigcap_{i=1}^{n} A_{x_i}) \cap B_{x_j}) = \emptyset$$

Logo, $A = \bigcap_{i=1}^n A_{x_i}$ é um aberto contido em $X \setminus F$ e que contém y. Logo, $X \setminus F$ é aberto, portanto F é fechado.

(c) Seja $f : X \to Y$ contínua e X compacto. Seja $\{A_\lambda\}_{\lambda\in\Lambda}$ uma cobertura aberta de $f(X)$. Considerando $f(X)$ como espaço topológico com a topologia induzida, $A_\lambda \cap f(X)$ são abertos de $f(X)$ para cada $\lambda \in \Lambda$. Como f é contínua $f^{-1}(A_\lambda \cap f(X))$ são abertos de X. Além disso:

$$\bigcup_{\lambda\in\Lambda} (A_\lambda \cap f(X)) = f(X) \implies \bigcup_{\lambda\in\Lambda} f^{-1}(A_\lambda \cap f(X)) = X$$

Logo, $\{(A_\lambda \cap f(X))\}_{\lambda\in\Lambda}$ é uma cobertura aberta de X. Pela compacidade de X, esta admite subcobertura finita, então existem $\{A_{\lambda_i}\}_{i=1}^n$ tais que

$$\bigcup_{i=1}^{n} f^{-1}(A_{\lambda_i} \cap f(X)) = X \implies \bigcup_{i=1}^{n} (A_{\lambda_i} \cap f(X)) = f(X)$$

Portanto, $f(X)$ é compacto.

□

Seja $f : X \to Y$ uma aplicação sobrejetora de um espaço topológico para um conjunto Y. A topologia quociente de Y é a topologia que consiste em todos os subconjuntos V tal que $f^{-1}(V)$ é aberto em X. Logo, f é contínua e, de fato, a topologia quociente é a mais fraca tal que f é contínua.

1.5.2 Grupos topológicos

Definição 1.5.6. *Um **grupo topológico** G é um espaço topológico munido de uma estrutura de grupo tal que as aplicações $m : G \times G \to G$ e $i : G \to G$, definidas por $m(x, y) = xy$ e $i(x) = x^{-1}$, são contínuas.*

Exemplo 1.5.7. $(\mathbb{R}, +)$, $(\mathbb{R}^n, +)$, $(\mathbb{R}^*, \times)$, $(\mathbb{C}, +)$, $(\mathbb{C}^*, \times)$ *são grupos topológicos com a topologia usual.*

Exemplo 1.5.8. *Qualquer grupo finito G é um grupo topológico com a topologia discreta (todo subconjunto é aberto).*

O próximo lema coleciona alguns resultados básicos de grupos topológicos.

Lema 1.5.9. *Seja G um grupo topológico. Então*

(a) *i é homeomorfismo. Para cada $g \in G$ as aplicações $x \to xg$ e $x \to gx$ são homeomorfismos.*

(b) *Se H é um subgrupo aberto (resp. fechado) de G, então cada classe lateral Hg ou gH em G é aberto (resp. fechado).*

(c) *Cada subgrupo aberto de G é fechado, e cada subgrupo fechado de índice finito é aberto. Se G é compacto, cada subgrupo aberto tem índice finito.*

(d) *Se H é um subgrupo que contém um subconjunto aberto $U \neq \emptyset$, então H é aberto.*

(e) *Se H é um subgrupo de G então H é um grupo topológico com a topologia induzida. Se K é um subgrupo normal, então G/K é o grupo topológico com topologia quociente. O homomorfismo quociente $q : G \to G/K$ é aberto.*

(f) *G é Hausdorff se, e somente se, $\{1\}$ é fechado em G; se K é um subgrupo normal, então G/K é Hausdorff se, e somente se, K é fechado em G. Se G é totalmente desconexo, então G é Hausdorff.*

(g) *Se G é compacto Hausdorff e C, D são subconjuntos fechados, então CD é fechado.*

Lema 1.5.10. *Seja G um grupo topológico compacto. Se C é subconjunto aberto-fechado que contém 1, então C contém subgrupo aberto normal.*

Definição 1.5.11. *Um grupo topológico G é um **grupo profinito** se G é compacto e totalmente desconexo.*

Pelo item (c) de 1.5.9, em um grupo profinito G todo subgrupo aberto tem índice finito. Então, se N é um subgrupo aberto normal de G, G/N será um grupo finito. Também, como consequência de (f) de 1.5.9, todo grupo profinito é Hausdorff.

Definição 1.5.12. *Um **pro-p grupo** é um grupo profinito G tal que, para todo $N \trianglelefteq_o G$, G/N é um p-grupo.*

Proposição 1.5.13. *Seja G um grupo profinito. Então*

(a) *Cada subconjunto aberto de G é uma união de classes laterais de subgrupos abertos normais.*

(b) *Um subconjunto é aberto-fechado se, e somente se, ele é uma união de número finito de classes laterais de subgrupos abertos normais.*

(c) *Se X é um subconjunto de G, então $\overline{X} = \bigcap_{N \trianglelefteq_o G} NX$. Particularmente, a interseção de todos os subgrupos normais abertos é trivial.*

Proposição 1.5.14. *Seja G um grupo profinito, então um subgrupo H de G é profinito com a topologia induzida se, e somente se, H é fechado.*

Definição 1.5.15. *Sejam G um grupo profinito e X um subconjunto de G. Dizemos que G é **topologicamente gerado** por X se $\overline{\langle X \rangle} = G$. Um grupo profinito G é dito **finitamente gerado** se G contém um subconjunto finito X que gera G.*

Note que, pela definição anterior, $\overline{G'} = \overline{\langle [x, y] \mid x, y \in G \rangle}$. Então, a princípio, $\overline{G'}$ e G' podem não coincidir, ou seja, G' pode não ser fechado.

A seguir temos um resultado que será utilizado na demonstração do Teorema B para mostrar que, nas condições do referente teorema, G' é fechado.

Proposição 1.5.16 ([5], Proposição 1.19)**.** *Se G é um pro-p grupo finitamente gerado, então o subgrupo comutador G' é fechado em G.*

1.6 Fórmula de Compilação de Hall-Petresco

Complementando o estudo de comutadores, nessa seção demonstraremos a Fórmula de Compilação de Hall-Petresco, pois será um resultado bastante utilizado ao longo desse trabalho. Além disso, é interessante estudá-la por si só para compreender melhor o papel dos comutadores na tentativa de comutar elementos. Também vamos relacioná-la com o resultado de [6]. A demonstração utilizada baseia-se em [7].

Os principais resultados que serão demonstrados ao longo da seção são:

Fórmula de Compilação de Hall-Petresco: *Sejam G um p-grupo e $x, y \in G$. Então existem elementos $c_i = c_i(x,y) \in \gamma_i(\langle x, y\rangle)$ tais que*

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

para todo $n \in \mathbb{N}$.

O seguinte é um corolário desse resultado, e é conhecido como Identidade de Hall-Petresco.

Identidade de Hall-Petresco: *Sejam G um p-grupo e $x, y \in G$. Então*

(a) $(xy)^p \equiv x^p y^p \pmod{(G')^p \gamma_p(G)}$.
(b) $[x^p, y] \equiv [x, y]^p \pmod{(N')^p \gamma_p(N)}$, onde $N = \langle x, [x, y]\rangle$.

Antes de começar a demonstração, é interessante entender o que está por trás da fórmula a partir de casos simples. Como comentado anteriormente, podemos interpretar o comutador como o "preço" a se pagar para comutar dois elementos, pois, dados x, y em um grupo G, $xy = yx[x, y]$. Entretanto, em escalas maiores e em situações mais gerais, esse preço começa a tornar-se custoso e de difícil manipulação. Por exemplo, se tentarmos relacionar $x^n y^n$ com $(xy)^n$ em um grupo qualquer G. Para $n = 2$ temos:

$$x^2y^2 = x(xy)y = x(yx[x,y])y = xyx([x,y]y) = (xy)^2[x,y][x,y,y]$$

Mas, para $n = 3$:

$$x^3y^3 = x(x^2y^2)y = x(xy)^2[x,y][x,y,y]y = x(xy)^2y[x,y][x,y,y][[x,y][x,y,y],y]$$

$$= (xy)^3[(xy)^2,y][x,y][x,y,y][[x,y][x,y,y],y] \tag{1.4}$$

O resultado já é bem mais complexo, e se torna ainda mais para casos maiores e para

um n geral, tornando os cálculos explícitos impraticáveis.

Hall e Petresco encontraram uma fórmula que relaciona $x^n y^n$ com $(xy)^n$ em qualquer grupo G (não só p-grupos) a custo de alguns comutadores, que em geral não sabemos explicitar, mas sabemos em que nível estão na série $\gamma_i(\langle x, y\rangle)$.

Por exemplo, para $n = 2$, considere $c_2 = [x, y][x, y, y]$, então $x^2y^2 = (xy)^2 c_2$ e $c_2 \in \gamma_2(\langle x, y\rangle)$. Para $n = 3$, podemos reescrever a igualdade 1.4 como:

$$x^3y^3 = (xy)^3[(xy)^2, y]c_2[c_2, y] \tag{1.5}$$

Pelo Teorema 1.2.4, temos que $[xy, y] = [x, y][x, y, y] = c_2$ e consequentemente:

$$[(xy)^2, y] = [xy, y][xy, y, xy][xy, y] = c_2[c_2, xy]c_2 = {c_2}^2[c_2, xy][c_2, xy, c_2]$$

Então, substituindo em (1.5) temos:

$$x^3y^3 = (xy)^3{c_2}^2[c_2, xy][c_2, xy, c_2]c_2[c_2, y] = (xy)^3{c_2}^3c_3$$

para algum elemento $c_3 \in \gamma_3(\langle x, y\rangle)$.

Para o caso geral, obteremos uma expressão relacionando $x^n y^n$ com $(xy)^n$ graças a um engenhoso argumento baseado no princípio geral de rearranjo do Lema 1.6.2 abaixo. Vamos começar então construindo o contexto para esse Lema.

Seja $X = \{x_1, ..., x_m\}$ uma sequencia finita de elementos em um grupo e seja $p = x_1...x_m$ o seu produto (Apenas nessa seção p não é um primo!). Mesmo que haja repetição entre os elementos x_i, nós os consideraremos como diferentes por conta dos seus distintos nomes simbólicos.* Nós particionaremos X em subconjuntos $X_1, ..., X_n$, e agora queremos reordenar os elementos do produto p de forma que os elementos que pertencem a X_1 apareçam primeiro, seguidos pelos elementos pertencentes a X_2, e assim por diante. Isso requer mover alguns elementos para esquerda com trocas da forma $ab = ba[a, b]$, e isso significa que, além dos próprios elementos $x_1, ..., x_m$, na expressão de p aparecerão alguns comutadores cujos componentes são alguns dos x_i.

Para qualquer subconjunto S de $R = \{1, ..., n\}$ com mais de um elemento, denote por X_S o conjunto dos comutadores superiores cujos componentes são exclusivamente retirados de X_i, com $i \in S$, e que tem pelo menos um componente de cada um desses

*Para os que estão familiarizados com a teoria de grupos livres, o conjunto natural para o resultado que segue é na verdade o grupo livre F gerado livremente pelos $x_1, ..., x_m$. Isso torna o argumento do texto mais claro, já que os elementos do produto $p = x_1...x_m$ são realmente diferentes nesse caso. Então qualquer fórmula de rearranjo que obtemos do produto p pode ser transferida para produtos de elementos em um grupo arbitrário, já que o subgrupo que esses elementos geram é uma imagem homomórfica de F. Inclusive, isso mostra que as fórmulas que obtemos são universais, as mesmas para todos os grupos.

subconjuntos.

Exemplo 1.6.1. *Façamos um exemplo simples para ficar mais claro quem são esses objetos. Digamos que* $X = \{x_1, x_2, x_3, x_4, x_5, x_6\}$*, então:*

- $p = x_1x_2x_3x_4x_5x_6$
- *Podemos escolher como partição* $X_1 = \{x_2, x_5\}$*,* $X_2 = \{x_1, x_3\}$*,* $X_3 = \{x_4\}$*,* $X_4 = \{x_6\}$*.*
- $S \subseteq \{1, 2, 3, 4\}$ *e* $|S| > 1$*. Escolha* $S = \{1, 2, 4\}$*.*
- X_S *será composto por comutadores superiores, ou seja, elementos da forma* $[x_i, ..., x_j, ..., x_k]$*, mas cada um desses* $x_i \in X_1 \cup X_2 \cup X_4 = \{x_2, x_5, x_1, x_3, x_6\}$*, e precisam existir* i, j, k *tais que* $x_i \in X_1$*,* $x_j \in X_2$*,* $x_k \in X_4$*. Por exemplo,* $[x_6, x_1, x_3, x_2] \in S$*, mas* $[x_6, x_4, x_3, x_2] \notin S$ *e* $[x_6, x_1, x_3] \notin S$*.*

Agora estamos prontos para enunciar e demonstrar o lema.

Lema 1.6.2 ([7], Lema 2.5)**.** *Ordene os subconjuntos não vazios de* $R = \{1, ..., n\}$ *de acordo com seu tamanho e, entre os subconjuntos de mesmo tamanho, lexicograficamente. Então*

$$p = \prod_{\emptyset \neq S \subseteq R} q_S$$

onde os fatores ocorrem na ordem estabelecida para os subconjuntos de R *e cada* q_S *é um produto de elementos de* X_S*.*

Demonstração. Vamos começar colocando para a esquerda os elementos de X_1. Como observado acima, isso tem o efeito de produzir comutadores da forma $[a, b] \in X_{1i}$ para algum $i \geq 2$ (Nós derrubamos o parênteses e a vírgula do conjunto $\{1, i\}$ para simplificar a notação.) Então podemos escrever $p = q_1p'$, onde q_1 é o produto de elementos de X_1 e p' é um produto de elementos de $X_2, ..., X_n, X_{12}, ..., X_{1n}$.

Continuamos o processo coletando para esquerda os elementos de X_2, e depois com o resto dos subconjuntos X_S, de acordo com a ordem estabelecida para os subconjuntos S de R. Suponha que, em algum momento, nós já tenhamos movido para esquerda todos os elementos correspondentes dos subconjuntos X_T para $T \subseteq R$ que é "menor" que S.

Então nosso próximo passo é coletar os elementos em X_S. Para esse propósito, vamos ter que realizar mudanças da forma $ab = ba[a, b]$, onde $b \in X_S$ e $a \in X_T$ para algum T "maior" do que S. O novo elemento que aparecerá no produto p é o comutador $[a, b]$, que

pertence a $X_{S\cup T}$. Como o subconjunto $S \cup T$ é posterior a S na ordem que escolhemos para os subconjuntos de R, podemos assumir que:

(i) Essas mudanças não alteram a coleção de elementos que obtivemos até agora.

(ii) Nenhum novo elemento de X_S aparece quando coletamos para a esquerda um elemento de X_S. Consequentemente os elementos de X_S podem ser coletados em um número finito de passos.

Como R possui um número finito de subconjuntos, esse processo eventualmente acaba e nós obtemos a fórmula estabelecida no lema.

□

A demonstração do lema mostra claramente que os elementos $q_1, ..., q_n$ da fórmula são produtos de elementos em $X_1, ..., X_n$, respectivamente, multiplicados na mesma ordem em que eles aparecem no produto $p = x_1...x_m$. Por exemplo, em 1.6.1 temos $p = x_1x_2x_3x_4x_5x_6$ e $X_1 = \{x_2, x_5\}$, então $q_1 = x_2x_5$.

Para qualquer subconjunto não vazio S de R, seja p_S o produto dos elementos nos conjuntos X_i, $i \in S$, na mesma ordem de $p = x_1...x_m$. No exemplo 1.6.1, se escolhermos $S = \{2, 3\}$, então $p_S = x_1x_3x_4$. É equivalente dizer que p_S é o resultado de substituir por 1 em p os elementos nos conjuntos X_i, $i \notin S$.

Observe que, pelo Lema 1.6.2,

$$p_S = \prod_{\emptyset \neq T \subseteq S} q_T \tag{1.6}$$

pois qualquer comutador superior que possui um componente igual a 1 é ele mesmo igual a 1.

Podemos agora proceder para a demonstração do resultado principal dessa seção.

Teorema 1.6.3 (Fórmula de Compilação de Hall-Petresco, [7], Teorema 2.6)**.** *Seja G um p-grupo e $x, y \in G$. Então existem elementos $c_i = c_i(x, y) \in \gamma_i(\langle x, y\rangle)$ tais que*

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

para todo $n \in \mathbb{N}$.

Demonstração. Compilaremos os elementos no produto $p = x^n y^n$ escolhendo que X_1 será composto pelo primeiro x e pelo primeiro y aparecendo em p, X_2 pelo segundo x e o segundo y, e assim por diante até X_n. Seja $R = \{1, ..., n\}$. De acordo com o Lema 1.6.2 podemos escrever

$$x^n y^n = \prod_{\emptyset \neq S \subseteq R} q_S = (xy)^n \prod_{S \subseteq R, |S| \geq 2} q_S \tag{1.7}$$

Veja que $q_i = xy$, $i \in \{1, ..., n\}$, então o que fizemos nesse primeiro passo foi separar para a esquerda o produto $q_1 ... q_n$.

Seja S um subconjunto qualquer de R com i elementos. Temos que $p_S = x^i y^i$ depende apenas de i e não de S, porque, afinal, os X_i são iguais, ainda que "simbolicamente" diferentes. Segue da equação (1.6) que

$$p_S = x^i y^i = (xy)^i \prod_{T \subseteq S, |T| \geq 2} q_T \tag{1.8}$$

Seja $S' \subseteq R$ e $|S'| = i$. Então, da mesma forma,

$$p_{S'} = x^i y^i = (xy)^i \prod_{T' \subseteq S', |T'| \geq 2} q_{T'}$$

e assim

$$\prod_{T' \subseteq S', |T'| \geq 2} q_{T'} = \prod_{T \subseteq S, |T| \geq 2} q_T$$

Por indução, segue que $q_T = q_{T'}$. Logo, todos os q_S em (1.7) tais que $|S| = i$ assumem um mesmo valor c_i. Além disso, esse valor depende de i e não de n. O Lema 1.6.2 mostra que os c_i são um produto de comutadores superiores em x, y com comprimento no máximo i. Segue do Corolário 1.2.16 que $c_i \in \gamma_i(\langle x, y \rangle)$. Agora, R possui $\binom{n}{i}$ subconjuntos com i elementos, então c_i aparece $\binom{n}{i}$ vezes na expressão 1.7. Como essas ocorrências de c_i são consecutivas, por conta da ordem estabelecida, concluímos que

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

como desejado.

□

Observação 1.6.4. *Pelo comentário na nota de rodapé da primeira página da seção, segue que a fórmula do teorema anterior é universal e não depende dos elementos x, y nem do grupo G.*

Utilizando a Fórmula de Compilação de Hall-Petresco no contexto do resultado principal desse trabalho obtemos algo interessante. Lembrando que, no Teorema A de [6],

mostra-se que se G é um p-grupo tal que $d(G') = 2$, então existe $x \in G$ tal que $G' = \{[x, g] \mid g \in G\}$. Então, nesse caso, para quaisquer $a, b \in G$, teremos:

$$a^n b^n = (ab)^n [x, g]$$

para algum $g \in G$. Ou seja, o resultado simplifica significativamente a fórmula. Temos agora apenas um comutador, e o único elemento desconhecido é g, e não mais $c_2, ..., c_n$.

Uma consequência quase imediata da Fórmula de Compilação Hall-Petresco é o seguinte Teorema, que será utilizado na demonstração dos resultados principais (Teorema 3.13) e nas demonstrações dos resultados de grupos *powerful* no Capítulo 2.

Teorema 1.6.5 ([1], Teorema A.1.4)**.** *Seja G um p-grupo e $x, y \in G$.*
(a) $(xy)^p \equiv x^p y^p \pmod{(G')^p \gamma_p(G)}$.
(b) $[x^p, y] \equiv [x, y]^p \pmod{(N')^p \gamma_p(N)}$, *onde* $N = \langle x, [x, y] \rangle$.

Demonstração. **(a)** Pela Fórmula de Compilação Hall-Petresco (1.6.3), existem $c_i \in \gamma_i(G)$, para $i = 2, ..., p$, tais que $(xy)^p = x^p y^p c_2^{\binom{p}{2}} c_3^{\binom{p}{3}} ... c_p$. Como p é primo, $c_2^{\binom{p}{2}}, c_3^{\binom{p}{3}}, ..., c_{p-1}^p \in (G')^p$, e $c_p \in \gamma_p(G)$. Assim o resultado de (a) segue.

(b) Por (a), obtemos

$$(x[x, y])^p \equiv x^p [x, y]^p \pmod{(N')^p \gamma_p(N)}$$

,

onde $N = \langle x, [x, y] \rangle$. Mas

$$(x[x, y])^p = (xx^{-1}y^{-1}xy)^p = (y^{-1}xy)^p =$$

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

Então

$$x^p [x, y]^p \equiv x^p [x^p, y] \pmod{(N')^p \gamma_p(N)}$$

Após cancelar, obtemos o resultado desejado.

□

O Teorema anterior pode ser generalizado para p^k. Apresentamos apenas essa versão simplificada do resultado com $n = p$ pois é a que será mais utilizada ao longo do trabalho.

Capítulo

2

Grupos *powerful*

Esse capítulo tem como objetivo estabelecer resultados sobre grupos *powerful*, pois são a chave da estratégia da demonstração do resultado principal. A teoria apresentada nesse capítulo foi estudada nos livros [5] e em [16], mas é importante ressaltar que essa teoria foi desenvolvida por Lubotzky e Mann em [18]. Os exemplos em sua maioria vêm de [7]. Algumas demonstrações foram reescritas utilizando a Fórmula de Compilação Hall-Petresco (Teorema 1.6.5) e por isso distinguem-se um pouco das referências.

Definição 2.1. *Um p-grupo finito G é dito* ***powerful*** *quando $G' \leq G^p$, para p ímpar; e $G' \leq G^4$ para $p = 2$.*

Exemplo 2.2. *(Exemplos de powerfull)*

- *Todo p-grupo finito abeliano é powerful. Se G é abeliano, então $G' = 1 \leq G^{p^2}$.*
- *$G = \langle a, b \mid a^{p^3} = b^{p^2} = 1, [a, b] = a^p \rangle$, com p primo ímpar, é powerful. $G' = \langle a^p \rangle$ e $\langle a^p, b^p \rangle \leq G^p$, logo, $G' \leq G^p$.*
- *$G = \langle a, b, c \mid a^{p^2} = b^p = c^p = 1, [a, b] = [a, c] = 1, b^c = ba^p \rangle$, com p primo ímpar, é powerful. $G' = \langle a^p \rangle \leq G^p$.*
- *$G = \langle a, b, c \mid a^{p^3} = b^p = c^{p^2} = 1, [a, b] = 1, a^c = a^{1+p}, b^c = ba^p \rangle$, com p primo ímpar, é powerful. $G' = \langle a^p \rangle \leq G^p$, logo, $G' \leq G^p$.*
- *$M_m(p) = \langle a, b \mid a^{p^{m-1}} = b^p = 1,\ a^b = a^{p^{m-2}+1} \rangle$, com p primo e $m \geq 4$, pois $[a, b] = a^{p^{m-2}} = (a^{p^2})^{(2^{m-4})}$ pertence a $M_m(p)^{p^2}$, logo, $M_m(p)' \leq M_m(p)^{p^2}$. Nesse caso podemos ter $p = 2$, então esse é o primeiro exemplo de $2-$grupo powerful não abeliano.*

Para o próximo exemplo precisaremos introduzir o conceito de grupos regulares.

Definição 2.3. *Um p-grupo G é dito* ***regular*** *se $x^p y^p \equiv (xy)^p \mod (\langle x, y\rangle')^p$ para todo $x, y \in G$. Equivalentemente, considerando os c_i da Fórmula de Compilação Hall-Petresco (1.6.3), $c_p(x, y) \in (\langle x, y\rangle')^p$.*

- *Se G é regular, então G^p é powerful, se p é um primo ímpar. Afinal, se G é regular, do Teorema 2.14 de [7] podemos concluir que $(G^p)' = [G^p, G^p] = ([G, G])^{p^2} \leq G^{p^2} \leq (G^p)^p$.*

Exemplo 2.4. *(Exemplos de não powerful)*

- *Diedrais. $D_{2^m} = \langle a, b \mid a^{2^{m-1}} = b^2 = 1,\ a^b = a^{-1}\rangle$, $m \geq 3$, não é powerful, pois $\overline{D_{2^m}} = D_{2^m}/D^4_{2^m} = \langle \overline{a}, \overline{b} \mid \overline{a}^4 = \overline{b}^2 = 1, \overline{a}^{\overline{b}} = \overline{a}^{-1}\rangle \cong D_8$ não é abeliano, logo $D'_{2^m} \nleq D^4_{2^m}$.*

- *Quaternios. $Q_{2^m} = \langle a, b \mid a^{2^{m-1}} = 1,\ a^{2^{m-2}} = b^2,\ a^b = a^{-1}\rangle$, $m \geq 3$, não é powerful. Afinal, se $m = 3$, $(Q_8)' = \langle a^2\rangle$ e $(Q_8)^4 = 1$, logo, $(Q_8)' \nleq (Q_8)^4$. Se $m \geq 4$, $\overline{Q_{2^m}} = Q_{2^m}/Q^4_{2^m} = \langle \overline{a}, \overline{b} \mid \overline{a}^4 = \overline{b}^2 = 1, \overline{a}^{\overline{b}} = \overline{a}^{-1}\rangle \cong D_8$, pois $a^{2^{m-2}} = (a^{2^2})^{2^{m-4}} = 1 = b^2$, e como tal grupo não é abeliano temos $Q'_{2^m} \nleq Q^4_{2^m}$.*

- *$G = \langle a, b, c \mid a^p = b^p = c^p = 1,\ a^c = ab,\ [a, b] = [b, c] = 1\rangle$, com p ímpar, não é powerful. Afinal, $G' = \langle b\rangle$ mas $G^p = 1$ (Obs: esse grupo é regular, mas não powerful).*

Essa sequência de exemplos tem por objetivo construir uma visão mais concreta desses grupos, e trazer a ideia de que o mundo dos *powerful* não é tão restrito a ponto de serem apenas alguns grupos em redomas de vidro no museu dos grupos exóticos, nem é tão vasto ou tão óbvio a ponto de se tornar desinteressante.

Definição 2.5. *Um subgrupo N de um p-grupo finito G é dito powerful embedded (p.e.) em G se $[N, G] \leq N^p$, para p ímpar; para $p = 2$, $[N, G] \leq N^4$. Escrevemos N p.e. G.*

Exemplo 2.6. *É claro que 1 é powerful e que 1 p.e. G. Também, G é powerful se, e somente se, G p.e. G.*

Exemplo 2.7. *O centro $Z(G)$ de um p-grupo finito G é não trivial e $Z(G)$ p.e. G, afinal, $[Z(G), G] = 1 \leq (Z(G))^{p^2}$.*

Observação 2.8. *Se N p.e. G, então $[N, N] \leq [N, G] \leq N^p \leq N$ ($[N, G] \leq N^4$, se $p = 2$), logo, $N \trianglelefteq G$ e N é powerful. .*

Corolário 2.9. *Seja G um p-grupo finito powerful. Então*

$$|G : G^p| = p^{d(G)} \tag{2.1}$$

Demonstração. Quando G é *powerful* e p é ímpar, temos $G' \leq G^p$. Se $p = 2$, G/G^2 é um grupo em que todos os elementos tem ordem 2, então é abeliano e $G' \leq G^2$. Como $\Phi(G) = G'G^p$, nesses casos teremos $\Phi(G) = G^p$. Pelo Teorema da Base de Burnside, $|G : \Phi(G)| = p^{d(G)}$, logo $|G : G^p| = p^{d(G)}$.

□

Lema 2.10 ([5], Lema 2.2)**.** *Sejam G um p-grupo finito e N, K e W subgrupos normais de G, com $N \leq W$.*

(i) *Se φ é um homomorfismo de G e N p.e. G, então N^φ p.e. G^φ. Em particular, se $L \trianglelefteq G$, então NL/L p.e. G/L.*

(ii) *Se p é ímpar e $K \leq N^p$, ou se $p = 2$ e $K \leq N^4$, então N p.e. G se, e somente se, N/K p.e. G/K.*

(iii) *Se N p.e. G e $x \in G$ então $\langle N, x\rangle$ é powerful.*

(iv) *Se N não é powerful embedded em W, então existe um subgrupo normal J de G tal que*

- *se p é ímpar,*

$$N^p[N, W, W] \leq J < N^p[N, W] \quad e \quad |N^p[N, W] : J| = p$$

- *se $p = 2$,*

$$N^4[N, W]^2[N, W, W] \leq J < N^4[N, W] \quad e \quad |N^4[N, W] : J| = 2$$

Demonstração. **(i)** Se φ é um homomorfismo de G, então $(N^\varphi)^p = (N^p)^\varphi$ (isso porque $N^p = \langle x^p \mid x \in N\rangle$ e $\varphi(x)^p = \varphi(x).^p.\varphi(x) = \varphi(x^p)$) então $[N^\varphi, G^\varphi] = [N, G]^\varphi \leq (N^p)^\varphi = (N^\varphi)^p$, ou seja, N^φ p.e. G^φ. A demonstração é análoga no caso em que $p = 2$ e $[N, G] \leq N^4$.

(ii) A ida segue do item (i). Suponha que N/K p.e. G/K, então:

$$[N/K, G/K] \underset{1.2.4}{=} [N, G]K/K \leq (N/K)^p \underset{1.4.17}{=} N^pK/K$$

Como $K \leq N^p$, $N^pK/K = N^p/K$. Sendo então $[N,G]K/K \leq N^p/K$, pelo Teorema da Correspondência, $[N,G]K \leq N^p$, e novamente de $K \leq N^p$ temos que $[N,G] \leq N^p$. Logo, N p.e. G. A demonstração do caso $p = 2$ e $K \leq N^4$ é análoga.

(iii) Seja $H = \langle N, x\rangle$. Como $N \trianglelefteq H$, podemos usar (ix) do Teorema 1.2.4, daí:

$$[H,H] = [H,\langle N,x\rangle] = [H,\langle x\rangle][H,N] = [N,\langle x\rangle][H,N] = [H,N]$$

Então se N p.e. G, $[H,H] = [N,H] \leq N^p \leq H^p$ (respectivamente, $[H,H] \leq H^4$ se $p = 2$). Logo, $H = \langle N, x\rangle$ é *powerful*.

(iv) Suponha que p é ímpar e que $[N,W] \nleq N^p$. Então $N^p < N^p[N,W] = M$, digamos. Como G é um p-grupo, e M e N são normais em G, olhando para G/N^p e considerando $M/N^p \trianglelefteq G/N^p$, podemos aplicar o Teorema 1.4.4 e concluir que existe $J \trianglelefteq G$ tal que $N^p \leq J < M$ e $|M : J| = p$. Então M/J tem ordem p em G/J, daí, pelo Teorema 1.4.1 , M/J é central em G/J, ou seja, $M/J \leq Z(G/J)$. Isso significa que $[M,G] \leq J$. Como $[N,W] \leq M$, temos que $[N,W]/J$ também é central, então $[N,W,W] \leq J$. Logo, $N^p[N,W,W] \leq J < N^p[N,W]$, como desejávamos.

No caso em que $p = 2$, a demonstração é quase análoga. Temos $[N,W] \nleq N^4$. Então $N^4 < N^4[N,W] = M$. Mais do que isso, como $[N,W]^2 \leq \Phi([N,W])$, e $\Phi([N,W])$ são os elementos não geradores, temos que $N^4[N,W]^2 < N^4[N,W] = M$. Logo, se considerarmos o quociente $G/N^4[N,W]^2$ e sendo $M/N^4[N,W]^2 \trianglelefteq G/N^4[N,W]^2$, novamente pelo Teorema 1.4.4 existe $J \trianglelefteq G$ tal que $N^4[N,W]^2 \leq J \leq M$ e $|M : J| = 2$. Como M/J tem ordem p, M/J é central. Sendo $[N,W]/J \leq M/J$ também o é, logo, $[N,W,W] \leq J$. Assim, $N^4[N,W]^2[N,W,W] \leq J < N^4[N,W]$.

□

Observação 2.11. *O ponto da propriedade (iv) é que para estabelecer que N p.e. W, onde N e W são subgrupos normais de um p-grupo G, nós podemos quocientar por um J adequado e desse modo reduzir ao caso em que $N^p = 1$ (se p é ímpar) ou $N^4 = 1$ (se $p = 2$), e $[N,W]$ possui ordem p e é central em G (ou seja, $[N,W,G] = 1$). Dessa forma, $[N,W] = 1$ é equivalente à $[N,W] \leq J$, mas nesse caso não existiria tal $J < N^p[N,W]$ ($J < N^4[N,W]$, se $p = 2$), e, pela contra-positiva de (iv), N p.e. W.*

Essa técnica é ilustrada na demonstração do próximo resultado.

Proposição 2.12 ([5], Proposição 2.3)**.** *Sejam G um p-grupo finito e $N \trianglelefteq G$. Se N p.e. G, então N^p p.e. G. Em particular, se G é powerful então G^p é powerful.*

Demonstração. Caso 1: quando p é ímpar. É dado que $[N,G] \leq N^p$, então $[N,G,G] \leq [N^p,G]$. E, pelas considerações anteriores podemos assumir que $(N^p)^p = 1$ e que $[N^p,G]$ é central e tem ordem p. Então, queremos mostrar que $[N^p,G] = 1$.

Sendo $[N^p,G]$ central, $[N^p,G] \leq Z(G)$, daí $[N,G] \leq N^p \implies [N,G,G] \leq [N^p,G] \leq Z(G)$.

Dado $x \in N$ e $g \in G$, pelo Teorema 1.6.5, temos que:

$$[x^p,g] \equiv [x,g]^p \pmod{(W')^p\gamma_p(W)} \tag{2.2}$$

Onde $W = \langle x,[x,g]\rangle$. Veja que $W' \leq [N,G,G]$ implica $(W')^p \leq [N,G,G]^p = 1$ e $\gamma_p(W) \leq \gamma_3(W)$, pois p é ímpar. Como $[W,W] \leq [N,G,G]$, que é central, temos que $\gamma_3(W) = [W,W,W] \leq [N,G,G,G] = 1$. Logo, de 2.2 temos que $[N^p,G] = [N,G]^p \leq (N^p)^p = 1$, e temos o que queríamos.

Caso 2: $p = 2$. Nesse caso, $[N,G] \leq N^4$. Novamente, pelas considerações já feitas, podemos assumir que $(N^2)^4 = 1$ e que $[N^2,G]$ é central e tem ordem 2. Em síntese:

$$[N^2,G,G] = [N^2,G]^2 = (N^2)^4 = 1$$

Para $x \in N$ e $g \in G$ temos, como no caso anterior, pelo Teorema 1.6.5:

$$[x^4,g] \equiv [x^2,g]^2 \pmod{(Y')^2\gamma_2(Y)} \tag{2.3}$$

Nesse caso, $Y = \langle x^2,[x^2,g]\rangle$ então $Y' \leq [N^2,G,G] = 1$. Veja que $(Y')^2\gamma_2(Y) = (Y')^2Y' = Y'$. Então $[N^4,G] = [N^2,G]^2 = 1$. Isso significa que N^4 é central.

Como $N^8 \leq (N^2)^4 = 1$, o expoente de N divide 8, então N^4 é gerado por elementos de ordem 2, por isso $(N^4)^2 = 1$. Então com x e g como anteriormente temos, pelo Teorema 1.6.5:

$$[x^2,g] \equiv [x,g]^2 \pmod{(Z')^2\gamma_2(Z)} \tag{2.4}$$

Novamente, $(Z')^2\gamma_2(Z) = Z'$. Como $Z' \leq [N,G,G] \leq [N^4,G] = 1$, segue que $[N^2,G] = [N,G]^2 \leq (N^4)^2 = 1$, como queríamos demonstrar.

□

Definição 2.13. *Seja G um p-grupo finito. Então:*

$$G_1 = G, \quad G_{i+1} = G_i^p[G_i,G] \quad \textit{para} \quad i \geq 1.$$

Lema 2.14 ([5], Lema 2.4)**.** *Seja G um p-grupo powerful.*

(i) *Para cada i, G_i p.e. G, e $G_{i+1} = G_i^p = \Phi(G_i)$*

(ii) *Para cada i, a função $x \mapsto x^p$ induz um homomorfismo de G_i/G_{i+1} para G_{i+1}/G_{i+2}.*

Demonstração. **(i)** Como $G = G_1$ é *powerful*, G_1 p.e. G. Suponha que G_i p.e. G para $i \geq 1$. Então $G_{i+1} = G_i^p[G_i, G] = G_i^p$, e a Proposição 2.12 mostra que G_{i+1} p.e. G. Como $G_i^p \leq \Phi(G_i) = G_i^p[G_i, G_i] \leq G_{i+1}$, isso também implica que $G_{i+1} = \Phi(G_i)$. O resultado segue por indução.

(ii) A parte (i) mostra que G_i é *powerful*, então, mudando a notação, podemos assumir que $G_i = G_1 = G$, $G_{i+1} = G_2$ e $G_{i+2} = G_3$. Agora, substituindo G por G/G_3 (que também será *powerful* por (i) do Lema 2.10) e podemos assumir que $G_3 = 1$; Sendo G *powerful*, $[G, G] \leq G^p = G_2$, e como $(G_2)^p = G_3 = 1$, segue que $[G, G] \leq G_2 \leq Z(G)$. Então para $x, y \in G$ temos, pelo Teorema 1.6.5:

$$(xy)^p = x^p y^p \pmod{(G')^p \gamma_p(G)}$$

Como $G' \leq G^p = G_2$, então $(G')^p \leq (G_2)^p = G_3 = 1$. Além disso, sendo $p \geq 3$, $\gamma_p(G) \leq [G', G] = 1$ pois $G' \leq G_2$, e G_2 é central. Logo, $(xy)^p = x^p y^p$.

Se $p = 2$ então $[G, G] \leq G^4 \leq (G^2)^2 \leq G_3 = 1$. Por isso em todo caso temos $(xy)^p = x^p y^p$. Como $G_2^p = G_3 = 1$ e $G^p = G_2$, isso mostra que $x \mapsto x^p$ induz um homomorfismo de G/G_2 para G_2/G_3, completando a prova.

□

Lema 2.15 ([5], Lema 2.5)**.** *Seja $G = \langle a_1, ..., a_d \rangle$ um p-grupo powerful. Então $G^p = \langle a_1^p, ..., a_d^p \rangle$.*

Demonstração. Seja $\theta : G/G_2 \to G_2/G_3$ o homomorfismo dado no lema anterior. Então G_2/G_3 é gerado por $\{(a_1 G_2)^\theta, ..., (a_d G_2)^\theta\}$. Logo, $G_2 = \langle a_1^p, ..., a_d^p \rangle G_3$. Pelo Lema 2.14, $G_3 = \Phi(G_2)$, então pelo Teorema da Base de Burnside (1.4.11), $G_2 = \langle a_1^p, ..., a_d^p \rangle$. Novamente pelo Lema 2.14, $G_2 = G^p$ e o resultado segue. □

O resultado a seguir mostra algo que comentamos anteriormente, que os grupos *powerful* são uma classe de grupos em que G^p coincide com o conjunto das p-ésimas potências.

Proposição 2.16 ([5], Proposição 2.6)**.** *Se G é um p-grupo powerful então todo elemento de G^p é uma potência de p, ou seja, $G^p = \{x^p \mid x \in G\}$.*

Demonstração. Argumentaremos por indução em $|G|$. Pelo Lema 2.14, como visto na demosntração anterior, $G_2 = \langle a_1^p, ..., a_d^p \rangle G_3$, então dado $g \in G_2$, existem $x \in G$ e $y \in G_3$

tais que $g = x^p y$. Considere $H = \langle G^p, x\rangle$. Novamente pelo Lema 2.14, $G^p = G_2$ p.e. G. Assim, o item (iii) do Lema 2.10 implica que H é *powerful*. Também, $g \in H^p$, pois $y \in G_3 = G_2^p$. Se $H \neq G$ então a hipótese de indução nos dá que g é uma potência de p em H. Se $H = G$, então, como G é *powerful*, $\Phi(G) = G^p$ e pelo Teorema da Base de Burnside (1.4.11), $G = \langle x\rangle$ é cíclico, e nesse caso o resultado é trivial. □

Entretanto, não é um se e somente se, ou seja, ter essa propriedade satisfeita não é suficiente para que o grupo seja *powerful*, como podemos ver no exemplo a seguir.

Exemplo 2.17 ([7], Exercício 2.4)**.** *Seja p um primo ímpar e seja $G = N \rtimes H$ onde $H = \langle b\rangle \cong C_{p^2}$ e $N = \langle a_1\rangle \times \langle a_2\rangle \times ... \times \langle a_{p-1}\rangle \cong C_{p^2} \times C_p \times ... \times C_p$ com respeito a ação dada por*

$$a_1^b = a_1 a_2,\ a_2^b = a_2 a_3,\ ...,\ a_{p-1}^b = a_{p-1} a_1^{-p}$$

e com a relação

$$b^p = a_1^p.$$

Tal grupo tem ordem p^{p+1}. É claro que $\langle a_1^p\rangle \leq G^p$. Como $(a_1^p)^b = (a_1^b)^p = (a_1 a_2)^p = a_1^p$ temos que a_1^p comuta com todos os geradores de G, logo, a_1^p é central em G. Então podemos olhar para o quociente $G/\langle a_1^p\rangle$, que tem ordem p^p e é gerado por elementos de ordem p. Pelo Teorema 2.8 de [7], tal grupo é regular e pelo Corolário 2.11 da mesma referência, $exp(G/\langle a_1^p\rangle) = p$. Logo, $(G/\langle a_1^p\rangle)^p$ é trivial. Isso significa que todas as outras potências de p de G caem em $\langle a_1^p\rangle$. Portanto, $G^p = \langle a_1^p\rangle$, ou seja, G^p coincide com o conjunto das p-ésimas potências de G. Por outro lado, é fácil ver que $G' = \langle a_2, a_3, ..., a_{p-1}, a_1^{-p}\rangle$. Como $\langle a_1^{-p}\rangle = \langle a_1^p\rangle$, segue que $G^p < G'$, logo, esse grupo não é powerful

Podemos agora resumir as principais características da série G_i em um p-grupo *powerful*:

Teorema 2.18 ([5], Teorema 2.7)**.** *Seja $G = \langle a_1, ..., a_d\rangle$ um p-grupo powerful, e seja $G_1 = G$ e $G_{i+1} = G_i^p[G_i, G]$ para cada i. Então:*

(i) *G_i p.e. G;*

(ii) *$G_{i+k} = G_i^{p^k}$ para cada $k \geq 0$;*

(iii) *$G_i = G^{p^{i-1}} = \{x^{p^{i-1}} \mid x \in G\} = \langle a_1^{p^{i-1}}, ..., a_d^{p^{i-1}}\rangle$;*

(iv) *Para cada i e k, a função $x \mapsto x^{p^k}$ induz um homomorfismo de G_i/G_{i+1} para G_{i+k}/G_{i+k+1}.*

Demonstração. Nós já estabelecemos (i) no Lema 2.14.

Para demonstrar (iii), veja que por esse mesmo lema temos $G_{i+1} = G_i^p$ para cada i, o que nos garante a base da indução. Segue da Proposição 2.16 que $G_{i+1} = \{x^p \mid x \in G_i\}$. Por indução, $G_i = \{x^{p^{i-1}} \mid x \in G\}$, então para cada $x \in G_i$ existe $y \in G$ tal que $x = y^{p^{i-1}}$, assim $G_{i+1} = \{(y^{p^{i-1}})^p \mid y \in G\} = \{y^{p^i} \mid y \in G\} \leq G^{p^i}$. Como G_{i+1} é um subgrupo temos que $G_{i+1} = G^{p^i}$. De maneira similar, repetidas aplicações do Lema 2.15 mostram que $G_i = \langle a_1^{p^{i-1}}, ..., a_d^{p^{i-1}} \rangle$, concluindo a prova de (iii).

Para demonstrar (iv), utilizaremos indução. O Lema 2.14, item (ii), nos garante o passo base da indução. Seja $\theta_k : G_i/G_{i+1} \to G_{i+k}/G_{i+k+1}$ o homomorfismo que mapeia $x \mapsto x^{p^k}$. Por conta de (iii), sabemos que esse homomorfismo é sobrejetivo. Considere $\rho : G_{i+k}/G_{i+k+1} \to G_{i+k+1}/G_{i+k+2}$, a função que mapeia $x^{p^k} \mapsto x^{p^{k+1}}$ que, novamente por (ii) do Lema 2.14, é um homomorfismo. Então podemos fazer a composição: $\theta_{k+1} = \theta_k \circ \rho : G_i/G_{i+1} \to G_{i+k+1}/G_{i+k+2}$, que leva $x \mapsto x^{p^{k+1}}$ e é um homomorfismo, demonstrando (iv).

Por fim, tomando G_i no lugar de G e $k+1$ no lugar de i em (iii), obtemos

$$G_i^{p^k} = \{x^{p^k} \mid x \in G_i\} = \{y^{p^{i-1+k}} \mid y \in G\} = G_{i+k},$$

nos dando o resultado de (ii).

□

Observação 2.19. *Pelo item (iii) do teorema anterior, podemos reescrever o item (iv) dizendo que a função $x \mapsto x^p$ induz um homomorfismo de $G^{p^{i-1}}/G^{p^i}$ para $G^{p^i}/G^{p^{i+1}}$. É nesse formato que esse resultado será utilizado na demonstração do Teorema 3.13. Também, se G powerful, pelo item (ii) e (iii) do teorema anterior, temos que*

$$((G)^{p^{i-1}})^p = (G_i)^p = G_{i+1} = (G)^{p^i}.$$

Por isso, no Capítulo 3 usaremos livremente que, em um grupo powerful G, $((G)^{p^{i-1}})^p = (G)^{p^i}$.

Munidos dos resultados colocados, agora a ideia de que fazer o quociente por G^{p^i} limita o expoente nos trará a seguinte consequência:

Corolário 2.20 ([5], Corolário 2.8)**.** *Seja $G = \langle a_1, ..., a_d \rangle$ um p-grupo powerful, então $G = \langle a_1 \rangle ... \langle a_d \rangle$.*

Demonstração. Seja $p^e = exp(G)$, então $G_e > G_{e+1} = 1$. Se $e = 1$, $G_2 = G^p = 1$. Como G é *powerful*, $\Phi(G) = G^p = 1$, então $G = \langle a_1, ..., a_d \rangle$ é abeliano elementar, logo, G é produto dos subgrupos cíclicos $\langle a_i \rangle$. Suponha que o resultado vale para grupos de expoente $< p^e$. Considere $G/G_e = \langle a_1 G_e, ..., a_d G_e \rangle$. Como comentamos anteriormente, $G/G_e = G/G^{p^{e-1}}$

é um grupo de expoente p^{e-1}, então pela hipótese de indução $G/G_e = \langle a_1 G_e\rangle ... \langle a_d G_e\rangle$. Logo, $G = \langle a_1\rangle ... \langle a_d\rangle G_e$. Por (iii) do Teorema 2.18, $G_e = \langle a_1^{p^{e-1}}, ..., a_d^{p^{e-1}}\rangle$ e por (i) do mesmo Teorema, G_e p.e G, ou seja, $[G_e, G] \leq (G_e)^p = G_{e+1} = 1$, e isso implica que G_e é central em G. Portanto, $G = \langle a_1\rangle ... \langle a_d\rangle$.

□

O maior resultado dessa seção, e que será bastante utilizado na demonstração dos resultados principais, relaciona a propriedade de ser *powerful* com a existência de conjuntos geradores "menores" para os subgrupos de um p-grupo, ou seja, se G é um p-grupo *powerful* e $H \leq G$, então $d(H) \leq d(G)$. Esse resultado é surpreendente porque não ocorre de forma geral. Segue um contra-exemplo de tal propriedade:

Exemplo 2.21. *Seja $G = C_p \wr C_p$ o produto entrelaçado de C_p com C_p, ou seja, $G = (\langle a_1\rangle \times ... \times \langle a_p\rangle) \rtimes \langle b\rangle \cong (C_p \times \underset{p}{...} \times C_p) \rtimes C_p$ com a ação dada por*

$$a_1^b = a_2,\ a_2^b = a_3,\ ...\ a_{p-1}^b = a_p,\ a_p^b = a_1$$

Temos que $G = \langle b, a_1\rangle$, mas G possui um subgrupo próprio $H = \langle a_1, ..., a_p\rangle$, e $d(H) = p$. Se p é um primo ímpar, $d(H) \geq d(G)$. Portanto, esse grupo não é powerful.

Na demonstração do próximo teorema, lembre-se que $d(G)$ é também a dimensão de $G/\Phi(G)$ como espaço vetorial sobre $\mathbb{F}_p$ (Teorema 1.4.11). Denotaremos a dimensão de um espaço vetorial V por $dim(V)$. Também vamos recorrer diversas vezes na demonstração do resultado seguinte ao Teorema do Núcleo e da Imagem, resultado clássico de Álgebra Linear, que afirma que, dados U e V espaços vetoriais de dimensão finita, se T é uma transformação linear $T : V \to U$ então $dim(Im(T)) = dim(V) - dim(Ker(T))$.

Teorema 2.22 ([16], Teorema 11.18)**.** *Se G é um p-grupo powerful e $H \leq G$, então $d(H) \leq d(G)$.*

Demonstração. Seja $E_i = G_i/G_{i+1}$. Pelo Lema 2.14, $\Phi(G_i) = G_{i+1}$, logo, pelo Teorema da Base de Burnside (1.4.11), E_i é abeliano elementar, e E_i pode ser visto como espaço vetorialsobre F. Além disso, $dim(E_i) = d(G_i) \leq d$, por conta do Lema 2.15.

Para um subgrupo arbitrário $H \leq G$, construiremos os geradores de H indutivamente como elementos de $(H \cap G_i) \setminus G_{i+1}$. Denotaremos por V_i o quociente $(H \cap G_i)G_{i+1}/G_{i+1}$ visto como um subespaço vetorial de E_i.

Escolha $h_1, ..., h_{n_1}$ em H tais que suas imagens em G/G_2 formem uma base de $V_1 = HG_2/G_2$. Note que $dim(E_1/V_1) = d - n_1$.

Suponha que tenhamos construído elementos:

- $h_1, ..., h_{n_1} \in H \cap G$
- $h_{n_1+1}, ..., h_{n_2} \in H \cap G_2$
  $\vdots$
- $h_{n_{k-2}+1}, ..., h_{n_{k-1}} \in H \cap G_{k-1}$

tais que as imagens de $h_1^{p^{k-2}}, ..., h_{n_1}^{p^{k-2}}, h_{n_1+1}^{p^{k-3}}, ..., h_{n_2}^{p^{k-3}}, ..., h_{n_{k-2}+1}, ..., h_{n_{k-1}}$ em E_{k-1} geram V_{k-1} e $dim(E_{k-1}/V_{k-1}) \leq d - n_{k-1}$. Para ficar mais claro, lembre-se que $E_{k-1} = G_{k-1}/G_k$ e $G_{k-1} = G^{p^{k-2}}$, então, como $h_i \in G_i = G^{p^{i-1}} = \{x^{p^{i-1}} \mid x \in G\}$ pelo Teorema 2.18, existe $x \in G$ tal que $h_i = x^{p^{i-1}}$, daí $h_i^{p^{k-i-1}} = (x^{p^{i-1}})^{p^{k-i-1}} = x^{p^{k-2}} \in G_{k-1}$, por isso que as imagens dessas potências de h_j recaem em E_{k-1}.

Seja W o subespaço de E_k gerado pela imagem dos elementos $h_1^{p^{k-1}}, ..., h_{n_1}^{p^{k-1}}, h_{n_1+1}^{p^{k-2}}, ..., h_{n_2}^{p^{k-2}}, ..., h_{n_{k-2}+1}^{p}, ..., h_{n_{k-1}}^{p}$ em E_k. Então $dim(E_k/W) \leq d - n_{k-1}$, porque pegar potências de p induz um homomorfismo de E_{k-1}/V_{k-1} em E_k/W, como vimos no item (iv) do Teorema 2.18.

Escolha elementos $h_{n_{k-1}+1}, ..., h_{n_k} \in H \cap G_k$ (possivelmente, um conjunto vazio) tais que suas imagens formam uma base de V_k/W. Então

$$dim(E_k/V_k) = dim(E_k/W) - dim(V_k/W) = dim(E_k/W) - (n_k - n_{k-1}) \leq d - n_k$$

A definição está completa.

A construção acima termina alcançando o subgrupo identidade $G_{e+1} = G^{p^e} = 1$, onde $p^e = exp(G)$. A última desigualdade para dimensão, $d - n_{e+1} \geq dim(E_e/V_e) \geq 0$, implica que $d \geq n_{e+1}$, ou seja, o número total de elementos h_j construídos será no máximo d.

Provaremos por indução no expoente de G que os h_j juntos geram H. Para $e = 1$, $G_2 = G^p = 1$, e nesse caso $E_1 = G/G_2 = G$ e $V_1 = H = \langle h_1, ..., h_{n_1} \rangle$. Para $e > 1$, temos $H/G_e \leq \langle h_1 G_e, ..., h_{n_e} G_e \rangle$ pela hipótese de indução, então $H = \langle h_1, ..., h_{n_e} \rangle G_e$. Como $\langle h_1, ..., h_{n_e} \rangle \leq H$, resta expressar um elemento arbitrário de $H \cap G_e = (H \cap G_e)G_{e+1}/G_{e+1} = V_e$ nos $h_j's$, o que é possível, de acordo com a construção feita.

□

O próximo resultado é feito no próprio artigo de Fernández-Alcober e De Las Heras [6], e já se volta para o contexto do resultado principal desse trabalho, de grupos 2-gerados.

Lema 2.23 ([6], Lema 2.2)**.** *Seja G um p-grupo finito powerful. Então:*

(i) *Se $H \leq G$ também é powerful então $|G^{p^i} : H^{p^i}| \leq |G : H|$ para todo $i \geq 0$.*

(ii) *Se $d(G) = 2$ então todo subgrupo de G também é powerful.*

Demonstração. **(i)** Mostraremos por indução em i. Como G é *powerful*, pelo Teorema 2.22, $d(H) \leq d(G)$, e como H também é *powerful*, temos que e $|G : G^p| = p^{d(G)}$, logo $|H : H^p| \leq |G : G^p|$. Temos que:

$$|G : H||H : H^p| = |G : G^p||G^p : H^p|$$

Como $|H : H^p| \leq |G : G^p|$, para que essa igualdade valha é necessário que $|G^p : H^p| \leq |G : H|$, então o resultado segue para $i = 1$.

Suponha que o resultado vale para naturais menores que i. Temos que $G^{p^i} = (G^p)^{p^{i-1}}$ e $H^{p^i} = (H^p)^{p^{i-1}}$. Como G e H são *powerful*, pelo Lema 2.12 G^p e H^p também o são. Sendo assim, podemos aplicar a hipótese de indução à G^p e H^p, logo:

$$|G^{p^i} : H^{p^i}| = |(G^p)^{p^{i-1}} : (H^p)^{p^{i-1}}| \leq |G^p : H^p| \leq |G : H|$$

demonstrando o resultado.

(ii) Demonstraremos por indução na ordem do grupo. Se $|G| = p$ ou p^2, G é abeliano e seus subgrupos são abelianos, logo são *powerful*. Suponha que a hipótese valha para qualquer grupo de ordem menor que a ordem de G. Se M é um maximal de G, e sendo G *powerful*, pelo Teorema 2.22, $d(M) \leq d(G)$, então $d(M) = 1$ ou 2. Se $d(M) = 1$, então M é abeliano e todos os seus subgrupos são *powerful*. Podemos supor então $d(M) = 2$. Se M for *powerful*, pela hipótese de indução todos os seus subgrupos também serão, e como M é um maximal arbitrário e todo subgrupo de G está contido em algum maximal, então o resultado se estende para G. Logo, é suficiente mostrar que M é *powerful*.

Como G é *powerful* e $d(G) = 2$, $|G : G^p| = p^2$ e, sendo M um maximal de um p-grupo, $|G : M| = p$ e $G^p = \Phi(G) \leq M$, então podemos escrever:

$$\underbrace{|G : G^p|}_{p^2} = \underbrace{|G : M|}_{p} |M : G^p|$$

Logo, $|M : G^p| = p$, ou seja, existe $x \in M$ tal que $M = \langle x \rangle G^p$. Sendo G^p *powerful embedded* em G Teorema 2.12 segue do Lema 2.10 que M é *powerful*.

□

Capítulo

3

Comutadores em p-grupos finitos com subgrupo comutador 2-gerado

Nesse capítulo demonstraremos os principais resultados estudados na dissertação, o Teorema A e o Teorema B de [6] citados na Introdução.

Vamos começar relembrando o seguinte resultado de Blackburn [2, Teorema 1], que vai nos permitir reduzir a demonstração do Teorema A ao caso em que G' é *powerful*.

Lema 3.1. *Seja G um p-grupo finito tal que $d(G') \leq 2$. Então ou G' é abeliano ou pode ser gerado por dois elementos a e b com relações definidas por $a^{p^m} = b^{p^{n+k}} = 1$ e $[a,b] = b^{p^n}$, com $k > 0$ e $n \geq m \geq 2k$.*

Como consequência, se o subgrupo comutador de um p-grupo G pode ser gerado por dois elementos, temos $G'' \leq (G')^{p^2}$ e G' é *powerful*.

Afinal, se G' é abeliano, então já temos que G' é *powerful*; se não, pelo Lema 3.1, $G' = \langle a, b\rangle$ com relações $a^{p^m} = b^{p^{n+k}} = 1$ e $[a,b] = b^{p^n}$, com $k > 0$ e $n \geq m \geq 2k$. Considere $N = \langle [a,b]\rangle = \langle b^{p^n}\rangle$. Então

$$a^{-1}b^{-1}ab = b^{p^n}$$

$$a^{-1}b^{-1}a = b^{p^n-1}$$

$$aba^{-1} = b^{-(p^n-1)}$$

$$ab^{p^n}a^{-1} = (aba^{-1})^{p^n} = (b^{-(p^n-1)})^{p^n} = (b^{p^n})^{-(p^n-1)}$$

Ou seja, a e b normalizam N, logo $N \trianglelefteq G'$. Como $ab = ba[a,b]$, temos que em G'/N os geradores aN e bN comutam, então G'/N é abeliano e $G'' \leq N$. Como $N = \langle [a,b] \rangle \leq G''$, segue que $G'' = \langle [a,b] \rangle$. Mas $[a,b] = b^{p^n}$ e $k > 0$ implica que $n \geq 2$, portanto $G'' \leq (G')^{p^2}$ e assim G' é *powerful*.

O próximo passo é ver como podemos estender uma cobertura de comutadores de um elemento fixo x de um quociente para um grupo.

Lema 3.2. *Sejam G um grupo e $N \leq L \leq G$, com N normal em G. Suponha que para algum $x \in G$ as duas condições seguintes valem:*

(i) $L/N \subseteq K_{xN}(G/N)$.

(ii) $N \subseteq K_x(G)$.

Então $L \subseteq K_x(G)$.

Demonstração. Provaremos que para todo $y \in L$, $yN \subseteq K_x(G)$ (isso é suficiente pois $y \in yN$ daí $y \in K_x(G)$ e $L \subseteq K_x(G)$). De (i) temos que $\exists g \in G$ tal que:

$$yN = [xN, gN] = [x,g]N$$

Usando $N \trianglelefteq G$ e a condição (ii), temos que:

$$yN = [x,g]N = [x,g]N^g \subseteq [x,g]K_x(G)^g$$

Qualquer elemento de $[x,g]K_x(G)^g$ é da forma:

$$[x,g][x,h]^g = [x,hg] \in K_x(G)$$

Então o resultado segue.

□

O próximo lema será necessário em combinação com os resultados seguintes.

Lema 3.3. *Seja G um grupo e seja $N \leq L \leq G$, com N normal em G. Se $L/N = \langle [x,s]N \mid s \in S \rangle$ para algum $x \in G$ e algum $S \subseteq G$ com $[L,S] \subseteq N$, então $L/N \subseteq K_{xN}(\langle S \rangle N/N) \subseteq K_{xN}(G/N)$.*

Demonstração. Temos que $L/N = \langle [x,s] \mid s \in S \rangle$ e $K_{xN}(\langle S \rangle N/N) = \{[xN, sN], s \in \langle S \rangle\} = \{[x,s]N \mid s \in \langle S \rangle\}$. Então, para concluir que $L/N \subseteq K_{xN}(\langle S \rangle N/N)$, mostraremos que, dados $[x,s_1]N$ e $[x,s_2]N$ geradores de L/N:

$$[x,s_1]N[x,s_2]N = [x,s_2s_1]N \tag{3.1}$$

Como $[L,S] \subseteq N$, então $\forall l \in L$ e $\forall s \in S$, $l^{-1}s^{-1}ls \in N$ e daí $s^{-1}ls \subseteq lN$. Então $[x,s_2]^{s_1} \subseteq [x,s_2]N$. Assim, mudando o representante da classe lateral, temos:

$$[x,s_1][x,s_2]N = [x,s_1][x,s_2]^{s_1}N = x^{-1}s_1^{-1}xs_1 \cdot s_1^{-1} \cdot x^{-1}s_2^{-1}xs_2 \cdot s_1N$$

$$= x^{-1}s_1^{-1}s_2^{-1}xs_2s_1N = [x,s_2s_1]N$$

□

Agora veremos um lema que é a chave para a demonstração do Teorema A. Ele mostra que, sobre algumas condições específicas, cobrir o quociente L/L^p com comutadores de um dado elemento x é suficiente para cobrir L.

Recordamos que, se L e N são dois subgrupos normais de um grupo G e $n \in \mathbb{N}$, então o Lema 1.2.19 garante que

$$[L^n, N] \leq [L,N]^n[L,N,L]$$

.

Lema 3.4. *Seja G um p-grupo finito e seja $N \leq L$ subgrupos normais de G, com L powerful e $d(L) \leq 2$. Então segue que:*

(i) *Se existem $x, g \in G$ tais que $L/N = \langle [x,g]N \rangle$ e $[x,g,g] \in N^p$, então $L^{p^i}/N^{p^i} = \langle [x,g^{p^i}]N^{p^i} \rangle$ para todo $i \geq 1$.*

(ii) *Assuma ainda que $L^p \leq N$ e $|L:N| = p$. Se existem $x,g,h \in G$ tais que $L/N = \langle [x,g]N \rangle$ e $N/L^p = \langle [x,h]L^p \rangle$ com $[x,g,g] \in N^p$ e $[x,h,h] \in L^{p^2}$, então $L \subseteq K_x(G)$.*

Demonstração. **(i)** Argumentaremos por indução em i. Assuma primeiro que $i = 1$. Como L é *powerful* e $L = \langle [x,g], N \rangle$, pelo Lema 2.15, $L^p = \langle [x,g]^p, N^p \rangle$, então $L^p/N^p = \langle [x,g]^p N^p \rangle$.

Temos que $[[x,g],g] \in N^p$, ou seja, $[x,g]N^p$ e gN^p comutam, e com isso podemos usar a equação (3.1) do Lema 3.3 com $\langle [x,g]N^p \rangle$ e $S = \{g\}$, daí:

$$[x,g^p] \equiv [x,g]^p \pmod{N^p} \tag{3.2}$$

E consequentemente $L^p/N^p = \langle [x,g^p]N^p \rangle$. Agora seja $i > 1$. Por (ii) do Lema 2.2, N também é *powerful* ($N \leq L$, L é *powerful* e $d(L) = 2$). Se provarmos que $[x,g^p,g^p] \in N^{p^2}$, então podemos usar a hipótese de indução com L^p no lugar de L, N^p no lugar de N e g^p no lugar de g, e isso termina a demonstração.

Como L é *powerful*, $d(L) \leq 2$ e $N^p \leq L$, novamente por (ii) do Lema 2.2, N^p é *powerful* e pelo Teorema 2.22, temos $d(N^p) \leq d(L) \leq 2$, então pelo Corolário 2.9, $|N^p : N^{p^2}| \leq p^2$. Como $N \trianglelefteq G$, segue do Lema dos Três Subgrupos (1.2.5) que $[N^p, [G, G]] \leq [[N^p, G], G]$.

Como $N^p \trianglelefteq G$ (pois N é normal em G e N^p é característico em N) , $[N^p, G] \leq N^p$ e $|N^p : [N^p, G]| \geq p$, pelo que foi explicado na Observação 1.3.2. Analogamente, $|N^p : [N^p, G, G]| \geq p^2$. Isso implica que, em N^p/N^{p^2}, $[N^p, G, G]/N^{p^2}$ "recai" na identidade que é N^{p^2}, porque N^p/N^{p^2} tem ordem no máximo p^2. Ou seja:

$$\underbrace{N^{p^2} \text{——} \overbrace{[N^p, G, G] \text{——} N^p}^{\geq p^2}}_{\leq p^2}$$

implica que $[N^p, G, G] \leq N^{p^2}$.

Também, $[N^p, G] \leq N^p$ implica $[N^p, G]^p \leq N^{p^2}$. Como consequência de ambos, aplicando o Lema 1.2.19, temos: $[N^p, G^p] \leq [N^p, G]^p [N^p, G, G] \leq N^{p^2}$. Por conta de (3.2), temos que $[[x, g^p], g^p] \equiv [[x, g]^p, g^p] \pmod{[N^p, G^p]}$, então, agora com a desigualdade anterior, temos $[[x, g^p], g^p] \equiv [[x, g]^p, g^p] \pmod{N^{p^2}}$.

Por outro lado, $[x, g, g] \in N^p$ significa que $[x, g]$ e g comutam módulo N^p, mas então $[x, g]$ e g^p também, ou seja, $[[x, g], g^p] \in N^p$. Segue que

$$[[x, g], g^p, [x, g]] \in [N^p, G'] \leq [N^p, G^p] \leq N^{p^2},$$

ou seja, $[[x, g], g^p]$ e $[x, g]$ comutam módulo N^{p^2}, e, assim como anteriormente, $[[x, g]^p, g^p] \equiv [[x, g], g^p]^p \pmod{N^{p^2}}$. Concluímos que:

$$[[x, g^p], g^p] \equiv [[x, g]^p, g^p] \equiv \underbrace{[[x, g], g^p]^p}_{\in N^{p^2}} \equiv 1 \pmod{N^{p^2}}$$

Então $[x, g^p, g^p] \in N^{p^2}$, como queríamos.

(ii) Considere a seguinte série normal em G:

$$L \geq N \geq L^p \geq N^p \geq L^{p^2} \geq N^{p^2} \geq \ldots \geq 1. \tag{3.3}$$

Por hipótese, $|L : N| = p$. E como L é *powerful* e $d(G) \leq 2$, temos $|L : L^p| \leq p^2$, por (2.9), e portanto $|N : L^p| \leq p$. Como consequência, se R e S são dois termos

consecutivos da série (3.3), então $|R : S| \leq p$, usando (i) do Lema 2.23. Então a seção R/S é central em G/S ($R/S \trianglelefteq G/S \underset{1.4.1}{\Longrightarrow} R/S \cap Z(G/S) \neq \emptyset \implies R/S \leq Z(G/S)$), ou seja, $[R, G] \leq S$.

Por outro lado, por (i), $R/S = \langle [x, y]S \rangle$ para algum $y \in G$. Então, pelo Lema 3.3, $R/S \subseteq K_{xS}(G/S)$. Se $S = 1$, $S \subseteq K_x(G)$, e pelo Lema 3.2 isso implica que $R \subseteq K_x(G)$. Subindo por indução a série (3.3) concluímos que $L \subseteq K_x(G)$.

□

Como uma ilustração do método baseado no Lema 3.4, vamos provar o resultado de que se G é um p-grupo finito e G' é cíclico, então G' consiste de comutadores.

Lema 3.5. *Seja G um p-grupo finito com G' cíclico. Então existe $x \in G$ tal que $G' = \{[x, g] \mid g \in G\}$.*

Demonstração. Para isso, aplicaremos o Lema 3.4 com $L = G'$ e $N = (G')^p$, pois, nesse caso, $|L : N| = |G' : (G')^p| = p$ (aplicando a equação (2.9), e sendo $d(G') = 1$) o que se encaixa com uma das hipóteses requeridas no Lema 3.4.

Resta mostrar que $G'/(G')^p = \langle [x, y](G')^p \rangle$, com x e y tais que $[x, y, y] \in (G')^{p^2}$. Note que já sabemos que G' é cíclico, mas isso não é suficiente para termos $G'/(G')^p = \langle [x, y](G')^p \rangle$, pois G', e consequentemente $G'/(G')^p$, poderiam ter como gerador um produto de comutadores, e não por um comutador. Além disso, precisamos de um gerador que satisfaça a segunda condição. Então a demonstração a seguir consiste em mostrar que G' pode ser gerado por um adequado comutador. Para encontrá-lo, utilizaremos o centralizador $C^* = C_G(G'/(G')^{p^2})$.

Suponha $G' = \langle g \rangle$ e $|G'| = p^m$. Então $(G')^{p^2} = \langle g^{p^2} \rangle$ e $\left|\frac{G'}{(G')^{p^2}}\right| = \frac{p^m}{p^{m-2}} = p^2$, daí $G'/(G')^{p^2} \cong C_{p^2}$. Se $K \trianglelefteq G$, $K^g = K$, então g induz um automorfismo em K, que será a identidade apenas quando $g \in C_G(K)$, ou seja, $G/C_G(K)$ é isomorfo a um subgrupo de $Aut(K)$. Nesse caso, temos que G/C^* é isomorfo a um subgrupo de $Aut(G'/(G')^{p^2}) \cong Aut(C_{p^2})$ e $|Aut(C_{p^2})| = p^2 - p = p(p-1)$. Sendo G/C^* um p-grupo, e sendo p a maior potência de p que divide $|Aut(C_{p^2})|$, temos que $|G : C^*| \leq p$. Sendo G/C^* cíclico, segue do Lema 1.2.18 que $G' = [G, C^*]$. Sendo G' cíclico, G' é *powerful*, então $\Phi(G') = (G')^p$, e olhando para $[G, C^*]/\Phi(G') = [G, C^*]/(G')^p$ vemos que não é possível que todo comutador recaia em $(G')^p$ pois $(G')^p < G'$, dessa forma, existem $x \in G$ e $y \in C^*$ tais que $\langle [x, y]\Phi(G') \rangle = G'/\Phi(G')$. Pelo Teorema da Base de Burnside (1.4.11), $G' = \langle [x, y] \rangle$.

Lembrando que $C^* = C_G(G'/(G')^{p^2})$, ou seja, $[G', C^*] \leq (G')^{p^2}$. Assim, $[x, y, y] \in [G, C^*, C^*] = [G', C^*] \leq (G')^{p^2}$. Com isso conseguimos aplicar o Lema 3.4 e obter o resultado desejado. Organizando o que obtemos da seguinte forma fica mais claro como as coisas se encaixam nas hipóteses do referido Lema, com $L = G'$ e $N = (G')^p$:

- $(G')^p \leq G' \trianglelefteq G$, G' *powerful* e $d(G') \leq 2$;
- $|L : N| = |G' : (G')^p| = p$;
- $L/N = G'/(G')^p = \langle [x, y](G')^p \rangle$ e $[x, y, y] \in (G')^{p^2}$;
- $N/L^p = (G')^p/(G')^p \cong \{1\}$, então podemos escrever $(G')^p/(G')^p = \langle [x, 1](G')^p \rangle$ e $[x, 1, 1] \in (G')^{p^2}$.

Concluímos que $G' = K_x(G)$.

□

Observação 3.6. *No entanto, se $d(G') = 2$, a situação é mais complicada e, na verdade, nem sempre é possível aplicar o Lema 3.4 com $L = G'$. É necessário começar um "efeito dominó" semelhante ao que foi feito na demonstração de (ii) do Lema 3.4. Além disso, precisamos cobrir com comutadores de um único elemento x dois fatores principais que assumirão os papeis de L/N e N/L^p, em vez de um como no caso de G' cíclico, e isso é mais complicado em alguns casos quando estamos lidando com $p = 2$. Por isso introduzimos os subgrupos $D(T)$ e $R(U)$ das Definições 3.11 e 3.15 abaixo, que, como será mostrado nos Lemas 3.12 e 3.16, satisfazem a propriedade de cobertura desejada para qualquer elemento x que estiver fora deles.*

O próximo subgrupo que introduziremos desempenha um papel fundamental na prova de Guralnick no caso em que G' é abeliano, no artigo [12], e também será importante nesse trabalho.

Definição 3.7. *Seja G um p-grupo finito com G' powerful. Definimos $C = C_G(G'/(G')^p)$,*

Observação 3.8. *Essa definição significa que se $c \in C$ e $g \in G'$ então $c^{-1}gc(G')^p = g(G')^p$, ou seja, $[c, g] \in (G')^p$. Em outras palavras, C é o maior subgrupo de G tal que $[G', C] \leq (G')^p$. Disso vemos também que, se $\sigma \in Aut(G)$, então $[x^\sigma, (G')^\sigma] \leq ((G')^p)^\sigma \implies [x^\sigma, G'] \leq (G')^p$, pois G' e $(G')^p$ são característicos em G; logo, C também é característico em G.*

Observação 3.9. *Sendo G' powerful, temos que $[G', G'] \leq (G')^p$, logo, $G' \leq C$. Quando p é ímpar, $[G', C] \leq (G')^p$ implica que G' é powerful embedded em C, mas isso não é suficiente no caso $p = 2$, pois precisaríamos ainda que $[G', C] \leq (G')^4$. No caso p ímpar, pelo Lema 2.12, $(G')^{p^i}$ é powerful embedded em C para todo $i \in \mathbb{N}$. Em outras palavras, temos $[(G')^{p^i}, C] \leq (G')^{p^{i+1}}$.*

No lema seguinte, que foi colocado de forma um pouco mais geral do que realmente precisamos, mostramos que isso ocorre para todos os primos (inclusive o 2), e mostramos também que inclusões similares valem para outros subgrupos comutadores envolvendo C.

Lema 3.10. *Seja G um p-grupo finito com G' powerful. Então:*

(i) $[(G')^{p^i}, C^{p^j}] \leq (G')^{p^{i+j+1}}$ *para todo* $i, j \geq 0$.

(ii) $[G, C^{p^j}] \leq (G')^{p^j}$ *para todo* $j \geq 0$.

(iii) *Se* $d(G') \leq 2$, *então* $|G : C| \leq p$.

Demonstração. **(i)** Usaremos indução em j. Assuma primeiro que $j = 0$, e mostraremos que $[(G')^{p^i}, C] \leq (G')^{p^{i+1}}$ por indução em i. Para $i = 0$, $[G', C] \leq (G')^p$ segue da definição de C, como já foi comentado. Agora, para $i > 0$, aplicando o Lema 1.2.19 e a hipótese de indução, temos que:

$$[(G')^{p^i}, C] \leq \underbrace{[(G')^{p^{i-1}}, C]}_{\leq (G')^{p^i}\,(h.i.)}{}^{p} [(G')^{p^{i-1}}, C, (G')^{p^{i-1}}] \leq (G')^{p^{i+1}} [(G')^{p^i}, (G')^{p^{i-1}}]$$

Naturalmente, $(G')^{p^{i-1}} \leq G'$, e sendo G' *powerful*, G'^{p^i} é *powerful embedded* em G' (pelo Teorema 2.18), então:

$$(G')^{p^{i+1}} [(G')^{p^i}, (G')^{p^{i-1}}] \leq (G')^{p^{i+1}} [(G')^{p^i}, G'] \leq (G')^{p^{i+1}}.$$

Agora, se $j > 0$, usando novamente o Lema 1.2.19 temos:

$$[(G')^{p^i}, C^{p^j}] \leq [(G')^{p^i}, C^{p^{j-1}}]^p [(G')^{p^i}, C^{p^{j-1}}, C^{p^{j-1}}]$$

Pela hipótese de indução, $[(G')^{p^i}, C^{p^{j-1}}] \leq (G')^{p^{i+j}}$, então:

$$[(G')^{p^i}, C^{p^{j-1}}]^p [(G')^{p^i}, C^{p^{j-1}}, C^{p^{j-1}}] \leq (G')^{p^{i+j+1}} [(G')^{p^{i+j}}, C] \leq (G')^{p^{i+j+1}}$$

Nessa primeira desigualdade usamos também que $C^{p^{j-1}} \leq C$ e na segunda usamos o passo base da indução.

(ii) Novamente, argumentamos por indução em j. No caso $j = 0$, $[G, C] \leq [G, G] = G'$. Se $j > 0$, utilizando que $[G, C^{p^{j-1}}] \leq (G')^{p^{j-1}}$ pela hipótese de indução e pelo Lema 1.2.19, segue que:

$$[G, C^{p^j}] \leq [G, C^{p^{j-1}}]^p [G, C^{p^{j-1}}, C^{p^{j-1}}] \leq (G')^{p^j} [(G')^{p^{j-1}}, C] \leq (G')^{p^j},$$

onde a última inclusão segue de (i).

(iii) Se $d(G') \leq 2$, como G' *powerful*, temos que $|G' : (G')^p| \leq p^2$ (pelo Corolário 2.9). Logo, sendo $C = C_G(G'/(G')^p)$, G/C induz automorfismos em $G'/(G')^p$ de forma que G/C é isomorfo a um subgrupo de $Aut(G'/(G')^p)$. De $|G' : (G')^p| \leq p^2$ concluímos que $G'/(G')^p \cong C_{p^2}$, $C_p \times C_p$ ou C_p. Em todo caso, a maior potência de p que divide $|Aut(G'/(G')^p)|$ é p. Dessa forma, $|G : C| \leq p$.

□

Para obter $G' = K_x(G)$ quando G' é 2-gerado, primeiro precisamos que $G' = [x, G]$, que é uma condição mais fraca. Na definição seguinte, construiremos o conjunto dos elementos que **não** satisfazem $G' = [x, G]$. Assim, para fazer o papel especial de um x tal que $G' = K_x(G)$ buscaremos por elementos fora desse conjunto.

Começaremos a trabalhar com os subgrupos $T\ max_G\ G'$, ou seja, T é maximal entre os subgrupos próprios de G' que são normais em G. É importante lembrar que, para grupos em geral, $T\ max_G\ G'$ não significa que T é maximal em G'. Por exemplo, em S_n, $n \geq 5$, o subgrupo comutador é A_n e o único subgrupo de A_n que é normal em S_n é 1, que não é maximal em A_n. Entretanto, em p-grupos $T\ max_G\ G'$ implica que $T\ max\ G'$. Afinal, suponha que $T\ max_G\ G'$ mas T não é maximal em G'. Considere $\overline{G} = G/T$, então, pelo Teorema 1.4.4, existe uma série normal tal que:

$$T = \overline{N_0} \trianglelefteq \overline{N_1} \ ... \ \overline{N_{k-2}} \trianglelefteq \overline{N_{k-1}} \trianglelefteq \overline{N_k} = \overline{G'}$$

sendo que cada $\overline{N_k}$ é normal em $\overline{G}$ e $|\overline{N_i} : \overline{N_{i-1}}| = p$. Mas assim teríamos $N_i \trianglelefteq G'$. Logo, pela escolha maximal de T, não pode haver N_i's além dos triviais, portanto, T é maximal em G'. Isso implica que $|G' : T| = p$ e que $\Phi(G') \leq T$, que serão fatos bastante utilizados.

Definição 3.11. *Seja G um p-grupo finito não abeliano. Para cada $T\ max_G\ G'$, definimos o subgrupo $D(T)$ pela condição*

$$D(T)/T = Z(G/T),$$

ou seja, $D(T)$ é o maior subgrupo de G que satisfaz $[D(T), G] \leq T$. Definimos também o conjunto $D = \bigcup\{D(T) \mid T\ max_G\ G'\}$.

Veja que, como $T \trianglelefteq G$, pelo menos $T \leq D(T)$. O próximo lema nos mostrará algumas propriedades de $D(T)$ e de D.

Lema 3.12. *Se G é um p-grupo finito não abeliano, então $[x, G] = G'$ se, e somente se, $x \notin D$. Além disso, se $d(G') \leq 2$, então:*

(i) *Para todo T max_G G', temos $\Phi(G) \leq D(T) \leq C$ e $log_p|G : D(T)|$ é par.*

(ii) *D é um subconjunto próprio de G.*

Demonstração. Veja que, dado $g \in G$,

$$[x, g]^h = h^{-1}[x, g]h = h^{-1}x^{-1}g^{-1}xgh = [h, x]x^{-1}h^{-1}g^{-1}xgh = [x, h]^{-1}[x, gh] \in [x, G].$$

Logo, $[x, G] \trianglelefteq G$. Sendo assim, se $[x, G]$ for um subgrupo próprio de G', $[x, G]$ necessariamente estará dentro de algum T max_G G'

($\Longrightarrow$) Suponha que $[x, G] = G'$. Então para qualquer T max_G G', $[x, G] \not\leq T$, ou seja, $x \notin D(T)$. Logo, $x \notin D$.

($\Longleftarrow$) Suponha que $x \notin D$. Logo, $x \notin D(T)$, ou seja, $[x, G] \not\leq T$ para todo T max_G G'. Então é necessário que $[x, G] = G'$.

Agora, vamos assumir que $d(G') \leq 2$. Lembrando que, nesse caso, G' é *powerful* pelo Lema 3.1 e $|G' : (G')^p| \leq p^2$ pelo Corolário 2.9.

(i) Seja T max_G G'. Para mostrar que $\Phi(G) \leq D(T)$ mostraremos que $[\Phi(G), G] \leq T$. Pelo item (ii) do Teorema 1.4.16 e pelo item (ix) do Teorema 1.2.4, temos que:

$$[\Phi(G), G] = [G^pG', G] = [G^p, G][G', G]$$

$$= [G^p, G]\gamma_3(G) \underset{1.2.19}{=} [G, G]^p[G, G, G]\gamma_3(G) = (G')^p\gamma_3(G)$$

Já temos que $\Phi(G') = (G')^p \leq T$ para qualquer T max_G G'. Agora, como $|G' : T| = p$, no quociente G'/T temos que $[G', G]/T$ necessariamente recai na identidade pois $[G', G]$ é próprio em G'. Assim, $(G')^p\gamma_3(G) \leq T$. Então $[\Phi(G), G] \leq T$ e com isso $\Phi(G) \leq D(T)$. Isso também implica que $G/D(T)$ pode ser visto como um espaço vetorial sobre $\mathbb{F}_p$.

Pelo Lema dos Três Subgrupos (1.2.5) e pela definição de $D(T)$, temos que:

$$[D(T), G'] \leq [D(T), G, G] \leq [T, G]$$

Como $|G' : T| = p$, e $[T, G]$ é próprio em T, então $|G' : [T, G]| \geq p^2$. Por isso, em $G'/(G')^p$, que tem ordem p^2, $[T, G]$ necessariamente recai na identidade que

é $(G')^p$, ou seja, $[T, G] \leq (G')^p$. Pelas desigualdades anteriores, isso implica que $[D(T), G'] \leq (G')^p$, e portanto $D(T) \leq C$.

Sendo $G/D(T)$ um espaço vetorial sobre $\mathbb{F}_p$ e $|G'/T| = p$, temos que G'/T pode ser visto como $\mathbb{F}_p$. Assim, podemos considerar a seguinte forma bilinear:

$$f : G/D(T) \times G/D(T) \to G'/T$$

$$(xD(T), yD(T)) \mapsto [x, y]T$$

Vamos mostrar que essa função está bem definida, é alternada e não-singular.

Se $(x_1D(T), y_1D(T)) = (x_2D(T), y_2D(T))$ então existem $d, d' \in D(T)$ tais que $x_1 = x_2d$ e $y_1 = y_2d'$. Então:

$$f(x_1D(T), y_1D(T)) = [x_1, y_1]T = [x_2d, y_2d']T \quad (1)$$

Usando a propriedade (iii) do Teorema 1.2.4:

$$(1) \ = [x_2, y_2d'] \underbrace{[x_2, y_2d', d]}_{\in T} \underbrace{[d, y_2d']}_{\in T} T = [x_2, y_2d']T$$

$$= \underbrace{[x_2, d]}_{\in T}[x_2, y_2] \underbrace{[x_2, y_2, d]}_{\in T} T = [x_2, y_2]T = f(x_2D(T), y_2D(T)),$$

portanto, f está bem definida. Além disso, f é alternada pois:

$$f(x_1D(T), x_2D(T)) = [x_1, x_2]T = [x_2d, x_2]T$$

$$[x_2, x_2] \underbrace{[x_2, x_2, d][x_2, d]}_{\in T} = [x_2, x_2]T = T$$

Por fim, f é não-singular pois se existe $d \in G$ tal que $[x, d] \in T \ \forall x \in G$ então $d \in D(T)$, que é a identidade de $G/D(T)$.

Com isso, pelo Corolário 5.1.7, temos que $dim_{\mathbb{F}_p}(G/D(T)) = log_p|G : D(T)|$ é par.

(ii) Suponha, por contradição, que $D = G$. Lembrando que $|G' : (G')^p| \leq p^2$, então analisaremos os dois casos: quando $|G' : (G')^p| = p$ e quando $|G' : (G')^p| = p^2$.

Se $|G' : (G')^p| = p$, então $(G')^p$ é maximal de G' e é normal em G, ou seja, $(G')^p \ max_G \ G'$, logo $D((G')^p) \in D$. Além disso, dado $T \ max_G \ G'$ temos que $(G')^p = \Phi(G') \leq T$. Mas como ambos são maximais em G', teremos $(G')^p = T$.

Logo, $D((G')^p) = D$. Consequentemente, $G' = [D, G] = [D((G')^p), G] \leq (G')^p$. Contradição! Então é necessário que $|G' : (G')^p| = p^2$.

Seja $x \in G$ arbitrário. Se $G = D$, então $x \in D$ e portanto $[x, G] < G'$. Como $|G'/(G')^p| = p^2$, a imagem de $[x, G]$ em $G'/(G')^p$ tem ordem no máximo p.

Temos que $[x, G] = \langle\ x^{-1}g^{-1}xg \mid g \in G\ \rangle = \langle\ x^{-1}x^g \mid g \in G\ \rangle$, então $[x, G]$ tem $|x^G|$ geradores. Logo, se $[x, G](G')^p$ tem ordem no máximo p, a classe de conjugação de $x(G')^p$ em $G'/(G')^p$ tem tamanho no máximo p. Isso implica que o tamanho de todas as classes de conjugação em $G'/(G')^p$ são iguais a 1 ou p, ou seja, $G/(G')^p$ é um p-grupo de largura no máximo 1, ou seja, $b(G) \leq 1$ (notação do Lema 1.4.18).

Logo, pelo Lema 1.4.18, isso implica que $|G'/(G')^p| \leq p$, o que nos leva novamente a uma contradição. Portanto, $D < G$.

□

Segue agora um exemplo simples de T e $D(T)$ para nos auxiliar a visualizar esses grupos.

Exemplo 3.0.1. *Considere o p-grupo* $G = \langle a, b, c \mid a^{p^3} = b^p = c^{p^2} = 1,\ [a, b] = 1,\ a^c = a^{1+p},\ b^c = ba^p \rangle$, *com p ímpar.*

Temos que $G' = \langle a^p \rangle$. *Sendo* G' *cíclico (e portanto powerful) segue que* $|G' : (G')^p| = p$. *Sendo* $G'/(G')^p$ *central em* $G/(G')^p$, *teremos* $C = G$.

Nesse caso simples, $T = (G')^p = \langle a^{p^2} \rangle$ *é o único maximal de* G', *então* $D = D(T)$.

Observe que $[a, G] = [b, G] = [c, G] = G'$, *portanto* $a, b, c \notin D$. *Também, já sabemos que* $\Phi(G) = \langle a^p \rangle \leq D(T)$. *Agora, pela Identidade de Hall-Petresco (Teorema 1.6.5) temos que*

$$[c^p, b] \equiv [c, b]^p \pmod{(N')^p \gamma_p(N)}$$

sendo $N = \langle c, [b, c] \rangle = \langle c, a^p \rangle$. *Então* $N' = \langle a^{p^2} \rangle$ *e* $(N')^p = 1$. *Também, para p ímpar,* $\gamma_p(N) = 1$. *Portanto,* $[c^p, b] = [c, b]^p = a^{p^2}$. *Analogamente mostra-se que* $[c^p, a] = a^{p^2}$.

Logo, $[c^p, G] \leq T$*, portanto* $D(T) = \langle a^p, c^p \rangle$*. Resumindo:*

$$\begin{array}{c} G = C \\ | \\ D(T) = \langle a^p, c^p \rangle \\ | \\ G' = \langle a^p \rangle \\ | \\ T = (G')^p = \langle a^{p^2} \rangle \end{array}$$

De forma mais geral, o último lema nos mostra que sempre teremos a seguinte situação:

$$(G')^p \text{ —— } T \text{ —— } G' \text{ —— } \Phi(G) \text{ —— } D(T) \text{ —— } C \text{ —— } G$$

Pelo Lema 3.12, se $d(G') \leq 2$ então D é próprio em G. Logo, sempre existe um elemento $x \in G$ tal que $G' = [x, G]$. Já que $|G : C| \leq p$ pelo Lema 3.10 e $D \subseteq C$, podemos escolher $x \notin D$ de modo que $G = \langle x \rangle C$ e $G' = [x, C]$, pois $G' = [x, G] = [x, \langle x \rangle C] = [x, C]$. Agora estamos em posição de provar o Teorema A para $p > 2$.

Teorema 3.13. *Seja* G *um* p*-grupo finito, em que* p *é um primo ímpar, e suponha que* $d(G') = 2$*. Então* $G' = K_x(G)$ *para um certo* $x \in G$*.*

Demonstração. Nos comentários anteriores vimos que $G' = [x, C]$ para algum $x \notin D$. Então $G'/(G')^p = \langle [x, u](G')^p \mid u \in C \rangle$ e, pela definição de C, $[G', C] \subseteq (G')^p$. Logo, estamos em condições de aplicar o Lema 3.3, que nos dá $G'/(G')^p \subseteq K_{x(G')^p}(C/(G')^p) \subseteq K_{x(G')^p}(G/(G')^p)$. Como $G'/(G')^p = \langle [x, u](G')^p \mid u \in C \rangle$, isso implica que $G'/(G')^p = \{[x, u](G')^p \mid u \in C\}$. Pelo Lema 3.2, se tivermos $G'/(G')^p \subseteq K_{x(G')^p}(G/(G')^p)$ e $(G')^p \subseteq K_x(G)$, conseguimos que $G' = K_x(G)$. Então nos resta mostrar que $(G')^p \subseteq K_x(G)$. Para isso utilizaremos o Lema 3.4, então o resto da demonstração buscará satisfazer as condições desse lema. Como segue diretamente se $(G')^p$ for trivial, assumiremos que $(G')^p \neq 1$.

Considere agora a função:

$$\rho : G'/(G')^p \to (G')^p/(G')^{p^2}$$

$$g(G')^p \mapsto g^p(G')^{p^2}$$

Pelo Teorema 2.18, ρ é um homomorfismo. Além disso, sendo G' *powerful*, $(G')^p = \{x^p \mid x \in G'\}$ pelo Lema 2.16, logo, ρ é um epimorfismo (homomorfismo sobrejetivo). Assim, $G'/(G')^p = \{[x,u](G')^p \mid u \in C\}$ implica que $(G')^p/(G')^{p^2} = \{[x,u]^p(G')^{p^2} \mid u \in C\}$.

Agora, se $u \in C$, então, pela Identidade de Hall-Petresco (1.6.5), $[x,u^p] = [x,u]^p w$ para algum $w \in (H')^p\gamma_p(H)$, onde $H = \langle (u^{-1})^x, u\rangle = \langle u, [x,u]\rangle$. Vamos mostrar que $(H')^p\gamma_p(H) \leq (G')^{p^2}$.

Temos que $H' = \langle [x,u], u\rangle' \leq [[G,C],C]$. Como $G' = [x,C]$, $[G,C,C] = [G',C]$. Lembrando que $C = C_G(G'/(G')^p)$, então $[G',C] \leq (G')^p$. Logo, $H' \leq (G')^p$, o que implica $(H')^p \leq (G')^{p^2}$. Como $C \trianglelefteq G$, $[G,C] \leq C$, então $[x,u] \in C$, daí $H = \langle u, [x,u]\rangle \leq C$. E por (i) do Lema 3.10, $[(G')^p, C] \leq (G')^{p^2}$. Com isso, podemos ver que:

- $\gamma_2(H) = [H,H] = H' \leq (G')^p$
- $\gamma_3(H) = [H,H,H] = [H',H] \leq [(G')^p, H] \leq [(G')^p, C] \leq (G')^{p^2}$
- $\gamma_q(H) \leq \gamma_3(H) \leq (G')^{p^2}$, para $q > 3$ (Observação 3.14).

Portanto, $[x,u]^p \equiv [x,u^p] \pmod{(G')^{p^2}}$ para todo $u \in C$. Como $G' = [x,C]$, $(G')^p = [x,C]^p$. Pelo epimorfismo $\rho : G'/(G')^p \to (G')^p/(G')^{p^2}$, concluímos que todo elemento de $(G')^p$ é da forma $[x,u^p]$ módulo $(G')^{p^2}$ para algum $u \in C$.

Agora escolhemos um subgrupo T entre $(G')^p$ e $(G')^{p^2}$ com $|(G')^p : T| = p$ (que certamente existe pelo Teorema 1.4.4). Sendo G' *powerful*, $(G')^p$ também o é, e como $d((G')^p) \leq d(G) = 2$, temos que $|(G')^p : (G')^{p^2}| \leq p^2$. Assim, tanto $(G')^p/T$ quanto $T/(G')^{p^2}$ são cíclicos, gerados pela imagem de algum comutador $[x,u^p]$ com $u \in C$. Pelo Lema 3.10, temos $[x,u^p,u^p] \in [G,C^p,C^p] \leq [(G')^p, C^p] \leq (G')^{p^3}$.

Veja que reunimos as hipóteses necessárias para aplicar (ii) do Lema 3.4 com $L = (G')^p$ e $N = T$:

- $T \leq (G')^p$, T e $(G')^p$ são normais em G, $(G')^p$ é *powerful* e $d((G')^p) \leq 2$,
- $(G')^{p^2} \leq T$ e $|(G') : T| = p$,
- $(G')^p/T = \langle [x,u^p]T\rangle$ e $T/(G')^{p^2} = \langle [x,u^p](G')^{p^2}\rangle$,
- $[x,u^p,u^p] \in (G')^{p^3} \leq T^p$.

Portanto, $(G')^p \subseteq K_x(G)$, como desejado.

□

Observação 3.14. *O ponto da demonstração que vale para todo primo ímpar mas não vale para $p = 2$ é exatamente quando é necessário usar que $\gamma_q(H) \leq \gamma_3(H)$, o que só ocorre para q primo ímpar. No caso $p = 2$, não conseguimos essa inclusão, ou seja, nesse caso o $w \in (H')^p\gamma_p(H)$ pode não estar dentro de $(G')^4$. Daí não conseguimos utilizar a Identidade de Hall-Petresco para obter que $(G')^2/(G')^4$ consiste de comutadores da forma $[x, g](G')^4$, $g \in G$. Quando $p = 2$ e $C = G$, cobrir $(G')^2/(G')^4$ com comutadores de $K_x(G)$ será imprescindível, e essa será a parte mais complicada da demonstração.*

Isso finaliza a demonstração para os primos ímpares, restando apenas nos preocuparmos com a prova do Teorema A para 2-grupos finitos, que é consideravelmente mais complexa, principalmente quando $C = G$. Para lidar com esse caso, introduzimos os seguintes subgrupos:

Definição 3.15. *Seja G um 2-grupo finito tal que $(G')^2 \neq 1$. Para cada U max_G $(G')^2$, definimos o subgrupo $R(U)$ pela condição:*

$$R(U)/U = C_{G/U}(G^2/U)$$

Em outras palavras, $R(U)$ é o maior subgrupo de G que satisfaz $[R(U), G^2] \leq U$. Definimos $R = \bigcup\{R(U) \mid U\ max_G\ (G')^2\}$.

Vale lembrar que, assim como no caso de T max_G G', U max_G $(G')^2$ também implica que U é maximal em $(G')^2$.

Lema 3.16. *Seja G um 2-grupo finito com $d(G') \leq 2$. Além disso, suponha que $C = G$ e que $(G')^2 \neq 1$. Então o seguinte vale:*

(i) $[G, G^2] = (G')^2$.

(ii) $[x, G^2] = (G')^2$ *se e somente se* $x \notin R$.

(iii) $G^2 \leq R(U) < G$ *para todo* U max_G $(G')^2$.

(iv) $R(U) \cap R(V) \leq R(W)$ *para todo* U, V, W max_G $(G')^2$ *tais que* $U \neq V$.

Demonstração. **(i)** Pelo Lema 1.2.19, $[G, G^2] = [G, G]^2[G, G, G] = (G')^2\gamma_3(G)$, ou seja, $[G, G^2]$ e $(G')^2$ coincidem módulo $\gamma_3(G)$. Temos que G/G^2 tem expoente 2, e isso implica que o grupo é abeliano. Logo, $G' \leq G^2$. Conjugando de ambos os lados vemos que $\gamma_3(G) \leq [G, G^2]$. Temos que $[G, G^2] = (G')^2\gamma_3(G)$ equivale à $[G, G^2]\gamma_3(G) = (G')^2$, então $[G, G^2] = (G')^2$.

(ii) Se $x \in R$, então existe U max_G $(G')^2$ tal que $[x, G^2] \leq U < (G')^2$. Então, se $[x, G^2] = (G')^2$, é necessário que $x \notin R$. Por outro lado, se $[x, G^2] \neq (G')^2$ então $[x, G^2] < (G')^2$ por (i). Seja $N = [x, G^2](G')^4$. Então $N < (G')^2$, porque $[x, G^2]$ é próprio e $(G')^4 = \Phi((G')^2)$. Além disso, N é normal em G, pois $[(G')^2, G] \leq (G')^4$ pelo item (i) do Lema 3.10, daí $[N, G] \leq [(G')^2, G] \leq (G')^4 \leq N$. Considerando U max_G $(G')^2$ contendo N, teremos $[x, G^2] \leq N \leq U$, assim, $x \in R(U) \subseteq R$, o que prova o resultado.

(iii) Temos que $[R(U), G^2] \leq U < (G')^2$, então, pelo item (i), $R(U)$ é um subgrupo próprio de G. Por outro lado, utilizando o Lema 1.2.19 e o item (i), temos:

$$[G^2, G^2] \leq [G, G^2]^2[G, G^2, G] = (G')^4[(G')^2, G] = (G')^4$$

Dado que $(G')^4 \leq U$, segue que $G^2 \leq R(U)$.

(iv) Como G' é *powerful*, $(G')^2$ também é, então $(G')^4 = \Phi((G')^2)$. Como $d((G')^2) \leq 2$, segue que $|(G')^2 : (G')^4| \leq 4$. Temos que U é subgrupo próprio de $(G')^2$ e $U \cap V$ é subgrupo próprio de U dado que $U \neq V$, assim:

$$(G')^4 \overset{1}{\text{——}} U \cap V \overset{\geq 2}{\text{——}} U \overset{\geq 2}{\text{——}} (G')^2$$

Logo, $U \cap V = (G')^4 \leq W$. Se $x \in R(U) \cap R(V)$ então $[x, G^2] \leq U$ e $[x, G^2] \leq V$, então $[x, G^2] \leq U \cap V \leq W$, daí $x \in R(W)$.

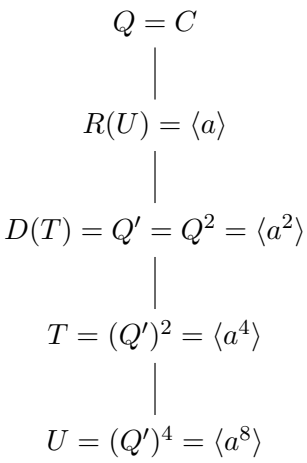
□

Segue um exemplo simples para visualizarmos os subgrupos $R(U)$ e $D(T)$.

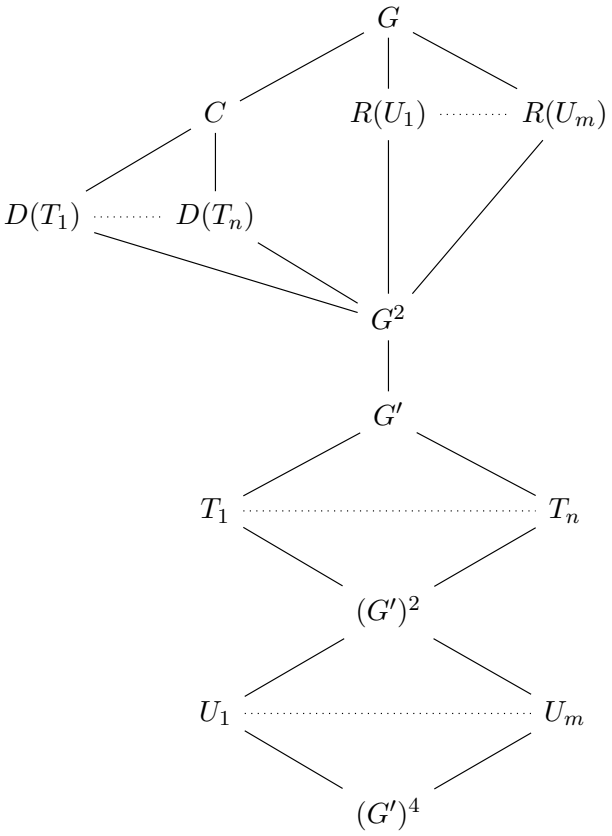
Exemplo 3.0.2. *Seja* $Q = \langle a, b \mid a^{2^{m-1}} = 1,\ a^{2^{m-2}} = b^2,\ a^b = a^{-1} \rangle$, $m \geq 4$, *o grupos dos Quatérnios de ordem* 2^m. *Nesse caso,* $Q' = \langle a^2 \rangle$, *por isso* $(Q')^2 = \langle a^4 \rangle = T$ *e* $(Q')^4 = \langle a^8 \rangle = U$ *(mas em geral* $(G')^2$ *e* $(G')^4$ *não coincidem com* T *e* U, *isso é particular desse exemplo). Além disso, novamente* $C = G$ *pois* $Q'/(Q')^2$ *é central em* $Q/(Q')^2$.

Como $[a, Q] = [b, Q] = Q'$, $a, b \notin D(T)$. *Mas* $[a^2, b] = a^{-4} \leq T$. *Logo,* $D(T) = \langle a^2 \rangle$.

Sendo $Q^2 = \langle a^2 \rangle$, *é claro que* $[a, Q^2] \leq U$. *Então* $\langle a \rangle \leq R(U)$. *Mas veja que* $[b, a^2] = a^4 \notin U$. *Logo,* $b \notin R(U)$. *Portanto,* $R(U) = \langle a \rangle$. *Resumindo, temos a seguinte situação:*



Esse é um exemplo simples para que fosse possível explicitar os subgrupos fazendo os cálculos a mão, mas no geral teremos vários subgrupos da forma T, U, $D(T)$ e $R(U)$, e que podem não coincidir com outros subgrupos como no exemplo. Em geral, dados $T_1, ..., T_n$ os maximais normais de G' e $U_1, ..., U_m$ os maximais normais de $(G')^2$ a situação é:



O próximo resultado nos permitirá completar facilmente a prova do Teorema A no caso em que $p = 2$ e $C = G$. Sua prova é longa e técnica, e requer uma análise cuidadosa das posições relativas dos subgrupos $D(T)$ e $R(U)$, onde $T\ max_G\ G'$ e $U\ max_G\ (G')^2$, porque a ideia da demonstração é mostrar que $D \cup R$ não cobre todo o grupo G. Na proposição seguinte, queremos um $x \in G$ que satisfaça tanto $G' = [x, G]$ quanto $(G')^2 = [x, G^2]$. Pelo Lema 3.12, qualquer $x \notin D$ satisfaz $G' = [x, G]$, e pelo Lema 3.16, se $x \notin R$ então $(G')^2 = [x, G^2]$, ou seja, se $x \notin D \cup R$ então x satisfaz as duas condições requeridas.

Proposição 3.17. *Seja G um 2-grupo finito com $d(G') = 2$ e $C = G$. Então existe $x \in G$ tal que $G' = [x, G]$ e $(G')^2 = [x, G^2]$.*

Demonstração. Pelo item (ii) do Lema 3.12, sabemos que existe $a \notin D$ tal que $G' = [a, G]$, e como $d(G') = 2$, existem $b, c \in G$ tais que $G' = [a, G] = \langle [a, b], [a, c] \rangle$. Se definirmos $H = \langle a, b, c \rangle$, então $H' = G'$, e o resultado segue imediatamente para G assim que for provado para H. Afinal, $[x, G] \leq G' = H' = [x, H] \leq [x, G]$ então $G' = [x, G]$; agora, levando em consideração que $[G^2, G] = (G')^2$ pelo item (i) do Lema 3.16, temos que $(G')^2 = (H')^2 = [x, H^2] = [G, G^2] \geq [x, G^2]$, e como $[x, H^2] \leq [x, G^2]$ segue que $(G')^2 = [x, G^2]$. Portanto, podemos assumir que $d(G) \leq 3$. Assumiremos também que $(G')^2 \neq 1$, pois, como visto no Teorema 3.13, nesse caso o resultado segue trivialmente.

No restante da prova, considere $Z/(G')^2$ como o centro de $G/(G')^2$, ou seja, $[Z, G] \leq (G')^2$. Vamos mostrar que $|G : Z| > 4$. Suponha, por contradição, que $|G : Z| \leq 4$. Então G/Z é abeliano. Como G não é abeliano, G/Z não pode ser cíclico, logo, $G/Z \cong C_2 \times C_2$. Podemos escrever $G/Z = \{Z, aZ, bZ, abZ\} = \langle aZ, bZ \rangle$, e assim fica fácil ver que $G = \langle a, b, Z \rangle$. Como G/Z é abeliano, $\langle [a, b] \rangle \leq Z$, ou seja, $\langle [a, b](G')^2 \rangle$ comuta com todos os elementos de $G/(G')^2$; em particular, $\langle [a, b](G')^2 \rangle \trianglelefteq G/(G')^2$. Se fizermos o quociente de $G/(G')^2$ por $\langle [a, b](G')^2 \rangle$ veremos que as imagens dos elementos $a(G')^2$ e $b(G')^2$ comutam, e os outros elementos geradores são imagem de $Z/(G')^2$, ou seja, são centrais, logo, esse quociente é abeliano e portanto $G'/(G')^2 = \langle [a, b](G')^2 \rangle$. Mas se $G'/(G')^2$ é cíclico, como $\Phi(G') = (G')^2$, pelo Teorema da Base de Burnside (1.4.11), G' também será cíclico, o que é uma contradição. Assim, $|G : Z| > 4$ como desejado.

Pelo item (i) do Lema 3.16, $[G, G^2] \leq (G')^2$, ou seja, $G^2/(G')^2$ é central em $G/(G')^2$, então $G^2 \leq Z$. Sendo G um 2-grupo, G/G^2 é um grupo em que todos os elementos tem ordem 2, então G/G^2 é abeliano elementar e por isso $\Phi(G) = G^2 \leq Z$. Pela equação (2.9), $|G : G^2| \leq 2^3 = 8$ e:

$$\underbrace{|G : G^2|}_{\leq 8} = \underbrace{|G : Z|}_{>4} |Z : G^2|$$

Então $|G : Z| = 8$ e $Z = G^2$.

Agora começaremos as análises dos subgrupos $D(T)$ e $R(U)$ para mostrar que $D \cup R$ não cobre todo o grupo G. Pelo item (i) do Lema 3.12, $G^2 = \Phi(G) \leq D(T)$ para todo $T\ max_G\ G'$ e pelo item (iii) do Lema 3.16, $G^2 \leq R(U)$ para todo $U\ max_G (G')^2$, então podemos mostrar a

propriedade de não cobertura trabalhando apenas com o grupo G/G^2 de ordem 8. Considere então $\overline{G} = G/G^2$, $\overline{D} = DG^2/G^2$ e $\overline{R} = RG^2/G^2$. Mostraremos que $|\overline{D} \cup \overline{R}| \leq 7$. Faremos isso primeiro determinando a ordem de $\overline{D}$ e depois analisando a posição dos subgrupos $R(U)$ com respeito a D e entre eles mesmos.

Antes de proceder, observe que as seções $G'/(G')^2$ e $(G')^2/(G')^4$ são centrais em G pelo Lema 3.10 e porque $G = C$, ou seja, $[G', G] \leq (G')^2$ e $[(G')^2, G] \leq (G')^4$. Como $(G')^2 \leq T$ para todo T *max* G' (porque $\Phi(G') = (G')^2$), temos que $[T, G] \leq [G', G] \leq (G')^2 \leq T$, então $T \trianglelefteq G$. De forma análoga mostra-se que $U \trianglelefteq G$ para todo U *max* $(G')^2$. Então as condições T max_G G' e U max_G $(G')^2$ são equivalentes à T *max* G' e U *max* $(G')^2$, respectivamente.

Alegamos que $|\overline{D}| = 4$ e que D é um subgrupo maximal de G. Vamos considerar T max_G G' arbitrário, e observe que, como $d(G') = 2$, pelo Corolário 1.4.12, temos três opções para T. Primeiramente, como $log_2|G : D(T)|$ é par e $D(T)$ é próprio em G pelo Lema 3.12, temos:

$$\overbrace{G^2 \text{———} \underbrace{D(T) \text{———} G}_{2^2}}^{8} \implies |\overline{D(T)}| = 2$$

Então existe $y \in D(T)$ tal que $D(T) = \langle y \rangle G^2$. Utilizando o item (ix) da Proposição 1.2.4, $D(T)' = [D(T), D(T)] = [D(T), \langle y \rangle G^2] = [D(T), G^2]$. Agora, utilizando o Lema 1.2.19, $D(T)' = [D(T), G^2] \leq [D(T), G]^2[G, D(T), G] \leq (G')^2[T, G] \leq (G')^2$. A última inclusão segue de que, como $|G'/(G')^2| = 4$ e T é próprio em G', $|T/(G')^2| = 2$, daí $|[T, G]/(G')^2| = 1$ (observação 1.3.2), ou seja, $[T, G] \leq (G')^2$. Agora seja S max_G G' com $S \neq T$. Pelo mesmo argumento anterior, $S \cap T = (G')^2$, e como $[D(S), G] \leq S$ e $[D(T), G] \leq T$, temos $[D(S), D(T)] \leq S \cap T = (G')^2$. Disso, e de $D(T)' \leq (G')^2$, temos que $\langle D \rangle' \leq (G')^2$.

Também, se $D(S) = D(T)$ então $[D(T), G] \leq T$ e $[D(T), G] \leq S$, então $[D(T), G] \leq S \cap T = (G')^2$, logo $D(T) \leq Z = G^2$, mas aí $|\overline{D(T)}| = 1$, o que é uma contradição. Logo, se $S \neq T$, então $D(S) \neq D(T)$. Por isso, $\overline{D}$ é a união de três diferentes grupos de ordem 2, e assim, $|\overline{D}| = 4$. É claro que $\overline{D} \subseteq \langle \overline{D} \rangle \leq \overline{G}$, e como $\langle D \rangle' \neq G'$, sabemos que $\langle D \rangle$ é um subgrupo próprio de G, então $\langle \overline{D} \rangle < \overline{G}$. Assim, como $|\overline{D}| = 4 \leq |\langle \overline{D} \rangle| < 8 = |\overline{G}|$, temos que $D = \langle D \rangle$ e D é um subgrupo maximal de G.

Agora começamos a análise das posições dos subgrupos da forma $R(U)$. Como argumentado na demonstração do item (iv) do Lema 3.16, $|(G')^2 : (G')^4| \leq 4$ e, novamente pelo Corolário 1.4.12, $(G')^2$ possui no máximo três subgrupos maximais. Ainda na demonstração do item (iv) do Lema 3.16 vimos que a interseção de dois diferentes maximais de $(G')^2$ é $(G')^4$. Pelo item (iii) do Lema 3.16, todos os $R(U)$ são próprios em G. Se nenhum deles for maximal em G, então $|G : R(U)| \geq 4$ e $|R(U) : G^2| \leq 2$, daí existe $a \in R(U)$ tal que $R(U) = \langle a \rangle G^2$. Seja V max_G $(G')^2$, e $b \in R(V)$ tal que $R(V) = \langle b \rangle G^2$. Se $R(U) \neq R(V)$, então $U \neq V$, logo $\overline{R} = \{G^2, \langle a \rangle G^2, \langle b \rangle G^2, \langle ab \rangle G^2\}$. Assim, $|\overline{R} \cup \overline{D}| = 7 < 8$ e temos o que queríamos. Se $R(U) = R(V)$ para algum $V \neq U$, daí $|\overline{R}| < 4$ e o resultado segue. Se $R(U)$ for maximal, $|G : R(U)| = 2$ e $|R(U) : G^2| = 4$, então $|\overline{R}| \geq 4$ e não temos o resultado garantido ainda. Se

$R(U) = D$ sempre que $R(U)$ max G, então no pior caso existem $R(V)$ e $R(W)$ diferentes de D, onde V, W max_G $(G')^2$, mas aí $|\overline{R} \cup \overline{D}| \leq |\overline{D}| + |\overline{R(V)}| + |\overline{R(W)}| - 2 = 4 + 1 + 1 = 6 < 8$ e o resultado segue. Portanto, podemos assumir que existe U $max_G (G')^2$ tal que $R(U)$ max G, ou seja, $|\overline{R(U)}| = 4$ e ainda $R(U) \neq D$.

Lembrando que $|G/G^2| = 8$ e $\Phi(G) = G^2$, então $G/G^2 \cong C_2 \times C_2 \times C_2$. Então os maximais são da forma $C_2 \times C_2$, logo, quaisquer dois maximais tem interseção não trivial. Segue que $|\overline{R(U)} \cap \overline{D}| = 2$ e $|\overline{D} \cup \overline{R(U)}| = 6$.

Então podemos assumir que existe outro V max_G $(G')^2$ tal que $R(V) \nsubseteq D \cap R(U)$, pois caso contrário já estaria resolvido. Se $(G')^2$ possui dois maximais distintos, então $(G')^2$ não é cíclico, logo $d((G')^2) = 2$ e $(G')^2$ possui exatamente 3 subgrupos maximais distintos.

Além disso, sendo G' *powerful*, pelo item (iii) e (iv) do Teorema 2.18 a função:

$$f : G'/(G')^2 \to (G')^2/(G')^4$$

$$x(G')^2 \mapsto x^2(G')^4$$

é um homomorfismo sobrejetivo, e é injetivo porque $d(G') = 2 = d((G')^2)$; logo, é um isomorfismo.

Como consequência,

$$g \in G' \setminus (G')^2 \implies g^2 \in (G')^2 \setminus (G')^4. \tag{3.4}$$

Por isso, todos os três subgrupos maximais de $(G')^2$ têm a forma T^2, onde T max_G G'.

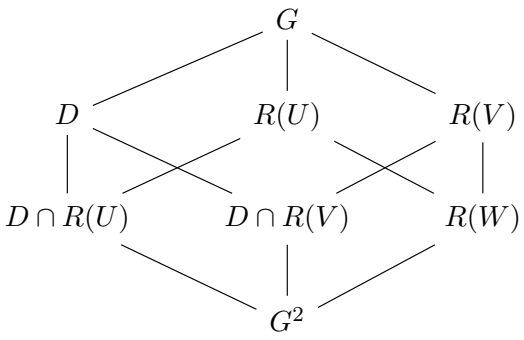
Seja W o terceiro subgrupo maximal de $(G')^2$, diferente de U e V. Se $\overline{R(W)} = \overline{1}$, então, visto que $R(U) \cap R(V) \subseteq R(W)$ por (iv) do Lema 3.16, segue que $|\overline{R(V)}| \leq 2$ (se $|\overline{R(V)}| \geq 4$, $\overline{R(V)}$ seria maximal de $\overline{G}$ e teria interseção não trivial com $\overline{R(U)}$), e consequentemente $|\overline{D} \cup \overline{R}| = |\overline{D} \cup \overline{R(U)}| + |\overline{R(V)} \setminus \overline{1}| + |\overline{R(W)} \setminus \overline{1}| \leq 6 + 1 + 0 = 7$. Portanto, podemos assumir que $|\overline{R(W)}| \geq 2$.

Agora vamos considerar dois casos separados:

Caso 1: $R(W) \leq R(U)$.

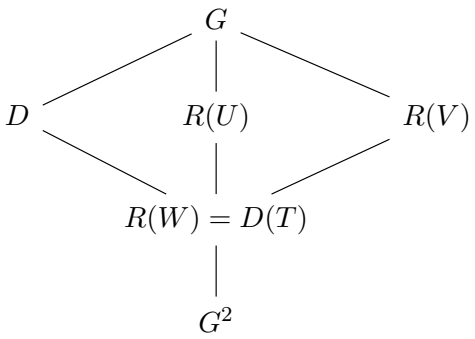
Novamente, pelo item (iv) do Lema 3.16, obtemos $R(W) = R(U) \cap R(W) < R(V)$, com inclusão própria, uma vez que $R(V) \nleq R(U)$. Em particular, $|\overline{R(W)}| = 2$ e $|\overline{R(V)}| = 4$, o que implica $|\overline{R}| = |\overline{R(U)}| + |\overline{R(V)} \setminus \overline{R(W)}| = 4 + 2 = 6$.

Suponha primeiramente que $D \cap R(U) \neq D \cap R(V)$. Nesse caso, temos $|\overline{D} \cap \overline{R}| \geq 3$ e, portanto, $|\overline{D} \cup \overline{R}| = |\overline{D}| + |\overline{R}| - |\overline{D} \cap \overline{R}| \leq 4 + 4 - 3 = 7$, como desejado.



Caso $D \cap R(U) \neq D \cap R(V)$

Agora, suponha que $D \cap R(U) = D \cap R(V)$, então essa interseção coincide com $R(W)$, pois $R(U) \cap R(V) = R(W)$. Agora, como visto no oitavo parágrafo da prova, $\overline{D}$ possui três subgrupos de ordem 2, e são todos da forma $\overline{D(T)}$. Assim, $R(W) = D(T)$ para algum T max_G G'.



Caso $D \cap R(U) = D \cap R(V)$

Escolha $g \in R(W) \setminus G^2$. Então, $[g, G] \leq T$ (pois $g \in D(T)$), mas como $Z = G^2$ é o centro de $G/(G')^2$ e $g \notin Z$, então $[g, G] \not\leq (G')^2$ ($x \in Z \iff [x, G] \leq (G')^2$). Como $R(U)$ e D são dois maximais distintos, temos $G = \langle R(U), D \rangle$ e, sendo $g \in D(T) \leq D$, $[g, D] \leq D' \leq (G')^2$ (essa última inclusão foi mostrada no sétimo parágrafo da prova). Então podemos escolher $h \in R(U)$ tal que $[g, h] \in T \setminus (G')^2$.

Agora, temos que

$$[g, h^2] \in [R(W), G^2] \leq [R(U), G^2] \cap [R(V), G^2] \leq U \cap V \leq (G')^4,$$

e, por outro lado, por (iii) do Teorema 1.2.4:

$$[g, h^2] = [g, h]^2 [g, h, h],$$

onde $[g, h]^2 \in T^2 \setminus (G')^4$ por (3.4), e $[g, h, h] \in [h, G'] \leq [h, G^2] \leq U$, pois $G' \leq G^2$ e $h \in R(U)$.

Com isso, mostraremos que necessariamente $U = T^2$. Lembrando que $(G')^2/(G')^4 \cong C_2 \times C_2$. Seja $[g, h]^2 = a \in T^2 \setminus (G')^4$ e $[g, h, h] = b \in U$. Primeiro, não podemos ter $b \in (G')^4$ pois $ab \in$

$(G')^4$ mas $a \notin (G')^4$. Sendo $ab \in (G')^4$, a é o inverso de b em $(G')^2/(G')^4$, daí $b(G')^4 = a(G')^4$, e como $T^2/(G')^4 = \langle a\rangle(G')^4$ e $U/(G')^4 = \langle b\rangle(G')^4$, temos que $U = T^2$.

Uma vez que o mesmo argumento pode ser aplicado com V no lugar de U, pois $R(V)$ também é maximal, deduzimos que $U = V$, o que é uma contradição.

Caso 2: $R(W) \not\leq R(U)$.

Vamos provar que este caso é impossível. Escolha um elemento $x \in R(V)\setminus(D \cup R(U))$. Então $G = R(U) \cup xR(U)$, porque $R(U)$ é maximal logo $|G : R(U)| = 2$. Uma vez que $R(W) \not\leq R(U)$, $R(W) \cap xR(U) \neq \emptyset$, então existe $y \in R(U)$ tal que $xy \in R(W)$. Note que $y \notin G^2$ pois, caso contrário, $y \in R(V)$ e $xy \in R(V) \cap R(W) \leq R(U)$, o que não pode ocorrer pela escolha de x.

Temos que $[xy, x^2] = y^{-1}x^{-1}x^{-2}xyx^2 = [y, x^2]$. Como $xy \in R(W)$, $[xy, x^2] \in W$; e, como $y \in R(U)$, temos $[y, x^2] \in U$, logo $[xy, x^2] = [y, x^2] \in W \cap U = (G')^4$, e então

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

$$[y, x]^2 = [y, x^2][y, x, x]^{-1} \in V,$$

pois $[y, x, x] \in [G', x] \leq [G^2, x] \leq V$ (porque $x \in R(V)$).

Usando que $[yx, y^2] = [x, y^2]$ e que $yx = xx^{-1}yx = (xy)^x \in R(W)$, obtemos da mesma forma que $[y, x]^2 \in U$. Portanto, $[y, x]^2 \in U \cap V = (G')^4$ e então, pela relação (3.4), temos $[y, x] \in (G')^2$.

Por outro lado, como $x \notin D$, temos

$$G' = [x, G] = [x, \langle x\rangle R(U)] = [x, R(U)].$$

Como $y \notin G^2$ e $|\overline{R(U)}| = 4$, então $\overline{R(U)} = \{G^2, zG^2, yG^2, zyG^2\}$ para algum z, e sendo $G^2 = \Phi(G)$, pelo Teorema da Base de Burnside (1.4.11), podemos escrever $R(U) = \langle y, z, G^2\rangle$. Agora, uma vez que $[x, y] \in (G')^2$ e $[x, G^2] \leq (G')^2$, temos $G' = [x, R(U)] = \langle [x, z], (G')^2\rangle$, e como $(G')^2 = \Phi(G')$, novamente pelo Teorema da Base de Burnside (1.4.11), isso implica que G' é cíclico, o que é uma contradição.

□

Podemos agora proceder para provar o Teorema A para o primo 2.

Teorema 3.18. *Seja G um 2-grupo finito, e assuma que $d(G') \leq 2$. Então $G' = K_x(G)$ para algum $x \in G$ adequado.*

Demonstração. Podemos assumir que $d(G') = 2$. Vamos dividir a prova em dois casos:

Caso 1: $C \neq G$.

Seja $T = \gamma_3(G)(G')^2$. A condição $C \neq G$ implica que $[G, G'] \neq [C, G'] \leq (G')^2$ pela definição de C, ou seja, $[G, G'] = \gamma_3(G) \not\leq (G')^2$, então $(G')^2 < T$. Como $\Phi(G') = (G')^2$ e $\gamma_3(G) < G'$, temos $T < G'$. Logo, $T\ max_G\ G'$. Além disso, como $(G')^2 < T < G'$ e $|G' : (G')^2| \leq 4$, temos $T\ max\ G'$, e isso também implica que G'/T e $T/(G')^2$ são cíclicos, fatos que serão utilizados

diversas vezes na prova. Por outro lado, se $U\ max_G\ G'$, então $\gamma_3(G)(G')^2 \leq U$, como mostrado no item (i) do Lema 3.12, assim $T = U$. Por isso, se $N \trianglelefteq G$ e $N < G'$ então $N \leq T$. Também, $D = D(T)$ é um subgrupo de G e $[D, G] \leq T$.

Por outro lado, pelo Lema dos Três Subgrupos (1.2.5) e pela definição de C, temos:

$$[G, C'] \leq [G, C, C] \leq [G', C] \leq (G')^2,$$

enquanto que

$$[G, G'] = \gamma_3(G) \not\leq (G')^2.$$

Logo, $C' < G'$ e consequentemente $C' \leq T$.

Pelo Lema 3.12, temos $G' = [x, G]$ para todo $x \notin D$. Vamos mostrar que o Lema 3.4 pode ser aplicado com $L = G'$ e $N = T$ ou com $L = T$ e $N = (G')^2$, dependendo dos valores de alguns subgrupos comutadores. No último caso, o Lema 3.2 completará a prova.

Suponha primeiro que $[G', C] \leq T^2$. Então escolhemos $x \notin C$, o que, pelo item (i) Lema 3.12, implica $x \notin D$. Pelo item (iii) do Lema 3.10, $d(G') = 2$ e $C \neq G$ implicam que $|G : C| = 2$, então $G = \langle x \rangle C$. Logo, $G'/T = \langle [x, y]T \rangle$ para algum $y \in C$. Como $x \notin C$, $[x, [x, y]] \notin (G')^2$, então $T/(G')^2 = \langle [x, [x, y]](G')^2 \rangle$. Agora, temos $[x, y, y] \in [G', C] \leq T^2$ e $[x, [x, y], [x, y]] \in [G', G'] = (G')' \leq (G')^4$, já que G' é *powerful*.

Assim, aplicando o Lema 3.4 com $L = G'$ e $N = T$, concluímos neste caso. Para ficar mais claro, encaixamos o que temos nas hipóteses do lema da seguinte forma:

- $T \leq G'$ são ambos normais em G, G' é *powerful* e $d(G') \leq 2$,
- $(G')^2 \leq T$ e $|G' : T| = 2$,
- $G'/T = \langle [x, y]T \rangle$ e $[x, y, y] \in T$,
- $T/(G')^2 = \langle [x, [x, y]](G')^2 \rangle$ e $[x, [x, y], [x, y]] \in (G')^4$.

Logo, $G' \subseteq K_x(G)$.

Portanto, assumimos que $[G', C] \not\leq T^2$ daqui em diante. Observe que $|(G')^2 : T^2| \leq |G' : T| = 2$ pelo Lema 2.23. Como $[G', C]$ está contido em $(G')^2$ (pela definição de C) mas não em T^2, $T^2 < (G')^2$, então $|(G')^2 : T^2| = 2$. Também, $|T^2 : (G')^4| \leq 2$.

Suponha que $[T, G] \not\leq T^2$. Temos que $G = \langle G \setminus C \rangle$ pois, dado $g \in G$, se $g \in G \setminus C$, então $g \in \langle G \setminus C \rangle$; e se $g \in C$, escolha $h \in G \setminus C$, então $gh^{-1} \in G \setminus C$ (caso contrário, teríamos $h^{-1} \in C$) logo, $gh^{-1}h = g \in \langle G \setminus C \rangle$. Se tivéssemos $[T, x] \leq T^2$ para todo $x \in G \setminus C$, teríamos $[T, G] = [T, \langle G \setminus C \rangle] \leq T^2$, o que contradiz a hipótese. Então existe $x \in G \setminus C$ tal que $[T, x] \not\leq T^2$. Logo, podemos escolher $x \notin C$ e $t \in T$ tal que $(G')^2/T^2 = \langle [x, t]T^2 \rangle$.

Temos que:

$$[x, t, t] \in [(G')^2, G'] \leq [G', G']^2 [G', G', G'] \leq (G'')^2 [G'', G']$$

$$\leq (G')^8[(G')^4, G'] \leq (G')^8 \leq T^4$$

Para concluir que $[(G')^4, G'] \leq (G')^8$ utilizamos o item (i) do Lema 3.10 e o fato de que $G' \leq C$.

Podemos argumentar com o fator principal $T/(G')^2$ da mesma forma que no caso $[G', C] \leq T^2$, ou seja, $T/(G')^2 = \langle [x, [x, y]](G')^2 \rangle$ e $[x, [x, y], [x, y]] \leq (G')^4$. Agora podemos aplicar os lemas para concluir esse caso. Explicitando o encaixe nas hipóteses do Lema 3.4:

- $(G')^2 \leq T$ são ambos normais em G, T é *powerful* e $d(T) \leq 2$,
- $T^2 \leq (G')^2$ e $|T : (G')^2| = 2$,
- $T/(G')^2 = \langle [x, [x, y]](G')^2 \rangle$ e $[x, [x, y], [x, y]] \in (G')^4$,
- $(G')^2/T^2 = \langle [x, t]T^2 \rangle$ e $[x, t, t] \in T^4$.

Com isso, $T \subseteq K_x(G)$. Como G'/T é cíclico, $G'/T \subseteq K_{xT}(G/T)$. Portanto, pelo Lema 3.2, $G' \subseteq K_x(G)$ nesse caso.

Finalmente, suponha que $[T, G] \leq T^2$. Pelo Lema dos Três Subgrupos (1.2.5):

$$[G', D] \leq [D, G, G] \leq [T, G] \leq T^2$$

Mas $[G', C] \not\leq T^2$, então existem $x \in C \setminus D$ e $g \in G'$ tais que $(G')^2/T^2 = \langle [x, g]T^2 \rangle$. Então $[x, g, g] \in [(G')^2, G'] \leq G'' \leq (G')^4$. Como $\Phi(G') = (G')^2$, $[(G')^2, G']$ é próprio em G'', e é normal em G, logo, $[(G')^2, G'] \leq T^4$ e assim $[x, g, g] \in T^4$.

Além disso, como $x \notin D$, temos $G' = [x, G]$, então existe $y \in G$ tal que $G'/T = \langle [x, y]T \rangle$. Como $C' \leq T$, temos $y \notin C$, afinal, se $y \in C$ teríamos $[x, y] \in C' \leq T$ e $[x, y]T$ não seria gerador de G'/T. Então $[x, y, y] \in [G', y] \not\subseteq (G')^2$ pois $y \notin C$, mas $[x, y, y] \in [G', G] \leq T$, logo, $T/(G')^2 = \langle [x, y, y](G')^2 \rangle$. Dado que $[x, y^2] = [x, y]^2[x, y, y]$, temos que $[x, y^2] \equiv [x, y, y] \pmod{(G')^2}$, logo, $T/(G')^2 = \langle [x, y^2](G')^2 \rangle$. Agora, utilizando a hipótese de que $[T, G] \leq T^2$ e o Lema 1.2.19:

$$[x, y^2, y^2] \in [T, G^2] \leq [T, G]^2[T, G, G] \leq T^4[T^2, G] \leq (G')^4,$$

Nas últimas inclusões utilizamos que $(T^2)^2 = T^4$, o que pode ser feito porque, pelo Lema 2.23, T é *powerful*; e também que, como $|(G')^2 : (G')^4| = 4$ e $(G')^2/T^2$ é cíclico, $|T^2/(G')^4| = 2$ e assim $[T^2, G] \leq (G')^4$.

Aplicando o Lema 3.4:

- $(G')^2 \leq T$, ambos são normais em G, T é *powerful* e $d(T) \leq 2$,
- $T^2 \leq (G')^2$ e $|T : (G')^2| = 2$,
- $T/(G')^2 = \langle [x, y^2](G')^2 \rangle$ e $[x, y^2, y^2] \in (G')^4$,

- $(G')^2/T^2 = \langle [x,g]T^2 \rangle$ e $[x,g,g] \in T^4$.

Assim, $T \subseteq K_x(G)$. Como $G'/T \subseteq K_{xT}(G/T)$ pelo Lema 3.3, conseguimos novamente $G' \subseteq K_x(G)$ aplicando o Lema 3.2.

Caso 2: $C = G$.

Pela Proposição 3.17, existe $x \in G$ tal que $G' = [x, G]$ e $(G')^2 = [x, G^2]$. Uma vez que $C = G$, as seções $G'/(G')^2$ e $(G')^2/(G')^4$ são centrais em G, então segue do Lema 3.3 que:

$$G'/(G')^2 = \langle [x,G](G')^2 \rangle \; e \; [G', G] \leq (G')^2 \implies G'/(G')^2 = K_{x(G')^2}(G/(G')^2)$$

e

$$(G')^2/(G')^4 = \langle [x,G^2](G')^4 \rangle \; e \; [(G')^2, G^2] \leq (G')^4 \implies (G')^2/(G')^4 = K_{x(G')^2}(G^2/(G')^4)$$

Por outro lado, de acordo com o Lema 3.10, temos

$$[x, G^2, G^2] \leq [(G')^2, G^2] = [(G')^2, C^2] \leq (G')^8$$

. Portanto, podemos aplicar o Lema 3.4 com $L = (G')^2$ e qualquer $N \; max_G \; (G')^2$:

- $N \leq (G')^2$ são normais em G, $(G')^2$ é *powerful* e $d((G')^2) \leq 2$,
- $(G')^4 \leq N$ e $|(G')^2 : (G')^4| = 2$,
- $(G')^2/(G')^4 = \langle [x,G^2](G')^4 \rangle \implies (G')^2/N = \langle [x,G^2]N \rangle$ e $[x, G^2, G^2] \in (G')^8 \leq N^4 \leq N^2$,
- $N/(G')^4 = \langle [x,y](G')^4 \rangle$, para $y \in G^2$ tal que $[x,y] \in N \setminus (G')^4$; e $[x,y,y] \in [x, G^2, G^2] \in (G')^8$.

Obtendo $(G')^2 \subseteq K_x(G)$. Como $G'/(G')^2 = K_{x(G')^2}(G/(G')^2)$, concluímos aplicando o Lema 3.2 que $G' \subseteq K_x(G)$.

□

Por fim, provaremos o Teorema B. Para isso, utilizaremos a Proposição 1.5.16, que estabelece que se G' é fechado se G é em um grupo pro-p finitamente gerado. O nosso grupo profinito G não é necessariamente finitamente gerado, mas mostraremos que G' está dentro de um subgrupo fechado finitamente gerado para concluir que G' é fechado em G.

Temos que o subgrupo comutador $\overline{G'}$ é topologicamente 2-gerado, então existem $x, y \in \overline{G'}$ tais que $\overline{\langle x, y \rangle} = \overline{G'}$. Digamos que $x = [x_1, x_2]...[x_{n-1}, x_n]$ e $y = [y_1, y_2]...[y_{m-1}, y_m]$, para $x_1, ..., x_n, y_1, ..., y_m \in G$. Considere $H = \overline{\langle x_1, ..., x_n, y_1, ..., y_m \rangle}$. Temos que $H' = G'$ e H é finitamente gerado. Sendo H fechado, pela Proposição 1.5.14, H é profinito com a topologia induzida, logo também é pro-p. Pela Proposição 1.5.16, $H' = G'$ é fechado em H. Como H

é fechado em G, segue que G' é fechado em G. Com isso, podemos descartar a operação de fechamento de $\overline{G'}$.

Teorema 3.19. *Seja G um pro-p grupo. Se G' pode ser topologicamente gerado por 2 elementos, então $G' = \{[x, g] \mid g \in G\}$ para um adequado $x \in G$.*

Demonstração. Sendo G um grupo pro-p, para todo $N \trianglelefteq_o G$, G/N é um p-grupo. Como $(G/N)' = G'N/N$, $(G/N)'$ também é 2-gerado. Então, pelo Teorema A, todos os elementos do subgrupo comutador $(G/N)'$ podem ser escritos como comutadores de um único elemento.

Defina $X_N = \{x \in G \mid (G/N)' = K_{xN}(G/N)\}$, ou seja, X_N é o conjunto dos $x \in G$ tais que $G'N/N = \{[xN, gN] \mid gN \in G/N\} = \{[x, g]N \mid g \in G\}$. É claro que para qualquer $y \in xN$ temos $yN = xN$, então se $x \in X_N$, temos $(G/N)' = K_{xN}(G/N) = K_{yN}(G/N)$, logo, $y \in X_N$. Dessa forma, $X_N = \bigcup_{x \in X_N} xN$. Sendo N aberto, cada xN é aberto ((b) de 1.5.9) e uma união arbitrária de abertos é um aberta. Logo, X_N é aberto, e como em G todo aberto é fechado ((c) de 1.5.9), X_N é fechado.

A família de fechados $\{X_N\}_{N \trianglelefteq_o G}$ satisfaz a propriedade de interseção finita (qualquer interseção finita de subconjuntos dessa família é não vazia). Afinal, considere $N_1, ..., N_s$, $s \in \mathbb{N}$, subgrupos normais abertos de G. Então, $N = N_1 \cap N_2 \cap ... \cap N_s$ é também um subgrupo aberto normal (interseção finita de abertos é aberto, e interseção de normais é normal). Logo, G/N é finito e pelo Teorema A existe $xN \in G/N$ tal que $G'/N = K_{xN}(G/N)$. Mas considerando o homomorfismo $\phi : G/N \to G/N_i$ definido por $\phi(gN) = gN_i$, para $g \in G$ e $i \in \{1, ..., s\}$, temos que

$$(G'/N)^\phi = K_{xN}(G/N)^\phi = \{[xN, gN]^\phi \mid g \in G\} = \{[xN_i, gN_i] \mid g \in G\} = K_{xN_i}(G/N_i)$$

Ou seja, se $x \in X_N$, então $x \in X_{N_i}$ para $i = 1, ..., s$. Logo, qualquer interseção finita de $\{X_N\}_{N \trianglelefteq_o G}$ é não vazia.

Sendo G compacto, pelo Lema 1.5.2, $\bigcap_{N \trianglelefteq_o G} X_N \neq \emptyset$. Se x pertence a esta interseção, então $(G/N)' = K_{xN}(G/N)$ para todo $N \trianglelefteq_o G$. Logo, utilizando que G' é fechado e o item c) da Proposição 1.5.13, temos que:

$$G' = \overline{G'} = \bigcap_{N \trianglelefteq_o G} G'N = \bigcap_{N \trianglelefteq_o G} K_x(G)N = \overline{K_x(G)} = K_x(G)$$

como desejado. Observe que a última igualdade decorre do fato de que $K_x(G)$ é a imagem de G sob a função contínua $g \mapsto x^{-1}g^{-1}xg$, e pelo Lema 1.5.5 item c), $K_x(G)$ é compacto. Portanto, $K_x(G)$ é compacto no espaço de Hausdorff G, então pelo Lema 1.5.5 item b), $K_x(G)$ é fechado em G.

□

Capítulo

4

Considerações finais

Ao longo deste trabalho, mostramos que se G é um p-grupo finito com $d(G') = 2$, então existe $x \in G$ tal que $G' = \{[x, g] \mid g \in G\}$. Apresentamos a seguir alguns resultados posteriores relacionados com a questão de, em um p-grupo G, G' coincidir ou não com o conjunto de comutadores.

Um ano após [6], em [3] De Las Heras estendeu esse resultado para $d(G') = 3$:

Teorema 4.1. *Seja G um p-grupo finito com $p \geq 5$. Se G' pode ser gerado por 3 elementos, então G' consiste somente de comutadores.*

Nesse caso, a hipótese $p \geq 5$ é necessária pois para para $p = 2$ e 3 e $d(G') = 3$ Guralnick apresentou contra-exemplos em [12]. Além disso, ainda em [3] o autor observa que ter um elemento especial $x \in G$ tal que $G' = \{[x, g] \mid g \in G\}$, como no caso em que $d(G') = 2$, em geral não ocorre com $d(G') = 3$.

Agora, para $d(G') = 4$, no Exemplo 5.4 de [13] , Kappe e Morse apresentam um grupo com $d(G') = 4$ e que $G' \neq K(G)$, ou seja, em geral a condição $G' = K(G)$ não pode ser estendida para $d(G') = 4$. Mas em [3] o autor também mostra que com mais algumas condições garantimos que o resultado vale para $d(G') \geq 4$.

Teorema 4.2. *Seja G um p-grupo finito e escreva $d = log_p|G' : (G')^p|$. Se $d \leq p - 1$ e a ação de G em G' é uniserial módulo $(G')^p$, então existe $x \in G$ tal que $G' = \{[x, g] \mid g \in G\}$.*

Por fim, no mesmo artigo o autor mostra que os análogos dos Teoremas 4.1 e 4.2 valem para grupos *pro-p*.

Outros resultados interessantes sobre essa questão são os de Kaushik e Yadav, que em 2021 apresentaram em [14] uma classificação dos p-grupos G com G' de ordem p^4 e expoente p tais que

$G' \neq K(G)$; e no mesmo ano apresentaram em [15] uma classificação dos p-grupos G de ordem p^7 tais que $G' \neq K(G)$. Em ambos os casos, os autores também obtiverem que, se $G' \neq K(G)$, então os elementos de G' podem ser escritos como produto de no máximo dois comutadores.

Uma forma de generalizar a questão é por meio de palavras de grupos.

Uma palavra w em k variáveis é um elemento não trivial do grupo livre F_k com k geradores. Para qualquer grupo G, a palavra w pode ser associada com uma função:

$$w : G \times \underset{k}{...} \times G \to G$$
$$(x_1, ..., x_k) \mapsto w(x_1, ..., x_k)$$

A imagem dessa função é o conjunto de w-valores de G e é denotado por G_w. O subgrupo gerado por esse conjunto é chamado subgrupo verbal de w em G, e é denotado por $w(G)$. Assim, em um sentido mais geral, podemos nos perguntar: dado um grupo G e uma palavra w, quando que $w(G) = G_w$, ou seja, quando que o subgrupo verbal $w(G)$ coincide com o conjunto de w-valores de G?

Podemos definir palavras centrais inferiores pela regra $\gamma_1(x_1) = x_1$ e

$$\gamma_r(x_1, \ldots, x_r) = [\gamma_{r-1}(x_1, \ldots, x_{r-1}), x_r] = [x_1, ..., x_r]$$

para $r \geq 2$. Assim, o subgrupo verbal $\gamma_r(G)$ da palavra γ_r em um grupo G coincide com o r-ésimo termo da série central inferior de G. Nesses termos, a questão de quando $G' = K(G)$ se traduz como $\gamma_2(G) = G_{\gamma_2}$. Para as palavras centrais inferiores, de las Heras e Morigi provaram em [4] o seguinte resultado:

Teorema 4.3. *Sejam G um p-grupo finito e $r \geq 2$. Se $\gamma_r(G)$ é cíclico ou se p é ímpar e $\gamma_r(G)$ pode ser gerado por 2 elementos, então existem $x_1, \ldots, x_{j-1}, x_{j+1}, \ldots, x_r \in G$ com $1 \leq j \leq r$ tais que*

$$\gamma_r(G) = \{[x_1, \ldots, x_{j-1}, g, x_{j+1}, \ldots, x_r] \mid g \in G\}.$$

Os autores também mostraram no mesmo artigo que o análogo do resultado vale no caso em que G é um *pro-p* grupo.

Outra sequência interessante de palavras são as palavras derivadas δ_k, em 2^k variáveis, definidas recursivamente por

$$\delta_0 = x_1, \quad \delta_k = [\delta_{k-1}(x_1, \ldots, x_{2^{k-1}}), \delta_{k-1}(x_{2^{k-1}+1}, \ldots, x_{2^k})], \quad \text{para } k \geq 1.$$

O subgrupo verbal correspondente à palavra δ_k é o familiar k-ésimo subgrupo comutador de G, geralmente denotado por $G^{(k)}$. Então podemos olhar para problemas de mesma natureza com a referida série. Por exemplo, ainda segue em aberto:

Problema. Seja G um p-grupo finito tal que $G^{(r)}$ é cíclico para algum $r \geq 3$. É verdade que

$G^{(r)} = G_{\delta_r}$, onde δ_r denota a r-ésima palavra derivada?

Outra forma de mergulhar na questão, indo para além dos p-grupos, é estudar em grupos de ordem mista não apenas os comutadores, mas mais especificamente os comutadores coprimos, ou seja, comutadores $[x, y]$ onde x e y possuem ordem coprima, o que Shumyatsky faz em [24]. Como já citado, em [17] foi provada a Conjectura de Ore, que estabelece que em um grupo simples não abeliano todo elemento é um comutador. Em 2012 no artigo [24] Shumyatsky conjectura que em um grupo simples não abeliano todo elemento é um comutador coprimo. No mesmo artigo, o autor prova que:

Teorema 4.4. *Seja $n \geq 5$. Todo elemento do grupo alternado A_n é um comutador de um elemento de ordem ímpar e um elemento de ordem que divide 4.*

Em Dezembro do mesmo ano, Shumyatsky e Pellegrini mostram em [22]:

Teorema 4.5. *Seja $q > 3$ uma potência de primo. Todo elemento de $PSL(2, q)$ é um comutador coprimo.*

Caminhando assim na direção de demonstrar afirmativamente a conjectura.

Capítulo

5

Apêndice

5.1 Formas Bilineares

Na demonstração do Lema 3.12 utilizamos uma forma bilinear alternada. Esse apêndice contêm o mínimo necessário que precisa-se conhecer de formas bilineares alternadas para entender o argumento utilizado nessa demonstração.

Lembrando que, se F é um corpo, a característica de F é definida como sendo o menor inteiro positivo m tal que $ma = a+a+...+a = 0$ para todo $a \in F$. Se tal m não existir, a característica do corpo é definida como 0.

Definição 5.1.1. *Uma* ***forma bilinear*** *de um espaço vetorial V sobre um corpo F é uma função $f : V \times V \to F$ que, para todos $u, v, w \in V$ e $\lambda \in F$, satisfaz as regras:*

- $f(\lambda u + v, w) = \lambda f(u, w) + f(v, w)$
- $f(u, \lambda v + w) = \lambda f(u, v) + f(u, w)$.

.

Definição 5.1.2. *Uma forma bilinear $f : V \times V \to F$ é dita:*

- ***simétrica*** *se $f(u, v) = f(v, u)$ para todo $u, v \in V$.*
- ***anti-simétrica*** *se $f(u, v) = -f(v, u)$ para todo $u, v \in V$.*
- ***alternada*** *se $f(v, v) = 0$ para todo $v \in V$.*

Uma forma bilinear alternada é sempre anti-simétrica, afinal:

$$f(u + v, u + v) = 0$$

$$f(u,u) + f(u,v) + f(v,u) + f(v,v) = 0$$

$$f(u,v) + f(v,u) = 0$$

$$f(u,v) = -f(v,u)$$

Por outro lado, se a característica de F não é 2, então uma forma bilinear anti-simétrica é alternada. Afinal, $f(v,v) = -f(v,v) \implies 2f(v,v) = 0 \implies f(v,v) = 0$ se $char(F) \neq 2$. Mas se $char(F) = 2$, uma forma bilinear pode ser anti-simétrica sem ser alternada.

Definição 5.1.3. *Escrevemos $u \perp v$ quando $f(u,v) = 0$ (o que é equivalente a $f(v,u) = 0$ em todo caso) e dizemos que u e v são **perpendiculares** ou **ortogonais** (com respeito à forma f).*

Definição 5.1.4. *Escrevemos $S^{\perp} = \{v \in V \mid v \perp s \text{ para todo } s \in S\}$, para qualquer subconjunto S de V, ou seja, $S^{\perp}$ é o conjunto de dos vetores de V que são perpendiculares à todos os vetores de S. Dizemos que $S^{\perp}$ é o **espaço perpendicular** de S.*

Definição 5.1.5. *Um vetor não nulo que é perpendicular a ele mesmo é chamado **isotrópico**, ou seja, $u \in V^*$ é isotrópico se $f(u,u) = 0$. De forma mais geral, $f(v,v)$ é chamado **norma** de v. (Essa não é a mesma definição usual sobre $\mathbb{C}$, que é a raiz quadrada de $f(v,v)$.)*

Definição 5.1.6. *O **radical** de f, escrito como rad f, é $V^{\perp}$, ou seja, o conjunto de vetores de V perpendiculares a todos os vetores de V. Dizemos que f é **não-singular** se rad $f = 0$ e f é **singular** caso contrário.*

Dado uma forma bilinear alternada f sobre o espaço V, queremos encontrar uma base para V que seja conveniente para f. Se existem vetores u, v tais que $f(u,v) = \lambda \neq 0$ então escolha os primeiros dois vetores da base $e_1 = u$ e $h_1 = \lambda^{-1}v$. Então com respeito à base $\{e_1, h_1\}$ a forma f satisfaz:

- $f(e_1, e_1) = f(h_1, h_1) = 0$
- $f(e_1, h_1) = -f(h_1, e_1) = 1$

Agora restrinja a forma para $\{e_1, h_1\}^{\perp}$ e continue. Escolha u_2, v_2 tais que $f(u_2, v_2) = \lambda_2 \neq 0$, se existirem, e então $e_2 = u_2$ e $h_2 = \lambda_2^{-1}v_2$. Então com respeito à $\{e_1, h_1, e_2, h_2\}$ teremos:

- $f(e_1, e_1) = f(h_1, h_1) = f(e_2, e_2) = f(h_2, h_2) = 0$
- $f(e_1, e_2) = f(e_1, h_2) = 0$
- $f(h_1, e_2) = f(h_1, h_2) = 0$
- $f(e_1, h_1) = -f(h_1, e_1) = 1$
- $f(e_2, h_2) = f(h_2, e_2) = 1$

Continuando assim, eventualmente teremos escolhido vetores bases $e_1, ..., e_m$ e $h_1, ..., h_m$ tais que $f(u, v) = 0$ para todos u, v vetores da base, exceto $f(e_i, h_i) = -f(h_i, e_i) = 1$. Então ou teremos uma base para todo o espaço, no caso em que f é não-singular e $dim(V) = 2m$ é par, ou se não $f(u, v) = 0$ para todo $u, v \in \{e_1, ..., h_m\}^{\perp} \neq 0$, e nesse caso f é singular, e podemos completar para uma base da forma como escolhermos. Note que no último caso temos $f(u, v) = 0$ para qualquer $u \in \{e_1, ..., h_m\}^{\perp}$ e qualquer $v \in V$.

Corolário 5.1.7. *Seja f é uma forma bilinear alternada e não-singular de um espaço vetorial V sobre um corpo F. Então $dim(V)$ é par.*

Referências Bibliográficas

[1] Y. Berkovich. *Volume 1.* De Gruyter, Berlin, New York, 2008.

[2] N. Blackburn. On prime-power groups in which the derived group has two generators. *Mathematical Proceedings of the Cambridge Philosophical Society*, 53(1):19–27, 1957.

[3] I. de las Heras. Commutators in finite p-groups with 3-generator derived subgroup. *Journal of Algebra*, 546:201–217, 2020.

[4] I. de las Heras and M. Morigi. Lower central words in finite p-groups. *Publicacions Matemàtiques*, 65(1):243 – 269, 2021.

[5] J. D. Dixon, M. P. F. Du Sautoy, A. Mann, and D. Segal. *Analytic Pro-P Groups*. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2 edition, 1999.

[6] G. A. Fernández-Alcober and I. de las Heras. Commutators in finite p-groups with 2-generator derived subgroup. *Israel Journal of Mathematics*, 232(1):109–124, Aug 2019.

[7] G. A. Fernández-Alcober. An introduction to finite p-groups: regular groups and p-groups of maximal class, 2000.

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

[9] M. Garonzi. Notas de aula de grupos profinitos, 2018.

[10] M. Garonzi. Notas de aula de representação de grupos 1, 2022.

[11] R. M. Guralnick. *Expressing group elements as products of commutators*. PhD thesis, UCLA, 1977.

[12] R. M. Guralnick. Commutators and commutator subgroups. *Advances in Mathematics*, 45(3):319–330, 1982.

[13] L. C. Kappe and R. F. Morse. On commutators in groups. *Groups St Andrews 2005*, 2:531–558, 2007.

[14] R. Kaushik and M. K. Yadav. Commutators and commutator subgroups of finite p-groups. *Journal of Algebra*, 568:314–348, 2021.

[15] R. Kaushik and M. K. Yadav. Commutators in groups of order p^7, 2021.

[16] E. I. Khukhro. *p-Automorphisms of Finite p-Groups*. London Mathematical Society Lecture Note Series. Cambridge University Press, 1998.

[17] M. W. Liebeck, E. A. O'Brien, A. Shalev, and P. H. Tiep. The ore conjecture. *J. Eur. Math. Soc.*, 12(4):939–1008, 2010.

[18] A. Lubotzky and A. Mann. Powerful p-groups. i. finite groups. *Journal of Algebra*, 105(2):484–505, 1987.

[19] I. D. Macdonald. On Cyclic Commutator Subgroups. *Journal of the London Mathematical Society*, s1-38(1):419–422, 01 1963.

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

[21] O. Ore. Some remarks on commutators. *Proc. Amer. Math. Soc.*, (2):307–314, 1951.

[22] M.A. Pellegrini and P. Shumyatsky. Coprime commutators in psl(2, q). *Arch. Math. 99*, pages 501–507, 2012.

[23] D. M. Rodney. On Cyclic Derived Subgroups. *Journal of the London Mathematical Society*, s2-8(4):642–646, 10 1974.

[24] P. Shumyatsky. Commutators of elements of coprime orders in finite groups, 2012.

[25] J. S. Wilson. *Profinite groups*. Clarendon Press; Oxford University Press, 1998.

[26] S. Zalesski, P. e Chagas. Notas de aula de grupos profinitos, 2023.