Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

Sobre Grupos Finitos e Profinitos Quase Engel

por

Sara Raissa Silva Rodrigues

Brasília
2017

Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

Sara Raissa Silva Rodrigues

Sobre Grupos Finitos e Profinitos Quase Engel

Dissertação apresentada ao Programa de Pós-Graduação em Matemática da Universidade de Brasília, como requisito parcial para obtenção do título de Mestre em Matemática.

Orientadora: Profa. Dra. Cristina Acciarri.

Brasília, 22 de fevereiro de 2017.

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

RR696s

Rodrigues, Sara Raissa Silva
Sobre Grupos Finitos e Profinitos Quase Engel / Sara Raissa Silva Rodrigues; orientador Cristina Acciarri. -- Brasília, 2017.
105 p.

Dissertação (Mestrado - Mestrado em Matemática) -- Universidade de Brasília, 2017.

1. Condições de tipo-Engel. 2. Grupos Profinitos. 3. Comutadores. 4. Subgrupo de Fitting. I. Acciarri, Cristina, orient. II. Título.

Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

Sobre Grupos Finitos e Profinitos Quase Engel

por

Sara Raissa Silva Rodrigues[1]

Dissertação apresentada ao Corpo Docente do Programa de Pós-graduação em Matemática – UnB, como requisito parcial para obtenção do grau de

MESTRE EM MATEMÁTICA

Brasília, 22 de fevereiro de 2017

Comissão Examinadora:

Cristina Acciarri

Profa. Dra. Cristina Acciarri – MAT/UnB (Orientadora)

Aline Gomes S. Pinto

Profa. Dra. Aline Gomes da Silva Pinto – MAT/UnB (Membro)

Profa. Dr. Ilir Snopche – MAT/UFRJ (Membro)

[1]o autor foi bolsista da CAPES durante a elaboração desta dissertação.

“Nunca desista dos seus sonhos, faça a sua parte e confie em Deus que tudo dará certo.”

Agradecimentos

A Deus por ser a minha base, o meu tudo, por sempre estar presente em minha vida, dando-me sabedoria e força para superar qualquer adversidade que a vida me impõe. À Nossa Senhora de Nazaré por ser minha fiel intercessora junto ao seu filho Jesus e aos meus santinhos queridos pela intercessão junto ao Pai.

À minha mãe Ana Maria, por ser o meu esteio, a minha base, o meu amor maior, por sempre fazer o possível e o impossível para que eu possa realizar todos os meus sonhos e por sempre estar ao meu lado incondicionalmente; esta conquista deve-se em grande parte a ela. Ao meu pai Adinilson Fialho, que mesmo ausente, sempre orientou-me a nunca desistir dos meus sonhos, ao meu irmão, cunhada, enfim, a todos os meus familiares pelo apoio.

À minha querida orientadora Cristina Acciarri não somente pela eficiente, excelente e paciente orientação, mas também por tudo, por ter sido fundamental para o início e término do meu mestrado, por sempre ter acreditado em mim, pelos conselhos valiosos e sobretudo por nunca ter desistido de mim. Obrigada pelas suas maravilhosas e profundas aulas que fizeram eu amar ainda mais à álgebra, especialmente a teoria de grupos. A senhora com certeza tem um lugar no meu coração.

À minha amada madrinha e professora Nazaré Bezerra, pelas orações, torcida, amizade, pelos conselhos valiosos e por ser a minha psicóloga sem diploma. À minha amada professora Adma Muriel por sempre torcer por mim, pelas orações, amizade, enfim, por tudo.

Aos professores Aline Pinto e Ilir Snopche por terem aceitado participar da minha banca examinadora e pelas suas valiosas sugestões para a melhoria deste trabalho.

À professora Daniela Amato, pelas suas excelentes aulas, torcida, por deixar a álgebra ainda mais bonita com suas explicações e pela sua letra top no quadro.

De um modo geral gostaria de agradecer a todos os meus professores da UnB que de alguma forma contribuíram para a minha formação, dentre os quais destaco os professores: Alexei, Aline, Cátia, Daniele Baratela, Irina, João Paulo, Luciana, Luís Miranda, Noraí e Ricardo Ruviaro. E a todos os servidores do Mat/UnB.

Às minhas queridas professoras da UFPA Cristina Vaz, Joelma e Rúbia por todo apoio, torcida e amizade. E aos professores Giovany Figueiredo e Sandra Imaculada pelas cartas de recomendação.

Aos amigos queridos que conquistei ao longo destes anos em Brasília, especialmente os da matemática: Bruno, Christe, Karen, Lumena, Maria, Mayra, Nathália, Rafael, Regiane, Valter e Welinton. E aos amigos queridos do pensionato: Bruna Busson, Claúdia, Dariana, Eliete, Giovana, Larissa, Luciana, Willyane e Zé Pedro. Obrigada a todos pela cumplicidade, ajuda, apoio, torcida, orações, amizade, por me aguentarem todos estes anos e por me escutarem.

Aos meus queridos amigos que sempre me acompanham: Ana Lídia, Érico, Francimaria, Layane, Mayara, Priscyla, Renan e Thays pela torcida, orações, amizade e por me escutarem nos momentos que precisei conversar.

À Cristine, Emerson e Iolanda, pessoas especiais, queridas e amigas que me acolheram muito bem em Brasília e sempre ajudaram-me.

À Elza Líbia pelas orações, carinho, amizade, por sempre ajudar-me e pela torcida. À minha prima Joseana pelo carinho e por ter ajudado-me quando precisei. E à minha madrinha Charlane pelas orações, carinho e torcida.

Ao Lucas Bezerra por toda ajuda dada durante esses últimos meses.

À Capes pelo apoio financeiro ao longo de todo o mestrado.

Enfim, obrigada a todos que acreditaram em mim e que de certa forma contribuíram para a minha formação acadêmica.

Dedicatória

A Deus, aos meus pais Ana Maria e Adinilson Fialho (in memoriam) e à minha madrinha Nazaré Bezerra.

Resumo

Um grupo G é chamado um grupo Engel se para todos x e g em G a identidade $[x, g, \ldots, g] = 1$ vale em G, onde g é repetido no comutador um número suficiente de vezes que depende de x e g. É bem conhecido que qualquer grupo localmente nilpotente é um grupo Engel. Mas, a recíproca não vale em geral. No entanto, em [**26**] J. S. Wilson e E. I. Zelmanov provaram que todo grupo profinito Engel é localmente nilpotente.

Dados um elemento g em G e um inteiro positivo n, seja $E_n(g)$ o subgrupo gerado por todos os comutadores $[x, g, \ldots, g]$ onde, x varia em G e g é repetido n vezes. Esta dissertação está baseada no artigo *Almost Engel finite and profinite groups* [**13**] de E. I. Khukhro e P. Shumyatsky. Mostramos que se G é um grupo profinito tal que, para todo g em G existe um inteiro positivo $n = n(g)$ com a propriedade que $E_n(g)$ é finito, então G possui um subgrupo normal finito N tal que G/N é localmente nilpotente. Um resultado da mesma natureza e de tipo quantitativo é provado para um grupo finito G, deduzindo informações sobre a ordem do subgrupo residual nilpotente $\gamma_\infty(G)$ de G.

Palavras-chave: grupos profinitos, subgrupo de Fitting, condições de tipo-Engel, comutadores.

Abstract

A group G is called an Engel group if for every x and g in G the equation $[x, g, \ldots, g] = 1$ holds in G, where g is repeated in the commutator sufficiently many times depending on x and g. It is well known that any locally nilpotent group is an Engel group, but the converse does not hold in general. However, in [**26**] J. S. Wilson and E. I. Zelmanov proved that any Engel profinite group is locally nilpotent.

Given an element g in G and a positive integer n, let $E_n(g)$ be the subgroup generated by all commutators $[x, g, \ldots, g]$ over x in G, where g is repeated n times. This master's dissertation is based on the article *Almost Engel finite and profinite groups* [**13**] of E. I. Khukhro e P. Shumyatsky. It is shown that if G is a profinite group such that, for every g in G there is a positive integer $n = n(g)$ such that $E_n(g)$ is finite, then G has a finite normal subgroup N such that G/N is locally nilpotent. A similar result of quantitative nature holds for a finite group G, and it gives information about the order of the nilpotent residual subgroup $\gamma_\infty(G)$ of G.

Keywords: profinite groups, Fitting subgroup, Engel-like conditions, commutators.

Sumário

Introdução

Seja G um grupo qualquer, dizemos que G é localmente nilpotente se todo subgrupo finitamente gerado de G é nilpotente. Querendo relaxar a hipótese de ser localmente nilpotente, podemos considerar grupos Engel. Um grupo G é dito Engel se para todos x e g em G a identidade $[x, g, \dots, g] = 1$ vale em G, onde g é repetido no comutador um número suficiente de vezes que depende de x e g. É fácil ver que qualquer grupo localmente nilpotente é Engel, mas a implicação oposta não vale em geral (veja o Capítulo 2 para exemplos disto). Em contraposição com esta observação negativa J. S. Wilson e E. I. Zelmanov provaram em [**26**] que todo grupo profinito Engel é sempre localmente nilpotente, de fato provando que os dois conceitos são equivalentes para um grupo profinito.

Na literatura são muitos os resultados sobre grupos Engel ou sobre grupos satisfazendo condições de tipo-Engel, pois de fato são estas propriedades muito relacionadas com os mais bem estudados conceitos de nilpotência e nilpotência local. Entre os resultados clássicos sobre grupos de Engel cabe mencionar o Teorema de Baer [**7**, Satz III.6.15] que diz que em um grupo finito G qualquer elemento Engel, ou seja, qualquer elemento g em G tal que para todo x em G existe $n = n(x, g)$ tal que a identidade $[x, \underbrace{g, \dots, g}_{n}] = 1$ vale, precisa pertencer ao subgrupo de Fitting de G que é o único maior subgrupo nilpotente normal de G.

Em busca de generalizações do clássico Teorema de Baer, E. I. Khukhro e P. Shumyatsky introduziram em [**14**] uma família de subgrupos que ajudam no estudo de condições de tipo-Engel. Mais especificamente, dado um elemento g em um grupo G e para todo inteiro positivo n é possível definir o subgrupo $E_n(g)$, que é o subgrupo gerado por todos os comutadores da forma $[x, g, \ldots, g]$, onde x varia em G e g é fixado e repetido n vezes no comutador.

Existe uma versão quantitativa do conceito de elemento Engel em um grupo, ou seja, o de elemento n-Engel: um elemento g em G é dito n-Engel se g respeita a identidade $[x, \underbrace{g, \ldots, g}_{n}] = 1$ para todo x em G com o mesmo inteiro positivo n. Com isso, vemos que os subgrupos $E_n(g)$, definidos em [**14**], dão uma forma de "medir" quão longe de ser n-Engel um elemento g está. Digamos que os subgrupos são uma forma de expressar o "desvio" de um elemento g de ser n-Engel.

Mais tarde no artigo *Almost Engel Finite and Profinite Groups* [**13**], que é a referência principal desta dissertação, E. I. Khukhro e P. Shumyatsky provaram outros resultados em termos dos subgrupos $E_n(g)$ descritos acima. O principal destes resultados é o seguinte sobre grupos profinitos.

Teorema A. *Suponha que G é um grupo profinito tal que, para cada $g \in G$, existe um inteiro positivo $n = n(g)$ tal que $E_n(g)$ é finito. Então G possui um subgrupo normal finito N tal que G/N é localmente nilpotente.*

Na demonstração do Teorema A a teoria dos grupos pronilpotentes (análogos profinitos dos grupos nilpotentes finitos) é relevante, assim como o resultado de Wilson e Zelmanov enunciado anteriormente. A ideia principal da prova do Teorema A é mostrar que o subgrupo residual pronilpotente $\gamma_\infty(G)$ de G é finito e satisfaz as propriedades pedidas no enunciado. Veremos que isto é obtido com um argumento indutivo sobre a ordem de $G/F(G)$, onde $F(G)$ é o maior subgrupo normal pronilpotente de G.

Nas hipóteses do Teorema A é dada uma condição de finitude para os subgrupos $E_n(g)$. Quando consideramos grupos finitos é natural definir, para todo g em G, também o subgrupo $E(g)$ definido como sendo a interseção de todos os $E_n(g)$, de forma a "condensar" em um único subgrupo todas as informações contidas nos $E_n(g)$ para g fixado. Uma vez definidos estes novos subgrupos é natural pensar que exista uma hipótese e consequente resultado análogos aos do Teorema A para grupos finitos. Mais precisamente, em [**13**] também foi provado o seguinte resultado.

Teorema B. *Suponha que G é um grupo finito e existe um inteiro positivo m tal que $|E(g)| \leq m$ para todo $g \in G$. Então a ordem do subgrupo residual nilpotente $\gamma_\infty(G)$ é limitada em termos de m.*

O Teorema B pode ser pensando como uma generalização do Teorema de Zorn [**7**, Satz III.6.3], que afirma que um grupo finito Engel é sempre nilpotente.

É importante destacar que o Teorema B é usado na demonstração do Teorema A e além disso, uma consequência dele é poder limitar em termos de m o índice do subgrupo de Fitting em G.

Desde que as ordens dos subgrupos $E_n(g)$ possuam uma limitação uniforme, ou seja, independente da escolha do elemento g, o Teorema B tem uma imediata consequência para grupos profinitos, como enunciado a seguir.

Corolário C. *Suponha que G é um grupo profinito e existe um inteiro positivo m tal que para cada $g \in G$ existe $n = n(g)$ tal que $|E_n(g)| \leq m$. Então G possui um subgrupo normal finito N de ordem limitada em termos de m tal que G/N é localmente nilpotente.*

Observemos como a hipótese mais restritiva no Corolário C sobre a limitação das ordens dos $E_n(g)$ implica uma conclusão mais forte.

Terminamos observando que esta dissertação está dividida em cinco capítulos. No primeiro capítulo, relembramos alguns resultados da teoria de grupos que são funcionais ao longo deste trabalho. No Capítulo 2, apresentamos todos os conceitos relativos a grupos Engel e condições de tipo-Engel, inclusive as propriedades dos subgrupos $E_n(g)$ e $E(g)$ mencionados antes. No Capítulo 3, vamos discutir uma série de resultados, sobre grupos finitos, preparatórios para a apresentação da prova do Teorema B. Os detalhes da demonstração do Teorema B também são discutidos neste capítulo. O Capítulo 4 está dedicado a um estudo mais detalhado dos grupos profinitos, com particular ênfase para a classe dos grupos pronilpotentes. Por fim, no Capítulo 5, daremos espaço a resultados técnicos sobre grupos profinitos relacionados com as hipóteses do Teorema A e apresentaremos as demonstrações do Teorema A e do Corolário C.

1

Preliminares

Neste capítulo, temos por objetivo relembrar definições e resultados sobre teoria de grupos que serão essenciais para esta dissertação. Assumiremos conhecidos alguns teoremas, dentre eles, o Teorema de Lagrange, os Teoremas de Sylow, os teoremas de isomorfismos e o teorema de correspondência. As referências principais utilizadas neste capítulo são os livros de E. I. Khukhro [**11**], I. M. Isaacs [**15**] e [**16**], D. J. S. Robinson [**21**] e de J. S. Rose [**22**].

1.1. Comutadores

Nesta seção vamos definir o conceito de comutadores, objeto fundamental em nosso estudo e ressaltar suas principais propriedades que serão utilizadas ao longo deste trabalho.

Seja G um grupo. Dados x e y em G, o *comutador* de x e y é o elemento de G definido por $[x, y] = x^{-1}y^{-1}xy$. Podemos definir de maneira recursiva comutadores da seguinte forma: por convenção $[x_1] = x_1$ e $[x_1, \ldots, x_n] = [[x_1, \ldots, x_{n-1}], x_n]$, para todos $x_1, \ldots, x_n \in G$ e $n \geqslant 2$. Sejam x e y elementos de G. O *conjugado* de x por y é o elemento $x^y = y^{-1}xy$. Assim, podemos escrever $[x, y] = x^{-1}x^y$.

A proposição a seguir reúne as principais propriedades de comutadores e serão bastante usadas ao longo desta dissertação.

Proposição 1.1.1. *Sejam G um grupo e x, y e z elementos de G. As seguintes identidades de comutadores valem:*
(i) $x^y = x[x, y]$;
(ii) $[x, y] = [y, x]^{-1}$;
(iii) $[xy, z] = [x, z]^y[y, z]$;
(iv) $[x, yz] = [x, z][x, y]^z$;
(v) $[x, y^{-1}, z]^y[y, z^{-1}, x]^z[z, x^{-1}, y]^x = 1$ *(Identidade de Hall-Witt);*

(vi) $[x,z]^y = [x,z][x,z,y]$;
(vii) *para qualquer homomorfismo* φ *de* G, *temos* $\varphi([x,y]) = [\varphi(x),\varphi(y)]$;
(viii) *para* $n \geqslant 1$ *e* $x_1,\dots,x_n,y \in G$ *temos*

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

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

Sejam H e K dois subgrupos de um grupo G. O *subgrupo comutador* de H e K é definido como o subgrupo gerado por todos os comutadores $[h,k]$ onde $h \in H$ e $k \in K$. Denotamos este subgrupo por $[H,K]$. Assim, temos

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

Por outro lado, se $H_1,\dots,H_n$ são subgrupos de G, definimos o subgrupo comutador de $H_1,\dots,H_n$ por

$$[H_1,\dots,H_n] = [[H_1,\dots,H_{n-1}],H_n],$$

para todo $n \geqslant 2$.

Um caso particular de subgrupo comutador é quando consideramos $H = K = G$, isto é, $G' = [G,G] = \langle [x,y] \mid x,y \in G\rangle$, este subgrupo é chamado de *subgrupo derivado* de G.

O *centro* de um grupo G é o subgrupo definido por

$$Z(G) = \{x \in G \mid [x,g] = 1 \text{ para todo } g \in G\}.$$

A próxima proposição reúne várias propriedades a respeito de subgrupo comutador. As demonstrações podem ser obtidas combinando as definições com as propriedades de comutadores listadas na Proposição 1.1.1.

Proposição 1.1.2. *Sejam* H *e* K *dois subgrupos de um grupo* G. *Então as seguintes afirmações valem:*
(i) $[H,K] = [K,H]$;
(ii) *para qualquer homomorfismo* φ *de* G, *temos* $\varphi([H,K]) = [\varphi(H),\varphi(K)]$;
(iiii) *se* N *é um subgrupo normal de* G, *então*

$$[HN/N, KN/N] = [H,K]N/N;$$

(iv) *se* H,K *e* L *são subgrupos normais de* G, *então* $[HK,L] = [H,L][K,L]$;
(v) *se* $K \lhd G$ *e* $K \leq H \leq G$, *então*

$$[H,G] \leq K \text{ se, e somente se, } H/K \leq Z(G/K).$$

Fazendo indução sobre n e usando a Proposição 1.1.2 item (iv), obtemos o seguinte corolário.

Corolário 1.1.3. *Sejam $H_1, \ldots, H_n$ e K subgrupos normais de um grupo G. Então $[H_1 \cdots H_n, K] = [H_1, K] \cdots [H_n, K]$.*

Seja X um subconjunto não vazio de um grupo G. O *centralizador de X em G* é o subgrupo $C_G(X) = \{g \in G \mid xg = gx, \forall\, x \in X\}$. Agora, seja g um elemento de G, o *conjugado* de X por g é o conjunto dado por $X^g = \{x^g \mid x \in X\}$. O *fecho normal* de X em G é a interseção de todos os subgrupos normais de G que contém X. Denotamos este subgrupo por $\langle X^G \rangle$. Claramente, $\langle X^G \rangle$ é um subgrupo normal de G e pode-se mostrar que $\langle X^G \rangle = \langle X^g \mid g \in G \rangle$. O *normalizador* de X em G é o subgrupo definido por $N_G(X) = \{g \in G \mid X^g = X\}$. Se $X \leq G$, então temos que $N_G(X)$ é o maior subgrupo de G no qual X é normal.

Vejamos agora um lema que nos fornece uma caracterização de como se comportam os subgrupos comutadores dos subgrupos, no qual um está contido no centralizador ou no normalizador do outro.

Lema 1.1.4. *Sejam H e K subgrupos de um grupo G. Então,*
(i) *$K \leq C_G(H)$ se, e somente se, $[K, H] = 1$.*
(ii) *$K \leq N_G(H)$ se, e somente se, $[H, K] \leq H$.*

Demonstração. Mostraremos o item (i). De fato, se $K \leq C_G(H)$, então para todo $k \in K$ temos que $k \in C_G(H)$, assim $[k, h] = 1$ para todos $k \in K$ e $h \in H$. Logo, $[K, H] = 1$. Por outro lado, como $[K, H] = 1$, tem-se que $[k, h] = 1$ para todos $k \in K$ e $h \in H$. Assim, para todo $k \in K$, segue que $[k, h] = 1$ para todo $h \in H$. Logo, $K \leq C_G(H)$.

Agora, vamos mostrar o item (ii). Se $K \leq N_G(H)$, então dados $k \in K$ e $h \in H$, temos pela hipótese que $[h, k] = h^{-1}h^k \in H$. Logo, $[H, K] \leq H$. Por outro lado, suponhamos que $[H, K] \leq H$. Pela Proposição 1.1.1 item (i), temos que $h^k = h[h, k]$. Assim, segue da hipótese que para todo $h \in H$ e todo $k \in K$, temos que $h^k \in H$. Portanto, $K \leq N_G(H)$. $\square$

O lema a seguir será muito usado ao longo deste trabalho, sua demonstração pode ser encontrada em [**11**, Lemma 1.9].

Lema 1.1.5. *Seja G um grupo. Para qualquer subgrupo H de G, temos que $C_G(H)$ é normal em $N_G(H)$ e $N_G(H)/C_G(H)$ é isomorfo a um subgrupo de $Aut(H)$.*

O próximo resultado nos garante em que condição o centralizador de um subgrupo é normal.

Lema 1.1.6. *Se H é um subgrupo normal (ou característico) de G, então ambos $N_G(H)$ e $C_G(H)$ são subgrupos normais (ou característico) de G.*

Provaremos agora um lema muito útil para deduzir relações entre subgrupos comutadores.

Lema 1.1.7 (dos Três Subgrupos). *Sejam H, K e L subgrupos de um grupo G e N um subgrupo normal de G. Se $[[H,K],L] \leq N$ e $[[K,L],H] \leq N$, então $[[L,H],K] \leq N$.*

Demonstração. Como N é um subgrupo normal de G, podemos considerar o grupo quociente G/N e assumir que $N = 1$. Assim, $[[H,K],L] = [[K,L],H] = 1$. Agora, usando isto e a Identidade de Hall-Witt, Proposição 1.1.1 item (v), temos para todos $h \in H, k \in K$ e $l \in L$ que $[l, h^{-1}, k]^h = 1$, isto segue que $[l, h^{-1}, k] = 1$. Daí, substituindo h^{-1} por h, obtemos $[l, h, k] = 1$ para todos $h \in H, k \in K$ e $l \in L$. Então, $[l, h] \in C_G(K)$ para todos $h \in H$ e $l \in L$. Disto segue que $[L, H] \leq C_G(K)$. Logo, pelo Lema 1.1.4 item (i), concluímos que $[[L,H],K] = 1$. Portanto, $[[L,H],K] \leq N$. □

Segue do lema dos três subgrupos o seguinte corolário.

Corolário 1.1.8. *Seja G um grupo. Se H, K e L são subgrupos normais de G. Então,*

$$[[L,H],K] \leq [[H,K],L] \cdot [[K,L],H].$$

Demonstração. Como subgrupos comutadores de subgrupos normais são normais, segue que $N = [[H,K],L] \cdot [[K,L],H]$ é normal em G. Agora, como $[[H,K],L] \leq N$ e $[[K,L],H] \leq N$, temos pelo Lema 1.1.7 que $[[L,H],K] \leq N$. □

1.2. Grupos Nilpotentes e Solúveis

Nesta seção definiremos o conceito de grupo nilpotente e enunciaremos as propriedades mais relevantes acerca dos grupos finitos nilpotentes. Também definiremos grupos solúveis, o subgrupo de Fitting e o subgrupo de Fitting generalizado de um grupo finito e veremos algumas propriedades relacionadas a estes conceitos.

Uma *série normal* de um grupo G é uma sequência de subgrupos

$$1 = N_0 \leq N_1 \leq \cdots \leq N_r = G,$$

com $N_i \lhd G$ para todo $0 \leq i \leq r$.

Uma *série central* de G é uma série normal tal que

$$N_i/N_{i-1} \leq Z(G/N_{i-1}), \quad \forall\ 1 \leq i \leq r.$$

Definição 1.2.1. Dado G um grupo, dizemos que G é *nilpotente* se G possui uma série central.

Vamos agora construir uma série central, que será útil para verificarmos se um dado grupo G é nilpotente.

Seja G um grupo. Definamos os subgrupos $Z_n(G)$ recursivamente da seguinte forma: $Z_0(G) = 1$ e para cada $i \geqslant 1$, $Z_i(G)$ é o único subgrupo normal em G tal que

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

Assim, temos

$$1 = Z_0(G) \leq Z_1(G) = Z(G) \leq \cdots$$

e esta sequência ascendente de subgrupos é chamada *série central ascendente* de G. Observe que pela definição dos $Z_i(G)$, os mesmos são característicos em G.

Note que, dado um grupo G, sempre podemos construir a série central ascendente de G, mas não necessariamente a série alcança o grupo G. Pode-se mostrar que quando isto acontecer, ou seja, quando existir um inteiro $r \geqslant 1$ tal que $Z_r(G) = G$, o grupo G será nilpotente. Assim, G é nilpotente se, e somente se, existe um inteiro $r \geqslant 1$ tal que $Z_r(G) = G$.

Um grupo G é chamado de *perfeito* se $G = G'$. O lema a seguir é um fato básico sobre grupos perfeitos.

Lema 1.2.2 (de Grün). *Seja G um grupo perfeito, então $G/Z(G)$ possui centro trivial.*

Demonstração. De fato, consideremos $Z(G)$ e $Z_2(G)$ os dois primeiros termos da série central ascendente de G. Sabemos por definição que $Z_2(G)$ é o único subgrupo normal de G tal que

$$Z_2(G)/Z(G) = Z(G/Z(G)). \tag{1.2.1}$$

Vamos mostrar que $Z(G) = Z_2(G)$ e o resultado segue. Por um lado, como vale (1.2.1), temos pela Proposição 1.1.2 item (v) que $[Z_2(G), G] \leq Z(G)$. Observemos que pelo Lema 1.1.4 item (i) tem-se $[Z(G), G] = 1$. Agora, considerando os subgrupos $[Z_2(G), G, G]$ e $[G, Z_2(G), G]$, temos o seguinte

$$[Z_2(G), G, G] = [[Z_2(G), G], G] \leq [Z(G), G] = 1.$$

$$[G, Z_2(G), G] = [[G, Z_2(G)], G] \leq [Z(G), G] = 1.$$

Então, aplicando o Lema 1.1.7, obtemos que $[G, G, Z_2(G)] = 1$. Como G é perfeito, segue que $[Z_2(G), G] = 1$. Logo, usando o Lema 1.1.4 item (i), tem-se que $Z_2(G) \leq Z(G)$. Portanto, $Z_2(G) = Z(G)$, como desejado. $\square$

O resultado seguinte, devido a I. Schur, nos dá informações sobre o subgrupo derivado a partir do índice do centro de um grupo.

Teorema 1.2.3 (de Schur). [**20**, Theorem 4.12] *Se G é um grupo cujo centro possui índice finito n, então G' é finito e $(G')^n = 1$.*

Notamos que também vale uma versão quantitativa do resultado anterior, afirmando que se $[G : Z(G)] = n$, então a ordem de G' é limitada em termos de n (veja [**20**, pág. 102]).

A próxima proposição nos fornece uma caracterização dos subgrupos $Z_i(G)$, dando-nos uma caracterização alternativa dos elementos de $Z_i(G)$, que explica melhor como estes elementos se portam com respeito ao fazer comutadores com outros elementos em G. O resultado pode ser mostrado com um argumento indutivo sobre n.

Proposição 1.2.4. *Seja G um grupo. Para todo $n \geqslant 1$, temos que o n-ésimo termo da série central ascendente de G é dado por*

$$Z_n(G) = \{x \in G \mid [x, g_1, \ldots, g_n] = 1, \quad \forall\ g_1, \ldots, g_n \in G\}.$$

É possível mostrar que quando G é um grupo nilpotente, a série central ascendente é a série de comprimento menor possível entre todas as séries centrais de G. Assim, podemos definir o conceito de classe de nilpotência de um grupo.

Seja G um grupo nilpotente. O *menor* natural r tal que $Z_r(G) = G$ é chamado de *classe de nilpotência* de G.

Agora, vamos definir mais uma série central que nos permite identificar se um dado grupo é nilpotente.

Dado um grupo G, definamos os subgrupos $\gamma_i(G)$ recursivamente da seguinte forma: $\gamma_1(G) = G$ e $\gamma_{i+1}(G) = [\gamma_i(G), G]$, para $i \geqslant 1$. Assim, temos

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

e esta sequência descendente de subgrupos é chamada *série central descendente* de G. Note que os subgrupos $\gamma_i(G)$ são característicos em G.

Pode-se mostrar que um grupo G é nilpotente se, e somente se, existe um inteiro c tal que $\gamma_{c+1}(G) = 1$. E que as séries ascendente e descendente de um grupo nilpotente possuem o mesmo comprimento. Assim, o menor inteiro c tal que $\gamma_{c+1}(G) = 1$, coincide com a classe de nilpotência de G.

O lema a seguir nos dá uma caracterização para os termos da série central descendente de um grupo quociente G/N, onde $N \lhd G$.

Lema 1.2.5. *Seja N um subgrupo normal de um grupo G. Então, temos que $\gamma_i(G/N) = \gamma_i(G)N/N$, para todo $i \geq 1$.*

Notamos que a prova deste resultado consiste em um argumento indutivo sobre i que usa o item (iii) da Proposição 1.1.2.

Seja G um grupo, o *residual nilpotente* de G é o subgrupo definido por

$$\gamma_\infty(G) = \bigcap_{i=1}^{\infty} \gamma_i(G),$$

onde o subgrupo $\gamma_i(G)$ é o i-ésimo termo da série central descendente de G.

Se G é um grupo finito, então o subgrupo residual nilpotente de G é dado por $\gamma_\infty(G) = \gamma_n(G)$ para algum n suficientemente grande. Desta maneira, segue pelo Lema 1.2.5 que

$$\gamma_\infty(G/N) = \gamma_\infty(G)N/N, \tag{1.2.2}$$

para qualquer subgrupo normal N de G.

Lema 1.2.6. *Sejam G um grupo finito e N um subgrupo normal de G. Se G/N é nilpotente, então $\gamma_\infty(G) \leq N$.*

Demonstração. De fato, desde que G/N é um grupo nilpotente, segue que existe um inteiro c tal que $\gamma_{c+1}(G/N) = 1$. Agora, pelo Lema 1.2.5, tem-se

$$\gamma_{c+1}(G/N) = \gamma_{c+1}(G)N/N = 1.$$

Logo, obtemos que $\gamma_{c+1}(G) \leq N$. Portanto, $\gamma_\infty(G) \leq N$. □

Consequentemente, aplicando o Lema 1.2.6, concluímos que

Lema 1.2.7. *Se G é nilpotente, então $\gamma_\infty(G) = 1$.*

Verifica-se facilmente que subgrupo de um grupo nilpotente é nilpotente e quociente de nilpotente é nilpotente.

Seja G um grupo e H um subgrupo de G. Lembramos que H é dito um *subgrupo maximal* de G se H é próprio e sempre que existir $K \leq G$ tal que $H \leq K \leq G$, então ou $H = K$ ou $K = G$. Vamos denota-lo por H max G.

O próximo resultado nos dá uma caracterização para os grupos finitos nilpotentes. A demonstração pode ser vista em [**15**, Theorem 1.26].

Teorema 1.2.8. *Seja G um grupo finito. São equivalentes as seguintes afirmações.*
(i) *G é nilpotente.*
(ii) *$H < N_G(H)$, para todo subgrupo próprio $H < G$.*
(iii) *Todo subgrupo maximal de G é normal.*
(iv) *Todo p-subgrupo de Sylow de G é normal.*
(v) *G é o produto direto de seus subgrupos de Sylow.*

O teorema a seguir nos diz que o produto de dois subgrupos normais nilpotentes é um subgrupo nilpotente e nos fornece informações sobre a classe de nilpotência do produto em termos das classes de nilpotência dos dois fatores. A demonstração pode ser encontrada em [**21**, 5.2.8]

Teorema 1.2.9 (de Fitting). *Sejam G um grupo, H e K subgrupos normais de G. Se H e K são nilpotentes de classes de nilpotência c e d respectivamente, então HK é nilpotente de classe de nilpotência no máximo $c+d$.*

O resultado anterior nos motiva a definir um subgrupo muito relevante na teoria de grupos nilpotentes.

Definição 1.2.10. Seja G um grupo, definimos o *subgrupo de Fitting* de G por

$$F(G) = \langle N \mid N \trianglelefteq G \text{ e } N \text{ nilpotente}\rangle.$$

Note que se G é finito, então $F(G)$ é nilpotente e é o único maior subgrupo normal nilpotente de G. E claramente $F(G)$ é um subgrupo característico de G.

Se considerarmos a interseção de todos os subgrupos maximais em G obtemos um importante subgrupo característico.

Definição 1.2.11. Seja G um grupo. O *subgrupo de Frattini* de G é definido por

$$\Phi(G) = \bigcap_{H\, max\, G} H.$$

Se G não possui subgrupos maximais, então $\Phi(G) = G$.

Seja G um grupo. Um elemento $g \in G$ é dito um *não-gerador* de G se sempre que $G = \langle X, g\rangle$, então $G = \langle X\rangle$, onde X é um subconjunto de G. Pode-se mostrar a seguinte caracterização para o subgrupo de Frattini de um dado grupo G.

$$\Phi(G) = \{g \in G \mid g \text{ é um não-gerador de } G\}.$$

Seja p um primo. Lembremos que um grupo G é dito ser um *p-grupo* se para todo g em G a ordem de g é uma potência de p. Se G é um grupo finito, então G é um p-grupo se, e somente se, $|G| = p^n$ para algum $n \in \mathbb{N}$.

O próximo resultado descreve em detalhe o subgrupo de Frattini de um p-grupo finito P e, como consequência, dá uma propriedade interessante sobre a cardinalidade dos conjuntos de geradores de P. Os detalhes da demonstração podem ser encontrados em [**21**, 5.3.2].

Teorema 1.2.12 (da Base de Burnside). *Seja G um p-grupo finito. Então, valem as seguintes afirmações.*
(i) $\Phi(G) = G'G^p$;
(ii) *Se $[G : \Phi(G)] = p^d$, então dado X um subconjunto de geradores de G existe Y subconjunto de X tal que $G = \langle Y \rangle$ e $|Y| = d$.*

Vamos lembrar a definição de outra classe importante de grupos.

Definição 1.2.13. Um grupo G é dito *solúvel* se possui uma série normal

$$1 = G_0 \leq G_1 \leq \cdots \leq G_r = G,$$

tal que cada quociente G_i/G_{i-1} é abeliano para cada $1 \leq i \leq r$.

Assim como fizemos em grupos nilpotentes, vamos também aqui definir algumas séries que nos ajudam a mostrar se um dado grupo G é solúvel.

Dado um grupo G, definamos os subgrupos $G^{(i)}$ recursivamente da seguinte forma: $G^{(0)} = G, G^{(1)} = G' = [G, G]$ e $G^{(i+1)} = [G^{(i)}, G^{(i)}]$ para $i \geqslant 1$. Assim, temos

$$G = G^{(0)} \geqslant G^{(1)} \geqslant \cdots$$

e esta sequência descendente de subgrupos é chamada *série derivada* de G. Note que os subgrupos $G^{(i)}$ são característicos em G.

Pode-se mostrar que um grupo G é solúvel se, e somente se, existe um inteiro $m \geqslant 1$ tal que $G^{(m)} = 1$. Além disso, subgrupos, quocientes e extensões de solúveis são também solúveis. Em particular, como produto de subgrupos normais solúveis é um subgrupo normal solúvel, para um grupo finito G podemos definir o *radical solúvel* de G, que será denotado por $R(G)$, como o único maior subgrupo normal solúvel de G. Obviamente por definição $R(G)$ é também característico em G.

Seja G um grupo solúvel. Sendo a série derivada de G a de comprimento menor entre as séries normais descendentes de G com fatores abelianos que alcançam 1, podemos definir o *menor* inteiro m tal que $G^{(m)} = 1$ como o *comprimento derivado* de G.

Dizemos que um grupo G é *metabeliano* se G é solúvel de comprimento derivado menor ou igual a 2. Assim, G é metabeliano se possui um subgrupo normal abeliano cujo quociente é abeliano.

Sabemos que todo grupo nilpotente é solúvel, mas a recíproca não vale em geral. O próximo teorema nos dá um interessante critério de solubilidade. Os detalhes da demonstração podem ser vistos em [**7**, Satz III.5.1].

Teorema 1.2.14 (de Schmidt). *Se todo subgrupo próprio de G é nilpotente, então G é solúvel.*

Do Teorema de Schmidt obtemos uma observação que será útil ao longo do nosso estudo.

Lema 1.2.15. *Seja G um grupo finito. Se G é não nilpotente, então G contém um subgrupo solúvel não nilpotente.*

Demonstração. A prova será feita por indução sobre a ordem de G. Se $|G| = 1$, então o resultado é óbvio. Suponhamos que $|G| > 1$ e que o resultado seja válido para qualquer grupo de ordem estritamente menor que a ordem de G. Se G é solúvel e não nilpotente, então o resultado segue considerando o próprio G. Agora, suponhamos que G seja não solúvel. Como, por hipótese, G é não nilpotente segue pelo Teorema 1.2.14 que existe um subgrupo próprio H de G que não é nilpotente. Assim, aplicando a hipótese de indução a H, temos que H contém um subgrupo solúvel não nilpotente e o resultado segue. □

Dado G um grupo, um subgrupo S de G é dito *subnormal* se existem subgrupos $\{H_i\}$ de G tais que

$$S = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_{r-1} \trianglelefteq H_r = G,$$

com $r < \infty$ e $H_i \trianglelefteq H_{i+1}$ para todo $i \geqslant 0$.

Falaremos agora de mais uma série relevante no estudo de grupos solúveis.

Seja G um grupo finito. Definamos os subgrupos $F_n(G)$ recursivamente da seguinte forma: $F_0(G) = 1$ e para cada $i \geqslant 1$, $F_i(G)$ é o único subgrupo normal em G tal que

$$F_i(G)/F_{i-1}(G) = F(G/F_{i-1}(G)).$$

Assim, temos

$$1 = F_0(G) \leq F_1(G) = F(G) \leq F_2(G) \leq \cdots$$

Esta sequência ascendente de subgrupos é chamada *série de Fitting* de G. Note que para qualquer grupo solúvel finito G, existe a série de Fitting e a série alcança todo o grupo G. De fato, pode-se mostrar que G é solúvel se, e somente se, existe um inteiro $n \geqslant 1$ tal que $F_n(G) = G$. Em geral, para um grupo finito não solúvel a série de Fitting se estabiliza no radical solúvel $R(G)$.

Dado G um grupo solúvel finito, mostra-se que a série de Fitting de G é a série de comprimento menor possível entre as séries subnormais ascendentes de G com fatores nilpotentes. Assim, podemos definir o conceito de *altura de Fitting* de G como o *menor* inteiro n tal que $F_n(G) = G$ e o denotamos por $h(G)$.

Vejamos um lema sobre a altura de Fitting que será usado posteriormente.

Lema 1.2.16. *Seja G um grupo solúvel finito não trivial. Então,*

$$h(G) = h(G/F(G)) + 1.$$

Demonstração. Seja $\overline{G} = G/F(G)$ e suponhamos que $h(\overline{G}) = n$. Assim, temos que a série de Fitting para $\overline{G}$ é dada por

$$1 = \overline{F_0}(\overline{G}) \leq \overline{F_1}(\overline{G}) \leq \cdots \leq \overline{F_n}(\overline{G}) = \overline{G}.$$

Para cada $0 \leq i \leq n$, seja $F_i(G)$ a imagem inversa de $\overline{F_i}(\overline{G})$ em G. Assim, temos a seguinte série para G

$$F(G) = F_0(G) \leq F_1(G) \leq \cdots \leq F_n(G) = G. \tag{1.2.3}$$

Como

$$\overline{F_i + 1}(\overline{G})/\overline{F_i}(\overline{G}) = F\left(\overline{G}/\overline{F_i}(\overline{G})\right),$$

segue pelo terceiro teorema do isomorfismo que

$$F_{i+1}(G)/F_i(G) = F\left(G/F_i(G)\right) \qquad \forall\ 0 \leq i \leq n-1.$$

e como $F(G)$ é nilpotente, temos que a série (1.2.3) torna-se

$$1 \leq F(G) \leq F_1(G) \leq \cdots \leq F_n(G) = G,$$

que é uma série de Fitting para G de comprimento $n+1$. Claramente, temos que $h(G) = n+1$, pois caso contrário poderíamos construir uma série de Fitting para $\overline{G}$ de altura menor do que n que é um absurdo, e assim o resultado segue. □

Notamos que o subgrupo de Fitting desenvolve um papel muito importante no estudo da estrutura de um grupo finito solúvel. Em particular, é importante lembrar que se G é um grupo solúvel finito, então $Z(F(G)) = C_G(F(G)) \leq F(G)$. Então, isto significa que podemos "representar" G módulo $Z(F(G))$ como um subgrupo de $Aut(F(G))$ e isso ajuda no estudo da estrutura de G (para mais detalhes sobre isto veja [**1**, Sections 4 and 31]).

Em geral, se G é um grupo finito não solúvel, o subgrupo de Fitting não possui a propriedade de ser auto-centralizante, portanto é preciso definir outro subgrupo característico de G que desenvolve um papel semelhante, o subgrupo de Fitting generalizado. Antes disso, vejamos algumas definições.

Um grupo finito G é dito ser *quase simples* se $G/Z(G)$ é simples e $G = G'$. Um subgrupo quase simples subnormal de G é chamado uma *componente* de G. Denotemos por $\mathrm{Comp}(G)$ o conjunto de todas as componentes de G e $E(G)$ o subgrupo gerado por $\mathrm{Comp}(G)$, isto é, $E(G) = \langle \mathrm{Comp}(G) \rangle$. Note que $E(G)$ é o produto das componentes de G e também é característico em G. Na literatura $E(G)$ é as vezes chamado "layer" de G. Um grupo G pode não possuir componentes, por exemplo, isto ocorre quando o mesmo é solúvel, então $E(G) = 1$.

Veremos no próximo resultado que as componentes de um grupo finito comutam. A demonstração deste fato pode ser encontrada em [**15**, Theorem 9.4].

Proposição 1.2.17. *Sejam G um grupo finito e H e K componentes distintas de G. Então, $[H, K] = 1$.*

Desta maneira segue da Proposição 1.2.17 que as componentes de um grupo finito normalizam-se e cada componente é normal em $E(G)$.

Agora, estamos prontos para definir o subgrupo de Fitting generalizado de um grupo finito G.

Definição 1.2.18. Seja G um grupo finito, o *subgrupo de Fitting generalizado* de G é definido por

$$F^*(G) = F(G)E(G).$$

Veremos em seguida, que o subgrupo de Fitting generalizado também possui a propriedade de ser auto-centralizante. A demonstração deste teorema pode ser vista em [**15**, Theorem 9.8 e Corollary 9.9].

Teorema 1.2.19. *Para qualquer grupo finito G, tem-se:*
(i) $C_G(F^*(G)) \subseteq F^*(G)$*;*
(ii) $F(G) \leq F^*(G)$ *e a igualdade vale se, e só se,* $C_G(F(G)) \leq F(G)$*.*

Assim, vemos que o fato de $F^*(G)$ ser auto-centralizante dá uma "representação" do grupo G módulo $Z(F^*(G))$ como um subgrupo de $Aut(F^*(G))$ e isso ajuda no estudo do grupo G (para mais detalhes sobre isto veja [**1**, Sections 4 and 31]).

Seja G um grupo. O *expoente* de G, que denotamos por $\exp(G)$, é o menor inteiro positivo m tal que $g^m = 1$ para todo $g \in G$. Então, para cada grupo finito G, temos por Lagrange, que $\exp(G)$ divide $|G|$, também para cada grupo G que possui expoente tem-se que a ordem de cada elemento divide $\exp(G)$.

Um fato conhecido relativo a altura de Fitting de um grupo solúvel é o seguinte:

Teorema 1.2.20. *Seja G um grupo solúvel finito de expoente n. Então $h(G)$ é limitada em termos de n.*

Este resultado é considerado um corolário do trabalho de P. Hall e G. Higman em [**5**].

Finalizamos esta seção lembrando um resultado central da teoria de Hall sobre grupos solúveis.

Sejam π um conjunto não vazio de primos e π' o seu complementar, isto é, $\pi' = \mathbb{P} \backslash \pi$, onde $\mathbb{P}$ é o conjunto de todos os primos. Dizemos que $m \in \mathbb{N}$ é um π-*número* se dado qualquer primo p que divide m temos que $p \in \pi$. Um elemento de um grupo é chamado um π-*elemento* se sua ordem é um π-número. Analagomente define-se π'-*número* e π'-*elemento.*

Definição 1.2.21. Sejam G um grupo finito e π um conjunto não vazio de primos.
(i) Um subgrupo H de G é dito um π-*subgrupo* de G se $|H|$ é um π-número.
(ii) Um subgrupo H de G é dito um π-*subgrupo de Hall* de G se $|H|$ é um π-número e $[G : H]$ é um π'-número.

O próximo teorema, devido a P. Hall, pode ser visto como uma generalização da teoria Sylow para grupos solúveis, onde ao invés de considerarmos subgrupos de Sylow consideramos π-subgrupos de Hall. A demonstração deste resultado pode ser encontrada em [**2**, Theorem 2.1].

Teorema 1.2.22 (P. Hall). *Seja G um grupo solúvel finito. Então, as seguintes afirmações valem:*
(i) *para todo π conjunto de primos, existe um π-subgrupo de Hall de G;*
(ii) *seja π um conjunto de primos fixado. Então, todos os π-subgrupos de Hall de G são conjugados;*
(iii) *se H é um π-subgrupo de G, para algum conjunto de primos π, então existe um π-subgrupo de Hall K de G tal que $H \leq K$.*

1.3. Ação de Grupos

Nesta seção falaremos de ações de grupos, em especial de ação coprima e ressaltaremos suas principais propriedades.

Sejam G um grupo e Ω um conjunto não vazio. Dizemos que G *age* sobre o conjunto Ω quando para cada par $(g, x) \in G \times \Omega$ existe um único elemento $x^g \in \Omega$ satisfazendo as seguintes condições:

(i) $x^1 = x \ \forall \ x \in \Omega$;
(ii) $x^{gh} = (x^g)^h \ \forall \ g, h \in G$ e $\forall \ x \in \Omega$.

Se um grupo G age sobre Ω, dizemos que Ω é um G-*espaço*. Para cada g em G definimos uma aplicação $\rho_g : \Omega \longrightarrow \Omega$ dada por $\rho_g(x) = x^g$. Mostra-se que ρ_g é um elemento do grupo $\mathrm{Sym}(\Omega)$ de permutações de Ω. Então, temos que a aplicação $\rho : G \longrightarrow \mathrm{Sym}(\Omega)$ que leva g em ρ_g, é bem definida e é um homomorfismo. Assim, $Ker\rho = C_G(\Omega)$ é o núcleo da ação de G sobre Ω. Se $Ker\rho = 1$, dizemos que a *ação é fiel* ou que G *age fielmente* sobre Ω. Neste caso, podemos pensar em G como isomorfo a um grupo de permutação de Ω.

Seja G um grupo e Ω um G-espaço. Para cada $x \in \Omega$, a *órbita de* x, que denotamos por $\mathcal{O}(x)$, é o subconjunto de Ω dado por

$$\mathcal{O}(x) = \{x^g \mid g \in G\}.$$

E o *estabilizador* de x, que denotamos por G_x, é o subgrupo de G definido por

$$G_x = \{g \in G \mid x^g = x\}.$$

O resultado a seguir relaciona a órbita de um elemento em Ω com o seu estabilizador. A prova deste resultado pode ser encontrada em [**16**, Theorem 4.9].

Teorema 1.3.1 (**Órbita-Estabilizador**). *Seja Ω um G-espaço e $x \in \Omega$. Então, $|\mathcal{O}(x)| = [G : G_x]$. Se além disso, G é finito temos que $|\mathcal{O}(x)|$ divide $|G|$.*

Vamos agora considerar a ação de um grupo H sobre outro grupo N. Este conceito será muito usado no decorrer desta dissertação.

Sejam H e N grupos, dizemos que H *age por automorfismos* sobre N se H age sobre N, como conjunto, e além disso para cada $h \in H$ a aplicação $\varphi_h : N \longrightarrow N$ dada por $n \longmapsto \varphi_h(n) := n^h$ é um automorfismo de N, ou seja, $\varphi_h(xy) = \varphi_h(x)\varphi_h(y)$ para todos x e y elementos de N. Assim, H age por automorfismos sobre N se N é um H-espaço e existe um homomorfismo $\psi : H \longrightarrow Aut(N)$. Observe que cada homomorfismo $\psi : H \longrightarrow Aut(N)$ define uma ação por automorfismos de H sobre N. Reciprocamente, uma ação por automorfismos de H sobre N determina um homomorfismo de H em $Aut(N)$.

Dado um grupo H que age por automorfismos sobre N, dizemos que a *ação é coprima* se $(|H|, |N|) = 1$.

Suponhamos que um grupo H age por automorfismos sobre um grupo N. Então, existe um homomorfismo $\varphi : H \longrightarrow Aut(N)$ definido por $h \longmapsto \varphi_h$. Assim, podemos sempre construir um grupo, unicamente determinado por H, N e o homomorfismo φ, que é o produto *semidireto* de H e N, que denotamos por $N \rtimes H$.

Notemos que o grupo $G = N \rtimes H$ possui um subgrupo N_0 normal isomorfo a N e um subgrupo H_0 isomorfo a H, tais que $G = N_0H_0$ e $N_0 \cap H_0 = 1$. Além disso, a ação por conjugação de $h_0 \in H_0$ sobre $n_0 \in N_0$ se identifica com a ação por automorfismos de $h \in H$ sobre $n \in N$, ou seja, temos que $n_0^{h_0} = \psi_0(\varphi_h(n)) = \psi_0(h^n)$, onde $\psi_0 : N \longrightarrow N_0$ é o isomorfismo que identifica N com N_0.

De modo particular, o grupo de automorfismos de um grupo G será considerado como um subgrupo do produto semidireto $G \rtimes Aut(G)$. Em geral, sempre que um grupo A age por automorfismos em um grupo G, consideraremos A como um subgrupo do produto semidireto $G \rtimes A$.

Dados G um grupo e $\varphi \in A$ que age por automorfismos sobre G, definimos o *subgrupo dos pontos fixos* de φ em G por

$$C_G(\varphi) = \{g \in G \mid g^\varphi = g\}.$$

Em particular, podemos ver o subgrupo comutador $[G, \varphi]$ da seguinte maneira $[G, \varphi] = \langle g^{-1}g^\varphi \mid g \in G\rangle$. Mais geralmente, temos que $[G, A]$ pode ser visto como $[G, A] = \langle [G, \varphi] \mid \varphi \in A\rangle$.

Sejam G um grupo e $\varphi \in A$. Dizemos que um subgrupo H de G é *φ-invariante* se $\varphi \in N_{G \rtimes A}(H)$, ou de modo equivalente se $[H, \varphi] \leq H$. Observe que se H é um subgrupo A-invariante de $G \rtimes A$, então $C_G(H)$ é A-invariante também. Em particular, se G é um grupo e $\varphi \in Aut(G)$, então, $C_G(\varphi^n)$ é um subgrupo φ-invariante. Pois, note que $C_G(\varphi^n) = C_G(\langle\varphi^n\rangle)$ e claramente $\langle\varphi^n\rangle$ é um subgrupo φ-invariante.

Sejam G um grupo, $\varphi \in Aut(G)$ e N um subgrupo normal e φ-invariante de G. Então, podemos considerar a aplicação $\overline{\varphi}$ do grupo quociente G/N, induzida por φ, definida por $(Ng)^{\overline{\varphi}} = Ng^\varphi$. Como N é φ-invariante, temos que $\overline{\varphi}$ está bem definida e claramente é um automorfismo de G/N, chamado de *automorfismo induzido* de G/N. Observemos que a ordem de $\overline{\varphi}$ divide a ordem de φ. É importante observar que em geral temos $C_G(\varphi)N/N \leq C_{G/N}(\overline{\varphi})$, mas nem sempre temos a igualdade, ou seja poderíamos ter que a imagem inversa de um ponto fixo de $\overline{\varphi}$ pode não ser um ponto fixo de φ. Vejamos agora um resultado muito útil que diz que isto nunca acontece se considerarmos uma ação coprima. A prova deste resultado pode ser vista em [**11**, Lemma 2.11].

Lema 1.3.2. *Sejam φ um automorfismo de ordem n de um grupo finito G e N um subgrupo normal φ-invariante de G tal que $(|N|, |\varphi|) = 1$. Então*

$$C_{G/N}(\overline{\varphi}) = C_G(\varphi)N/N.$$

Faremos um abuso de notação indicando $\overline{\varphi}$ por apenas φ.

O teorema a seguir, conhecido como Teorema de Maschke, será usado no próximo resultado. A sua demonstração pode ser encontrada em [**21**, 8.1.2 pág 216].

Teorema 1.3.3 (de Maschke). *Sejam G um grupo finito, F um corpo cuja característica não divide a ordem de G e V um FG-módulo. Se U é um FG-submódulo de V, então existe um FG-submódulo W de V tal que $V = U \oplus W$.*

Notamos que usando o Teorema de Maschke é possível provar o seguinte resultado.

Teorema 1.3.4. *Seja G um grupo finito que age por automorfismos sobre um grupo abeliano U tal que $(|G|, |U|) = 1$. Então cada somando direto G-invariante de U possui um complemento direto G-invariante, isto é, se $U = V \oplus T$, com V um subgrupo G-invariante, então existe um subgrupo G-invariante W de U tal que $U = V \oplus W$.*

Reunimos no enunciado a seguir, alguns resultados relativos a ação coprima que serão bastante utilizados ao longo desta dissertação.

Corolário 1.3.5. *Seja G um grupo finito e φ um automorfismo de G tal que $(|G|, |\varphi|) = 1$. Então, as seguintes afirmações valem:*
(i) *$G = C_G(\varphi)[G, \varphi]$;*
(ii) *$[G, \varphi] = [[G, \varphi], \varphi]$;*
(iii) *se G é abeliano, então (usando notação aditiva) temos que*

$$G = C_G(\varphi) \oplus [G, \varphi].$$

Demonstração. Vamos mostrar o item (i). Por hipótese, temos que φ age por automorfismos sobre G e esta ação é coprima. Agora, note que $g^{\varphi} = g[g, \varphi]$ para qualquer $g \in G$. Vejamos que φ age trivialmente sobre $G/[G, \varphi]$. De fato, fazendo $N = [G, \varphi]$, observe que N é um subgrupo normal φ-invariante de G. Assim, podemos considerar o automorfismo induzido de φ em G/N. Daí, usando que $g^{\varphi} = g[g, \varphi]$, temos $(gN)^{\varphi} = g^{\varphi}N = g[g, \varphi]N = gN$, para qualquer $g \in G$. Logo, φ age trivialmente sobre $G/[G, \varphi]$, como queríamos. Isto implica que $C_{G/N}(\varphi) = G/N$. Então, aplicando o Lema 1.3.2, obtemos que $G/N = C_G(\varphi)N/N$. Portanto, concluímos que $G = C_G(\varphi)[G, \varphi]$, como desejado.

Vejamos o item (ii). De fato, aplicando o item (i) deste corolário e usando propriedade de comutadores, obtemos

$$\begin{aligned} [G,\varphi] &= [C_G(\varphi)[G,\varphi],\varphi] = \langle [\alpha,\varphi] \mid \alpha \in C_G(\varphi)[G,\varphi]\rangle \\ &= \langle [a,\varphi]^b[b,\varphi] \mid a \in C_G(\varphi), b \in [G,\varphi]\rangle \end{aligned}$$

Como $[C_G(\varphi),\varphi] = 1$, segue que

$$[G,\varphi] \;=\; \langle [b,\varphi] \mid b \in [G,\varphi]\rangle = [[G,\varphi],\varphi],$$

como desejado.

Por fim, vejamos o item (iii). Vamos usar a notação aditiva. Sabendo que $C_G(\varphi)$ é φ-invariante e que G é um grupo abeliano, segue pelo Teorema 1.3.4 que existe um subgrupo U φ-invariante de G tal que $G = C_G(\varphi) \oplus U$. Assim, por U ser um complemento direto φ-invariante de $C_G(\varphi)$, temos que $C_U(\varphi) = 0$. Agora, aplicando o item (i) deste corolário, em U, obtemos que $U = [U,\varphi]$. Então, temos

$$[G,\varphi] = [C_G(\varphi) \oplus U,\varphi] = [C_G(\varphi),\varphi] \oplus [U,\varphi] = U.$$

Logo, concluímos que $G = C_G(\varphi) \oplus U = C_G(\varphi) \oplus [G,\varphi]$, como desejado. □

Concluímos esta seção dedicada a ação coprima com um resultado muito útil relativo a automorfismos coprimos e quociente de um grupo G pelo subgrupo de Frattini $\Phi(G)$.

Teorema 1.3.6. *Sejam G um grupo finito e α um automorfismo de G tal que a ordem de α é coprima com $|\Phi(G)|$. Se $g^\alpha\Phi(G) = g\Phi(G)$ para todo $g \in G$, ou seja, α age como o automorfismo idêntico em $G/\Phi(G)$, então $\alpha = 1$.*

A prova deste resultado pode ser encontrada em [**7**, Satz III.3.18].

2

Condições de Tipo-Engel

Neste capítulo definiremos os conceitos de grupo localmente nilpotente e grupo Engel. Veremos algumas propriedades relacionadas com condições de Engel e também vamos definir duas importantes famílias de subgrupos que serão fundamentais nesta dissertação.

Vamos primeiramente definir o conceito de grupo localmente nilpotente.

Definição 2.0.7. Um grupo G é dito *localmente nilpotente* se todo subgrupo finitamente gerado de G é nilpotente.

Pode-se mostrar que subgrupos e quocientes de um grupo localmente nilpotente são localmente nilpotente. Claramente todo grupo nilpotente é localmente nilpotente. Mas existem grupos localmente nilpotentes que não precisam ser nilpotentes como, por exemplo, o grupo diedral generalizado, isto é, $A \rtimes C_2$, onde A é o grupo abeliano $\mathbb{Z}_{2^\infty}$, ou seja, o 2-grupo de Prüfer, C_2 é um grupo cíclico de ordem 2 e o gerador de C_2 age sobre A levando qualquer elemento em seu inverso. Note que $G = \mathbb{Z}_{2^\infty} \rtimes C_2$ não é nilpotente, já que a classe de nilpotência dele coincidiria com o comprimento da série de Frattini de $\mathbb{Z}_{2^\infty}$, ou seja, a série descendente de $\mathbb{Z}_{2^\infty}$ definida a cada passo considerando o subgrupo de Frattini do termo anterior. Mas, claramente esta série não existe para $\mathbb{Z}_{2^\infty}$ uma vez que $\Phi(\mathbb{Z}_{2^\infty}) = \mathbb{Z}_{2^\infty}$. Por outro lado, observe que G é localmente nilpotente. De fato, temos que $\mathbb{Z}_{2^\infty}$ e C_2 são abelianos e qualquer subgrupo próprio de $\mathbb{Z}_{2^\infty}$ é finito. Além disso se K é um subgrupo de G tal que $K \nsubseteq \mathbb{Z}_{2^\infty}$, então K possui um elemento $g \notin \mathbb{Z}_{2^\infty}$. Portanto, temos que g é um elemento de ordem 2 e podemos pensar G como $\mathbb{Z}_{2^\infty} \rtimes \langle g \rangle$. Assim, $K = (\mathbb{Z}_{2^\infty} \cap K) \rtimes \langle g \rangle$, logo K é isomorfo ao grupo diedral generalizado construído a partir de $\mathbb{Z}_{2^\infty} \cap K$ e portanto é nilpotente.

A seguir vamos dar a definição de elemento Engel em um grupo G que generaliza o conceito de localmente nilpotente.

Definição 2.0.8. Seja G um grupo. Um elemento g em G é chamado *elemento Engel (à esquerda)* se para todo x em G existe um inteiro positivo $n = n(x, g)$, que depende possivelmente de x e g, tal que

$$[x, \underbrace{g, \ldots, g}_{n}] = 1.$$

De modo análogo podemos definir elemento Engel à direita. Nesta dissertação vamos considerar elementos Engel à esquerda em um grupo G e os chamaremos apenas de elementos Engel.

Vejamos agora uma versão quantitativa do conceito de elemento Engel que é a definição de elemento n-Engel.

Definição 2.0.9. Seja G um grupo. Um elemento g em G é chamado *elemento n-Engel (à esquerda)* se para todo x em G existe um inteiro positivo $n = n(g)$, o mesmo inteiro para todo $x \in G$, tal que

$$[x, \underbrace{g, \ldots, g}_{n}] = 1.$$

Novamente, de modo análogo podemos definir elemento n-Engel à direita. Nesta dissertação consideraremos elementos n-Engel à esquerda e os chamaremos apenas de elementos n-Engel.

A seguir vamos definir grupos onde todos os elementos são Engel e n-Engel.

Definição 2.0.10. Seja G um grupo.

(i) Dizemos que G é um grupo *Engel*, se todos os elementos de G são Engel.
(ii) G é dito um grupo *n-Engel* se todos os seus elementos são n-Engel para um mesmo inteiro n.

É fácil ver que grupos n-Engel implicam em grupos Engel.

A próxima proposição nos mostra que um grupo localmente nilpotente precisa ser Engel.

Proposição 2.0.11. *Se G é um grupo localmente nilpotente, então G é um grupo Engel.*

Demonstração. Dados x e g elementos de G, consideremos $N = \langle x, g \rangle$ o subgrupo gerado por esses elementos. Como G é localmente nilpotente segue que

N é nilpotente. Desta maneira, existe um inteiro $n = n(x, g)$, tal que $\gamma_{n+1}(N) = 1$. Em particular, temos que

$$[x, \underbrace{g, \ldots, g}_{n}] = 1. \tag{2.0.1}$$

Note que podemos repetir este argumento e obter (2.0.1) para qualquer par x e g de elementos de G. Portanto, concluímos que G é um grupo Engel. $\square$

Observemos que existem grupos Engel que não precisam ser localmente nilpotentes, como exemplo, podemos considerar os grupos descritos por Golod (veja [**8**, 18.3.2 Example]): para cada $d \geqslant 2$ existe um grupo G_d que é d-gerado e não nilpotente tal que todos os seus subgrupos $(d-1)$-gerados são nilpotentes. Notamos além disso, que cada um desses grupos é um p-grupo infinito e residualmente finito (para a definição de grupo residualmente finito veja Cap. 4, Seção 5).

Em contraposição com isto veremos que para grupos profinitos, que serão introduzidos no Capítulo 4, vale um resultado importante que dá equivalência entre as duas propriedades de ser localmente nilpotente e de ser grupo Engel.

O teorema a seguir, devido a Zorn, caracteriza grupos finitos que são Engel. A demonstração deste resultado pode ser encontrada em [**21**, 12.3.4].

Teorema 2.0.12 (de Zorn). *Um grupo finito Engel é nilpotente.*

Veremos que um dos resultados principais de [**13**], analisados nesta dissertação, pode ser considerado uma generalização do Teorema de Zorn.

O próximo resultado, devido a Baer, nos dá uma importante informação sobre os elementos Engel de um grupo finito. Os detalhes da prova podem ser vistos em [**7**, Satz III.6.15].

Teorema 2.0.13 (de Baer). *Seja G um grupo finito. Se x é um elemento Engel de G, então x pertence ao subgrupo de Fitting de G.*

Em [**14**] E. I. Khukhro e P. Shumyatsky introduziram a seguinte família de subgrupos para obter generalizações do Teorema de Baer.

Definição 2.0.14. Sejam G um grupo e g um elemento de G. Para um inteiro positivo n definimos o subgrupo $E_n(g)$ de G por

$$E_n(g) = \langle [x, \underbrace{g, \ldots, g}_{n}] \mid x \in G \rangle,$$

ou seja, o subgrupo gerado por todos os comutadores da forma $[x, \underbrace{g, \ldots, g}_{n}]$, onde x varia em G e o g fixado é repetido n vezes.

Obviamente, pelo Teorema de Baer, se $g \in G$ é tal que $E_n(g) = 1$, então g pertence ao subgrupo de Fitting de G.

Notemos que o subgrupo $E_n(g)$ não é um subgrupo subnormal de G. O interessante é que estes subgrupos são úteis para "medir" quanto um determinado elemento g esteja longe de ser n-Engel no grupo.

Para o caso particular de um grupo finito, os mesmos autores também introduziram a seguinte definição.

Definição 2.0.15. Sejam G um grupo finito e g um elemento de G, definimos o subgrupo $E(g)$ de G como

$$E(g) = \bigcap_{n=1}^{\infty} E_n(g).$$

Vejamos a seguir alguns fatos relacionados a esses subgrupos e que serão amplamente utilizados ao longo desta dissertação.

Antes disso, lembremos que uma *seção* de um grupo G é um grupo quociente M/N tal que M e N são subgrupos arbitrários de G com a propriedade que $N \trianglelefteq M$. Uma seção de G é dita *normal* se ambos os subgrupos M e N são normais em G.

Proposição 2.0.16. *Sejam G um grupo e g um elemento de G. As seguintes afirmações valem:*
(i) *seja N um subgrupo normal de G. Então, $\overline{E_n(g)} = E_n(\overline{g})$, onde as barras representam as imagens no quociente G/N;*
(ii) *sejam $H \leq G$ e $g \in H$. Então para todo inteiro positivo n, temos que o subgrupo $E_n(g)$ construído com respeito a H está contido no subgrupo $E_n(g)$ construído com respeito a G;*
(iii) *seja G um grupo finito e suponha que exista um inteiro positivo m tal que $|E(g)| \leq m$ para todo g em G. Então, temos que esta condição é herdada por qualquer seção de G;*
(iv) *seja G um grupo e suponha que para todo g em G exista um inteiro positivo $n = n(g)$ tal que $E_n(g)$ é finito. Então, temos que esta condição é também válida para qualquer seção de G.*

Demonstração. Vamos mostrar o item (i). Consideremos o epimorfismo canônico de G em G/N. Vejamos que $\overline{E_n(g)} = E_n(\overline{g})$. De fato, seja $u \in \overline{E_n(g)}$, então $u = aN$ para algum $a \in E_n(g)$. Daí, temos que

$$a = [x_1, \underbrace{g, \ldots, g}_{n}]^{\varepsilon_1} \cdots [x_m, \underbrace{g, \ldots, g}_{n}]^{\varepsilon_m},$$

com $x_i \in G$ e $\varepsilon_i = \{\pm 1\}$. Então, substituindo tem-se

$$u = [x_1, \underbrace{g, \dots, g}_{n}]^{\varepsilon_1} N \cdots [x_m, \underbrace{g, \dots, g}_{n}]^{\varepsilon_m} N,$$

e portanto, segue que $u \in E_n(\overline{g})$. Por outro lado, seja $u \in E_n(\overline{g})$, então temos que

$$\begin{aligned} u &= [\overline{x_1}, \underbrace{\overline{g}, \dots, \overline{g}}_{n}]^{\varepsilon_1} \cdots [\overline{x_m}, \underbrace{\overline{g}, \dots, \overline{g}}_{n}]^{\varepsilon_m} \\ &= ([x_1, \underbrace{g, \dots, g}_{n}]^{\varepsilon_1} \cdots [x_m, \underbrace{g, \dots, g}_{n}]^{\varepsilon_m})N \end{aligned}$$

onde cada $x_i \in G$ e $\varepsilon_i = \{\pm 1\}$. Assim, fazendo

$$a = [x_1, \underbrace{g, \dots, g}_{n}]^{\varepsilon_1} \cdots [x_m, \underbrace{g, \dots, g}_{n}]^{\varepsilon_m},$$

obtemos que $a \in E_n(g)$. Logo, $u = aN$ e assim $u \in \overline{E_n(g)}$. Portanto, segue que $\overline{E_n(g)} = E_n(\overline{g})$, como queríamos.

Para cada inteiro n, denotemos por $E_{n,H}(g) = \langle [x, \underbrace{g, \dots, g}_{n}] \mid x \in H \rangle$ o subgrupo construído para H e $E_{n,G}(g) = \langle [u, \underbrace{g, \dots, g}_{n}] \mid u \in G \rangle$ o subgrupo construído para G. Dado $a = [x, \underbrace{g, \dots, g}_{n}]$ um qualquer gerador de $E_{n,H}(g)$, como $x \in H$ é um elemento de G, obviamente a é também um gerador de $E_{n,G}(g)$. E isto implica que $E_{n,H}(g) \leq E_{n,G}(g)$, provando o item (ii).

Mostraremos o item (iii). Seja $\overline{M} = M/N$, onde $N \trianglelefteq M \leq G$, uma qualquer seção de G e denotemos por $E_{\overline{M}}(\overline{g}) = \bigcap_{n=1}^{\infty} E_{n,\overline{M}}(\overline{g})$. Vamos mostrar que $|E_{\overline{M}}(\overline{g})| \leq m$ para todo $\overline{g} \in \overline{M}$. De fato, por hipótese temos que $|E(g)| \leq m$ para todo $g \in G$. Como $M \leq G$, segue em particular, que $|E(g)| \leq m$ para todo $g \in M$. Por outro lado, para todo $g \in M$ temos, pelo item (ii) desta proposição, que $E_{n,M}(g) \leq E_{n,G}(g)$ para todo n. Disto segue que $\bigcap_{n=1}^{\infty} E_{n,M}(g) \leq \bigcap_{n=1}^{\infty} E_{n,G}(g)$. Logo, obtemos que $E_M(g) \leq E(g)$, onde $E_M(g) = \bigcap_{n=1}^{\infty} E_{n,M}(g)$. Portanto, segue que $|E_M(g)| \leq |E(g)| \leq m$, para todo $g \in M$. Agora, vejamos que $|E_{\overline{M}}(\overline{g})| \leq m$ para todo $\overline{g} \in \overline{M}$. Consideremos o epimorfismo canônico de M em $\overline{M}$. Note primeiramente que para todo $g \in M$ temos $\overline{E_M(g)} = E_{\overline{M}}(\overline{g})$. Com efeito, usando o item (i) desta proposição, obtemos

$$E_{\overline{M}}(\overline{g}) = \bigcap_{n=1}^{\infty} E_{n,\overline{M}}(\overline{g}) = \bigcap_{n=1}^{\infty} \overline{E_{n,M}(g)} = \overline{\left(\bigcap_{n=1}^{\infty} E_{n,M}(g) \right)} = \overline{E_M(g)}.$$

Observe que a terceira igualdade vale, pela definição dos subgrupos $E_n(g)$ e pelo fato do grupo ser finito.

Portanto, $\overline{E_M(g)} = E_{\overline{M}}(\overline{g})$. Agora, pelo segundo teorema do isomorfismo, tem-se

$$\overline{E_M(g)} = \frac{E_M(g)N}{N} \cong \frac{E_M(g)}{E_M(g) \cap N}.$$

Assim, por Lagrange segue que $|\overline{E_M(g)}|$ divide $|E_M(g)|$. O que implica em $|\overline{E_M(g)}| \leq |E_M(g)|$. Então, tem-se $|E_{\overline{M}}(\overline{g})| \leq m$, para todo $\overline{g} \in \overline{M}$, como queríamos.

Seja agora $H \leq G$, então pelo item (ii) desta proposição, temos que $E_{n,H}(g)$ é finito para todo $g \in H$. Vejamos que $E_n(\overline{g})$ é finito para todo $\overline{g} \in H/K$ onde H e K são subgrupos quaisquer de G e $K \trianglelefteq H$. Com efeito, consideremos o epimorfismo canônico de H em H/K. Pelo item (ii) desta proposição, tem-se $\overline{E_{n,H}(g)} = E_{n,\overline{H}}(\overline{g})$. Desta maneira, usando o segundo teorema do isomorfismo obtemos

$$\overline{E_{n,H}(g)} = E_{n,H}(g)K/K \cong E_{n,H}(g)/(K \cap E_{n,H}(g)).$$

Assim, uma vez que $E_{n,H}(g)$ é finito, segue que $\overline{E_{n,H}(g)}$ é finito e portanto tem-se que $E_{n,\overline{H}}(\overline{g})$ é finito, para todo $\overline{g} \in H/K$. Isto prova o item (iv) e conclui a prova. $\square$

3

Grupos Finitos Quase Engel

Neste capítulo vamos demonstrar o Teorema B, o resultado principal, do artigo de E. I. Khukhro e P. Shumyatsky [**13**], relacionado a grupos finitos. Para isto, na primeira seção apresentamos alguns resultados preparatórios que nos servirão de base para a demonstração do mesmo e na segunda seção veremos os detalhes da prova do Teorema B.

3.1. Resultados Preparatórios

O lema a seguir nos fornece informações sobre o residual nilpotente de um grupo finito com altura de Fitting igual a 2.

Lema 3.1.1. [**12**, Lemma 10] *Se G é um grupo finito com altura de Fitting $h(G) = 2$, então temos que*

$$\gamma_\infty(G) = \prod_q [F_q, G_{q'}], \tag{3.1.1}$$

onde F_q é o q-subgrupo de Sylow de $F(G)$ e $G_{q'}$ é um q'-subgrupo de Hall de G.

Demonstração. Como G possui altura de Fitting 2, temos que G é solúvel. Logo, segue que os subgrupos comutadores $[F_q, G_{q'}]$ não dependem da escolha do q'-subgrupo de Hall, pois pelo Teorema 1.2.22 item (ii), temos que os q'-subgrupos de Hall de G são conjugados. Assim, o produto em (3.1.1) está bem definido. Note que $[F_q, G_{q'}]$ é normal em G para todo primo q e disto segue que $\prod_q [F_q, G_{q'}]$ também é normal em G.

Sejam q um primo qualquer e G_q um q-subgrupo de Sylow de G. Observemos que $G = G_{q'}G_q$. Pois, como $G_{q'}$ é um q'-subgrupo de Hall de G temos que o índice $[G : G_{q'}]$ é uma potência de q e sendo G_q um q-subgrupo de Sylow de G, segue que $([G : G_{q'}], [G : G_q]) = 1$. Assim, como G é finito, concluímos que

$G = G_{q'}G_q$. Agora, consideremos o epimorfismo canônico de G em $G/[F_q, G_{q'}]$. Vejamos que o grupo $G/[F_q, G_{q'}]$ age sobre F_q como a imagem de G_q no quociente. Com efeito, uma vez que estamos considerando o quociente $G/[F_q, G_{q'}]$, podemos assumir que $[F_q, G_{q'}] = 1$. Desta maneira, segue que $G_{q'}$ age trivialmente sobre F_q. Assim, usando o fato que $G = G_{q'}G_q$ temos o que queremos. Disto resulta que o grupo $G/\prod_q[F_q, G_{q'}]$ é nilpotente. Agora, aplicando o Lema 1.2.6, concluímos que $\gamma_\infty(G) \leq \prod_q[F_q, G_{q'}]$.

Por outro lado, como a ação de $G_{q'}$ sobre F_q é coprima, segue do Corolário 1.3.5 item (ii), que $[F_q, G_{q'}] = [[F_q, G_{q'}], G_{q'}]$. Agora, usando esta observação e argumentando por indução sobre $i \geqslant 1$, é fácil mostrar que $[F_q, G_{q'}] \leq \gamma_i(G)$. Consequentemente, temos $[F_q, G_{q'}] \leq \gamma_\infty(G)$, para todo q. Isto implica que $\prod_q[F_q, G_{q'}] \leq \gamma_\infty(G)$. Portanto, concluímos que a igualdade em (3.1.1) vale, como queríamos. $\square$

Vejamos agora como se relaciona o subgrupo $E(g)$ com alguns particulares subgrupos comutadores.

Lema 3.1.2. *Se P é um p-subgrupo finito de um grupo G e g é um p'-elemento de G que normaliza P, então $[P, g] \leq E(g)$.*

Demonstração. O Teorema 1.2.12 implica que $V = [P, g]/\Phi([P, g])$ é um p-grupo abeliano elementar finito. Observe que $\langle g \rangle$ age sobre V e esta ação é coprima. Agora, vejamos que $V = [V, g]$. Com efeito, claramente tem-se que $[V, g] \leq V$. Por um lado, seja $v \in V$, então $v = uN$ com $u \in [P, g]$. Como a ação é coprima, tem-se pelo Corolário 1.3.5 item (ii) que $[P, g] = [P, g, g]$ e isto implica que $V = [V, g]$. Por outro lado, como V é abeliano segue pelo Corolário 1.3.5 item (iii) que $V = C_V(g) \oplus [V, g]$, mas sabendo que $V = [V, g]$ concluímos que $C_V(g) = 1$.

Agora, vamos verificar que $V = \{[v, g] \mid v \in V\}$. Com efeito, claramente $\{[v, g] \mid v \in V\} \leq V$. Por outro lado, seja $v \in V = [V, g]$, então

$$v = [v_1, g]^{\varepsilon_1} \cdots [v_n, g]^{\varepsilon_n},$$

onde $v_i \in V$ e $\varepsilon_i = \{\pm 1\}$. Uma vez que V é abeliano e usando as propriedades de comutadores listadas na Proposição 1.1.1 podemos escrever $v = [w, g]$ para algum $w \in V$, logo tem-se $v \in [V, g]$. Portanto, $V = \{[v, g] \mid v \in V\}$, como desejado. Disto segue, usando várias vezes a mesma observação que

$$V = \{[v, \underbrace{g, \ldots, g}_{n}] \mid v \in V\},$$

para qualquer n. Desta maneira, concluímos que $V \leq E_n(g)$ para todo n, e em particular que $V \leq E(g)$. Daí, para todo $v \in V$, temos que $v = x\Phi([P,g])$ com $x \in [P,g]$, mas v é também um elemento de $E(g)$. Isto implica $x \in E(g)\Phi([P,g])$. Portanto, concluímos que $[P,g] \leq E(g)\Phi([P,g])$. E consequentemente, lembrando que $\Phi([P,g])$ consiste de todos os não geradores de $[P,g]$, obtemos $[P,g] \leq E(g)$, como queríamos. $\square$

Antes de apresentarmos o próximo lema, precisamos introduzir um conceito que será utilizado ao longo desta dissertação.

Dados a e b parâmetros. Dizemos que um número k é *(a,b)-limitado* se k é limitado superiormente por uma função que depende apenas de a e b.

Lema 3.1.3. *Sejam V um q-grupo abeliano elementar e U um q'-grupo de automorfismos de V. Se $|[V,u]| \leq m$ para cada $u \in U$, então $|[V,U]|$ é m-limitada, e portanto $|U|$ é também m-limitada.*

DEMONSTRAÇÃO. Suponhamos primeiramente que U seja abeliano. Consideremos V como um $\mathbb{F}_qU$-módulo, pois V é um q-grupo abeliano elementar e U age por automorfismos sobre V. Observe que a ação de U sobre V é coprima. Escolhamos $u_1 \in U$ tal que $[V,u_1] \neq 0$. Uma vez que V é um grupo abeliano, segue pelo Corolário 1.3.5 item (iii), que $V = [V,u_1] \oplus C_V(u_1)$, onde $[V,u_1]$ e $C_V(u_1)$ são $\langle u_1\rangle$-invariantes. Agora, como que U é abeliano obtemos que $[V,u_1]$ e $C_V(u_1)$ são U-invariantes. Notamos que se $C_U([V,u_1]) = 1$, então sendo $N_U([V,u_1]) = U$ e usando o Lema 1.1.5, deduzimos que U é isomorfo a um subgrupo de $Aut([V,u_1])$. Desde que $|[V,u_1]| \leq m$ segue que $|Aut([V,u_1])|$ é m-limitada. Portanto, $|U|$ também é m-limitada e consequentemente temos que $[V,U]$ possui ordem m-limitada, uma vez que, por hipótese, $|[V,u]| \leq m$ para cada $u \in U$ e temos uma quantidade de fatores $|U|$ que é m-limitada. Caso contrário, existe $u_2 \in C_U([V,u_1])$ com $u_2 \neq 1$. Então, podemos aplicar novamente o mesmo raciocínio e temos que $V = [V,u_1] \oplus [V,u_2] \oplus C_V(\langle u_1,u_2\rangle)$. Por um lado lembremos que $V = [V,u_1] \oplus C_V(u_1)$. Por outro lado, note que $C_V(u_1)$ é $\langle u_2\rangle$-invariante. Assim, podemos considerar que $\langle u_2\rangle$ age por automorfismos sobre $C_V(u_1)$ e esta ação é coprima. Assim, tem-se pelo Corolário 1.3.5 item (iii) que $C_V(u_1) = [C_V(u_1),u_2] \oplus C_{C_V(u_1)}(u_2)$, onde $[C_V(u_1),u_2]$ e $C_{C_V(u_1)}(u_2)$ são $\langle u_2\rangle$-invariantes. Desta maneira obtemos

$$V = [V,u_1] \oplus [C_V(u_1),u_2] \oplus C_{C_V(u_1)}(u_2).$$

Agora, observemos que $[C_V(u_1), u_2] = [V, u_2]$. De fato, como $u_2 \in C_U([V, u_1])$, temos que $[V, u_1] \leq C_V(u_2)$. Então, disto segue que

$$[V, u_2] = [[V, u_1], u_2] \oplus [C_V(u_1), u_2] = [C_V(u_1), u_2].$$

Então, usando as definições podemos concluir que $C_{C_V(u_1)}(u_2) = C_V(\langle u_1, u_2\rangle)$. Portanto, tem-se

$$V = [V, u_1] \oplus [V, u_2] \oplus C_V(\langle u_1, u_2\rangle).$$

De novo se $C_U([V, u_1] \oplus [V, u_2]) = 1$, então da mesma forma como fizemos anteriormente, concluímos que $|U|$ é m-limitada e assim, $|[V, U]|$ também é m-limitada. Caso contrário, existe $u_3 \in C_U([V, u_1] \oplus [V, u_2])$ com $u_3 \neq 1$. E de modo semelhante ao que fizemos anteriormente, temos

$$V = [V, u_1] \oplus [V, u_2] \oplus [V, u_3] \oplus C_V(\langle u_1, u_2, u_3\rangle).$$

E assim, por diante. Se $C_U([V, u_1] \oplus \cdots \oplus [V, u_k]) = 1$ depois de um número k de passos, para algum inteiro k m-limitado, tem-se $|Aut([V, u_1] \oplus \cdots \oplus [V, u_k])|$ é m-limitada e usando o Lema 1.1.5 vamos concluir novamente que $|U|$ também é m-limitada. Caso contrário, se tivéssemos um número de passos não limitado em termos de m então considerando o elemento $w = u_1u_2\cdots u_k$ teríamos que $[[V, u_i], w] = [V, u_i] \neq 0$. Disto segue que $[V, w] = [V, u_1] \oplus \cdots \oplus [V, u_k]$ teria ordem maior que m, uma vez que k não é m-limitado, mas isto é um absurdo, pois por hipótese, $|[V, u]| \leq m$ para todo $u \in U$. Portanto o resultado vale no caso em que U é abeliano.

Vamos considerar o caso geral. Como cada elemento $u \in U$ age fielmente sobre $[V, u]$, temos que o expoente de U é m-limitado. Se P é um p-subgrupo de U, consideremos M um subgrupo normal abeliano maximal de P. Por M ser abeliano temos pelo caso abeliano que $|[V, M]|$ é m-limitada, então obtemos que $|Aut([V, M])|$ também é m-limitada. Agora, desde que M age fielmente sobre $[V, M]$, do Lema 1.1.5 segue que M é isomorfo a um subgrupo de $Aut([V, M])$. Daí, resulta que $|M|$ é m-limitada. Por como M foi definido, temos que $C_P(M) = M$ e como $N_P(M) = P$, novamente pelo Lema 1.1.5 temos que P/M é isomorfo a um subgrupo de $Aut(M)$. Disto resulta que $|P/M|$ é m-limitada e sabendo que $|M|$ é m-limitada, obtemos que $|P|$ também é m-limitada. Por outro lado, como $|U|$ possui somente uma quantidade m-limitada de divisores primos, obtemos que $|U|$ é m-limitada. Assim, como $[V, U] = \sum_{u \in U}[V, u]$ e sabendo que, por hipótese, cada $|[V, u]| \leq m$ para todo $u \in U$ e que $|U|$ é m-limitada, concluímos que $|[V, U]|$ é também m-limitada. Desta maneira, o resultado segue. $\square$

O próximo resultado será uma informação muito relevante ao longo da demonstração do Teorema B (veja Teorema 3.2.1).

Lema 3.1.4. *Se G é um grupo finito tal que $|E(g)| \leq m$ para todo $g \in G$, então $G/F(G)$ possui expoente m-limitado.*

DEMONSTRAÇÃO. Observemos primeiramente que para cada g em G, o subgrupo $E(g^k)$ é g-invariante para qualquer inteiro positivo k. Para isto, vejamos que $(E(g^k))^g \leq E(g^k)$. De fato, sejam k um qualquer inteiro positivo e $a^g \in (E(g^k))^g$, com $a \in E(g^k)$. Assim, $a \in E_n(g^k)$ para todo $n \geqslant 1$. Daí, temos para todo $n \geqslant 1$

$$a = [x_1, \underbrace{g^k, \ldots, g^k}_{n}]^{\varepsilon_1} \cdots [x_l, \underbrace{g^k, \ldots, g^k}_{n}]^{\varepsilon_l},$$

com $x_i \in G$ e $\varepsilon_i = \{\pm 1\}$. Então, conjugando a por g obtemos

$$a^g \quad = \quad [y_1, \underbrace{g^k, \ldots, g^k}_{n}]^{\varepsilon_1} \cdots [y_l, \underbrace{g^k, \ldots, g^k}_{n}]^{\varepsilon_l},$$

onde $y_i \in G$ e $\varepsilon_i = \{\pm 1\}$. Logo, $a^g \in E_n(g^k)$ para todo $n \geqslant 1$. Portanto, $a^g \in E(g^k)$ e afirmação segue. Consideremos o conjunto U de todos os grupos de ordem no máximo m. Observemos que U é não vazio, pois por hipótese, $E(g)$ está em U, para todo $g \in G$. Denotamos $k = max\{\exp(Aut(H)) \mid H \in U\}$. Note que se $H \in U$ então $|H| \leq m$, portanto $|Aut(H)|$ é m-limitada e logo $\exp(Aut(H))$ é m-limitado. Consequentemente, k é também m-limitado. Então como $E(g^k) \in U$, temos que $\exp(Aut(E(g^k))) \leq k$ e isso implica que g^k age trivialmente sobre $E(g^k)$. Assim, concluímos que $[E(g^k), g^k] = 1$. Em particular, temos que g^k é um elemento Engel de G. Pois, por G ser finito, temos que existe um inteiro n suficientemente grande tal que $E(g^k) = E_n(g^k)$. Agora, considerando um gerador qualquer de $E(g^k)$, isto é, um elemento da forma $[x, \underbrace{g^k \cdots g^k}_{n}]$, com x um elemento qualquer de G e lembrando que $[E(g^k), g^k] = 1$ obtemos

$$[[x, \underbrace{g^k \cdots g^k}_{n}], g^k] = [x, \underbrace{g^k \cdots g^k}_{n+1}] = 1.$$

Desta maneira, concluímos que g^k é um elemento Engel de G. Portanto, do Teorema 2.0.13 segue que $g^k \in F(G)$. Uma vez que g foi tomado arbitrariamente, obtemos para todo g em G que $g^k \in F(G)$, para o mesmo k, que lembramos ser um inteiro m-limitado. Daí tem-se que a ordem de qualquer elemento de $G/F(G)$ é m-limitada. Consequentemente, temos que o $\exp(G/F(G))$ também é m-limitado, como desejado. $\square$

Concluímos esta seção observando que um fato bem conhecido, consequência da classificação dos grupos finitos simples (veja [**3**]), é o seguinte:

Teorema 3.1.5. *Seja n um inteiro positivo. Então, existe só um número finito de grupos simples com expoente n.*

3.2. Resultado Principal Para Grupos Finitos

A partir dos resultados obtidos na seção anterior, estamos em condições de demonstrar o teorema principal deste capítulo.

Teorema 3.2.1. *Suponha que G seja um grupo finito e existe um inteiro positivo m tal que $|E(g)| \leq m$ para todo $g \in G$. Então a ordem do subgrupo residual nilpotente $\gamma_\infty(G)$ é limitada em termos de m.*

Vamos provar o resultado acima mostrando que $|\gamma_\infty(G)|$ é m-limitada e para isto, sendo o argumento bastante técnico, dividiremos a prova em dois casos: primeiro veremos que o resultado vale quando G é solúvel e logo consideremos o caso geral.

Afirmação 1. *O Teorema 3.2.1 vale com a hipótese ulterior que G seja um grupo solúvel.*

Demonstração. Por hipótese G é um grupo finito tal que $|E(g)| \leq m$ para todo $g \in G$, então temos pelo Lema 3.1.4 que $G/F(G)$ possui expoente m-limitado. Como G é solúvel finito, pelo Teorema 1.2.20, segue que a altura de Fitting de $G/F(G)$ é m-limitada. Uma vez que $F(G)$ é nilpotente, tem-se que $h(F(G)) = 1$ e sabendo que $h(G/F(G))$ é m-limitada, concluímos pelo Lema 1.2.16, que $h(G)$ é m-limitada.

Assim, podemos argumentar por indução sobre $h(G)$. Desta maneira, se $h(G) = 1$, então $F(G) = G$. Logo, G é nilpotente, aplicando o Lema 1.2.7 tem-se que $\gamma_\infty(G) = 1$ e o resultado é óbvio. Suponhamos agora que $h(G) \geqslant 2$ e consideremos o segundo subgrupo de Fitting $F_2(G)$. Observe que $h(F_2(G)) = 2$. Assim, aplicando o Lema 3.1.1 em $F_2(G)$ e notando que $F(F_2(G)) = F(G)$, obtemos que $\gamma_\infty(F_2(G)) = \prod_q [F_q, H_{q'}]$, onde F_q é um q-subgrupo de Sylow de $F(G)$, $H_{q'}$ é um q'-subgrupo de Hall de $F_2(G)$, e o produto é feito sobre os primos q divisores de $|F(G)|$. Dado um primo q, consideremos $\overline{H}_{q'} = H_{q'}/C_{H_{q'}}(F_q)$ e $V = F_q/\Phi(F_q)$. Note que $\overline{H}_{q'}$ é um q'-grupo e V é um q-grupo abeliano elementar. Assim, pelo Lema 1.1.5, $\overline{H}_{q'}$ é isomorfo a um subgrupo de $Aut(F_q)$. Então, temos que $\overline{H}_{q'}$ age por automorfismos sobre F_q e pelo fato desta ação ser coprima, segue do Teorema 1.3.6 que $\overline{H}_{q'}$ age fielmente sobre V.

Vamos mostrar a seguir que a ordem de $\gamma_\infty(F_2(G))$ é m-limitada. Para isto, vejamos primeiramente que, para cada $x \in \overline{H}_{q'}$, temos que $|[V,x]| \leq m$. Pois, como $x \in \overline{H}_{q'}$ e este por sua vez é uma seção de G, tem-se pela Proposição 2.0.16 item (iii) que $|E(x)| \leq m$ para todo $x \in \overline{H}_{q'}$. Agora, como V é um q-grupo finito e $x \in \overline{H}_{q'}$ é um q'-elemento, então pelo Lema 3.1.2 segue que $[V,x] \leq E(x)$. Portanto, $|[V,x]| \leq m$ para cada $x \in \overline{H}_{q'}$. Assim, aplicando o Lema 3.1.3, obtemos que a ordem de $\overline{H}_{q'}$ é m-limitada. Observe que $|[F_q,H_{q'}]| = |[F_q,\overline{H}_{q'}]|$. Agora mostraremos que $|[F_q,H_{q'}]| = |[F_q,\overline{H}_{q'}]|$ é m-limitada. Com efeito, por um lado, como $|\overline{H}_{q'}|$ é m-limitada, temos que $[F_q,\overline{H}_{q'}]$ é o produto de uma quantidade m-limitada de subgrupos da forma $[F_q,\overline{h}]$, com $h \in H_{q'}$. Por outro lado, usando o Lema 3.1.2, agora com F_q e $h \in H_{q'}$, tem-se que $[F_q,h] \leq E(h)$ para cada $h \in H_{q'}$. Logo, $|[F_q,h]| \leq m$ para todo $h \in H_{q'}$. Por isso, concluímos que $|[F_q,H_{q'}]|$ é m-limitada.

Desde que $|[F_q,H_{q'}]|$ é m-limitada para qualquer primo q, obtemos que os primos q, para os quais $[F_q,H_{q'}] \neq 1$, são menores do que ou iguais a m. Assim, como $|[F_q,H_{q'}]|$ é m-limitada para cada primo q e os primos q para os quais $[F_q,H_{q'}] \neq 1$ são também m-limitados, concluímos que $|\gamma_\infty(F_2(G))| = |\prod_q [F_q,H_{q'}]|$ é m-limitada.

Agora, consideremos $\overline{G} = G/\gamma_\infty(F_2(G))$, sendo uma seção de G, segue da Proposição 2.0.16 item (iii) que $|E(\overline{g})| \leq m$ para todo $\overline{g} \in \overline{G}$. E observe que $h(\overline{G}) < h(G)$. Assim, aplicando a hipótese de indução em $\overline{G}$, obtemos que a ordem de $\gamma_\infty(\overline{G})$ é m-limitada. Assim, usando (1.2.2) temos que

$$\gamma_\infty(\overline{G}) = \frac{\gamma_\infty(G)\gamma_\infty(F_2(G))}{\gamma_\infty(F_2(G))} = \frac{\gamma_\infty(G)}{\gamma_\infty(F_2(G))}.$$

Combinando este fato com o fato que $|\gamma_\infty(F_2(G))|$ é m-limitada, concluímos que $|\gamma_\infty(G)|$ é m-limitada, como queríamos. □

Agora, vejamos os detalhes da demonstração do caso geral do Teorema 3.2.1. Veremos como o caso solúvel mostrado antes desenvolverá um papel importante dentro da prova do caso geral.

Afirmação 2. *O Teorema 3.2.1 vale com G um grupo qualquer.*

Demonstração. Primeiro mostraremos que

$$G/R(G) \text{ possui ordem } m\text{-limitada},$$

onde $R(G)$ é o radical solúvel de G.

Seja E o subgrupo de Fitting generalizado de $G/R(G)$. Segue do Teorema 1.2.19 item (i) que E contém seu centralizador. Agora, pela Definição 1.2.18 temos que $E = FG_1 \cdots G_k$ onde F é o subgrupo de Fitting de $G/R(G)$ e $G_1, \ldots, G_k$ são as componentes de $G/R(G)$, isto é, são subgrupos subnormais quase simples. Para o nosso objetivo é suficiente mostrar que E possui ordem m-limitada. De fato, se E possui ordem m-limitada, temos que $Aut(E)$ também possui ordem m-limitada. Por outro lado, note que $N_{G/R(G)}(E) = G/R(G)$ e desde que $C_{G/R(G)}(E)$ está contido em E pelo Lema 1.1.5 temos que $G/R(G)/C_{G/R(G)}(E)$ é isomorfo a um subgrupo de $Aut(E)$. Disto segue que $G/R(G)/C_{G/R(G)}(E)$ também possui ordem m-limitada. Assim, como E e $[G/R(G) : C_{G/R(G)}(E)]$ possuem ordem m-limitada, concluímos que o índice $[G/R(G) : E]$ também possui ordem m-limitada. Isto implica que $G/R(G)$ também possui ordem m-limitada, como queremos.

Como estamos considerando o quociente pelo radical solúvel, temos que $F = 1$. E assim, usando [**15**, Lemma 9.5], tem-se $E = S_1 \times \cdots \times S_k$ é um produto direto de grupos S_i finitos simples não abelianos. Pelo Lema 3.1.4, temos que $\exp(G/F(G))$ é m-limitado, então $\exp(E)$ é também m-limitado. Pois, note que $F(G) \trianglelefteq R(G) \triangleleft G$ e

$$\frac{G/F(G)}{R(G)/F(G)} \cong G/R(G).$$

Agora, desde que E é o produto direto dos S_i e cada S_i é isomorfo a um subgrupo de E, segue que cada S_i possui expoente m-limitado. Portanto, pelo Teorema 3.1.5 temos que cada S_i possui ordem m-limitada. Resta mostrarmos que o número k de fatores é também m-limitado. Com efeito, desde que cada S_i é um grupo finito simples não abeliano, segue do Lema 1.2.15, que cada S_i contém um subgrupo solúvel não nilpotente, que denotaremos por R_i. Desta maneira, como cada R_i é não nilpotente, temos que $\gamma_\infty(R_i) \neq 1$. Assim, consideremos $T = R_1 \times \cdots \times R_k$, tem-se que T é solúvel. Agora, desde que T é um subgrupo de $G/R(G)$, que é uma seção de G, segue que $|E(t)| \leq m$ para todo $t \in T$. Em particular, aplicando a Afirmação 1 obtemos que $|\gamma_\infty(T)|$ é m-limitada. Observe que a ordem de $\gamma_\infty(R_i)$ é m-limitada para todo i, já que a ordem de S_i é m-limitada. Desta forma, sabendo que $|\gamma_\infty(T)| = |\gamma_\infty(R_1)| \cdots |\gamma_\infty(R_k)|$, pois tem-se $\gamma_\infty(T) \cong \gamma_\infty(R_1) \times \cdots \times \gamma_\infty(R_k)$, concluímos que o número de fatores, isto é k, é também m-limitado. Logo, segue que E possui ordem m-limitada e portanto, $|G/R(G)|$ é também m-limitada, como desejado.

Por outro lado, como $R(G)$ é solúvel e satisfaz a hipótese do teorema, segue pela Afirmação 1 que $|\gamma_\infty(R(G))|$ é m-limitada. Então, podemos considerar o quociente

$G/\gamma_\infty(R(G))$ e assim assumir que $R(G) = F(G)$ é nilpotente, pois $\gamma_\infty(R(G)) = 1$. Portanto, segue que $|G/F(G)|$ é m-limitada. Assim, podemos usar indução sobre $|G/F(G)| = k$ para mostrarmos que

$$\text{a ordem de}\, \gamma_\infty(G)\, \text{é}\, (m,k)\text{-limitada e portanto}\, m\text{-limitada.}$$

Notamos que a base desta indução inclue o caso trivial, isto é, se $|G/F(G)| = 1$, ou seja $G = F(G)$ é nilpotente. Portanto, $\gamma_\infty(G) = 1$ e o resultado é óbvio. Mas, a maior parte da base da indução está concentrada em considerar o caso quando $G/F(G)$ é um grupo simples. Observe que quando $G/F(G)$ é simples de ordem prima, então $G/F(G)$ é solúvel e portanto o resultado segue da Afirmação 1, o caso solúvel, provado antes.

Antes de dedicarmos a considerar o caso em que $G/F(G)$ é um grupo simples não-abeliano, que é a maior parte da prova, vejamos os detalhes do argumento indutivo, supondo ter provado o caso base.

Suponhamos agora que $G/F(G)$ possua um subgrupo normal próprio não trivial $N/F(G)$, com $F(G) < N \lhd G$. Notemos que $F(N) = F(G)$. Com efeito, como $F(G)$ é normal em N e nilpotente, segue pela definição de $F(N)$ que $F(G) \leq F(N)$. Por outro lado, uma vez que $F(N)$ é característico em N, que por sua vez é normal em G, temos que $F(N)$ é normal em G e nilpotente, assim pela definição de $F(G)$ obtemos que $F(N) \leq F(G)$. Portanto, $F(N) = F(G)$, como desejado. Agora, como $N \lhd G$, a hipótese do teorema também vale para N e além disso, sabendo que $F(N) < N \lhd G$, temos que $N/F(N) \lhd G/F(G)$ e $|N/F(N)| < |G/F(G)| = k$. Desta forma, aplicando a hipótese de indução em N, obtemos que $|\gamma_\infty(N)|$ é limitada em termos de m e da ordem $|N/F(N)|$ que é k-limitada e portanto m-limitada. Por outro lado, observe que $N/\gamma_\infty(N) \lhd G/\gamma_\infty(N)$. Daí, obtemos que $N/\gamma_\infty(N) \leq F(G/\gamma_\infty(N))$, uma vez que $N/\gamma_\infty(N)$ é nilpotente e normal em $G/\gamma_\infty(N)$. Desta forma, $|N/\gamma_\infty(N)| \leq |F(G/\gamma_\infty(N))|$ e pelo terceiro teorema do isomorfismo, segue que

$$\left|\frac{G/\gamma_\infty(N)}{F(G/\gamma_\infty(N))}\right| \leq |G/N|.$$

Como $F(G) < N \lhd G$, resulta que $|G/N| < |G/F(G)| = k$, e concluímos que $\left|\frac{G/\gamma_\infty(N)}{F(G/\gamma_\infty(N))}\right| < k$. Desde que $G/\gamma_\infty(N)$ é uma seção de G, tem-se pela Proposição 2.0.16 item (iii) que a hipótese do teorema também é válida para a mesma e aplicando a hipótese de indução obtemos que $|\gamma_\infty(G/\gamma_\infty(N))|$ também é limitada em termos de m e $|G/N| < k$, ou seja, é m-limitada. Usando (1.2.2) obtemos

$$\gamma_\infty\left(G/\gamma_\infty(N)\right) = \frac{\gamma_\infty(G)}{\gamma_\infty(N)}.$$

Disto segue que $|\gamma_\infty(G)/\gamma_\infty(N)|$ é m-limitada. Lembrando, como vimos antes, que $|\gamma_\infty(N)|$ é m-limitada, concluímos que $|\gamma_\infty(G)|$ é m-limitada, como desejado e o resultado segue.

Daqui em diante, vamos assumir que

$$G/R(G) \text{ é um grupo simples não abeliano de ordem } m\text{-limitada.}$$

Seja $g \in G$ um elemento qualquer. Notemos que o subgrupo $F(G)\langle g\rangle$ é solúvel e sendo $F(G)\langle g\rangle \leq G$, segue que $|E(x)| \leq m$ para todo $x \in F(G)\langle g\rangle$. Daí, pela Afirmação 1, temos que $|\gamma_\infty(F(G)\langle g\rangle)|$ é m-limitada. Desde que $\gamma_\infty(F(G)\langle g\rangle)$ é normal em $F(G)$, seu fecho normal $\langle\gamma_\infty(F(G)\langle g\rangle)^G\rangle$ em G é um produto de no máximo $|G/F(G)|$ conjugados, com cada um normal em $F(G)$. De fato, uma vez que $\gamma_\infty(F(G)\langle g\rangle)$ é normal em $F(G)$, temos que $F(G) \leq N_G(\gamma_\infty(F(G)\langle g\rangle)) \leq G$. Logo, segue que o índice $[G : N_G(\gamma_\infty(F(G)\langle g\rangle))]$ divide $[G : F(G)]$ que é m-limitado como vimos antes. Portanto, $\langle\gamma_\infty(F(G)\langle g\rangle)^G\rangle$ possui ordem m-limitada.

Agora, escolhamos um transversal $W = \{t_1, \ldots, t_k\}$ de $F(G)$ em G e definamos $K = \prod_{i=1}^{k}\langle\gamma_\infty(F(G)\langle t_i\rangle)^G\rangle$. Notemos que K é um subgrupo normal de G, pois para cada $i \in \{1, \ldots, k\}$ temos que $\langle\gamma_\infty(F(G)\langle t_i\rangle)^G\rangle$ é normal em G. Por outro lado, K possui ordem m-limitada, pois $|\langle\gamma_\infty(F(G)\langle t_i\rangle)^G\rangle|$ é m-limitada para cada $i \in \{1, \ldots, k\}$ e já vimos que k, que é a quantidade de fatores, é m-limitado. Portanto, para o nosso objetivo principal, é suficiente mostrar que $|\gamma_\infty(G/K)|$ é m-limitada. Então, usando (1.2.2) obtemos

$$\gamma_\infty(G/K) = \frac{\gamma_\infty(G)K}{K}.$$

Desta forma, se mostrarmos que $|\gamma_\infty(G/K)|$ é m-limitada e com o fato que $|K|$ é m-limitada, obtemos que a ordem de $\gamma_\infty(G)$ é m-limitada, como desejado. Logo, sem perda de generalidade, vamos assumir que $K = 1$. Primeiramente observemos que, para qualquer $g \in G$, temos

$$[F(G), g, \ldots, g] = 1, \tag{3.2.1}$$

onde g é repetido um número suficiente de vezes. De fato, como W é um transversal de $F(G)$ em G, temos que $G = F(G)W$. Desta maneira, seja $g \in G$, então $g \in F(G)t_i$ para algum $t_i \in W$. Como $K = 1$, temos que $\gamma_\infty(F(G)\langle t_i\rangle) = 1$, ou seja que $F(G)\langle t_i\rangle$ é nilpotente. Lembrando que $g \in F(G)\langle t_i\rangle$, a identidade em (3.2.1) segue.

Agora, vamos mostrar que

$$[F(G), G, \ldots, G] = 1, \tag{3.2.2}$$

onde G é repetido um número suficiente de vezes. Com efeito, desde que $F(G)$ é nilpotente finito, temos que $F(G)$ é isomorfo ao produto direto de seus subgrupos de Sylow. Então, usando propriedade de comutadores, para mostrar que (3.2.2) vale é suficiente mostrarmos que $[F_q, G, \ldots, G] = 1$ para todo q-subgrupo de Sylow F_q de $F(G)$. De fato, para qualquer h q'-elemento de G, podemos considerar que h age por automorfismos sobre F_q e esta ação é coprima. Então, segue pelo Corolário 1.3.5 item (ii) que $[F_q, h] = [F_q, h, h]$. Por um lado, usando esta propriedade, observamos que

$$[F_q, h] = [F_q, h, h] = [F_q, h, \ldots, h].$$

Por outro lado, como $F_q \leq F(G)$, usando (3.2.1) e a observação anterior tem-se que

$$[F_q, h] \leq [F(G), h, \ldots, h] = 1.$$

Portanto $[F_q, h] = 1$. Agora, seja H o subgrupo de G gerado por todos os q'-elementos. Então, segue que $[F_q, H] = 1$. Note que $G = F_qH$. Pois, desde que H seja normal em G e considerando o epimorfismo canônico de G em $G/F(G)$, tem-se que $F(G)H/F(G) \trianglelefteq G/F(G)$. Por $G/F(G)$ ser simples, resulta que $F(G)H/F(G) = G/F(G)$ e assim temos que $G = F(G)H$. Pela definição de H e das propriedades de $F(G)$, segue que $G = F_qH$. Combinando os fatos que $G = F_qH$ e $[F_q, H] = 1$, obtemos que

$$[F_q, G, \ldots, G] = [F_q, F_qH, \ldots, F_qH] = [F_q, F_q, \ldots, F_q].$$

Logo, como F_q é nilpotente, então tem-se

$$[F_q, G, \ldots, G] = [F_q, F_q, \ldots, F_q] = 1,$$

onde F_q é repetido um número suficiente de vezes no comutador. Portanto, $[F_q, G, \ldots, G] = 1$ para todo q-subgrupo de Sylow F_q de $F(G)$. Em particular, a identidade (3.2.2) vale, como queríamos.

Finalmente agora, estamos em condições de mostrar que $\gamma_\infty(G)$ possui ordem m-limitada. Para simplificarmos a notação, façamos $D = \gamma_\infty(G)$. Vamos mostrar primeiro que $D = [D, D]$. De fato, como $G/F(G)$ é um grupo simples não-abeliano, temos que D é não solúvel. Pois, caso contrário teríamos que $[D, D] < D$ e isto levaria uma contradição sendo $G/F(G)$ simples. Como D é não solúvel, temos que $[D,D] \leq D$. Assim, considerando o epimorfismo canônico de G em $G/F(G)$, resulta que $[D,D]F(G)/F(G) \trianglelefteq G/F(G)$. E por $G/F(G)$ ser simples não-abeliano, segue que $[D,D]F(G)/F(G) = G/F(G)$. Portanto, concluímos que

$$G = F(G)[D,D]. \tag{3.2.3}$$

Agora, aplicando comutação com G em ambos os lados da igualdade em (3.2.3), obtemos para todo $i \geqslant 1$ que

$$\gamma_i(G) = [G,\ldots,G] = [F(G)[D,D],G,\ldots,G] \leq [F(G),G,\ldots,G][D,D].$$

Assim, usando (3.2.2), temos que $\gamma_i(G) \leq [D,D]$ para um i suficientemente grande. Logo, $D = \bigcap_{i=1}^{\infty} \gamma_i(G) \leq \gamma_i(G) \leq [D,D]$. Portanto, concluímos que $D = [D,D]$.

Consideremos o comutador $[F(G)\cap D, D,\ldots,D]$, onde D é repetido um número suficiente de vezes no comutador como G em (3.2.2). Como $F(G)\cap D \leq F(G)$ e usando a identidade (3.2.2), concluímos que

$$[F(G)\cap D, D,\ldots,D] \leq [F(G),G,\ldots,G] = 1.$$

Logo,

$$[F(G)\cap D, D,\ldots,D] = 1. \tag{3.2.4}$$

Consequentemente temos que $F(G)\cap D \leq Z_n(D)$ para n suficientemente grande, onde $Z_n(D)$ é o n-ésimo termo da série central ascendente de D. De fato, por (3.2.4) tem-se que $[x,d_1,\ldots,d_n] = 1$ para todo $x \in F(G)\cap D$ e para quaisquer $d_1,\ldots,d_n \in D$. Logo, pela Proposição 1.2.4, obtemos que $x \in Z_n(D)$. Agora, como D é um grupo perfeito, temos pelo Lema 1.2.2 que $Z\left(D/Z(D)\right) = 1$, ou seja $Z(D) = Z_2(D)$. Disto segue com um argumento indutivo, que

$$Z(D) = Z_i(D) \qquad \forall\ i \geqslant 1. \tag{3.2.5}$$

Por outro lado, sabendo que $F(G)\cap D \leq Z_n(D)$ para n suficientemente grande e usando (3.2.5), obtemos que $F(G)\cap D \leq Z(D)$. E desta maneira, concluímos que $F(G)\cap D \leq Z(D)\cap D = Z(D)\cap[D,D]$. Agora, note que $F(G)\cap D \lhd D$. Daí, temos

$$\frac{D}{F(G)\cap D} \cong \frac{F(G)D}{F(G)} = \frac{F(G)[D,D]}{F(G)} = \frac{G}{F(G)},$$

onde na última igualdade usamos (3.2.3).

Assim, como $|G/F(G)|$ é m-limitada, resulta que $|D/(F(G) \cap D)|$ também é m-limitada. Por outro lado, como $F(G) \cap D \leq Z(D) \leq D$, obtemos que $[D : Z(D)]$ é m-limitada e pelo Teorema 1.2.3, segue que $D' = D$ possui ordem limitada em termos da ordem de $|G/F(G)|$ que é m-limitada. Portanto, $D = \gamma_\infty(G)$ possui ordem m-limitada, como queríamos. Isso completa o argumento no caso que $G/F(G)$ é simples não-abeliano. Assim, terminamos a prova da Afirmação 2 e isso completa também a demonstração do Teorema 3.2.1. $\square$

Concluímos este capítulo fazendo algumas considerações sobre o resultado do Teorema 3.2.1. Primeiro notemos que o Teorema 3.2.1 pode ser visto como uma generalização do conhecido teorema de Zorn (veja Teorema 2.0.12) que diz que um grupo finito Engel precisa ser nilpotente. Agora uma consideração técnica: do enunciado do Teorema 3.2.1 segue imediatamente que o índice do subgrupo de Fitting de G precisa ser m-limitado, pois é suficiente observar que pelo fato da ordem de $\gamma_\infty(G)$ ser m-limitada deduzimos que o índice de $C_G(\gamma_\infty(G))$ em G é m-limitado e assim, chegamos a limitar em termos de m o índice de $F(G)$ em G. Mas, note que essa informação sobre o índice de $F(G)$ em G é de fato um passo fundamental da mesma prova do Teorema 3.2.1. No Capítulo 4, veremos também como a partir do Teorema 3.2.1 é possível deduzir um resultado análogo de tipo quantitativo para grupos profinitos. Os detalhes serão apresentados no Corolário 5.2.3.

4

Grupos Profinitos

Neste capítulo vamos apresentar definições e os principais resultados de espaços topológicos que serão utilizados ao longo do trabalho, depois veremos o conceito de grupos topológicos e ressaltaremos suas propriedades mais relevantes. Em seguida, veremos a definição de limite inverso e daremos algumas caracterizações de grupos profinitos. Logo em seguida, definiremos completamentos de grupos abstratos e construíremos alguns exemplos. Depois, falaremos da teoria de Sylow em grupos profinitos, veremos que muitos dos resultados conhecidos de teoria de grupos podem ser estendidos a grupos profinitos. E por fim, caracterizaremos os grupos pronilpotentes. As principais referências utilizadas neste capítulo são os livros de J. S. Wilson [**25**] e L. Ribes e P. Zalesskii [**19**]. Este capítulo tem um caráter preliminar referente ao Capítulo 4.

4.1. Espaços Topológicos

Vamos começar esta seção introduzindo o conceito de topologia e também de espaço topológico.

Uma *topologia* num conjunto X é uma coleção τ de subconjuntos de X, chamados *conjuntos abertos*, satisfazendo as seguintes condições:
(i) o conjunto vazio $\varnothing$ e X são conjuntos abertos;
(ii) a interseção de quaisquer dois conjuntos abertos é um conjunto aberto;
(iii) a união de qualquer coleção de conjuntos abertos é um conjunto aberto.

Um *espaço topológico* é um par (X, τ) onde X é um conjunto não vazio e τ é uma topologia em X; frequentemente diremos apenas espaço topológico X mencionando τ somente quando for necessário.

Podemos considerar qualquer conjunto X como um espaço topológico, basta definirmos uma topologia na qual cada subconjunto de X é um aberto; chamamos esta topologia de *topologia discreta* em X. Então, X é dito um *espaço discreto*.

A seguir vamos lembrar algumas definições e conceitos básicos relacionados a espaços topológicos.

Seja Y um subconjunto de um espaço topológico X, a coleção de todos os subconjuntos da forma $Y \cap U$, com U aberto em X, é uma topologia em Y; esta é chamada a *topologia subespaço* e com respeito a esta topologia Y é dito um *subespaço* de X.

Dado X um espaço topológico, um subconjunto Y de X é dito *fechado* se seu complementar $X \backslash Y$ é aberto. Seja Y um subconjunto de X, o *fecho* de Y, o qual denotaremos por $\overline{Y}$, é a interseção de todos os conjuntos fechados contendo Y. Então, $\overline{Y}$ é um conjunto fechado. Dizemos que Y é *denso* em X se $\overline{Y} = X$.

Uma *vizinhança aberta* de um elemento x de X é um conjunto aberto que contém x. Uma *base* para a topologia em X é uma coleção $\{U_\lambda \mid \lambda \in \Lambda\}$ de conjuntos abertos tal que todo conjunto aberto é uma união de alguns dos conjuntos U_λ.

Um espaço topológico X é chamado *compacto* se, dada qualquer família de subconjuntos abertos $\{U_\alpha \mid \alpha \in A\}$ tal que $X = \bigcup_{\alpha \in A} U_\alpha$, existe uma subfamília finita $\{U_{\alpha_1}, \ldots, U_{\alpha_n}\}$ tal que $X = \bigcup_{i=1}^{n} U_{\alpha_i}$. Podemos definir compacidade de outra maneira, ou seja, X é dito *compacto* se sempre que $\{C_\alpha \mid \alpha \in A\}$ é uma família de subconjuntos fechados com a propriedade de que cada interseção de uma quantidade finita de conjuntos C_α é não vazia, segue que a interceção de todos os conjuntos C_α é não vazia. As duas definições são equivalentes.

Um espaço X é dito *localmente compacto* se cada elemento x em X possui uma vizinhança compacta. Notemos que todo espaço compacto é localmente compacto, pois o espaço em si é uma vizinhança compacta de qualquer um de seus elementos.

Um espaço X é chamado *Hausdorff* se para quaisquer elementos distintos x e y em X existem vizinhanças abertas U e V de x e y respectivamente tal que $U \cap V = \varnothing$. Observemos que se X é Hausdorff, então $\{x\}$ é fechado para cada $x \in X$, pois para cada $y \in X$ com $x \neq y$ existe uma vizinhança aberta U de y disjunta com $\{x\}$, então $X \backslash \{x\}$ é aberto.

Dizemos que um espaço X é *conexo* se não podemos escrevê-lo como uma união disjunta de dois abertos não vazios. Por outro lado, X é dito *totalmente desconexo* se todo subespaço conexo possui no máximo um elemento.

Os conceitos de espaços totalmente desconexo, Hausdorff e compacto são muito relevantes no nosso estudo, pois veremos que os grupos profinitos, objetos centrais na dissertação, são sempre espaços com essas características.

Sejam X e Y espaços topológicos. Dizemos que uma aplicação $f : X \longrightarrow Y$ é *contínua* se para cada conjunto aberto U de Y a imagem inversa $f^{-1}(U)$ é aberta em X. É fácil ver que composição de funções contínuas é contínua. Uma aplicação f entre espaços topológicos é dita um *homeomorfismo* se f é contínua e bijetora com inversa f^{-1} também contínua.

A seguir reunimos, em uma proposição, alguns resultados a respeito de aplicações contínuas, espaços compactos, totalmente desconexos e Hausdorff que serão bastante utilizados no decorrer deste capítulo.

Proposição 4.1.1. *Sejam X e Y espaços topológicos e $f, g : X \longrightarrow Y$ aplicações entre esses espaços. As seguintes afirmações valem:*
(i) *cada subconjunto fechado de um espaço compacto é compacto;*
(ii) *cada subconjunto compacto de um espaço Hausdorff é fechado;*
(iiii) *se f é contínua e X é compacto, então $f(X)$ é compacto;*
(iv) *se f é contínua e bijetora e se X é compacto e Y é Hausdorff, então f é um homeomorfismo;*
(v) *se f e g são funções contínuas e Y é um espaço Hausdorff, então o conjunto $\{x \in X \mid f(x) = g(x)\}$ é fechado em X;*
(vi) *seja X um espaço compacto e Hausdorff. Se X é também totalmente desconexo, então cada conjunto aberto é uma união de conjuntos que são simultaneamente fechados e abertos.*

Demonstração. Observe que os itens (i), (ii), (iii), (iv) e (vi) são simples exercícios, consequências das definições. Assim, vamos demonstrar somente o item (v).

Denotemos por $N = \{x \in X \mid f(x) \neq g(x)\}$ e vamos mostrar que N é aberto. Seja $y \in N$, então $f(y) \neq g(y)$ e por Y ser Hausdorff existem U e V conjuntos abertos de Y contendo $f(y)$ e $g(y)$ respectivamente que são disjuntos.

Como f e g são funções contínuas, temos que $f^{-1}(U)$ e $g^{-1}(V)$ são abertos em X, logo $f^{-1}(U) \cap g^{-1}(V)$ é uma vizinhança aberta de y e está contida em N. Deste modo, N é uma união de conjuntos abertos da forma $f^{-1}(U) \cap g^{-1}(V)$, logo N é aberto e o resultado segue. $\square$

O lema a seguir é muito útil quando queremos verificar se um subconjunto de um espaço topológico é denso. A prova deste resultado pode ser encontrada em [**17**, Proposition 3.1.15].

Lema 4.1.2. *Seja Y um subconjunto de um espaço topológico X. Dizemos que Y é denso em X se, e somente, se cada subconjunto aberto não vazio de X intersecta Y não trivialmente, isto é, se U é um aberto não vazio de X, então $Y \cap U \neq \varnothing$.*

Seja ρ uma relação de equivalência em um espaço topológico X e denotamos por X/ρ o conjunto quociente e q para a aplicação quociente de X para X/ρ que associa a cada elemento de X a sua classe de equivalência. A *topologia quociente* em X/ρ é a topologia cujos conjuntos abertos são os subconjuntos V de X/ρ tais que $q^{-1}(V)$ é um aberto em X. Note que esta definição de topologia quociente garante que, se X/ρ é considerado com a topologia quociente, então a aplicação $q : X \longrightarrow X/\rho$ é contínua.

Vamos agora lembrar a noção de produto Cartesiano para assim poder apresentar o conceito de produto de espaços topológicos e ver algumas propriedades relacionadas.

Um *produto Cartesiano* (ou simplesmente *produto*) de uma família de conjuntos $\{X_\lambda \mid \lambda \in \Lambda\}$ é o conjunto $C = \mathrm{Cr}(X_\lambda \mid \lambda \in \Lambda)$ cujos elementos são as aplicações x de Λ em $\bigcup_\lambda X_\lambda$ tal que $x(\lambda) \in X_\lambda$ para cada λ. Portanto, um elemento de C, pode ser pensando como um vetor da forma (x_λ) que corresponde a função que leva λ para x_λ.

Para cada $\lambda \in \Lambda$, existe uma aplicação $\pi_\lambda : C \longrightarrow X_\lambda$ definida por $(x_\lambda) \longmapsto x_\lambda$ chamada *projeção*.

Agora suponhamos que cada X_λ seja um espaço topológico. Dado C o produto dos X_λ, podemos tornar C um espaço topológico definindo uma topologia cujos conjuntos abertos são todas as uniões de conjuntos da forma

$$\pi_{\lambda_1}^{-1}(U_1) \cap \cdots \cap \pi_{\lambda_n}^{-1}(U_n),$$

com n finito, cada λ_i em Λ e U_i um aberto em X_{λ_i}. Esta topologia é chamada *topologia produto*. Note que como consequência desta definição cada aplicação projeção $\pi_\lambda : C \longrightarrow X_\lambda$ pode ser mostrada ser contínua.

Seja $f : Z \longrightarrow C$ uma aplicação, onde Z é um outro espaço topológico. Observe que f é contínua se, e somente se, cada aplicação $\pi_\lambda f$ é contínua.

Finalizamos esta seção, com um teorema que relaciona algumas propriedades topológicas de uma dada família de espaços toplógicos com o seu produto.

Teorema 4.1.3. *Sejam* $\{X_\lambda \mid \lambda \in \Lambda\}$ *uma família de espaços topológicos e* C *seu produto Cartesiano. As seguintes afirmações valem:*
(i) *se cada* X_λ *é Hausdorff, então* C *é Hausdorff;*
(ii) *se cada* X_λ *é totalmente desconexo, então* C *é totalmente desconexo;*
(iii) *se cada* X_λ *é compacto, então* C *é compacto (Teorema de Tychonoff).*

A demonstração deste fato pode ser vista em [**25**, Theorem 0.2.1]. Mas é válido ressaltar que o item (iii) não é elementar, uma vez que em sua prova usa-se o axioma da escolha.

4.2. Grupos Topológicos

Nesta seção vamos introduzir o conceito de grupo topológico, ou seja, um conjunto não apenas com uma estrutura de espaço topológico, mas também com a estrutura de grupo. Veremos como a coexistência dessas duas estruturas em um único conjunto X será fundamental para relaciona-las e obter consequências no estudo das propriedades de X. Nosso interesse principal, no estudo de grupos topológicos, está baseado no fato que todo grupo profinito, como veremos, é em particular um grupo topológico.

Definição 4.2.1. Um *grupo topológico* é um conjunto G que é ao mesmo tempo um grupo e um espaço topológico, para o qual a aplicação

$$\begin{array}{ccc} G \times G & \longrightarrow & G \\ (x, y) & \longmapsto & xy^{-1} \end{array}$$

é contínua. Claramente $G \times G$ está munido com a topologia produto.

Sejam G um grupo, g um elemento de G e U e V subconjuntos de G. Definimos os seguintes subconjuntos $Ug = \{ug \mid u \in U\}, gU = \{gu \mid u \in U\}$, $U^{-1} = \{u^{-1} \mid u \in U\}$ e $UV = \{uv \mid u \in U, v \in V\}$. Denotaremos por 1 o elemento neutro de um grupo.

As duas proposições seguintes reúnem os fatos mais relevantes acerca de grupos topológicos.

Proposição 4.2.2. *Seja* G *um grupo topológico. As seguintes afirmações valem:*
(i) *a aplicação de* $G \times G$ *em* G *definida por* $(x, y) \longmapsto xy$ *é contínua e a aplicação de* G *em* G *definida por* $x \longmapsto x^{-1}$ *é um homeomorfismo. E para cada* $g \in G$ *as aplicações de* G *em* G *dadas por* $x \longmapsto xg$ *e* $x \longmapsto gx$ *são homeomorfismos;*
(ii) *se* H *é um subgrupo aberto (res. fechado) de* G*, então toda classe lateral* Hg *ou* gH *de* H *em* G *é aberta (res. fechada);*

(iii) *todo subgrupo aberto de G é fechado e todo subgrupo fechado de índice finito é aberto. Além disso, se G é compacto, então todo subgrupo aberto de G tem índice finito;*
(iv) *se H é um subgrupo contendo um subconjunto aberto não vazio U de G, então H é aberto em G.*

Demonstração. Notemos que o item (i) é consequência das definições de grupo topológico e de aplicação contínua.

Agora mostraremos (ii). Seja H um subgrupo aberto (res. fechado) de G, para cada $g \in G$ definamos a aplicação $f : G \longrightarrow G$ dada por $x \longmapsto xg$. Pelo item (i), f é um homeomorfismo e por H ser aberto (res. fechado) temos que $f(H) = \{hg \mid h \in H\} = Hg$ é aberto (res. fechado), pois homeomorfismo leva aberto (res. fechado) em aberto (res. fechado). De um modo análogo, podemos provar que o conjunto gH é aberto (res. fechado).

Vamos provar (iii). Seja H um subgrupo de G. Observemos que podemos escrever $G \setminus H$ da seguinte forma $G \setminus H = \cup(Hg \mid g \notin H)$. Se H é aberto, então por (ii) Hg é aberto, logo $G \setminus H$ é aberto e portanto, H é fechado.

Se H é um subgrupo fechado de índice finito, temos que o número de classes laterais de H em G é finito, logo $G \setminus H$ é uma união de uma quantidade finita de classes laterais. Por H ser fechado, pelo item (ii) Hg é fechado, assim $G \setminus H$ é fechado, uma vez que o mesmo é a união de um número finito de conjuntos fechados, consequentemente obtemos que H é aberto.

Seja agora H um subgrupo aberto de G. Sabemos que podemos escrever G da seguinte forma $G = \bigcup_{g \in G} Hg$, onde cada Hg é aberto. Desde que G é compacto, existem $g_i \in G$ com $i \in \{1, \ldots, n\}$ tal que $G = \bigcup_{i=1}^{n} Hg_i$. Assim, segue que o índice de H em G é finito.

Vamos mostrar (iv). Para cada $h \in H$, consideremos a aplicação $f : G \longrightarrow G$ definida por $x \longmapsto xh$. Pelo item (i) temos que f é um homeomorfismo. Como U é aberto, então $f(U) = \{uh \mid u \in U\} = Uh$ é aberto. Vejamos que H pode ser escrito como $H = \bigcup_{h \in H} Uh$. Com efeito, por U está contido em H, que é subgrupo de G, obtemos claramente que $\bigcup_{h \in H} Uh \subseteq H$. Por outro lado, dado h elemento qualquer de H, como U é não vazio, existe u_1 em U, logo $u_1^{-1} \in H$ e assim tomando $h_1 = u_1^{-1}h \in H$ temos que $h = u_1 h_1 \in Uh_1$. Segue que $H \subseteq \bigcup_{h \in H} Uh$. Assim, H é uma união de abertos, portanto ele é aberto, como desejado. □

Proposição 4.2.3. *Seja G um grupo topológico. Então temos que:*
(i) *se G é compacto e Hausdorff e se C e D são subconjuntos fechados, então o subconjunto CD é fechado;*

(ii) *se H é um subgrupo de G e K é um subgrupo normal de G, então H é um grupo topológico com respeito a topologia subespaço e G/K é um grupo topológico com respeito a topologia quociente. Além disso, a aplicação quociente q de G em G/K leva subconjunto aberto em subconjunto aberto;*
(iii) *o grupo G é Hausdorff se, e somente se, $\{1\}$ é fechado em G. Se K é um subgrupo normal de G, então G/K é Hausdorff se, e somente se, K é fechado em G. Se G é totalmente desconexo, então G é Hausdorff;*
(iv) *suponha que G é compacto e seja $\{X_\lambda \mid \lambda \in \Lambda\}$ uma família de subconjuntos fechados com a propriedade que para todos $\lambda_1, \lambda_2 \in \Lambda$ existe um elemento $\mu \in \Lambda$ tal que $X_\mu \subseteq X_{\lambda_1} \cap X_{\lambda_2}$. Se Y é um subconjunto fechado de G, então temos que $(\bigcap_{\lambda\in\Lambda} X_\lambda)Y = \bigcap_{\lambda\in\Lambda} X_\lambda Y$.*

Demonstração. A prova do item (i) segue diretamente da Proposição 4.1.1 item (i). Os itens (ii) e (iii) podem ser facilmente provados usando o item (i) e propriedades de topologia quociente e de subespaço. Assim, vamos mostrar apenas o item (iv).

Agora, mostraremos o item (iv). Para simplificarmos a notação, vamos omitir o índice $\lambda \in \Lambda$. Claramente temos que $(\bigcap X_\lambda)Y \subseteq \bigcap X_\lambda Y$. Por outro lado, seja $g \in \bigcap X_\lambda Y$, suponhamos que $g \notin (\bigcap X_\lambda)Y$. Então, $gY^{-1} \cap (\bigcap X_\lambda) = \varnothing$. Como Y é fechado e G é compacto, segue que Y é compacto. Consideremos o homeomorfismo $f : G \longrightarrow G$ dado por $x \longmapsto x^{-1}$, tem-se que $f(Y) = Y^{-1}$ é fechado, logo gY^{-1} é fechado. Desta maneira, por G ser compacto e gY^{-1} e os conjuntos X_λ serem fechados com interserção vazia, segue que existe um conjunto finito $\{\lambda_1, \ldots, \lambda_n\} \in \Lambda$ tal que

$$gY^{-1} \cap X_{\lambda_1} \cap \cdots \cap X_{\lambda_n} = \varnothing. \tag{4.2.1}$$

Por outro lado, por hipótese, temos que para todos $\lambda_1, \lambda_2 \in \Lambda$ existe um elemento $\mu_1 \in \Lambda$ tal que $X_{\mu_1} \subseteq X_{\lambda_1} \cap X_{\lambda_2}$. Então, aplicando $n-1$ vezes o mesmo argumento, garantimos a existência de um $\mu \in \Lambda$ tal que

$$X_\mu \subseteq X_{\lambda_1} \cap \cdots \cap X_{\lambda_n}. \tag{4.2.2}$$

Agora, combinando (4.2.1) e (4.2.2), obtemos que $gY^{-1} \cap X_\mu = \varnothing$. O que implica em $g \notin X_\mu Y$. O que é um absurdo, pois por hipótese $g \in \bigcap X_\lambda Y$. Portanto, $g \in (\bigcap X_\lambda)Y$ e o resultado segue. $\square$

O lema a seguir será útil em alguns casos e sua demonstração pode ser encontrada em [**25**, Lemma 0.3.2].

Lema 4.2.4. *Seja G um grupo topológico compacto. Se C é um subconjunto que é ao mesmo tempo fechado e aberto e contém 1, então C contém um subgrupo normal aberto.*

A combinação do Lema 4.2.4 e das Proposições 4.1.1 e 4.2.3 nos fornecem a próxima proposição que caracteriza subgrupos abertos e fechados em um grupo topológico com determinadas propriedades. Os detalhes da demonstração podem ser encontrados em [**25**, Proposition 0.3.3]. Denotemos por $N \lhd_\circ G$ um subgrupo normal aberto N em G.

Proposição 4.2.5. *Seja G um grupo topológico, totalmente desconexo e compacto. As seguintes afirmações valem:*
(i) *cada conjunto aberto em G é uma união de classes laterais de subgrupos normais abertos;*
(ii) *um subconjunto de G é aberto e fechado se, e somente se, é uma união de um número finito de classes laterais de subgrupos normais abertos;*
(iii) *se X é um subconjunto de G, então seu fecho $\overline{X}$ satisfaz*

$$\overline{X} = \bigcap \{NX \mid N \lhd_\circ G\}.$$

Em particular, para cada subconjunto fechado C, temos

$$C = \bigcap \{NC \mid N \lhd_\circ G\},$$

e a interseção dos subgrupos normais abertos de G é trivial.

O lema a seguir nos diz que podemos tornar o produto Cartesiano de grupos topológicos em um grupo topológico. A demonstração deste fato, segue da definição de topologia produto.

Lema 4.2.6. *Sejam $\{G_\lambda \mid \lambda \in \Lambda\}$ uma família de grupos topológicos e o produto Cartesiano dos G_λ, isto é, $C = \mathrm{Cr}(G_\lambda \mid \lambda \in \Lambda)$. Defina em C a operação, componente a componente, ou seja, $(x_\lambda)(y_\lambda) = (x_\lambda y_\lambda)$ para todos $(x_\lambda), (y_\lambda) \in C$. Então C torna-se um grupo topológico com respeito a esta operação e a topologia produto.*

Concluímos esta seção observando que, em um grupo topológico Hausdorff, o centralizador de qualquer subconjunto e o normalizador de todo subgrupo fechado são fechados.

Lema 4.2.7. *Seja G um grupo topológico Hausdorff. Então:*
(i) *o centralizador de todo subconjunto S de G, isto é,*

$$C_G(S) = \{g \in G \mid gs = sg \ \forall s \in S\}$$

é fechado;
(ii) *o normalizador de todo subgrupo fechado H de G, isto é,*

$$N_G(H) = \{g \in G \mid g^{-1}hg \in H \ e \ ghg^{-1} \in H, \ \forall \ h \in H\}$$

é fechado.

DEMONSTRAÇÃO. Vamos mostrar o item (i). Fixamos $s \in S$ e consideremos as seguintes aplicações: $r_s : G \longrightarrow G$ dada por $g \longmapsto gs$ e $l_s : G \longrightarrow G$ definida por $g \longmapsto sg$. Observe que r_s e l_s são contínuas. Agora por G ser Hausdorff, segue pela Proposição 4.1.1 item (v) que o conjunto

$$C_G(s) = \{g \in G \mid gs = sg\} = \{g \in G \mid r_s(g) = l_s(g)\}$$

é fechado em G. Assim, como $C_G(S) = \bigcap_{s \in G} C_G(s)$, concluímos que $C_G(S)$ é fechado, como queríamos.

Com um argumento semelhante mostra-se o item (ii). □

4.3. Limites Inversos

Nesta seção, apresentamos todas as ferramentas necessárias para poder definir o conceito de grupo profinito, mais especificamente, discutiremos as noções de sistema inverso e limite inverso. Além disso, daremos alguns exemplos e enunciaremos várias propriedades. O conceito de limite inverso é central na definição de grupos profinitos, pois veremos que um grupo profinito será um limite inverso de uma determinada classe de grupos.

Seja I um conjunto parcialmente ordenado com respeito a uma relação de ordem " $\leqslant$ ". Dizemos que I é *dirigido* se para todos $i_1, i_2 \in I$ existe um elemento $j \in I$ tal que $i_1 \leqslant j$ e $i_2 \leqslant j$.

Definição 4.3.1. Um *sistema inverso* de espaços topológicos, indexado por um conjunto dirigido I, consiste de uma família $\{X_i \mid i \in I\}$ de espaços topológicos e uma família $\{\varphi_{ij} : X_j \longrightarrow X_i \mid i, j \in I, i \leqslant j\}$ de aplicações contínuas satisfazendo as seguintes propriedades:
(i) φ_{ii} é a aplicação identidade de X_i para cada $i \in I$;

(ii) o diagrama abaixo comuta, isto é, $\varphi_{ij}\varphi_{jk} = \varphi_{ik}$,

$$\begin{tikzcd}
X_k \arrow[rr, "\varphi_{ik}"] \arrow[dr, "\varphi_{jk}"'] & & X_i \\
& X_j \arrow[ur, "\varphi_{ij}"'] &
\end{tikzcd}$$

sempre que $i \leqslant j \leqslant k$.

Denotaremos um sistema inverso por (X_i, φ_{ij}) quando for claro sobre qual conjunto dirigido I o mesmo está sendo considerado.

Observe que conjuntos para os quais não especificamos uma determinada topologia serão sempre considerados como espaços topológicos munidos da topologia discreta.

Se cada X_i considerado na Definição 4.3.1 for um grupo topológico e cada φ_{ij} for um homomorfismo contínuo, então o par (X_i, φ_{ij}) é dito um sistema inverso de grupos topológicos. Analogamente, é possível definir um sistema inverso de anéis topológicos.

Vejamos alguns exemplos representativos de sistemas inversos que serão usados posteriormente.

Exemplo 4.3.2. Sejam $I = \mathbb{N}$, um conjunto dirigido com a relação de ordem usual, $\{X_i \mid i \in \mathbb{N}\}$ uma família de conjuntos finitos, onde $X_i = \{1, \ldots, i\}$, para cada $i \in I$ e considere $\varphi_{i,i+1} : X_{i+1} \longrightarrow X_i$ a aplicação definida por: $\varphi_{i,i+1}(x) = x$ se $x < i + 1$ e $\varphi_{i,i+1}(x) = i$ se $x = i + 1$. Definamos $\varphi_{ii} = Id_{X_i}$ para cada i e $\varphi_{ij} = \varphi_{i,i+1} \cdots \varphi_{j-1,j}$ para $j > i$. Então, temos que o par (X_i, φ_{ij}) é um sistema inverso de conjuntos finitos. Em particular, podemos representar graficamente as várias aplicações de X_{i+1} em X_i em sequência da seguinte forma:

$$\begin{tikzcd}
 & & & & & 6 \arrow[dl] & \arrow[l, dotted] \\
 & & & & 5 \arrow[dl] & 5 \arrow[l] & \arrow[l, dotted] \\
 & & & 4 \arrow[dl] & 4 \arrow[l] & 4 \arrow[l] & \arrow[l, dotted] \\
 & & 3 \arrow[dl] & 3 \arrow[l] & 3 \arrow[l] & 3 \arrow[l] & \arrow[l, dotted] \\
 & 2 \arrow[dl] & 2 \arrow[l] & 2 \arrow[l] & 2 \arrow[l] & 2 \arrow[l] & \arrow[l, dotted] \\
1 & 1 \arrow[l] & 1 \arrow[l] & 1 \arrow[l] & 1 \arrow[l] & 1 \arrow[l] & \arrow[l, dotted]
\end{tikzcd}$$

Exemplo 4.3.3. Sejam $I = \mathbb{N}$, um conjunto dirigido com a relação de ordem usual, p um número primo e para cada $i \in I$ definamos $G_i = \mathbb{Z}/p^i\mathbb{Z}$. Para $j \geqslant i$, consideremos a seguinte aplicação

$$\begin{array}{rccc} \varphi_{ij} : & G_j & \longrightarrow & G_i \\ & n + p^j\mathbb{Z} & \longmapsto & n + p^i\mathbb{Z} \end{array}$$

para cada $n \in \mathbb{Z}$. Então, (G_i, φ_{ij}) é um sistema inverso de anéis topológicos, pois, sabemos que cada G_i é anel topológico e claramente cada φ_{ij} é um homomorfismo contínuo de anéis. Agora observemos também que $\varphi_{ii} = Id_{G_i}$ para todo $i \in I$ e se $i \leqslant j \leqslant k$ tem-se $\varphi_{ij}\varphi_{jk} = \varphi_{ik}$. Com efeito, seja $n + p^k\mathbb{Z} \in G_k$, então

$$(\varphi_{ij}\varphi_{jk})(n + p^k\mathbb{Z}) = \varphi_{ij}(\varphi_{jk}(n + p^k\mathbb{Z})) = \varphi_{ij}(n + p^j\mathbb{Z}) = n + p^i\mathbb{Z} = \varphi_{ik}(n + p^k\mathbb{Z}).$$

Observe que o Exemplo 4.3.3 é também um exemplo de sistema inverso de grupos topológicos.

Vamos agora generalizar a ideia do exemplo anterior para um grupo G qualquer.

Exemplo 4.3.4. Sejam G um grupo e I uma família de subgrupos normais de G com a propriedade que para todos $U_1, U_2 \in I$ existe um subgrupo $V \in I$ tal que $V \leqslant U_1 \cap U_2$. Podemos considerar I como sendo um conjunto dirigido com respeito a ordem " $\leqslant'$ " definida por

$$U \leqslant' V \text{ se, e somente se, } V \leqslant U.$$

Para $U \leqslant' V$ considere a aplicação definida por:

$$\begin{array}{rccc} q_{UV} : & G/V & \longrightarrow & G/U \\ & Vg & \longmapsto & Ug \end{array}$$

para todo $g \in G$. Então, (G_U, q_{UV}) é um sistema inverso de grupos.

De fato, observe que G/U é um grupo topológico para todo $U \in I$ e claramente as aplicações q_{UV} são homomorfismos contínuos, tais que se $U = V$, obtemos $q_{UU} = Id_{G/U}$ e se $U \leqslant' V \leqslant' W$, tem-se pela definição de ordem que $W \leqslant V \leqslant U$ e portanto concluímos $q_{UV}q_{VW} = q_{UW}$, pois dado $Wg \in G/W$, temos que

$$(q_{UV}q_{VW})(Wg) = q_{UV}(q_{VW}(Wg)) = q_{UV}(Vg) = Ug = q_{UW}(Wg).$$

Dados (X_i, φ_{ij}) um sistema inverso de espaços topológicos sobre um conjunto dirigido I e Y um espaço topológico, dizemos que uma família de aplicações contínuas $\{\psi_i : Y \longrightarrow X_i \mid i \in I\}$ é *compatível* se temos $\varphi_{ij}\psi_j = \psi_i$, sempre que $i \leqslant j$, ou seja, se cada diagrama abaixo

$$\begin{tikzcd} & Y \arrow[dl, "\psi_j"'] \arrow[dr, "\psi_i"] & \\ X_j \arrow[rr, "\varphi_{ij}"'] & & X_i \end{tikzcd}$$

é comutativo.

Finalmente estamos em condições de definir o conceito de limite inverso de um sistema inverso de espaços topológicos.

Definição 4.3.5. Um *limite inverso* de um sistema inverso (X_i, φ_{ij}) de espaços topológicos, é um espaço topológico X juntamente com uma família compatível $\{\varphi_i : X \longrightarrow X_i\}$ de aplicações contínuas satisfazendo a seguinte propriedade universal: sempre que $\{\psi_i : Y \longrightarrow X_i\}$ é uma família compatível de aplicações contínuas de um espaço Y, existe uma única aplicação contínua $\psi : Y \longrightarrow X$ tal que $\varphi_i \psi = \psi_i$ para cada i, ou seja, de modo que cada um dos seguintes diagramas comute.

$$\begin{tikzcd} & Y \arrow[dl, dashed, "\psi"'] \arrow[dr, "\psi_i"] & \\ X \arrow[rr, "\varphi_i"'] & & X_i \end{tikzcd}$$

Denotamos um limite inverso de um sistema inverso (X_i, φ_{ij}) por (X, φ_i). Note que análogas definições podem ser enunciadas para o limite inverso de um sistema inverso de grupos topológicos e anéis topológicos.

O próximo resultado nos mostra que o limite inverso de um sistema inverso (X_i, φ_{ij}) de espaços topológicos existe e é único em um determinado sentido.

Proposição 4.3.6. *Seja (X_i, φ_{ij}) um sistema inverso de espaços topológicos (de grupos topológicos res.), indexado por I. Então as seguintes afirmações valem:*
(i) *se $(X^{(1)}, \varphi_i^{(1)})$ e $(X^{(2)}, \varphi_i^{(2)})$ são limites inversos do sistema inverso (X_i, φ_{ij}), então existe um homeomorfismo (isomorfismo topológico res.) $\phi : X^{(1)} \longrightarrow X^{(2)}$ tal que $\varphi_i^{(2)} \phi = \varphi_i^{(1)}$ para cada $i \in I$;*
(ii) *seja $C = \mathrm{Cr}(X_i \mid i \in I)$ e para cada $i \in I$ considere π_i a aplicação projeção de C para X_i. Defina o seguinte conjunto*

$$X = \{c \in C \mid \varphi_{ij}\pi_j(c) = \pi_i(c) \text{ para todos } i, j \text{ com } j \geqslant i\}$$

e $\varphi_i = \pi_i|_X$ para cada $i \in I$. Então (X, φ_i) é um limite inverso de (X_i, φ_{ij});
(iii) *se (X_i, φ_{ij}) é um sistema inverso de grupos topológicos e homomorfismos*

contínuos, então X é um grupo topológico e as aplicações φ_i são homomorfismos contínuos.

Demonstração. Vamos mostrar o item (i). De fato, primeiramente aplicando a propriedade universal de $(X^{(1)}, \varphi_i^{(1)})$ a família $(\varphi_i^{(2)})$ de funções compatíveis, temos que existe uma única aplicação contínua (homomorfismo contínuo res.) $\psi : X^{(2)} \longrightarrow X^{(1)}$ tal que para cada $i \in I$ tem-se $\varphi_i^{(1)}\psi = \varphi_i^{(2)}$. Analogamente, aplicando a propriedade universal de $(X^{(2)}, \varphi_i^{(2)})$ a família $(\varphi_i^{(1)})$ de funções compatíveis, obtemos que existe uma única aplicação contínua (homomorfismo contínuo res.) $\phi : X^{(1)} \longrightarrow X^{(2)}$ tal que para cada $i \in I$ tem-se $\varphi_i^{(2)}\phi = \varphi_i^{(1)}$. Novamente, aplicando a propriedade universal de $(X^{(1)}, \varphi_i^{(1)})$ a família $(\varphi_i^{(1)})$ de funções compatíveis, existe uma única aplicação contínua $\gamma : X^{(1)} \longrightarrow X^{(1)}$ tal que para cada $i \in I$ tem-se

$$\varphi_i^{(1)}\gamma = \varphi_i^{(1)}. \tag{4.3.1}$$

Note que $\psi\phi$ e $Id_{X^{(1)}}$ satisfazem (4.3.1). Logo, segue da unicidade de γ que $\psi\phi = Id_{X^{(1)}}$. De modo análogo, tem-se que $\phi\psi = Id_{X^{(2)}}$. Portanto, concluímos que ϕ é um homeomorfismo (isomorfismo topológico res.).

Agora, mostraremos o item (ii). Sejam Y um espaço topológico e uma família compatível $\{\psi_i : Y \longrightarrow X_i\}$ de aplicações contínuas. Vamos mostrar que existe uma única aplicação contínua $\psi : Y \longrightarrow X$ tal que $\varphi_i\psi = \psi_i$ para cada $i \in I$.

Com efeito, consideremos a aplicação $\overline{\psi} : Y \longrightarrow C$ que leva cada y no vetor $(\psi_i(y))$. Então, $\pi_i\overline{\psi} = \psi_i$ para cada $i \in I$, pois seja $y \in Y$ temos

$$(\pi_i\overline{\psi})(y) = \pi_i(\overline{\psi}(y)) = \pi_i((\psi_i(y))) = \psi_i(y).$$

Assim, obtemos que $\overline{\psi}$ é contínua. Se $j \geqslant i$, tem-se

$$\pi_i\overline{\psi} = \psi_i = \varphi_{ij}\psi_j = \varphi_{ij}\pi_j\overline{\psi},$$

pois como $\{\psi_i : Y \longrightarrow X_i\}$ é uma família compatível temos $\varphi_{ij}\psi_j = \psi_i$. Daí, concluímos que $\varphi_{ij}\pi_j\overline{\psi} = \psi_i$.

Disto segue que $\overline{\psi}$ leva Y em X. Assim, definamos $\psi : Y \longrightarrow X$ por $\psi(y) = \overline{\psi}(y)$ para cada $y \in Y$. Então, ψ é contínua, pois $\overline{\psi}$ o é, e claramente temos que $\varphi_i\psi = \psi_i$, para cada $i \in I$. Por outro lado, seja $\psi' : Y \longrightarrow X$ uma aplicação satisfazendo $\varphi_i\psi' = \psi_i$ para cada $i \in I$ e $y \in Y$. Assim, usando isto e que $\varphi_i\psi = \psi_i$ para cada $i \in I$, obtemos que a componente de $\psi'(y)$ em X_i é $\psi_i(y)$ para cada $i \in I$, portanto segue que as aplicações ψ' e ψ são iguais. Desta maneira,

ψ é a única aplicação, com a propriedade desejada. Logo, temos que (X, φ_i) é um limite inverso de (X_i, φ_{ij}).

O item (iii) segue do item (ii). $\square$

Pelo resultado anterior, como o limite inverso é único a menos de homeomorfismos (isomorfismos), falaremos do limite inverso de um sistema inverso (X_i, φ_{ij}) e vamos denota-lo por $\varprojlim(X_i, \varphi_{ij})$ ou por $\varprojlim_{i \in I} X_i$ ou simplesmente por $\varprojlim X_i$. Em alguns casos, é mais útil considerar o particular limite inverso, construído no item (ii) da proposição anterior e ele será denotado por $s \varprojlim X_i$.

Vamos voltar ao Exemplo 4.3.2 e determinar usando a Proposição 4.3.6 o limite inverso do sistema inverso (X_i, φ_{ij}).

Sejam $C = \mathrm{Cr}(X_i \mid i \in I)$, $\pi_i : C \longrightarrow X_i$ a aplicação projeção, como na Proposição 4.3.6 definamos o conjunto X,

$$X = \{c \in C \mid \varphi_{ij}\pi_j(c) = \pi_i(c) \text{ para todos } i, j \text{ com } j \geqslant i\}.$$

Vamos ver quem são os elementos de X. Seja $c \in C$, então obtemos que $c = (x_1, x_2, x_3, \ldots)$ com $x_i \in X_i$. Suponhamos que $c \in X$, logo c satisfaz

$$\varphi_{12}\pi_2(c) = \cdots = \varphi_{1j}\pi_j(c), \qquad j \geqslant 1.$$

Por outro lado, note que

$$\varphi_{12}\pi_2(c) = \pi_1(c) = \varphi_{11}\pi_1(c).$$

Portanto,

$$\pi_1(c) = \varphi_{12}\pi_2(c) = \cdots = \varphi_{1j}\pi_j(c), \qquad j \geqslant 1. \tag{4.3.2}$$

De modo análogo, concluímos para todo $i \geqslant 1$ que

$$\pi_i(c) = \varphi_{i2}\pi_2(c) = \cdots = \varphi_{ij}\pi_j(c), \qquad j \geqslant 1. \tag{4.3.3}$$

Agora, note que se $c \in C$ satisfaz (4.3.2), então segue que $\pi_1(c) = 1$, desta forma temos

$$1 = \varphi_{12}\pi_2(c) = \cdots = \varphi_{1j}\pi_j(c), \qquad j \geqslant 1. \tag{4.3.4}$$

Assim, por exemplo, o elemento $c = (1, 1, 1, \ldots) \in X$. Pois, satisfaz (4.3.4) e todas as demais condições. Em contrapartida o elemento $d = (1, 2, 1, 1, \ldots) \notin X$. Pois, não satisfaz (4.3.3) para $i = 2$, uma vez que $\varphi_{23}\pi_3(d) = 1$ e $\pi_2(d) = 2$.

Não é difícil ver que os elementos de X são da seguinte forma:

$$(1, 1, \ldots), (1, 2, 2, \ldots), (1, 2, 3, 3, \ldots), \ldots \text{etc.}$$

Por outro lado, consideremos o desenho do Exemplo 4.3.2, olhando o mesmo, imagine partir de 1 em baixo a esquerda e seguir "em sentido invertido das setas", conforme mostra a figura a seguir, fazendo todos os possíveis caminhos, obtemos todos os elementos do limite inverso de (X_i, φ_{ij}) que são essas n-uplas infinitas.

$$
\begin{tikzcd}
 & & & & & & & ? \arrow[dll, dotted] \\
 & & & & & 6 \arrow[dl] & {} \arrow[l, dotted] & (1,2,3,4,5,6,6,\ldots) \\
 & & & & 5 \arrow[dl] & 5 \arrow[l] & {} \arrow[l, dotted] & (1,2,3,4,5,5,\ldots) \\
 & & & 4 \arrow[dl] & 4 \arrow[l] & 4 \arrow[l] & {} \arrow[l, dotted] & (1,2,3,4,4,\ldots) \\
 & & 3 \arrow[dl] & 3 \arrow[l] & 3 \arrow[l] & 3 \arrow[l] & {} \arrow[l, dotted] & (1,2,3,3,\ldots) \\
 & 2 \arrow[dl] & 2 \arrow[l] & 2 \arrow[l] & 2 \arrow[l] & 2 \arrow[l] & {} \arrow[l, dotted] & (1,2,2,\ldots) \\
1 & 1 \arrow[l] & 1 \arrow[l] & 1 \arrow[l] & 1 \arrow[l] & 1 \arrow[l] & {} \arrow[l, dotted] & (1,1,\ldots)
\end{tikzcd}
$$

O seguinte resultado descreve a relação entre as principais propriedades topológicas e o conceito de limite inverso. A prova deste resultado pode ser encontrada em [**25**, Proposition 1.1.5].

Proposição 4.3.7. *Seja (X_i, φ_{ij}) um sistema inverso, indexado por I e denotamos por $X = \varprojlim X_i$. As seguintes afirmações são verdadeiras:*
(i) *se cada X_i é Hausdorff, então X é Hausdorff;*
(ii) *se cada X_i é totalmente desconexo, então X é totalmente desconexo;*
(iii) *se cada X_i é Hausdorff, então $s\varprojlim X_i$ é fechado no produto cartesiano $C = \mathrm{Cr}(X_i \mid i \in I)$;*
(iv) *se cada X_i é compacto e Hausdorff, então X é compacto e Hausdorff;*
(v) *se cada X_i é um espaço Hausdorff compacto não vazio, então X é não vazio.*

Finalizamos esta seção com uma proposição que nos mostra, entre outras coisas, como podemos verificar que um dado subconjunto do limite inverso de um sistema inverso é denso. A demonstração da mesma pode ser encontrada em [**25**, Proposition 1.1.6].

Proposição 4.3.8. *Seja (X, φ_i) um limite inverso de um sistema inverso (X_i, φ_{ij}) de espaços compactos, Hausdorff e não vazios, indexado por I. As seguintes afirmações valem:*

(i) $\varphi_i(X) = \bigcap_{j \geqslant i} \varphi_{ij}(X_j)$ *para cada* $i \in I$*;*
(ii) *os conjuntos* $\varphi_i^{-1}(U)$*, com* $i \in I$ *e* U *aberto em* X_i*, formam uma base para a topologia em* X*;*
(iii) *se* Y *é um subconjunto de* X *satisfazendo* $\varphi_i(Y) = X_i$ *para cada* $i \in I$*, então* Y *é denso em* X*;*
(iv) *se* θ *é uma aplicação de um espaço* Y *em* X*, então* θ *é contínua se, e somente se, cada aplicação* $\varphi_i\theta$ *é contínua.*

4.4. Caracterização de Grupos Profinitos

Nesta seção iremos finalmente definir grupos profinitos em termos de limite inverso e também obter caracterizações dos mesmos, que serão usadas ao longo desta dissertação.

Seja G um grupo topológico, escreveremos $H \leqslant G$ para denotar que H é um subgrupo fechado de G e $N \leq_\circ G$ para indicar que N é um subgrupo aberto de G.

Dizemos que uma família I de subgrupos normais de um grupo arbitrário G é uma *base filtrada* se para todos $K_1, K_2 \in I$ existe um subgrupo $K_3 \in I$ tal que $K_3 \subseteq K_1 \cap K_2$.

Os próximos dois resultados são técnicos e serão utilizados na caracterização de grupos profinitos. A demonstração dos mesmos pode ser encontrada em [**25**, Proposition 1.2.1] e [**25**, Proposition 1.2.2] respectivamente.

Proposição 4.4.1. *Sejam* (G, φ_i) *um limite inverso de um sistema inverso* (G_i) *de grupos topológicos compactos e de Hausdorff, e* $L \lhd_\circ G$*. Então,* $ker\varphi_i \leqslant L$ *para algum* i*. Assim,* G/L *é isomorfo, como grupo topológico, a um grupo quociente de um subgrupo de algum* G_i*. Se além disso, cada aplicação* φ_i *é sobrejetiva, então* G/L *é isomorfo a um grupo quociente de algum* G_i*.*

Proposição 4.4.2. *Sejam* G *um grupo topológico e* I *uma base filtrada de subgrupos normais fechados. Para todos* $K, L \in I$ *definamos* $K \leqslant' L$ *se, e somente se,* $L \leqslant K$*. Então,* I *é dirigido com respeito a ordem* $\leqslant'$ *e os homomorfismos sobrejetivos* $q_{KL} : G/L \longrightarrow G/K$*, definidos para* $K \leqslant' L$*, tornam os grupos quocientes* G/K *um sistema inverso. Denotemos por* $(\widehat{G}, \varphi_k) = \varprojlim G/K$*. Existe um homomorfismo contínuo* $\theta : G \longrightarrow \widehat{G}$ *tal que:*
(i) $ker(\theta) = \bigcap_{K \in I} K$*;*
(ii) *a imagem* $\theta(G)$ *é um subgrupo denso de* $\widehat{G}$*;*
(iii) *a aplicação composta* $\varphi_k\theta$ *é a aplicação quociente de* G *em* G/K *para cada* $K \in I$*;*

(iv) *se G é compacto, então θ é sobrejetora;*
(v) *se G é compacto e $\bigcap_{K\in I} K = 1$, então θ é um isomorfismo de grupos topológicos, ou seja, um isomorfismo de grupos e um homeomorfismo.*

Uma *classe* $\mathcal{C}$ de grupos finitos é uma família de grupos finitos fechada por imagens isomórficas, isto é, se $F_1 \in \mathcal{C}$ e $F_1 \cong F_2$, então $F_2 \in \mathcal{C}$.

Dizemos que uma *classe* $\mathcal{C}$ de grupos finitos é fechada: para subgrupos, se cada subgrupo de um $\mathcal{C}$-grupo é um $\mathcal{C}$-grupo; para quocientes, se cada grupo quociente de um $\mathcal{C}$-grupo é um $\mathcal{C}$-grupo e para produto direto finito de seus elementos, se $F_1, F_2 \in \mathcal{C}$, então $F_1 \times F_2 \in \mathcal{C}$.

Dada uma classe $\mathcal{C}$ de grupos finitos, dizemos que um grupo F é um *$\mathcal{C}$-grupo* se $F \in \mathcal{C}$. Chamamos G um *grupo pro-$\mathcal{C}$* se G é um limite inverso de $\mathcal{C}$-grupos, assim por exemplo, um limite inverso de p-grupos finitos é chamado um grupo pro-p. Observe que um $\mathcal{C}$-grupo é sempre um grupo pro-$\mathcal{C}$, pois basta considerarmos um sistema inverso com respeito a um conjunto dirigido com somente um elemento.

O teorema a seguir nos mostra algumas caracterizações de grupos pro-$\mathcal{C}$.

Teorema 4.4.3. *Sejam $\mathcal{C}$ uma classe de grupos finitos que é fechada para subgrupos e produtos diretos e G um grupo topológico. As seguintes afirmações são equivalentes.*
(i) *G é um grupo pro-$\mathcal{C}$.*
(ii) *G é isomorfo, como grupo topológico, a um subgrupo fechado de um produto cartesiano de $\mathcal{C}$-grupos.*
(iii) *G é compacto e $\bigcap\{N \mid N \lhd_\circ G, G/N \in \mathcal{C}\} = 1$.*
(iv) *G é compacto e totalmente desconexo, e para cada $L \lhd_\circ G$ existe um subgrupo $N \lhd_\circ G$ com $N \leqslant L$ e $G/N \in \mathcal{C}$.*
Se além disso, $\mathcal{C}$ é fechada para quocientes, então o item (iv) *pode ser substituído por*
(iv)$'$ *G é compacto e totalmente desconexo, e $G/L \in \mathcal{C}$ para cada $L \lhd_\circ G$.*

Demonstração. Como cada G_i é finito e estamos considerando a topologia discreta, temos que cada G_i é Hausdorff, compacto e totalmente desconexo. Agora, por hipótese, como G é um grupo pro-$\mathcal{C}$, temos que $G = \varprojlim_{i\in I} G_i$, onde cada G_i é um $\mathcal{C}$-grupo. Por G ser um grupo topológico, temos que cada G_i é também um grupo topológico. Uma vez que cada G_i é Hausdorff, segue pela Proposição 4.3.7 item (iii) que $s\varprojlim G_i$ é fechado no produto cartesiano de $\mathrm{Cr}(G_i \mid i \in I)$. Agora como $G \cong s\varprojlim G_i$, isto mostra que (i) implica (ii).

Vamos provar que (ii) implica (iii). Por hipótese, G é isomorfo a um subgrupo fechado $\widehat{G}$ de $C = \mathrm{Cr}(G_i \mid i \in I)$ onde cada G_i é um $\mathcal{C}$-grupo. Desta maneira, para cada $i \in I$ denotamos por K_i o núcleo da aplicação projeção de C em G_i. Segue que $K_i \lhd_\circ C$ para cada $i \in I$, uma vez que a projeção é contínua. Assim, como cada G_i é compacto, temos pelo Teorema 4.1.3 item (iii) que C é compacto. Deste modo, $\widehat{G}$ é compacto, pela Proposição 4.1.1 item (i). Logo, obtemos que G é compacto. Agora, para cada $i \in I$, escrevemos $N_i = K_i \cap \widehat{G}$. Como $K_i \lhd_\circ C$, temos que $N_i \lhd_\circ \widehat{G}$. Do fato que $\bigcap_{i \in I} K_i = 1$, segue que $\bigcap_{i \in I} N_i = 1$. Além disso, pelos teoremas de isomorfismo tem-se

$$\widehat{G}/N_i \cong \widehat{G}K_i/K_i \leqslant C/K_i \cong G_i.$$

e portanto $\widehat{G}/N_i \in \mathcal{C}$ para cada $i \in I$ e o resultado segue.
Provaremos que (iii) implica (i). Com efeito, escrevemos $I = \{N \lhd_\circ G \mid G/N \in \mathcal{C}\}$. Sejam $N_1, N_2 \in I$ e consideremos a aplicação f de G ao $\mathcal{C}$-grupo $G/N_1 \times G/N_2$ definida por $g \longmapsto (N_1 g, N_2 g)$. Vejamos que f é contínua. Com efeito, dado U aberto de $G/N_1 \times G/N_2$, temos que $f^{-1}(U) \subseteq G$ é aberto, pois G pode ser pensado com a topologia discreta. É fácil ver que f é um homomorfismo com núcleo $ker(f) = N_1 \cap N_2$. Assim $N_1 \cap N_2 \lhd_\circ G$ e

$$G/(N_1 \cap N_2) \cong Im(f) \leqslant G/N_1 \times G/N_2.$$

Como $G/N_1 \times G/N_2$ é um $\mathcal{C}$-grupo e $\mathcal{C}$ é fechada para subgrupos, obtemos que $G/(N_1 \cap N_2) \in \mathcal{C}$, logo segue $N_1 \cap N_2 \in I$. Observe que I é uma base filtrada, então aplicando a Proposição 4.4.2 concluímos que $G \cong \varprojlim_{N \in I} G/N$. Logo, G é um grupo pro-$\mathcal{C}$, como queríamos.

Por outro lado, segue pela Proposição 4.3.7, que G é compacto e totalmente desconexo, e para cada $L \lhd_\circ G$, usando a Proposição 4.4.1, temos que existe $N = ker\pi_i \lhd_\circ G$ para algum $i \in I$, com $N \leqslant L$ e $G/N \cong Im\pi_i = G_i$, assim $G/N \in \mathcal{C}$, isso mostra que (i) implica (iv).

A afirmação que (iv) implica (iii) segue da Proposição 4.2.5 item (iii).

Por fim, suponhamos que $\mathcal{C}$ seja fechada para quocientes. Assim, pela Proposição 4.4.1 temos que, para cada $L \lhd_\circ G$, existe $N \lhd_\circ G$ com $N \leqslant L$ e $G/N \in \mathcal{C}$ e, como $G/L \cong (G/N)/(L/N)$, podemos concluir que $G/L \in \mathcal{C}$, como desejado. $\square$

Desta forma considerando $\mathcal{C}$ como sendo a classe de *todos os grupos finitos*, temos imediatamente do teorema anterior uma caracterização para os grupos profinitos.

Corolário 4.4.4. *Seja G um grupo topológico. As seguintes afirmação são equivalentes.*
(i) *G é profinito.*
(ii) *G é isomorfo, como grupo topológico, a um subgrupo fechado de um produto Cartesiano de grupos finitos.*
(iii) *G é compacto e $\bigcap\{N \mid N \lhd_{\circ} G\} = 1$.*
(iv) *G é compacto e totalmente desconexo.*

O próximo teorema descreve como um grupo profinito, seus subgrupos e grupos quocientes podem ser pensados explicitamente como limites inversos.

Teorema 4.4.5. *As seguintes afirmações são verdadeiras:*
(i) *seja G um grupo profinito. Se I é uma base filtrada de subgrupos normais fechados de G tal que $\bigcap\{N \mid N \in I\} = 1$, então*

$$G \cong \varprojlim_{N \in I} G/N.$$

Além disso,

$$H \cong \varprojlim_{N \in I} H/(H \cap N),$$

para cada subgrupo fechado H de G e

$$G/K \cong \varprojlim_{N \in I} G/NK,$$

para cada subgrupo normal fechado K de G.
(ii) *se $\mathcal{C}$ é uma classe de grupos finitos que é fechada para subgrupos e produtos diretos, então subgrupos fechados, produtos Cartesianos e limites inversos de grupos pro-$\mathcal{C}$ são grupos pro-$\mathcal{C}$. Se além disso, $\mathcal{C}$ é fechada para quocientes, então grupos quocientes de grupos pro-$\mathcal{C}$ por subgrupos normais fechados são grupos pro-$\mathcal{C}$.*

Demonstração. Vamos mostrar o item (i). Vejamos primeiramente que $G \cong \varprojlim_{N \in I} G/N$. De fato, como G é profinito, segue que G é um grupo topológico, e por hipótese, I é uma base filtrada de subgrupos normais fechados de G. Então, aplicando a Proposição 4.4.2 a G, obtemos que $\widehat{G} = \varprojlim_{N \in I} G/N$ e um homomorfismo contínuo $\theta : G \longrightarrow \widehat{G}$. Novamente, pela hipótese, $\bigcap_{N \in I} N = 1$ e sabendo que G é compacto pelo Corolário 4.4.4, segue pela Proposição 4.4.2 item (v), que $G \cong \widehat{G} = \varprojlim_{N \in I} G/N$.

Por outro lado, mostraremos que $H \cong \varprojlim_{N \in I} H/(H \cap N)$, para H subgrupo fechado. Com efeito, por G ser um grupo topológico, temos que H também é um grupo topológico. Assim, consideremos o conjunto $S = \{H \cap N \mid N \in I\}$. Note que S é uma base filtrada de subgrupos normais fechados de H, então aplicando a Proposição 4.4.2 a H, obtemos que $\widehat{H} = \varprojlim_{N\in I} H/(H\cap N)$ e um homomorfismo contínuo $\theta : H \longrightarrow \widehat{H}$. Por outro lado, uma vez que $\bigcap_{N\in I} N = 1$, obtemos $\bigcap_{N\in I}(H\cap N) = 1$ e sabendo que H é compacto pelo Corolário 4.4.4, segue pela Proposição 4.4.2 item (v), que $H \cong \widehat{H} = \varprojlim_{N\in I} H/(H\cap N)$.

Por fim, consideremos a família $J = \{NK \mid N \in I\}$, temos que J é uma base filtrada de subgrupos normais fechados de G contendo K. Usando a Proposição 4.2.3 item (iv) obtemos

$$\bigcap\{M \mid M \in J\} = \bigcap\{NK \mid N \in I\} = \left(\bigcap\{N \mid N \in I\}\right) K = K.$$

Agora consideremos φ o epimorfismo canônico de G em G/K. Daí, podemos trabalhar no quociente G/K e assumir que $K = 1$. Como G é um grupo topológico, temos pela Proposição 4.2.3 item (ii) que G/K é também um grupo topológico. Por outro lado, consideremos o conjunto $\varphi(J) = \{NK/K \mid N \in I\}$, temos que $\varphi(J)$ é uma base filtrada de subgrupos normais fechados de G/K. Assim, aplicando a Proposição 4.4.2 a G/K e o terceiro teorema do isomorfismo, temos que

$$\widehat{(G/K)} = \varprojlim_{N\in I} \frac{G/K}{NK/K} \cong \varprojlim_{N\in I} G/NK.$$

Assim, desde que $\bigcap_{N\in I} NK = K$, segue que $\bigcap_{N\in I} NK/K = K$. Logo, novamente pela Proposição 4.2.3 item (iv), obtemos que

$$G/K \cong \widehat{(G/K)} = \varprojlim_{N\in I} \frac{G/K}{NK/K} \cong \varprojlim_{N\in I} G/NK.$$

e a afirmação segue.

Não vamos dar os detalhes da prova do item (ii), que podem ser encontrados em [**25**, Theorem 1.2.5], somente observamos que o item (ii) é consequência do item (i) e de propriedades topológicas vistas antes. □

O teorema a seguir de natureza topológica é uma ferramenta muito útil para trabalhar no contexto de grupos profinitos. Os detalhes da demonstração podem ser encontrados em [**9**, Theorem 35].

Teorema 4.4.6 (de Categoria de Baire). *Se G é um espaço Hausdorff localmente compacto e $\{A_i \mid i \in \mathbb{N}\}$ é uma família enumerável de conjuntos fechados tal que $G = \bigcup_{i\in\mathbb{N}} A_i$, então pelo menos um subconjunto A_i contém um conjunto aberto não vazio.*

Obviamente podemos dar uma reformulação imediata do resultado anterior para um grupo profinito G: se um grupo profinito é tal que $G = \bigcup_{i \in \mathbb{N}} A_i$, onde A_i são conjuntos fechados, então pelo menos um A_i contém um conjunto aberto não vazio.

O resultado a seguir é uma consequência direta do Teorema 4.4.6 e nos fornece uma útil observação.

Lema 4.4.7. *Sejam G um grupo profinito e $\{A_i \mid i \in \mathbb{N}\}$ uma família enumerável de conjuntos fechados tal que $G = \bigcup\limits_{i \in \mathbb{N}} A_i$. Então, existem um inteiro n, um elemento g em G e um subgrupo aberto H de G tal que $gH \subseteq A_n$.*

Demonstração. Como G é profinito, temos que G é Hausdorff e pelo Corolário 4.4.4 segue que G é compacto. Agora, por hipótese $G = \bigcup\limits_{i \in \mathbb{N}} A_i$ e assim segue, do Teorema 4.4.6, que existe um inteiro n tal que A_n contém um conjunto aberto não vazio U. Então, existe $g \in U$ e por U ser aberto, tem-se que $g^{-1}U$ é aberto. Agora, pela Proposição 4.1.1 item (vi) temos que $g^{-1}U = \bigcup S_i$, onde cada S_i é simultaneamente aberto e fechado. Como $1 \in g^{-1}U$, existe um inteiro m tal que $1 \in S_m$. Desta forma, usando o Lema 4.2.4, obtemos que existe $H \lhd_o G$ tal que $H \subseteq S_m$. Logo, $H \subseteq g^{-1}U$. Em particular, temos que $gH \subseteq U \subseteq A_n$ e o resultado segue. $\square$

Concluímos esta seção definindo os conceitos de transversais de subgrupos abertos e fechados de um grupo profinito.

Sejam G um grupo profinito e H um subgrupo fechado de G. Um *transversal à direita* de H em G é um conjunto fechado contendo um único elemento de cada classe lateral Hg de H em G. De modo análogo define-se o conceito de transversal à esquerda. Desta maneira, dizemos que S é um transversal à direita se, e somente se, S é fechado, G pode ser escrito da forma $G = HS$ e sempre que $s_1, s_2 \in S$ tais que $Hs_1 = Hs_2$, então $s_1 = s_2$. Vamos considerar apenas transversais à direita e chamaremos a estes de transversais.

Sabemos que, em um grupo profinito G, os subconjuntos finitos de G são fechados, pois como G é Hausdorff, temos que para cada $x \in G$ o conjunto $\{x\}$ é fechado, e portanto qualquer subconjunto finito A de G, pode ser escrito como $A = \bigcup\limits_{i=1}^{|A|} \{x_i\}$ com $x_i \in G$, o que mostra que A é fechado. Desta forma, é claro que para subgrupos abertos de G temos a existência de transversais.

Uma pergunta relevante seria se para subgrupos fechados de G sempre existem transversais. A resposta é afirmativa. Mas antes de garantirmos tal existência, precisamos definir uma versão relativa da noção de um transversal. Isto é, uma definição de transversal que depende de um outro subgrupo dado.

Sejam M e H subgrupos fechados de um grupo profinito G tais que $M \leqslant H$. Um *transversal* para H mod M em G é um subconjunto fechado S que é uma união de classes laterais da forma Mg e que satisfaz as seguintes condições:
(i) $G = HS$;
(ii) se $s_1, s_2 \in S$ com $Hs_1 = Hs_2$, então $s_1 s_2^{-1} \in M$.

Os dois próximos resultados nos permitem garantir a existência de transversais para um qualquer subgrupo fechado. A demonstração do primeiro pode ser vista em [**25**, Lemma 1.3.1].

Lema 4.4.8. *Sejam M e H subgrupos fechados de G tais que $M \leqslant H$ e S um transversal para H mod M. Considere $N \lhd_\circ G$ e $\widehat{M} = M \cap N$ e suponha que $\{g_1, \ldots, g_r\}$ seja um transversal para MN em G. Defina $S_i = Ng_i \cap S$ para $i \leqslant r$ e $\widehat{S} = S_1 \cup \cdots \cup S_r$. Então, $\widehat{S}$ é um transversal para H mod $\widehat{M}$.*

Finalizamos esta seção com uma proposição que nos garante que sempre existem transversais para subgrupos fechados.

Proposição 4.4.9. *Se H é um subgrupo fechado de G, então existe um transversal S para H tal que $1 \in S$.*

Demonstração. Usaremos o Lema de Zorn (veja [**9**, 25 Theorem, pág.33]). Mas para isto, vamos primeiramente construir o conjunto parcialmente ordenado. Consideremos I o conjunto dos pares (M, S) com $M \leq H$ e S um transversal para H mod M. Notemos que $I \neq \varnothing$, pois claramente $(H, G) \in I$. Agora, definamos a seguinte ordem em I, $(M_1, S_1) \leq (M_2, S_2)$ se, e somente se, $M_1 \geqslant M_2$ e $S_1 \supseteq S_2$. Seja C uma cadeia em I e defina

$$M_0 = \bigcap\{M \mid (M, S) \in C\}, \quad S_0 = \bigcap\{S \mid (M, S) \in C\}.$$

Vejamos que $(M_0, S_0) \in I$. De fato, como cada S é fechado, tem-se que S_0 é fechado. E S_0 é uma união de classes laterais de M_0. Pois, se $s \in S_0$, segue pela definição de M_0 e S_0 que $M_0 s \subseteq MS \subseteq S$, para todo $(M, S) \in C$ de modo que $M_0 s \subseteq \bigcap S = S_0$. Por outro lado, pela Proposição 4.2.3 item (iv) temos $HS_0 = H(\bigcap S) = \bigcap(HS) = G$. Agora, se $s_1, s_2 \in S_0$ e $Hs_1 = Hs_2$, então segue pela hipótese que $s_1 s_2^{-1} \in M$ para todo $(M, S) \in C$. Assim, $s_1 s_2^{-1} \in \cap M = M_0$. Então, concluímos que $(M_0, S_0) \in I$. Note que (M_0, S_0) é um limite superior para a cadeia C. Portanto, pelo Lema de Zorn, I possui elemento maximal e denotamos tal elemento por (M, S'). Se $M \neq 1$, então existe um subgrupo $N \triangleleft_{\circ} G$ tal que $\widehat{M} = N \cap M \neq M$, assim usando o Lema 4.4.8, podemos construir $\widehat{S}$ e teremos que $(\widehat{M}, \widehat{S}) > (M, S')$, o que é um absurdo, pois (M, S') é o elemento maximal. Então, tem-se que $M = 1$ e assim, segue que S' é um transversal para H. Por outro lado, seja $S' \cap H = \{h\}$, o conjunto $S = h^{-1}S'$ é também um transversal para H em G e temos que $1 \in S$, como desejado. $\square$

4.5. Completamentos de Grupos

Nesta seção vamos querer construir grupos profinitos a partir de grupos abstratos. Para isto precisaremos introduzir o conceito de completamento de um grupo, ressaltaremos suas principais propriedades e construíremos exemplos de dois tipos de completamento de um grupo abstrato.

Consideremos G um grupo abstrato e I uma base filtrada não vazia de subgrupos normais de índice finito. Podemos tornar G um grupo topológico, basta definirmos quem são os abertos da topologia, isto é, dizemos que um subconjunto de G é aberto se, e somente se, é uma união de classes laterais Kg com K um qualquer subgrupo em I. Com esta definição de topologia, G torna-se um grupo topológico. Observamos que se $K_1, K_2 \in I$, então a interseção $K_1g_1 \cap K_2g_2$, com $g_1, g_2 \in G$ ou é vazia ou é uma classe lateral do subgrupo $K_1 \cap K_2$.

O *completamento* de G com respeito à I é um par $(\widehat{G}, j)$, onde $\widehat{G}$ é um grupo profinito e j é um homomorfismo contínuo de G em $\widehat{G}$ que satisfaz a seguinte propriedade: sempre que $\theta : G \longrightarrow H$ é um homomorfismo contínuo, com H sendo um grupo finito, existe um único homomorfismo contínuo $\widehat{\theta} : \widehat{G} \longrightarrow H$ tal que $\theta = \widehat{\theta}j$, ou seja, tal que o diagrama abaixo

$$\begin{tikzcd} G \arrow[r, "j"] \arrow[d, "\theta"'] & \widehat{G} \arrow[dl, dashed, "\widehat{\theta}"] \\ H & \end{tikzcd}$$

comuta.

O próximo resultado nos mostra um exemplo de como construir um completamento de um grupo abstrato G, sua demonstração pode ser encontrada em [**25**, Proposition 1.4.1]. Lembramos que I denota uma base filtrada não vazia de subgrupos normais de índice finito em G.

Proposição 4.5.1. *Sejam $\widehat{G} = s\varprojlim_I G/K$ e j a aplicação de G em $\widehat{G}$ definida por $g \longmapsto (Kg)$. Então, o par $(\widehat{G}, j)$ possui as propriedades do completamento de G com respeito a I.*

Nosso objetivo agora é mostrar que o completamento de G com respeito a I é unicamente determinado, mas para isto precisamos dar uma formulação diferente do conceito de completamento, em termos de uma propriedade universal. A proposição a seguir nos mostra como fazemos isto. Os detalhes da demonstração da mesma podem ser encontrados em [**25**, Proposition 1.4.2].

Proposição 4.5.2. *Sejam G e I como acima e suponha que $\widehat{G}$ é um grupo profinito e $j : G \longrightarrow \widehat{G}$ um homomorfismo contínuo. Então, as seguintes afirmações são equivalentes.*
(i) *O par $(\widehat{G}, j)$ possui a propriedade que define um completamento de G com respeito a I.*
(ii) *Para cada diagrama*

$$\begin{tikzcd} G \arrow[rr, "\theta"] \arrow[dr, "j"'] & & H \\ & \widehat{G} & \end{tikzcd}$$

onde H é um grupo profinito e θ é um homomorfismo contínuo, existe um único homomorfismo contínuo $\widehat{\theta} : \widehat{G} \longrightarrow H$ que torna o diagrama a seguir comutativo.

$$\begin{tikzcd} G \arrow[rr, "\theta"] \arrow[dr, "j"'] & & H \\ & \widehat{G} \arrow[ur, dashed, "\widehat{\theta}"'] & \end{tikzcd}$$

O próximo resultado nos garante que o completamento de G com respeito a I é único a menos de isomorfismo.

Proposição 4.5.3. *Se $(\widehat{G_1}, j_1)$ e $(\widehat{G_2}, j_2)$ são completamentos de G com respeito a I, então existe um isomorfismo $\alpha : \widehat{G_1} \longrightarrow \widehat{G_2}$ satisfazendo $\alpha j_1 = j_2$.*

Demonstração. Considerando o completamento $(\widehat{G_1}, j_1)$ e o homomorfismo contínuo $j_2 : G \longrightarrow \widehat{G_2}$ temos, pela Proposição 4.5.2, que existe um único homomorfismo contínuo $\alpha : \widehat{G_1} \longrightarrow \widehat{G_2}$ tal que $\alpha j_1 = j_2$. De modo análogo, considerando $(\widehat{G_2}, j_2)$ como completamento de G e o homomorfismo contínuo $j_1 : G \longrightarrow \widehat{G_1}$, obtemos a existência do homomorfismo contínuo $\beta : \widehat{G_2} \longrightarrow \widehat{G_1}$ tal que $\beta j_2 = j_1$. Assim, fazendo algumas substituições tem-se que $j_1 = (Id_{\widehat{G_1}})j_1 = (\beta\alpha)j_1$. Agora considerando o completamento $(\widehat{G_1}, j_1)$ e o homomorfismo contínuo $j_1 : G \longrightarrow \widehat{G_1}$, temos que existe um único homomorfismo contínuo γ satisfazendo $\gamma j_1 = j_1$. Então, segue que $\beta\alpha = Id_{\widehat{G_1}}$. Analogamente, considerando o completamento $(\widehat{G_2}, j_2)$ obtemos $\alpha\beta = Id_{\widehat{G_2}}$. Portanto, segue que α é um isomorfismo, como queríamos. $\square$

A proposição a seguir é uma consequência imediata de resultados desta seção e da Proposição 4.4.1.

Proposição 4.5.4. *Seja $(\widehat{G}, j)$ o completamento de G com respeito a I. Então, as seguintes afirmações valem:*
(i) *a imagem $j(G)$ é densa em $\widehat{G}$;*
(ii) *$ker j = \bigcap_{K \in I} K$.*

Demonstração. Vamos provar o item (i). Usando as Proposições 4.5.1 e 4.5.3 e considerando $\widehat{G} = s \varprojlim G/K$ e a aplicação j definida por $g \longmapsto (Kg)$, o resultado segue da Proposição 4.4.1.

Agora, mostraremos o item (ii). Veja que um elemento g pertencente ao $ker j$, se e somente se, $j(g) = (K)$ para cada K em I, ou seja, se $Kg = K$. Segue que $g \in K$ para todo $K \in I$ e portanto $ker j = \bigcap_{K \in I} K$. $\square$

A seguir vamos abrir um parêntesis para lembrar o conceito de grupo residualmente finito e algumas propriedades básicas relevantes para o nosso estudo.

Um grupo abstrato G é dito *residualmente finito* se, para cada $g \neq 1$ em G, existe um subgrupo $N_g \lhd G$ tal que $g \notin N_g$ e G/N_g é finito.

A seguir veremos uma caracterização bastante útil de grupo residualmente finito.

Proposição 4.5.5. *Um grupo G é residualmente finito se, e somente se, a interseção de todos os subgrupos normais de G de índices finitos é trivial.*

Demonstração. Suponhamos que G seja residualmente finito. Consideremos I o conjunto de todos os subgrupos normais de índice finito em G e seja $H = \bigcap_{N \in I} N$. Suponhamos que $H \neq 1$, então existe $g \in H$ com $g \neq 1$. Assim, existe um subgrupo $N_g \lhd G$ tal que $g \notin N_g$ e G/N_g é finito. Note que $N_g \in I$. Disto segue que $g \in H \leq N_g$. Logo, $g \in N_g$, mas isto é um absurdo, pois por hipótese $g \notin N_g$. Portanto, concluímos que $H = 1$. Reciprocamente, suponhamos que $H = 1$ e seja $g \in G$ com $g \neq 1$, daí temos que $g \notin H$. Então, existe $N_g \lhd G$ com $[G : N_g]$ finito tal que $g \notin N_g$, caso contrário, g estaria em H. Como g foi tomado arbitrariamente, concluímos que G é residualmente finito e o resultado segue. $\square$

O próximo lema mostra que grupos profinitos são sempre residualmente finitos.

Lema 4.5.6. *Se G é um grupo profinito, então G é residualmente finito.*

Demonstração. Seja I o conjunto de todos os subgrupos normais abertos de G. Como G é um grupo profinito, temos pelo Corolário 4.4.4 que $\bigcap_{N \in I} N = 1$. Note que, para cada $N \in I$, o índice $[G : N]$ é finito, pela Proposição 4.2.2 item (iii). Assim, da Proposição 4.5.5 segue que G é residualmente finito. □

O resultado a seguir, consequência do Lema 4.5.6, é uma útil observação relativa a subconjuntos finitos de um grupo profinito.

Lema 4.5.7. *Seja G um grupo profinito. Se H é um subconjunto finito de G, então existe um subgrupo normal aberto N de G tal que $H \cap N = 1$.*

Demonstração. Como G é um grupo profinito, temos pelo Lema 4.5.6 que G é residualmente finito. Suponhamos que $|H| = n$, já que H é finito. Se $H = 1$, então não há nada a demonstrar. Suponhamos que $H \neq 1$. Assim, por G ser residualmente finito, segue que para cada $h_i \in H$ com $h_i \neq 1$, existe um subgrupo normal N_{h_i} tal que $h_i \notin N_{h_i}$ e G/N_{h_i} é finito. Em particular, podemos assumir que N_{h_i} seja aberto em G. Desta maneira, considerando $N = \bigcap_{i=1}^{n} N_{h_i}$, temos que N é um subgrupo normal aberto tal que $N \cap H = 1$. Pois, se $N \cap H \neq 1$, existiria um $h_i \in N \cap H$ com $h_i \neq 1$. Assim, teríamos que $h_i \in N_{h_i}$, o que é um contradição. E o resultado segue. □

Vejamos agora dois exemplos relevantes de completamento de um dado grupo abstrato G, são eles o completamento pro-p e o completamento profinito. Seja p um primo, o *completamento pro-p* de G é o completamento com respeito à família de todos os subgrupos normais de índice uma potência de p. Então, o pro-p completamento de G é um grupo pro-p. O *completamento profinito* de um grupo G é o completamento de G com respeito à família de todos os subgrupos normais de índice finito. Note que pela Proposição 4.5.4 a função j de G em seu completamento profinito $\widehat{G}$ é injetiva se, e somente se, $\bigcap_{K \in I} K = 1$. Lembramos que, pela Proposição 4.5.5, um grupo abstrato G tal que, a interseção de todos seus subgrupos normais de índice finito é trivial, é dito residualmente finito. Segue que para um grupo residualmente finito G, $j(G)$ é sempre uma cópia isomorfa a G no seu completamento profinito $\widehat{G}$.

Finalizamos esta seção construindo exemplos de um completamento pro-p e de um completamento profinito de $\mathbb{Z}$.

Seja p um primo fixado. Consideremos o sistema inverso $(\mathbb{Z}/p^i\mathbb{Z})$, conforme vimos no Exemplo 4.3.3.

Seja $\mathbb{Z}_p$ o conjunto das somas formais infinitas $\sum_{j=0}^{\infty} a_j p^j$ com $0 \leq a_j < p$ para cada j. Definamos para cada $i \geq 1$ as seguintes aplicações:

$$\begin{array}{rccc} \varphi_i : & \mathbb{Z}_p & \longrightarrow & \mathbb{Z}/p^i\mathbb{Z} \\ & z = \sum_{j=0}^{\infty} a_j p^j & \longmapsto & \sum_{j=0}^{i-1} a_j p^j + p^i\mathbb{Z} = \varphi_i(z). \end{array}$$

e

$$\begin{array}{rccc} \theta : & \mathbb{Z}_p & \longrightarrow & s\varprojlim \mathbb{Z}/p^i\mathbb{Z} \\ & z & \longmapsto & (\varphi_i(z) \mid i \geq 1). \end{array}$$

Lembrando que $s\varprojlim \mathbb{Z}/p^i\mathbb{Z}$ é um subgrupo fechado de $\mathrm{Cr}(\mathbb{Z}/p^i\mathbb{Z})$ onde $i \geq 1$.

Verifica-se facilmente que θ é uma aplicação bijetora. Nosso objetivo é mostrar que $\mathbb{Z}_p$ é o completamento pro-p de $\mathbb{Z}$. Para isto, precisamos introduzir em $\mathbb{Z}_p$ uma estrutura de anel topológico, desta maneira, vamos definir as operações de soma e produto em $\mathbb{Z}_p$ e quem são os conjuntos abertos.

Sejam z_1 e z_2 elementos de $\mathbb{Z}_p$, a soma e o produto em $\mathbb{Z}_p$ são definidos como $z_1 + z_2 =: \theta^{-1}(\theta(z_1) + \theta(z_2))$ e $z_1 z_2 =: \theta^{-1}(\theta(z_1)\theta(z_2))$. Pode-se mostrar que com estas operações $\mathbb{Z}_p$ torna-se um anel. Um subconjunto de $\mathbb{Z}_p$ é dito aberto se sua imagem com respeito a θ é um aberto. Assim, com estas definições estamos pedindo que θ seja um isomorfismo de anéis topológicos. Portanto, temos que

$$(\mathbb{Z}_p, \varphi_i) \cong \varprojlim \mathbb{Z}/p^i\mathbb{Z} \cong s\varprojlim \mathbb{Z}/p^i\mathbb{Z}.$$

Então, como $(\mathbb{Z}/p^i\mathbb{Z})$ é um sistema inverso de anéis finitos temos que $\mathbb{Z}_p$ é um anel pro-p, chamado o *anel dos inteiros p-ádicos*.

Podemos considerar $\mathbb{Z}$ como o subconjunto de $\mathbb{Z}_p$ formado pelas somas formais infinitas $\sum_{j=0}^{\infty} a_j p^j$ com $a_j = 0$ para todos exceto para uma quantidade finita de valores de j. Desta maneira, a aplicação θ coincide em $\mathbb{Z}$ com a aplicação natural de $\mathbb{Z}$ para $s\varprojlim \mathbb{Z}/p^i\mathbb{Z}$ e as operações de soma e produto definidas acima em $\mathbb{Z}_p$ estendem as ordinárias operações de soma e produto definidas em $\mathbb{Z}$. Assim, considerando o par $(\mathbb{Z}_p, j)$, onde $\mathbb{Z}_p \cong s\varprojlim \mathbb{Z}/p^i\mathbb{Z}$ e j a aplicação natural que é justamente a aplicação inclusão de $\mathbb{Z}$ em $\mathbb{Z}_p$, tem-se pela Proposição 4.5.1 que $\mathbb{Z}_p$ é o completamento pro-p de $\mathbb{Z}$. Note que estamos usando, como família I para construir o completamento, a família de todos os subgrupos normais de $\mathbb{Z}$ da forma $p^i\mathbb{Z}$ cujo índice é uma potência de p.

Agora vamos construir o completamento profinito de $\mathbb{Z}$. Para isto, enunciamos antes um lema técnico cuja demonstração pode ser encontrada em [**25**, Lemma 1.5.1].

Lema 4.5.8. *Sejam $D = \mathrm{Cr}(\mathbb{Z}_p \mid p$ primo$)$, $\delta : \mathbb{Z} \longrightarrow D$ a aplicação que leva cada $x \in \mathbb{Z}$ no vetor com todas as coordenadas igual a x e $\mathbb{Z}'$ a imagem de δ. Para cada inteiro $n > 0$ as seguintes afirmações valem:*
(i) $nD + \mathbb{Z}' = D$;
(ii) o grupo D/nD é cíclico de ordem n;
(iii) $nD \cap \mathbb{Z}' = n\mathbb{Z}'$.

A seguir veremos que o grupo D, juntamente com a aplicação δ definidos no lema anterior, é o completamento profinito de $\mathbb{Z}$. A demonstração deste fato pode ser vista em [**25**, Proposition 1.5.2].

Proposição 4.5.9. *O par (D, δ), onde $D = \mathrm{Cr}(\mathbb{Z}_p \mid p$ primo$)$ e δ é a aplicação de $\mathbb{Z}$ em D definida no Lema 4.5.8, é o completamento profinito de $\mathbb{Z}$.*

A seguinte proposição mostra que, dado um grupo profinito G, é sempre possível dar um sentido a "potência" g^z, de um elemento $g \in G$ com expoente um qualquer elemento z do completamento profinito $\widehat{\mathbb{Z}}$ de $\mathbb{Z}$, estendendo assim de forma natural o conceito de "potência inteira" de um elemento g de G. Os detalhes da demonstração podem ser encontrados em [**25**, Proposition 1.5.3].

Proposição 4.5.10. *Sejam G um grupo profinito, $\widehat{\mathbb{Z}}$ o completamento profinito de $\mathbb{Z}$ e considere $\mathbb{Z} \subseteq \widehat{\mathbb{Z}}$. As seguintes afirmações valem:*
(i) *existe uma única aplicação contínua $\widehat{\mathbb{Z}} \times G \longrightarrow G$ tal que $(n, g) \longrightarrow g^n$ para $n \in \mathbb{Z}$. Portanto, se $g \in G$ e $z \in \widehat{\mathbb{Z}}$, então a potência g^z está definida;*
(ii) *se $g \in G$ e $z_1, z_2 \in \widehat{\mathbb{Z}}$, então*
 (a) $g^{z_1+z_2} = g^{z_1}g^{z_2}$ *e*
 (b) $(g^{z_1})^{z_2} = g^{z_1 z_2}$.
(iii) *se $g_1, g_2 \in G$ e $z \in \widehat{\mathbb{Z}}$ e se g_1, g_2 comutam, então temos que $(g_1g_2)^z = g_1^z g_2^z$.*

4.6. A Ordem de um Grupo Profinito e Teoria de Sylow

Nesta seção vamos definir o conceito de ordem de um grupo profinito. Para isto precisamos introduzir o conceito de número supernatural, que nos ajudará a obter informações relevantes sobre o grupo. Também definiremos subgrupos de Sylow de um grupo profinito e ressaltaremos suas principais propriedades. Veremos que muitos dos resultados conhecidos em grupos finitos podem ser estendidos para grupos profinitos. Todos os subgrupos de um grupo profinito são considerados fechados, quando não forem será explicitamente indicado.

Iniciamos esta seção com uma proposição que nos dá informações relativas a cardinalidade de um grupo profinito.

Proposição 4.6.1. *Seja G um grupo profinito. Então, a cardinalidade de G é ou finita ou não enumerável.*

Demonstração. Vamos supor que a cardinalidade de G seja enumerável e mostraremos que G é finito. De fato, seja $G = \bigcup_{i\in\mathbb{N}}\{g_i\}$. Pelo Teorema 4.4.6 segue que existe $g_j \in G$ tal que $\{g_j\}$ é aberto. Agora usando a Proposição 4.2.2 item (i) obtemos que qualquer conjunto $\{x\}$ com $x \in G$ é um aberto. Como G é compacto e $G = \bigcup_{i\in\mathbb{N}}\{g_i\}$ temos que existe uma subfamília finita $\{g_{i_1}, \ldots, g_{i_r}\}$ tal que $G = \displaystyle\bigcup_{j=1}^{r}\{g_{i_j}\}$. Portanto, concluímos que G é finito, como queríamos. □

Consideremos G um grupo profinito, então por definição, $G = \varprojlim_{i\in I} G_i$, onde cada G_i é um grupo finito e I é uma base filtrada de subgrupos normais fechados de G. Se G é infinito, então saber sua cardinalidade nos fornece pouca informação a respeito do grupo, pois pela Proposição 4.6.1, sabemos que sempre será não enumerável. Desta maneira, precisamos definir uma quantidade numérica que reflita propriedades aritméticas dos grupos finitos G_i, seja independente da apresentação de G como um limite inverso de um sistema inverso de grupos finitos e expresse propriedades do grupo G que nos permitam definir, no contexto de grupos profinitos, conceitos como, por exemplo, de índices e de subgrupos de Sylow. Essa quantidade numérica será definida por meio do conceito de número supernatural que introduziremos a seguir.

Um *número supernatural* (ou *número de Steinitz*) é um produto formal infinito

$$n = \prod_p p^{n(p)}$$

onde p varia no conjunto de todos os números primos e $n(p)$ é um inteiro não negativo ou infinito. Por convenção simbólica, dizemos que $m < \infty, \infty + \infty = \infty + m = m + \infty = \infty$ para todo $m \in \mathbb{N}$.

Seja $m = \prod_p p^{m(p)}$ um outro número supernatural, se $m(p) \leq n(p)$ para todo primo p, então dizemos que m divide n.

Se $\{a_i = \prod_p p^{n(p,i)} \mid i \in I\}$ é uma família de números supernaturais, então definimos seu produto, mínimo múltiplo comum e máximo divisor comum da seguinte forma:

(i) $\prod_{i\in I} a_i = \prod_p p^{t(p)}$ onde $t(p) = \sum_{i\in I} n(p,i)$.
(ii) $mmc\{a_i \mid i \in I\} = \prod_p p^{s(p)}$ onde $s(p) = sup\{n(p,i) \mid i \in I\}$.
(iii) $mdc\{a_i \mid i \in I\} = \prod_p p^{u(p)}$ onde $u(p) = inf\{n(p,i) \mid i \in I\}$.

Note que o resultado das operações usadas para definir $t(p), s(p)$ e $u(p)$ pode ser ou um inteiro não negativo ou infinito.

Observe que dados $\{a_i \mid i \in I\}$ e $\{b_j \mid j \in J\}$ duas famílias de números supernaturais então temos que,

$$(mmc\{a_i \mid i \in I\})(mmc\{b_j \mid j \in J\}) = mmc\{a_ib_j \mid i \in I, j \in J\}. \tag{4.6.1}$$

Sejam G um grupo profinito e H um subgrupo fechado de G. O *índice* $[G : H]$ de H em G é o mínimo múltiplo comum dos índices dos subgrupos abertos de G contendo H. A *ordem* $|G|$ de G é $[G : 1]$ e a *ordem de um elemento* x de G é a ordem do fecho do subgrupo abstrato gerado por x, ou seja, $|\overline{\langle x\rangle}|$.

Equivalentemente, podemos definir o índice de um subgrupo H de um grupo profinito G como $[G : H] = mmc\{[G : NH] \mid N \lhd_\circ G\}$. De fato, pois sabemos que cada subgrupo aberto U de G, contém um subgrupo normal aberto N de G. E considerando um U tal que $H \leq U$, temos que NH é um subgrupo aberto de G. Assim como $NH \leq U \leq G$, segue pelo Teorema de Lagrange para índices finitos que $[G : U]$ divide $[G : NH]$. Portanto, temos que $mmc\{[G : U] \mid H \leq U \leq_\circ G\}$ divide $mmc\{[G : NH] \mid N \lhd_\circ G\}$. Por outro lado, como $H \leq NH \leq_\circ G$, vemos que $[G : NH] \in \{[G : U] \mid H \leq U \leq_\circ G\}$. Segue que as duas definições de índice são equivalentes.

Um grupo profinito G é um grupo pro-p se, e somente se, G/N possui ordem potência de p para cada $N \lhd_\circ G$. De fato, pois sendo G profinito temos que $G \cong \varprojlim_{N\in I} G/N$, onde I é a base filtrada de todos os subgrupos normais abertos de G e supondo que G seja um grupo pro-p temos que G/N é um p-grupo para cada $N \in I$. Por outro lado, supondo que para cada $N \lhd_\circ G$, G/N é um p-grupo, temos pela Proposição 4.4.1 e por G ser profinito que G é um grupo pro-p. Disto segue que os grupos pro-p são precisamente os grupos profinitos de ordem p^n com $n \leq \infty$.

A proposição a seguir nos mostra que podemos estender o Teorema de Lagrange para os grupos profinitos. A demonstração deste resultado pode ser encontrada em [**25**, Proposition 2.1.2 e Lemma 2.1.3].

Proposição 4.6.2. *Seja G um grupo profinito. As seguintes afirmações valem:*
(i) *sejam H e K subgrupos de G tais que $K \leq H \leq G$. Então*

$$[G : K] = [G : H][H : K].$$

(ii) *se $\{H_i \mid i \in I\}$ é uma família de subgrupos tal que para todos $i, j \in I$ existe um índice $k \in I$ com $H_k \leq H_i \cap H_j$, então*

$$\left[G : \bigcap_{i \in I} H_i\right] = mmc\left\{[G : H_i] \mid i \in I\right\}.$$

A seguir falaremos um pouco da teoria de Sylow em grupos profinitos, definiremos o conceito de p-subgrupo de Sylow de um grupo profinito G, mostraremos a existência destes subgrupos de Sylow e apresentaremos propriedades relevantes destes subgrupos que se assemelham ao que é conhecido para subgrupos de Sylow de grupos finitos.

Definição 4.6.3. Sejam G um grupo profinito e p um primo. Um *p-subgrupo de Sylow* de G é um subgrupo P tal que sua ordem $|P| = p^n$ é uma potência de p com $n \leq \infty$ e seu índice $[G : P]$ é coprimo com p.

Em particular, observamos que os p-subgrupos de Sylow de G são pro-p subgrupos maximais de G.

A proposição a seguir, nos mostra que os Teoremas de Sylow, que conhecemos em grupos finitos, podem ser estendidos para grupos profinitos.

Proposição 4.6.4. *Sejam G um grupo profinito e p um primo. As seguintes afirmações valem:*
(i) *o grupo G possui p-subgrupos de Sylow;*
(ii) *se P é um p-subgrupo de Sylow de G e T é um subgrupo pro-p de G, então $g^{-1}Tg \leq P$ para algum $g \in G$;*
(iii) *cada subgrupo pro-p de G está contido em um p-subgrupo de Sylow;*
(iv) *se P_1 e P_2 são p-subgrupos de Sylow de G, então $g^{-1}P_1g = P_2$ para algum $g \in G$.*

Demonstração. Iremos mostrar somente o item (i), a demonstração dos demais itens pode ser encontrada em [**25**, Proposition 2.2.2].
Com efeito, consideremos I o conjunto dos subgrupos de G de índice coprimo com p. Observemos que $I \neq \varnothing$, uma vez que $G \in I$ e I é um conjunto parcialmente ordenado com respeito a ordem $\leq'$ definida por $H_1 \leq' H_2$ se, e somente, se $H_2 \subseteq H_1$. Seja J uma cadeia de I, isto é, para todos $H_1, H_2 \in J$ temos $H_1 \leq' H_2$ ou $H_2 \leq' H_1$.

Consideremos a seguinte família de subgrupos $\{H_i \mid H_i \in J\}$. Vamos mostrar que para todos $H_i, H_j \in J$ existe $H_k \in J$ tal que $H_k \leq H_i \cap H_j$. De fato, suponhamos sem perda de generalidade que $H_i \leq' H_j$. Segue pela definição de ordem que $H_j \subseteq H_i$. Assim, tomando $H_k = H_j \in J$ obtemos $H_k \subseteq H_i \cap H_j$. Portanto, tem-se $H_k \leq H_i \cap H_j$. Então, aplicando a Proposição 4.6.2 item (ii), a família dos H_i em J, concluímos que $[G : \bigcap H_i] = mmc\{[G : H_i] \mid H_i \in J\}$. Por outro lado, sabendo que para cada $H_i \in J \leq I$, o índice $[G : H_i]$ é coprimo com p, isto resulta que o $mmc\{[G : H_i] \mid H_i \in J\}$ é coprimo com p, portanto o índice $[G : \bigcap H_i]$ é coprimo com p e dessa forma concluímos que $\bigcap\{H \mid H \in J\} \in I$ e que também é uma cota superior para J, pois para todo $H_i \in J$, temos $\bigcap\{H \mid H \in J\} \subseteq H_i$. Então, pelo Lema de Zorn, tem-se que I possui um elemento maximal, que denotamos por P.

Vamos mostrar agora que P é um p-subgrupo de Sylow. Uma vez que $P \in I$, tem-se que o índice $[G : P]$ é coprimo com p, então resta ver que P é um grupo pro-p. De fato, se P não é um grupo pro-p, então existe um $M \triangleleft_\circ P$ tal que $|P/M|$ não é uma potência de p. Como P/M é um grupo finito segue, pelo Teorema de Sylow para grupos finitos, que P/M possui um p-subgrupo de Sylow Q/M, assim $Q/M < P/M$ com $M < Q < P$. Como $[Q : M]$ é finito, temos que Q é união de um número finito de classes laterais de M, que é aberto em P. Isto implica que Q é fechado em P, assim $Q = U \cap P$ com U um subgrupo fechado de G. Como P é um subgrupo fechado de G, pois $P \in I$ tem-se, que Q é também um subgrupo fechado em G. Pelo Teorema de Lagrange, $[G : P]$ divide $[G : Q]$. Uma vez que $[G : P]$ e p são coprimos, resulta que $[G : Q]$ e p também o são. Assim, concluímos que $Q \in I$. Como $Q \subset P$, temos que $P \leq' Q$ e pela maximalidade de P, segue que $P = Q$, o que é um absurdo. Desta maneira, obtemos que P é um grupo pro-p. Portanto, P é um p-subgrupo de Sylow de G, como queríamos mostrar. $\square$

Finalizamos esta seção enunciando algumas propriedades relacionadas a subgrupos de Sylow de um grupo profinito. Em particular, temos uma versão para grupos profinitos do conhecido argumento de Frattini da teoria de grupos finitos. A demonstração destes resultados pode ser encontrada em [**25**, Proposition 2.2.3].

Proposição 4.6.5. *Sejam G um grupo profinito, K um subgrupo normal e P um p-subgrupo de Sylow de G. Então, as seguintes afirmações valem:*

(i) *o subgrupo $K \cap P$ é um p-subgrupo de Sylow de K;*

(ii) *o quociente KP/K é um p-subgrupo de Sylow de G/K;*

(iii) *temos que $G = N_G(Q)K$, para cada p-subgrupo de Sylow Q de K;*

(iv) *vale $H = N_G(H)$, sempre que H é um subgrupo que contém $N_G(Q)$ para algum p-subgrupo de Sylow Q de K.*

4.7. Grupos Pronilpotentes

Finalizemos este capítulo definindo grupos pronilpotentes, objeto relevante nesta dissertação e apresentaremos um resultado que caracteriza os grupos pronilpotentes.

Um grupo profinito G é dito um *grupo pronilpotente* se G for o limite inverso de um sistema inverso de grupos nilpotentes finitos.

O lema a seguir nos fornece um critério para um grupo profinito ser isomorfo ao produto Cartesiano de seus subgrupos. Sua prova pode ser vista em [**25**, Lemma 2.4.2].

Lema 4.7.1. *Seja $\{H_i \mid i \in I\}$ uma família de subgrupos normais de um grupo profinito G. Suponha que G seja o fecho do subgrupo abstrato gerado pela $\bigcup\{H_i \mid i \in I\}$ e, para cada i, denote por K_i o fecho do subgrupo abstrato gerado pela $\bigcup\{H_j \mid j \neq i\}$. Se $\bigcap\{K_i \mid i \in I\} = 1$, então G é isomorfo ao produto Cartesiano $\mathrm{Cr}(H_i \mid i \in I)$.*

Agora, podemos apresentar várias caracterizações para os grupos pronilpotentes que são semelhantes ao análogo resultado para grupos nilpotentes finitos, enunciado no Teorema 1.2.8.

Proposição 4.7.2. *Seja G um grupo profinito. As seguintes afirmações são equivalentes.*
(i) *O grupo G é pronilpotente.*
(ii) *Cada subgrupo de Sylow de G é normal em G.*
(iii) *O grupo G é isomorfo ao produto Cartesiano de seus subgrupos de Sylow.*
(iv) *Para cada subgrupo próprio aberto U de G, temos que $N_G(U) \neq U$.*

Demonstração. Vamos mostrar que (i) implica (iv). De fato, sejam U um subgrupo próprio aberto de G e $N = \bigcap_{g \in G} U^g$. Então, $N \leq U$ e $N \lhd_\circ G$, pois sabendo que $(\bigcap_{i \in I} U_i)^g = \bigcap_{i \in I}(U_i)^g$ para cada $g \in G$, segue que $N \lhd G$. Agora, por U ser aberto em G, temos que U^g é aberto, assim U^g é fechado em G, daí $G \backslash U^g$ é aberto. Disto segue que $N \lhd_\circ G$. Agora, como um quociente de um grupo nilpotente é nilpotente e G é pronilpotente por hipótese, segue do Teorema 4.4.3 item (iv)', que G/N é nilpotente. Como G/N é finito, temos pelo Teorema 1.2.8 item (ii) que $N_{G/N}(U/N) \neq U/N$ o que implica $\left[N_{G/N}(U/N) : U/N\right] \neq 1$. Vejamos que $[N_G(U) : U] \neq 1$. Com efeito, por definição

$$[N_G(U) : U] = mmc\{[N_G(U) : N_G(U) \cap UH] \mid H \lhd_\circ G\}.$$

Um vez que $N \lhd_\circ G$, temos que

$$[N_G(U) : N_G(U) \cap UN] \in \{[N_G(U) : N_G(U) \cap UH] \mid H \lhd_\circ G\}.$$

Agora note que $[N_G(U) : U] = \big[N_{G/N}(U/N) : U/N\big]$. Assim,

$$[N_G(U) : N_G(U) \cap UN] = [N_G(U) : U] = \big[N_{G/N}(U/N) : U/N\big] \neq 1.$$

Portanto, $[N_G(U) : U] \neq 1$ e logo concluímos que $N_G(U) \neq U$.

Provaremos que (iv) implica (ii). Seja P um p-subgrupo de Sylow de G e consideremos a seguinte família $\mathcal{F} = \{H \leq_\circ G \mid N_G(P) \leq H\}$, note que $\mathcal{F} \neq \varnothing$, pois $G \in \mathcal{F}$. Então, seja $U \in \mathcal{F}$, segue que $N_G(P) \leq U$. Agora, usando a Proposição 4.6.5 item (iv) obtemos que $U = N_G(U)$. Assim, pela hipótese em (iv) segue que $U = G$. Como P é um subgrupo fechado, temos que $N_G(P)$ também o é. Dessa forma, podemos escrever $N_G(P) = \bigcap\{NN_G(P) \mid N \lhd_\circ G\}$, e observamos que $N_G(P) = \bigcap_{H\in\mathcal{F}} H$. De fato, pela definição de $\mathcal{F}$, temos $N_G(P) \leq \bigcap_{H\in\mathcal{F}} H$. Por outro lado, considerando $\mathcal{F}' = \{NN_G(P) \mid N \lhd_\circ G\}$, temos $N_G(P) = \bigcap_{V\in\mathcal{F}'} V$ e note que $\mathcal{F}' \subseteq \mathcal{F}$, então segue que $\bigcap_{H\in\mathcal{F}} H \leq \bigcap_{V\in\mathcal{F}'} V = N_G(P)$. Deste modo, obtemos que $N_G(P) = \bigcap_{H\in\mathcal{F}} H$. Mas, mostramos que se $H \in \mathcal{F}$, então $H = G$. Assim, concluímos que $N_G(P) = G$ e portanto P é normal em G. Como P foi tomado arbitrariamente, o argumento vale para todo subgrupo de Sylow de G. Logo, obtemos que todo subgrupo de Sylow de G é normal.

Agora, provaremos que (ii) implica (iii). Sejam I o conjunto dos primos divisores de $|G|$ e $\{P_i \mid i \in I\}$ o conjunto dos subgrupos de Sylow de G. Para cada i denote por K_i o fecho do subgrupo abstrato gerado por $\bigcup_{j\neq i} P_j$. Vejamos que a ordem de K_i é coprima com $i \in I$. De fato, seja p um primo que divide $|K_i|$, mostraremos que $p \neq i$ e assim temos o que queremos. Com efeito, se p divide $|K_i|$, então para algum $M \lhd_\circ K_i$ temos que p divide $|K_i/M|$. Pois, supondo que p não divide $|K_i/M|$ para qualquer $M \lhd_\circ K_i$ tem-se por Lagrange que $[K_i : M]$ divide $|K_i|$, logo teríamos que p não divide $|K_i|$ o que é uma contradição com a nossa suposição. Agora, como cada P_j é um subgrupo de Sylow normal de G e $P_j \leq K_i$ para $j \neq i$, segue que P_j é um subgrupo de Sylow normal de K_i para todo $j \neq i$. Considerando o quociente finito K_i/M, temos por correspondência que cada P_jM/M é um subgrupo de Sylow normal de K_i/M, assim pelo mesmo ser finito, concluímos que apenas uma quantidade finita de subgrupos P_jM/M são não triviais e que K_i/M é nilpotente, assim K_i/M é o produto direto desses subgrupos não triviais. Então, como p divide $|K_i/M|$, segue que p divide $|P_jM/M|$

para algum $j \neq i$, desta maneira p divide $|P_j/M \cap P_j|$, logo p divide $|P_j|$. Uma vez que $j \neq i$, concluímos que $p \neq i$ e desta forma a ordem de K_i é coprima com i.

Segue então que $K_i \cap P_i = 1$ para cada i, pois seja $a \in K_i \cap P_i$, como a ordem de a é $|\overline{\langle a \rangle}|$, tem-se que $\overline{\langle a \rangle} \leq K_i$ e $\overline{\langle a \rangle} \leq P_i$, daí $|\overline{\langle a \rangle}|$ divide $|K_i|$ e $|P_i|$, por K_i e i serem coprimos, obtemos que $|\overline{\langle a \rangle}| = 1$, portanto $a = 1$, logo a interseção entre K_i e P_i é trivial. Consequentemente, $\bigcap K_i = 1$. Observemos que cada grupo profinito G é o fecho do grupo abstrato gerado por todos os seus subgrupos de Sylow, pois este fecho tem índice 1 em G. Note que este fato decorre da definição de índice, de *mdc* e do Teorema de Lagrange para grupos profinitos. Desta forma, estamos nas hipóteses do Lema 4.7.1, e portanto concluímos que G é isomorfo ao produto Cartesiano de seus subgrupos de Sylow, como queríamos.

Vamos provar que (iii) implica (i). Primeiramente, observemos que grupos pro-p são pronilpotentes, pois considerando G um grupo pro-p, temos por definição que G é o limite inverso de p-grupos finitos. Como p-grupos finitos são grupos nilpotentes finitos, tem-se que G é o limite inverso de grupos finitos nilpotentes, logo G é pronilpotente. Agora, uma vez que subgrupos de Sylow são grupos pro-p, segue então que os mesmos são pronilpotentes. Assim, obtemos que G é isomorfo ao produto Cartesiano de grupos pronilpotentes e usando o Teorema 4.4.5 item (ii), concluímos que este produto Cartesiano é pronilpotente. □

Lembremos que o subgrupo *residual pronilpotente* de um grupo profinito G é $\gamma_\infty(G) = \bigcap_{i=1}^{\infty} \gamma_i(G)$, onde os subgrupos $\gamma_i(G)$ são os (fechos dos) termos da série central descendente de G.

O próximo lema reúne várias propriedades sobre o subgrupo residual pronilpotente que serão muito utilizadas ao longo deste trabalho.

Lema 4.7.3. *Seja G um grupo profinito. As seguintes afirmações valem:*
(i) *o subgrupo residual pronilpotente $\gamma_\infty(G)$ de G é igual ao subgrupo gerado por todos os comutadores $[x, y]$, onde x e y são elementos de ordens coprimas;*
(ii) *para qualquer subgrupo normal N de G, temos*

$$\gamma_\infty(G/N) = \gamma_\infty(G)N/N;$$

(iii) *se G é pronilpotente, então $\gamma_\infty(G) = 1$;*
(iv) *o subgrupo residual pronilpotente $\gamma_\infty(G)$ de G é o menor subgrupo normal com quociente pronilpotente.*

Demonstração. Observe que o item (i) segue da Proposição 4.7.2 item (ii).

Vejamos o item (ii). Claramente temos que $\gamma_\infty(G)N/N \leq \gamma_\infty(G/N)$, pois sejam x e y elementos de G tais que $(\circ(x), \circ(y)) = 1$ e considerando o epimorfismo canônico de G em G/N, obtemos que $(\circ(\overline{x}), \circ(\overline{y})) = 1$, daí aplicando o item (i) desta proposição a inclusão segue. Por outro lado, vejamos que para todos os elementos $\overline{x}$ e $\overline{y}$ de ordens coprimas em qualquer quociente G/N de G, existem elementos x e y em G tais que $\overline{x} = xN, \overline{y} = yN$ e $(\circ(x), \circ(y)) = 1$. Com efeito, usando a Proposição 4.5.10 item (ii)(a), temos que cada $g \in G$ pode ser escrito da forma $g^1 = g^{1_p + 1_{p'}} = g^{1_p} g^{1_{p'}}$, onde 1_p é o gerador de $\mathbb{Z}_p$ e $1_{p'}$ é o gerador de $\prod_{q \neq p} \mathbb{Z}_q$. Note que g^{1_p} é um p-elemento, veja [**19**, Lemma 4.1.1] e $g^{1_{p'}}$ é um p'-elemento, desta forma, tem-se que $(\circ(g^{1_p}), \circ(g^{1_{p'}})) = 1$. Usando este fato segue facilmente que $\gamma_\infty(G/N) \leq \gamma_\infty(G)N/N$ e a igualdade vale.

Mostraremos o item (iii). De fato, como G é pronilpotente, segue pelo Teorema 4.4.5 item (i) que
$$G \cong \varprojlim_{N \in I} G/N,$$
onde I é a base filtrada de todos os subgrupos normais abertos de G e G/N é um grupo finito nilpotente para cada $N \in I$. Assim, como G/N é nilpotente finito, para cada $N \in I$, temos que $\gamma_\infty(G/N) = 1$. Então, pelo item (ii) deste lema tem-se $\gamma_\infty(G)N/N = 1$. Disto segue que $\gamma_\infty(G) \leq N$ para cada $N \in I$. Logo, $\gamma_\infty(G) \leq \bigcap_{N \in I} N$. Agora, sendo G profinito, temos pelo Corolário 4.4.4 item (iii) que $\bigcap_{N \in I} N = 1$. Portanto $\gamma_\infty(G) = 1$, como desejado.

Vamos mostrar o item (iv). Vejamos primeiramente que $G/\gamma_\infty(G)$ é pronilpotente. Como $\gamma_\infty(G)$ é fechado e normal em G, segue pelo Teorema 4.4.5 item (i) que
$$G/\gamma_\infty(G) \cong \varprojlim_{N \in I} G/\gamma_\infty(G)N,$$
onde I é a base filtrada de todos os subgrupos normais abertos de G. Assim, mostraremos que $G/\gamma_\infty(G)N$ é nilpotente finito, para cada $N \in I$. Com efeito, note que $G/\gamma_\infty(G)N$ é finito para cada $N \in I$. Por outro lado, seja $N \in I$, pelo terceiro teorema do isomorfismo, tem-se
$$G/\gamma_\infty(G)N \cong \frac{G/N}{\gamma_\infty(G)N/N}.$$

Agora, pelo item (ii) deste lema, segue que $\gamma_\infty(G/N) = \gamma_\infty(G)N/N$. Daí, substituindo obtemos
$$G/\gamma_\infty(G)N \cong \frac{G/N}{\gamma_\infty(G/N)}.$$

Desde que G/N é finito, temos que $\frac{G/N}{\gamma_\infty(G/N)}$ é nilpotente. Logo, $G/\gamma_\infty(G)N$ é nilpotente. Portanto, concluímos que $G/\gamma_\infty(G)$ é pronilpotente. Por outro lado, notemos que se G/M é um grupo pronilpotente, então $\gamma_\infty(G) \leq M$. De fato, como G/M é pronilpotente, temos pelo itens (ii) e (iii) deste lema que

$$\gamma_\infty(G/M) = \gamma_\infty(G)M/M = 1.$$

Portanto, $\gamma_\infty(G) \leq M$ e o resultado segue. □

O lema a seguir, nos mostra um resultado semelhante ao Teorema de Fitting 1.2.9 em grupos abstratos.

Lema 4.7.4. *Seja G um grupo profinito. Se K_1 e K_2 são subgrupos normais pronilpotentes de G, então o produto K_1K_2 também é pronilpotente.*

Demonstração. De fato, como G é um profinito e K_1 e K_2 são pronilpotentes temos, pelo Teorema 4.4.5 item (i), que

$$K_1 \cong \varprojlim_{N \in I} \frac{K_1}{K_1 \cap N} \quad \text{e} \quad K_2 \cong \varprojlim_{N \in I} \frac{K_2}{K_2 \cap N}.$$

onde I é a base filtrada de todos os subgrupos normais abertos de G, com $K_1/(K_1 \cap N)$ e $K_2/(K_2 \cap N)$ grupos nilpotentes finitos para todo $N \in I$. Vejamos que K_1K_2 é pronilpotente. Com efeito, por K_1K_2 ser um subgrupo fechado de G, temos novamente, pelo Teorema 4.4.5 item (i), que

$$K_1K_2 \cong \varprojlim_{N \in I} \frac{K_1K_2}{(K_1K_2) \cap N}.$$

Resta ver que $K_1K_2/((K_1K_2) \cap N)$ é nilpotente finito para cada $N \in I$. Note que

$$(K_1K_2)N/N \cong (K_1N/N)(K_2N/N).$$

Assim, como K_1N/N e K_2N/N são grupos nilpotentes normais finitos segue que $(K_1K_2)N/N$ é nilpotente finito. Logo, obtemos que $K_1K_2/((K_1K_2) \cap N)$ é nilpotente finito para cada $N \in I$. Portanto, concluímos que K_1K_2 é pronilpotente, como desejado. □

Fazendo indução sobre n e usando o Lema 4.7.4 obtemos o seguinte corolário.

Corolário 4.7.5. *Sejam G um grupo profinito e $K_1, \ldots, K_n$ subgrupos normais pronilpotentes de G. Então $K_1 \cdots K_n$ é também um subgrupo pronilpotente de G.*

Observação 4.7.6. Segue do lema anterior que em um grupo profinito G faz sentido definir o maior subgrupo normal pronilpotente de G. Este subgrupo será usado com frequência no capítulo seguinte.

5

Grupos Profinitos Quase Engel

Neste capítulo demonstraremos o Teorema A e o Corolário C, ou seja, os resultados principais do artigo de E. I. Khukhro e P. Shumyatsky [**13**] relativos a grupos profinitos.

Lembramos que, no contexto de grupos profinitos, a menos de indicações explícitas um subgrupo de um grupo profinito será sempre um subgrupo fechado, todos os homomorfismos serão contínuos e os quocientes serão por subgrupos normais fechados.

5.1. Resultados Preliminares

Nesta seção apresentamos vários resultados técnicos sobre grupos profinitos relacionados com as hipóteses do Teorema A, a fim de nos auxiliar para a demonstração do Teorema A.

Lembrando que no Capítulo 2, na Proposição 2.0.11, vimos que todo grupo localmente nilpotente é Engel. No entanto, sabemos que a recíproca não vale em geral. Mas, existe um importante resultado positivo devido a J. S. Wilson e E. I. Zelmanov. Eles em [**26**] provaram o teorema a seguir. Esse resultado será um dos ingredientes principais para a demonstração do Teorema A. A prova deste fato, pode ser encontrada em [**26**, Theorem 5].

Teorema 5.1.1 (de Wilson-Zelmanov). *Todo grupo profinito Engel é localmente nilpotente.*

Por comodidade vamos enunciar de forma separada a hipótese do Teorema A, pois quase todos os resultados deste capítulo terão esta hipótese no enunciado.

Hipótese 1. *Para cada elemento g de um grupo G existe um inteiro positivo $n = n(g)$ tal que $E_n(g)$ é finito.*

A seguir veremos um resultado que caracteriza grupos pronilpotentes satisfazendo a Hipótese 1. Na demonstração deste lema usaremos o Teorema 5.1.1.

Lema 5.1.2. [**13**, Lemma 3.2] *Um grupo profinito satisfazendo a Hipótese 1 é pronilpotente se, e somente se, é localmente nilpotente.*

Demonstração. Seja G um grupo profinito localmente nilpotente, vamos mostrar que G é pronilpotente. De fato, como G é um grupo profinito, temos pelo Teorema 4.4.5 item (i) que $G \cong \varprojlim_{N \in I} G/N$, onde I é a base filtrada de todos os subgrupos normais abertos de G. Por hipótese, G é localmente nilpotente, e disto segue que G/N com $N \lhd_{\circ} G$ é também localmente nilpotente. Assim, como G/N é localmente nilpotente e finito, concluímos que G/N é nilpotente, para todo $N \in I$. Portanto, G é pronilpotente.

Reciprocamente, suponhamos que G seja um grupo pronilpotente satisfazendo a Hipótese 1, mostraremos que G é localmente nilpotente. Com efeito, como G é pronilpotente, temos pelo Teorema 4.4.5 item (i) que $G \cong \varprojlim_{N \in I} G/N$, onde I é a base filtrada de todos os subgrupos normais abertos de G e G/N é nilpotente finito, para cada $N \in I$. Assim, como $E_{n(g)}(g)$ é finito, temos pelo Lema 4.5.7 que, para qualquer $g \in G$, existe um subgrupo normal aberto N com G/N nilpotente, tal que $E_{n(g)}(g) \cap N = 1$. Observemos que a imagem $\overline{g}$ de g no grupo quociente G/N é um elemento Engel. De fato, pois uma vez que G/N é nilpotente, existe um inteiro $m \geqslant 1$ tal que $\gamma_{m+1}(G/N) = 1$. Em particular, tem-se

$$[\overline{x}, \underbrace{\overline{g}, \ldots, \overline{g}}_{m}] = 1 \quad \forall\, \overline{x} \in G/N, \tag{5.1.1}$$

ou seja, $\overline{g}$ é um elemento Engel em G/N, como queríamos. Agora, vejamos que isso implica que g é um elemento Engel de G. Para isso, precisamos mostrar que existe $s = s(x,g)$ tal que $[x, \underbrace{g, \ldots, g}_{s}] = 1$ para todo $x \in G$. Vamos considerar dois casos. Primeiro, se $n(g) \geqslant m$, $\gamma_{m+1}(G/N) = 1$ implica em $\gamma_{n(g)+1}(G/N) = 1$. Em particular, tem-se

$$[\overline{x}, \underbrace{\overline{g}, \ldots, \overline{g}}_{n(g)}] = 1 \quad \forall\, \overline{x} \in G/N.$$

Desta forma, em G, obtemos que $[x, \underbrace{g, \ldots, g}_{n(g)}] \in N$ para todo $x \in G$. Uma vez que $[x, \underbrace{g, \ldots, g}_{n(g)}] \in E_{n(g)}(g)$, isto resulta que $[x, \underbrace{g, \ldots, g}_{n(g)}] \in E_{n(g)}(g) \cap N$. Como

$E_n(g) \cap N = 1$, temos que $[x, \underbrace{g, \ldots, g}_{n(g)}] = 1$ para todo $x \in G$. Assim, concluímos que g é um elemento Engel em G. Agora, se $n(g) < m$, como (5.1.1) vale, temos que $[x, \underbrace{g, \ldots, g}_{m}] \in N$ para todo $x \in G$, e vamos mostrar que $[x, \underbrace{g, \ldots, g}_{m}] \in E_{n(g)}(g)$. Note que podemos reescrever o comutador $[x, \underbrace{g, \ldots, g}_{m}]$ da seguinte maneira

$$[x, \underbrace{g, \ldots, g}_{m}] = [x, \underbrace{g, \ldots, g}_{n(g)}, \underbrace{g, \ldots, g}_{c}] = [[x, \underbrace{g, \ldots, g}_{n(g)}], \underbrace{g, \ldots, g}_{c}],$$

para algum $c \geqslant 1$ e que o comutador $[[x, \underbrace{g, \ldots, g}_{n(g)}], g] \in E_{n(g)}(g)$, pois

$$[x, \underbrace{g, \ldots, g}_{n(g)}], g] = [x, \underbrace{g, \ldots, g}_{n(g)}]^{-1}[x, \underbrace{g, \ldots, g}_{n(g)}]^g \in E_{n(g)}(g).$$

Assim, observando que g normaliza $E_{n(g)}(g)$ e repetindo o mesmo argumento acima várias vezes, se necessário, chegamos a concluir que $[x, \underbrace{g, \ldots, g}_{m}] \in E_{n(g)}(g)$. Disto segue que $[x, \underbrace{g, \ldots, g}_{m}] \in E_{n(g)}(g) \cap N = 1$. Portanto, concluímos que g é um elemento Engel em G. Como g foi tomado arbitrariamente em G, isto resulta que G é um grupo profinito Engel. Portanto, pelo Teorema 5.1.1, segue que G é localmente nilpotente, como queríamos. $\square$

O teorema a seguir, devido a P. Hall, fornece um critério para provar que um grupo é nilpotente. Sabemos que extensões de grupos nilpotentes não precisam ser nilpotentes, mas o resultado de Hall usa hipóteses próximas a extensões de nilpotentes. A demonstação deste resultado pode ser encontrada em [**11**, Theorem 3.26].

Teorema 5.1.3 (de Hall). *Seja B um subgrupo normal de um grupo A. Se B é nilpotente de classe c e A/B' é nilpotente de classe d, então A é nilpotente de classe no máximo $f(c, d) = \dfrac{(d-1)c(c+1)}{2} + c$.*

A próxima proposição generaliza, no item (i), o teorema de Hall, enunciado anteriormente para grupos abstratos. Pois, se considerarmos na proposição que $\gamma_d(A/B') = 1$, isto é, que A/B' seja nilpotente de classe no máximo d, recaímos nas hipóteses de Teorema 5.1.3 e concluímos que A é nilpotente de classe limitada. No item (ii) da mesma proposição, veremos uma "versão profinita" do resultado enunciado no primeiro item.

Proposição 5.1.4. *As seguintes afirmações valem:*
(i) *se B é um subgrupo normal de um grupo A tal que B é nilpotente de classe c e $\gamma_d(A/B')$ é finito de ordem k. Então, o subgrupo*

$$C = C_A(\gamma_d(A/B')) = \{a \in A \mid [\gamma_d(A), a] \leq B'\}$$

possui índice finito k-limitado e é nilpotente de classe (c, d)-limitada;
(ii) *suponha que B é um subgrupo normal de um grupo profinito A tal que B é pronilpotente e $\gamma_\infty(A/B')$ é finito. Então, o subgrupo*

$$D = C_A(\gamma_\infty(A/B')) = \{a \in A \mid [\gamma_\infty(A), a] \leq B'\}$$

é aberto e pronilpotente.

Demonstração. Vamos mostrar o item (i). De fato, do Lema 1.2.5 segue que $\gamma_d(A/B') = \gamma_d(A)B'/B'$, então $\gamma_d(A/B')$ é uma seção normal de A. Assim, podemos considerar a ação, por conjugação, de A sobre $\gamma_d(A/B')$, definida da seguinte forma: para todo $a \in A$ e $\overline{y} = yB' \in \gamma_d(A)B'/B'$, onde $y \in \gamma_d(A)B'$, temos que $\overline{y}^a = (yB')^a = y^aB'$. Em particular, podemos definir de forma natural o centralizador e o normalizador desta seção normal, respectivamente como

$$C = C_A(\gamma_d(A/B')) = \{a \in A \mid [\gamma_d(A), a] \leq B'\}.$$
$$N = N_A(\gamma_d(A/B')) = \{a \in A \mid \overline{y}^a \in \gamma_d(A/B'),\ \forall\ \overline{y} \in \gamma_d(A/B')\}.$$

Observemos que $N = A$, pois $\gamma_d(A/B')$ é uma seção normal. Assim, aplicando o Lema 1.1.5 com $\gamma_d(A/B')$, concluímos que A/C é isomorfo a um subgrupo de $Aut(\gamma_d(A/B'))$. Agora, como $|\gamma_d(A/B')| = k$, temos que $|Aut(\gamma_d(A/B'))|$ é k-limitada, e disto segue que A/C também possui ordem k-limitada.

Vamos agora mostrar que C é nilpotente de classe (c, d)-limitada. Com efeito, temos

$$[\underbrace{C, \ldots, C}_{d+1}, C, \ldots] \leq [[[\underbrace{A, \ldots, A}_{d}], C], C, \ldots] = [[\gamma_d(A), C], C, \ldots]. \tag{5.1.2}$$

Por como C foi definido, sabemos que $[\gamma_d(A), C] \leq B'$. Desta forma, substituindo em (5.1.2), tem-se

$$[\underbrace{C, \ldots, C}_{d+1}, C, \ldots] \leq [[B, B], C, \ldots].$$

Concluímos que $\gamma_{d+1}(C) \leq \gamma_2(B)$. Agora, consideremos o comutador $[[B, B], C]$. Aplicando o Corolário 1.1.8, temos

$$[[B, B], C] \leq [[B, C], B] \cdot [B, [B, C]]. \tag{5.1.3}$$

Então, usando (5.1.3) e o Corolário 1.1.8 quantas vezes for necessário, obtemos

$$[[B,B],\underbrace{C,\ldots,C}_{2d-1}] \leq \prod_{i+j=2d-1} [[B,\underbrace{C,\ldots,C}_{i}],[B,\underbrace{C,\ldots,C}_{j}]], \tag{5.1.4}$$

onde denotamos $[B,\underbrace{C,\ldots,C}_{0}] = B$. Agora, como $2d-1 = 2(d-1)+1$ temos que em cada comutador do produtório acima ou $i > d-1$ ou $j > d-1$. Portanto, cada termo do produtório contém um subcomutador da forma

$$[B,\underbrace{C,\ldots,C}_{l}] \quad \text{com} \quad l \geqslant d. \tag{5.1.5}$$

Assim, em cada comutador do produtório em (5.1.4), podemos "levar para a esquerda" o subcomutador da forma (5.1.5), pois sabemos que

$$[[B,\underbrace{C,\ldots,C}_{i}],[B,\underbrace{C,\ldots,C}_{j}]] = [[B,\underbrace{C,\ldots,C}_{j}],[B,\underbrace{C,\ldots,C}_{i}]].$$

Desta forma, teremos um produtório de comutadores, onde a primeira entrada de cada um é um subcomutador do tipo (5.1.5). Note que, cada um desses subcomutadores do tipo (5.1.5) está contido em $[B,\underbrace{C,\ldots,C}_{d}]$ e o outro subcomutador está obviamente contido em B, uma vez que B é normal. Então, aplicando essa observação a cada comutador de (5.1.4) obtemos que

$$\prod_{i+j=2d-1} [[B,\underbrace{C,\ldots,C}_{i}],[B,\underbrace{C,\ldots,C}_{j}]] \leq [[B,\underbrace{C,\ldots,C}_{d}],B]. \tag{5.1.6}$$

Assim, segue que

$$\begin{aligned} [[B,B],\underbrace{C,\ldots,C}_{2d-1},C,\ldots] &\leq \prod_{i+j=2d-1} [[B,\underbrace{C,\ldots,C}_{i}],[B,\underbrace{C,\ldots,C}_{j}],C,\ldots] \\ &\leq [[B,\underbrace{C,\ldots,C}_{d}],B,C,\ldots]. \end{aligned} \tag{5.1.7}$$

Lembrando que $[\gamma_d(A),C] \leq B'$, tem-se $[B,\underbrace{C,\ldots,C}_{d}] \leq B'$. Disto, segue que $[[[B,\underbrace{C,\ldots,C}_{d}],B],C,\ldots] \leq [[[B,B],B],C,\ldots]$ e concluímos, usando (5.1.7) que

$$[[B,B],\underbrace{C,\ldots,C}_{2d-1},C,\ldots] \leq [[[B,B],B],C,\ldots]. \tag{5.1.8}$$

Lembrando que $\gamma_{d+1}(C) \leq \gamma_2(B)$ e usando (5.1.8) temos

$$\begin{aligned}
[\gamma_{(d+1)+(2d-1)}(C), C, \ldots] &= [\gamma_{d+1}(C), \underbrace{C, \ldots, C}_{2d-1}, C, \ldots] \\
&\leq [[B, B], \underbrace{C, \ldots, C}_{2d-1}, C, \ldots] \\
&\leq [[[B, B], B], C, \ldots],
\end{aligned}$$

ou seja, que $\gamma_{(d+1)+(2d-1)}(C) \leq \gamma_3(B)$. Usando cálculos semelhantes e um argumento indutivo chegamos a ver que

$$\gamma_{(d+1)+(2d-1)+(3d-2)}(C) \leq \gamma_4(B),$$

e mais em geral, fazendo indução sobre $c \geqslant 1$, vamos concluir que $\gamma_{f(c,d)+1}(C) \leq \gamma_{c+1}(B)$, onde

$$f(c, d) = \frac{d(c(c+1))}{2} - \frac{c(c-1)}{2}.$$

A título de exemplo, observe que se $c = 1$, então $d + 1 = f(1, d) + 1$ e temos $\gamma_{d+1}(C) \leq \gamma_2(B)$, como foi mostrado antes.

De forma semelhante, se $c = 2$ tem-se $(d + 1) + (2d - 1) = f(2, d)$ e como mostrado obtemos que $\gamma_{(d+1)+(2d-1)}(C) \leq \gamma_3(B)$.

Portanto, com este argumento indutivo sobre c, um pouco técnico, chegamos a mostrar que C é nilpotente de classe (c, d)-limitada, como queríamos.

Vamos mostrar o item (ii). Uma vez que D, por definição, é o centralizador de uma seção normal de A, segue que D é um subgrupo normal fechado. De modo análogo ao que fizemos no item (i) desta proposição, obtemos que A/D é isomorfo a um subgrupo de $Aut(\gamma_\infty(A/B'))$. Como $\gamma_\infty(A/B')$ é finito, temos que $Aut(\gamma_\infty(A/B'))$ é finito. Assim, D possui índice finito e segue, pela Proposição 4.2.2 item (iii), que D é um subgrupo aberto de A. Agora, usando o item (i) desta proposição, vamos mostrar que a imagem de D, em qualquer quociente finito de A, é nilpotente. Isto será suficiente para mostrar que D é pronilpotente, pois como D é um subgrupo fechado e normal de A temos, pelo Teorema 4.4.5 item (i), que

$$D \cong \varprojlim_{N \in I} \frac{D}{D \cap N} \cong \varprojlim_{N \in I} \frac{DN}{N},$$

onde I é a base filtrada de todos os subgrupos normais abertos de A. Assim, é suficiente provar que para cada $N \in I$, DN/N é nilpotente, para concluir que D é pronilpotente. Então, seja $N \lhd_\circ A$ e consideremos o epimorfismo canônico de A em $A/N = \overline{A}$, onde com as barras denotamos as imagens em $\overline{A}$. Vejamos que

$\gamma_\infty(\overline{A}/\overline{B}') = \overline{\gamma_\infty(A/B')}$. De fato, do Lema 4.7.3 item (ii), segue

$$\gamma_\infty(\overline{A}/\overline{B}') = \frac{\gamma_\infty(\overline{A})\overline{B}'}{\overline{B}'} = \frac{\overline{\gamma_\infty(A)}\overline{B}'}{\overline{B}'} = \frac{\overline{\gamma_\infty(A)B'}}{\overline{B}'} = \overline{\gamma_\infty(A/B')}.$$

Observemos que $\overline{D} \leq C_{\overline{A}}(\gamma_\infty(\overline{A}/\overline{B}'))$. Com efeito, seja $\overline{d} \in \overline{D}$, ou seja $\overline{d} = dN$ com d tal que $[\gamma_\infty(A), d] \leq B'$. Isto implica que $[\gamma_\infty(A), d]N \leq B'N$. Logo, $[\gamma_\infty(\overline{A}), \overline{d}] \leq \overline{B}'$. Desta maneira, segue que $\overline{d} \in C_{\overline{A}}(\gamma_\infty(\overline{A}/\overline{B}'))$, para todo $\overline{d} \in \overline{D}$. Por outro lado, desde que $\overline{A}/\overline{B}'$ é finito, temos que $\gamma_\infty(\overline{A}/\overline{B}') = \gamma_d(\overline{A}/\overline{B}')$ para algum inteiro positivo d. Como, por hipótese, B é um subgrupo normal pronilpotente, temos que $\overline{B} = BN/N$ é um subgrupo normal nilpotente de $\overline{A}$. Portanto, estamos nas condições do item (i) e temos que $C_{\overline{A}}(\gamma_d(\overline{A}/\overline{B}'))$ é nilpotente. Como $\overline{D} \leq C_{\overline{A}}(\gamma_d(\overline{A}/\overline{B}'))$ segue que $\overline{D}$ também o é. Uma vez que o argumento acima é independente da escolha de N em I, concluímos que D é pronilpotente, como desejado. □

Lembramos que um grupo G é dito *central-por-finito* se o índice $[G : Z(G)]$ é finito. Outro conceito que precisaremos a seguir é o de FC-grupo: um grupo G é chamado de *FC-grupo* se toda classe de conjugação em G é finita. Pode-se mostrar que todo grupo central-por-finito é um FC-grupo, já que em um grupo central-por-finito o centralizador de qualquer elemento possui índice finito devido ao fato que contém o centro. O resultado seguinte, devido a B. H. Neumann, nos mostra que em determinadas condições um FC-grupo é central-por-finito. Os detalhes da demonstração podem ser encontrados em [**18**, Lemma 2].

Lema 5.1.5. *Se G é um FC-grupo e contém um subgrupo abeliano A tal que o índice $[G : A]$ é finito, então G é um grupo central-por- finito.*

Introduziremos a seguir um conceito, de natureza quantitativa, relacionado ao conceito de FC-grupo.

Um grupo G é chamado *BFC-grupo* se existe um inteiro positivo d tal que toda classe de conjugação de um elemento em G é finita e possui no máximo d elementos.

O próximo teorema, também devido a B. H. Neumann, caracteriza BFC-grupos em termos do seu subgrupo derivado. Os detalhes da demonstração podem ser encontrados em [**20**, Theorem 4.35].

Teorema 5.1.6. *Um grupo G é um BFC-grupo se, e somente se, G' é finito.*

Os resultados enunciados acima são fundamentais para entender o próximo teorema, devido a A. Shalev [**24**, Lemma 2.6], que nos dá informações sobre o subgrupo derivado de um FC-grupo profinito.

Teorema 5.1.7. *Seja G um FC-grupo profinito. Então G' é finito.*

Demonstração. Para cada $n \geqslant 1$ definimos o seguinte conjunto $\Delta_n = \{x \in G \mid [G : C_G(x)] \leq n\}$. Notemos que Δ_n é um subconjunto fechado de G para cada n. Pois, definindo a aplicação f de G em $\mathbb{N}$ dada por $f(x) = [G : C_G(x)]$ para todo $x \in G$, vemos que f é contínua. Daí, considerando para cada n fixado, o subconjunto fechado $A = \{1, \ldots, n\}$ de $\mathbb{N}$, temos que $f^{-1}(A) = \Delta_n$ é fechado. Agora, por definição, $\bigcup_{n\in\mathbb{N}} \Delta_n \subseteq G$. Por outro lado, por G ser um FC-grupo profinito, temos que para cada $x \in G$, o índice $[G : C_G(x)]$ é finito e igual a algum $n \in \mathbb{N}$. Desta forma, segue que $G \subseteq \bigcup_{n\in\mathbb{N}} \Delta_n$ e portanto $G = \bigcup_{n\in\mathbb{N}} \Delta_n$. Assim, aplicando o Lema 4.4.7, temos que existem um inteiro n, um elemento x em G e um subgrupo aberto H de G tal que $xH \subseteq \Delta_n$. Observe que se $x \in \Delta_n$, então $[G : C_G(x)] \leq n$. Por outro lado, como $|cl(x)| = |cl(x^{-1})|$, onde $cl(x)$ denota a classe de conjugação do elemento x, concluímos que $x^{-1} \in \Delta_n$. Por isso, $H = x^{-1}xH \subseteq \Delta_n\Delta_n$.

Agora, notemos que $\Delta_i\Delta_j \subseteq \Delta_{ij}$. De fato, seja $a \in \Delta_i\Delta_j$, então $a = xy$, onde $x \in \Delta_i$ e $y \in \Delta_j$. Consideremos $S = C_G(x) \cap C_G(y)$, como $[G : C_G(x)] \leq i$ e $[G : C_G(y)] \leq j$, tem-se $[G : S] \leq ij$. Claramente vemos que $S \leq C_G(xy)$, por isto $[G : C_G(xy)] \leq [G : S] \leq ij$. Logo, obtemos que $a \in \Delta_{ij}$. Disto segue que $H \subseteq \Delta_{n^2}$. Então, para todo $x \in H$, temos que $[G : C_G(x)] \leq n^2$. Portanto, H é um BFC-grupo. Assim, pelo Teorema 5.1.6, obtemos que H' é finito. Agora, como G é um FC-grupo, temos que G/H' é também um FC-grupo, e claramente também é um grupo abeliano-por-finito. Desta forma, pelo Lema 5.1.5 temos que G/H' é central-por-finito. Assim, do Teorema 1.2.3 segue que $(G/H)' = G'/H'$ é finito. Portanto, concluímos que G' é finito, como desejado. $\square$

5.2. Resultados Principais Para Grupos Profinitos

Nosso principal objetivo nesta seção é mostrar que em um grupo profinito G, satisfazendo a Hipótese 1, existe um subgrupo normal finito, tal que o quociente de G por este subgrupo seja localmente nilpotente. O primeiro passo será mostrar que se a Hipótese 1 é válida em um grupo profinito G, então G possui um subgrupo aberto localmente nilpotente. De fato, a proposição a seguir garante que, em um grupo profinito G satisfazendo a Hipótese 1, existe um subgrupo aberto normal pronilpotente. Assim aplicando, a este subgrupo, o Lema 5.1.2 temos a existência de um subgrupo aberto normal localmente nilpotente em G, como desejado.

Note que uma consequência indireta da proposição a seguir é que o maior subgrupo normal pronilpotente de G é aberto em G.

Proposição 5.2.1. *Se G é um grupo profinito satisfazendo a Hipótese 1, então G possui um subgrupo aberto normal pronilpotente.*

DEMONSTRAÇÃO. Como, por hipótese, $E_{n(g)}(g)$ é finito para cada $g \in G$, segue pelo Lema 4.5.7 que, para cada $g \in G$, existe um subgrupo normal aberto N_g de G tal que $E_{n(g)}(g) \cap N_g = 1$. Desta maneira g é um elemento Engel em $N_g\langle g\rangle$. Pois, sabendo que para o elemento g em G existe um inteiro $n(g)$, consideremos então o comutador $[x, \underbrace{g, \ldots, g}_{n(g)}]$, onde x é um elemento qualquer de $N_g\langle g\rangle$. Como $N_g \lhd G$, temos $[x, \underbrace{g, \ldots, g}_{n(g)}] \in N_g$ e, por outro lado, $[x, \underbrace{g, \ldots, g}_{n(g)}] \in E_{n(g)}(g)$, por definição. Assim, $[x, \underbrace{g, \ldots, g}_{n(g)}] \in E_{n(g)} \cap N_g$, o que implica em $[x, \underbrace{g, \ldots, g}_{n(g)}] = 1$ e a afirmação segue. Agora, para todo $H \lhd_\circ N_g\langle g\rangle$, como g é um elemento Engel em $N_g\langle g\rangle$, tem-se que $\overline{g}$, a imagem de g em $N_g\langle g\rangle/H$, é um elemento Engel em $N_g\langle g\rangle/H$. Desta forma, como $N_g\langle g\rangle/H$ é um grupo finito e $\overline{g}$ é um elemento Engel em $N_g\langle g\rangle/H$ segue, pelo Teorema 2.0.13, que $\overline{g}$ pertence ao subgrupo de Fitting de $N_g\langle g\rangle/H$. Uma vez que H foi tomado arbitrariamente, esta afirmação vale para qualquer quociente finito de $N_g\langle g\rangle$. Disto decorre que o (fecho do) subgrupo $[N_g, g]$ é pronilpotente. Com efeito, consideremos a imagem (do fecho) de $[N_g, g]$ em cada quociente finito $N_g\langle g\rangle/H$. Agora, sabendo que $\overline{g} \in F(N_g\langle g\rangle/H)$ concluímos que $[\overline{x}, \overline{g}]$ pertence ao $F(N_g\langle g\rangle/H)$ para todo $\overline{x} \in \overline{N_g}$. Disto segue que $[\overline{N_g}, \overline{g}] \leq F(N_g\langle g\rangle/H)$, para todo H subgrupo normal aberto de $N_g\langle g\rangle$. Assim, a imagem (do fecho) de $[N_g, g]$ em $N_g\langle g\rangle/H$ é um grupo nilpotente finito. Então, pelo Teorema 4.4.5 item (i), tem-se que o (fecho do) subgrupo $[N_g, g]$ é topologicamente isomorfo ao limite inverso de um sistema inverso de grupos finitos nilpotentes e portanto é pronilpotente. Indicamos, sem perda de generalidade, com $[N_g, g]$ o mesmo subgrupo ou o fecho dele, caso não seja fechado.

Seja $\widetilde{N_g}$ o fecho normal de $[N_g, g]$ em G. Uma vez que $[N_g, g]$ é normal em N_g, temos que $N_g \leq N_G([N_g, g])$. Como N_g possui índice finito em G, segue que $[N_g, g]$ possui somente uma quantidade finita de conjugados em G. Agora, por $[N_g, g]$ ser isomorfo a $[N_g, g]^x$ para cada $x \in G$, temos que $[N_g, g]^x$ é normal em N_g

e pronilpotente. Assim, $\widetilde{N_g}$ é um produto de uma quantidade finita de subgrupos normais de N_g, cada um dos quais é pronilpotente. Então, segue do Corolário 4.7.5 que $\widetilde{N_g}$ é pronilpotente. Portanto, todos os subgrupos do tipo $\widetilde{N_g}$, construídos ao variar g em G, estão contidos no maior subgrupo normal pronilpotente de G, que denotamos por K.

Notemos que G/K é um FC-grupo. Para isto, vejamos que cada elemento $\overline{g}$ de G/K é centralizado pela imagem de N_g no quociente G/K. Com efeito, consideremos $\overline{y} = yK$, com y um elemento qualquer de N_gK e dado $\overline{g}$ um elemento de G/K, temos que

$$C_{G/K}(\overline{g}) = \{\overline{x} \in G/K \mid [\overline{x}, \overline{g}] = 1\} = \{\overline{x} \in G/K \mid [x, g] \in K\}.$$

Note que como $y \in N_gK$, tem-se $y = zk$ com $z \in N_g$ e $k \in K$, então $[y, g] = [z, g]^k[k, g] \in [N_g, g]^K K$. Por outro lado, como K contém $\widetilde{N_g}$, obtemos que $[N_g, g]^K \leq K$. Logo, concluímos que $[y, g] \in K$. Portanto, $\overline{y} \in C_{G/K}(\overline{g})$ como desejado. Agora, como N_g é aberto, tem-se que $[G : N_gK]$ é finito e segue que $[G/K : N_gK/K]$ também é finito. Consequentemente, temos que $[G/K : C_{G/K}(\overline{g})]$ é finito para cada $\overline{g} \in G/K$. Portanto, G/K é um FC-grupo como queríamos mostrar. Agora, sendo G/K profinito, pelo Teorema 5.1.7, segue que o subgrupo derivado de G/K é finito. Assim, aplicando o Lema 4.5.7, temos que existe um subgrupo normal aberto H/K de G/K com $K \leq H \trianglelefteq G$, de modo que $H/K \cap (G/K)' = 1$. Em particular, temos que H/K é abeliano. Seja H sua imagem inversa em G. Então, H é um subgrupo aberto normal de G, pois H/K é aberto normal em G/K, com a propriedade que H' está contido em K. De fato, como $(H/K)' = H'K/K = 1$, tem-se que $H'K = K$, ou seja $H' \leq K$.

Consideremos o quociente metabeliano $M = H/K'$. Note que M claramente satisfaz a Hipótese 1, pois é uma seção de G. Usaremos provisoriamente os símbolos $E_i(g)$, para denotar os elementos de M e os correspondentes subgrupos. Assim, para cada par (i, j) de inteiros positivos, o conjunto $E_{i,j} = \{x \in M \mid |E_i(x)| \leq j\}$ é fechado. Pois, definindo a aplicação f de M em $\mathbb{N}$ dada por $f(x) = |E_i(x)|$ para cada $x \in M$, vemos que f é contínua, e temos que $f^{-1}(\{1, \ldots, j\}) = E_{i,j}$ é fechado. Agora, usando a Hipótese 1, tem-se que $M = \bigcup_{i,j} E_{i,j}$. De fato, uma inclusão é óbvia, e por outro lado, dado $x \in M$, como M satisfaz a Hipótese 1, existe um inteiro positivo $i = i(x)$ tal que $E_i(x)$ é finito, logo $|E_i(x)| = j$ para algum inteiro j. Assim, existe um par (i, j) tal que $|E_i(x)| \leq j$. Deste modo, $x \in E_{i,j}$, o que implica que M está contido em $\bigcup_{i,j} E_{i,j}$. A igualdade segue, como afirmamos acima.

Assim, como M é profinito e $\{E_{i,j} \mid i, j \in \mathbb{N}\}$ é uma família enumerável de conjuntos fechados com $M = \bigcup_{i,j} E_{i,j}$, segue, pelo Lema 4.4.7, que existem um par de inteiros n e m, um elemento $a \in M$ e um subgrupo aberto U de M tal que $aU \subseteq E_{n,m}$. Ou seja, $|E_n(au)| \leq m$, para todo $u \in U$.

Do argumento anterior segue que $|E_{2n+1}(u)| \leq m^2$ para qualquer $u \in U$. Com efeito, consideremos os subgrupos:

$$E_{M',n}(a) = \langle [x, \underbrace{a, \ldots, a}_{n}] \mid x \in M' \rangle \text{ e } E_{M',n}(au) = \langle [x, \underbrace{au, \ldots, au}_{n}] \mid x \in M' \rangle.$$

Observe que ambos os subgrupos estão contidos em $E_n(a)$ e $E_n(au)$ respectivamente e assim possuem ordem no máximo m. Desde que M é metabeliano, segue facilmente que $E_{M',n}(a)$ e $E_{M',n}(au)$ são subgrupos normais de M. Agora, considerando o quociente

$$\overline{M} = \frac{M}{E_{M',n}(a)E_{M',n}(au)},$$

os subgrupos $\overline{M'}\langle\overline{a}\rangle$ e $\overline{M'}\langle\overline{au}\rangle$ são normais nilpotentes de classe de nilpotência no máximo n. Desta forma, usando o Teorema 1.2.9, tem-se que o produto $A = \overline{M'}\langle\overline{a}\rangle\overline{M'}\langle\overline{au}\rangle$ é nilpotente de classe de nilpotência no máximo $2n$. Note que $\overline{u} \in A$ e dado um elemento qualquer $\overline{x}$ em $\overline{M}$, como $A \lhd \overline{M}$ temos que

$$[\overline{x}, \underbrace{\overline{u}, \ldots, \overline{u}}_{2n+1}] = 1.$$

Assim, em M segue que $[x, \underbrace{u, \ldots, u}_{2n+1}] \in [M', \underbrace{u, \ldots, u}_{2n}] \leq E_{M',n}(a)E_{M',n}(au)$. Portanto, $E_{2n+1}(u) \leq E_{M',n}(a)E_{M',n}(au)$. Logo, concluímos que $|E_{2n+1}(u)| \leq m^2$ para todo $u \in U$, como queríamos.

Assim, os subgrupos correspondentes $E_{2n+1}(u)$ construídos para todo u em U satisfazem a desigualdade uniforme $|E_{2n+1}(u)| \leq m^2$. Observemos que esta desigualdade também vale em cada quociente finito $\overline{U}$ de U, uma vez que esses quocientes são seções de U. Então, aplicando o Teorema 3.2.1, a cada um $\overline{U}$ desses quocientes finitos de U, concluímos que $|\gamma_\infty(\overline{U})| \leq k$, onde $k = k(m)$ é uma função somente de m. Disto segue que $|\gamma_\infty(U)| \leq k$. De fato temos, pelo Teorema 4.4.5 item (i), que

$$\gamma_\infty(U) \cong \varprojlim_{N \in I} \frac{\gamma_\infty(U)}{\gamma_\infty(U) \cap N} \cong \varprojlim_{N \in I} \frac{\gamma_\infty(U)N}{N},$$

onde I é a base filtrada de todos os subgrupos normais abertos de U.

Agora, consideremos o conjunto $J = \{\gamma_\infty(U) \cap N \mid N \in I\}$ e note que $\bigcap_{N\in I}(\gamma_\infty(U) \cap N) = 1$. Assim, aplicando a Proposição 4.6.2 item (ii), tem-se

$$\begin{aligned} |\gamma_\infty(U)| &= \left[\gamma_\infty(U) : \bigcap_{N\in I}(\gamma_\infty(U) \cap N)\right] \\ &= mmc\{[\gamma_\infty(U) : (\gamma_\infty(U) \cap N)] \mid N \in I\}. \end{aligned}$$

Por outro lado, usando o Lema 4.7.3 item (ii), temos que

$$\gamma_\infty(\overline{U}) = \frac{\gamma_\infty(U)N}{N} \cong \frac{\gamma_\infty(U)}{\gamma_\infty(U) \cap N},$$

para todo $N \in I$. Assim, como $|\gamma_\infty(\overline{U})| \leq k$, tem-se $|\gamma_\infty(U)/(\gamma_\infty(U) \cap N)| \leq k$ para todo $N \in I$. Portanto, concluímos que $|\gamma_\infty(U)| \leq k$.

Seja W a imagem inversa de U, que é um subgrupo aberto de G e consideremos Γ a imagem inversa de $\gamma_\infty(U)$. Agora, definamos

$$F = C_W(\gamma_\infty(U)) = \{w \in W \mid [\Gamma, w] \leq K'\}$$

e lembremos que K é pronilpotente. Assim, pela Proposição 5.1.4 item (ii), concluímos que F é um subgrupo aberto normal pronilpotente em G, como queríamos.

□

Finalmente estamos em condições de demonstrar o Teorema A. Para comodidade do leitor vamos enunciar o resultado na forma completa, repetindo explicitamente a Hipótese 1.

Teorema 5.2.2. *Suponha que G é um grupo profinito tal que, para cada $g \in G$, existe um inteiro positivo $n = n(g)$ tal que $E_n(g)$ é finito. Então G possui um subgrupo normal finito N tal que G/N é localmente nilpotente.*

Demonstração. Nosso objetivo é mostrar que $\gamma_\infty(G)$ é finito. Pois, como $G/\gamma_\infty(G)$ é pronilpotente, profinito e é uma seção de G, temos que a Hipótese 1 é válida. Então, aplicando o Lema 5.1.2 tem-se que $G/\gamma_\infty(G)$ é localmente nilpotente. Assim, o resultado vale considerando $N = \gamma_\infty(G)$.

Denotaremos por $F(L)$ o maior subgrupo normal pronilpotente de um grupo profinito L e sabemos pela Observação 4.7.6 que $F(L)$ sempre existe. Agora, da Proposição 5.2.1, segue que G possui um subgrupo aberto normal pronilpotente, então $F(G)$ é também aberto, uma vez que contém este subgrupo. Logo, $G/F(G)$ é finito.

Desta maneira, como $G/F(G)$ é finito, usaremos indução sobre $|G/F(G)|$ para mostrar que $\gamma_\infty(G)$ é finito. A base desta indução inclue o caso trivial, isto é, se

$|G/F(G)| = 1$, ou seja, $G = F(G)$. Neste caso particular G é pronilpotente, então pelo, Lema 4.7.3 item (iii), temos que $\gamma_\infty(G) = 1$ e o resultado é óbvio. Mas, a maior parte da base da indução está concentrada em considerar o caso quando $G/F(G)$ é um grupo finito simples.

De fato, uma vez mostrada a base da indução, podemos finalizar a demonstração com o seguinte argumento indutivo. Suponhamos que $G/F(G)$ não seja um grupo finito simples e portanto que exista um subgrupo normal próprio não trivial $N/F(G)$ de $G/F(G)$, com $F(G) < N \lhd G$. Notemos que $F(N) = F(G)$. Com efeito, como $F(G)$ é normal em N e pronilpotente, segue pela definição de $F(N)$ que $F(G) \leq F(N)$. Por outro lado, uma vez que $F(N)$ é característico em N, que por sua vez é normal em G, temos que $F(N)$ é normal em G e pronilpotente, assim pela definição de $F(G)$, obtemos que $F(N) \leq F(G)$. Observemos que, pela hipótese em G, em particular, para cada $g \in N$, existe um inteiro positivo $n = n(g)$ tal que $E_{n(g)}(g)$ é finito. Além disso, sabendo que $F(N) < N \lhd G$, temos por correspondência que $N/F(N) \lhd G/F(G)$ e $|N/F(N)| < |G/F(G)|$. Desta forma, aplicando a hipótese de indução em N, obtemos que $\gamma_\infty(N)$ é finito. Observemos, por outro lado, que $N/\gamma_\infty(N) \lhd G/\gamma_\infty(N)$. Daí, obtemos que $N/\gamma_\infty(N) \leq F(G/\gamma_\infty(N))$, uma vez que $N/\gamma_\infty(N)$ é pronilpotente e normal em $G/\gamma_\infty(N)$. Desta maneira, $|N/\gamma_\infty(N)| \leq |F(G/\gamma_\infty(N))|$ e, pelo terceiro teorema do isomorfismo, segue que $\left|\frac{G/\gamma_\infty(N)}{F(G/\gamma_\infty(N))}\right| \leq |G/N|$. Por outro lado, como $F(G) < N \lhd G$, resulta que $|G/N| < |G/F(G)|$. Assim, concluímos que $\left|\frac{G/\gamma_\infty(N)}{F(G/\gamma_\infty(N))}\right| < |G/F(G)|$. Desde que $G/\gamma_\infty(N)$ é uma seção de G, tem-se que a hipótese do teorema também é válida para a mesma. Portanto, aplicando a hipótese de indução em $G/\gamma_\infty(N)$, obtemos que o grupo $\gamma_\infty\left(G/\gamma_\infty(N)\right)$ é também finito. Então, aplicando o Lema 4.7.3 item (ii), tem-se

$$\gamma_\infty\left(G/\gamma_\infty(N)\right) = \frac{\gamma_\infty(G)\gamma_\infty(N)}{\gamma_\infty(N)} = \frac{\gamma_\infty(G)}{\gamma_\infty(N)}.$$

Disto segue que $\gamma_\infty(G)/\gamma_\infty(N)$ é finito. E lembrando que $\gamma_\infty(N)$ é finito, concluímos que $\gamma_\infty(G)$ é finito, como desejado. Assim, o argumento indutivo está completo e o resultado segue.

Daqui em diante, vamos portanto nos concentrar no caso base da indução, assumindo que $G/F(G)$ é um grupo finito simples qualquer (abeliano ou não abeliano). Consideremos o epimorfismo canônico de G em $G/F(G)$ e seja p um primo divisor de $|G/F(G)|$, então existe $\overline{g} \in G/F(G)$ tal que a ordem de $\overline{g}$ é igual a p. Portanto, consideremos $g \in G\backslash F(G)$ um elemento de ordem p^n com $n \leq \infty$. Para qualquer primo $q \neq p$, temos que o elemento g age por conjugação no q-subgrupo de Sylow Q de $F(G)$ como um automorfismo de ordem que divide p^n. De fato, como $F(G)$ é pronilpotente, temos que Q é um subgrupo normal de $F(G)$, para qualquer primo q, e sendo $F(G)$ um subgrupo característico de G, em particular, Q é um subgrupo normal de G.

Observe que o subgrupo $[Q, g]$ é normal em Q e este por sua vez é característico em $F(G)$, portanto $[Q, g]$ é normal em $F(G)$. Vejamos, a seguir, que a imagem de $[Q, g]$ em qualquer quociente finito de G está contida na imagem de $E_{n(g)}(g)$. Com efeito, sejam $N \lhd_o G$ e ϕ o epimorfismo canônico de G em G/N, temos que $\phi(Q) = \overline{Q} \leq G/N$ é um q-grupo finito, $\overline{g} \in G/N$ é um q'-elemento. Desta forma, pelo Lema 3.1.2, concluímos que

$$[\overline{Q}, \overline{g}] \leq E(\overline{g}) \leq E_{n(\overline{g})}(\overline{g}).$$

Claramente temos que $\phi([Q, g]) = [\overline{Q}, \overline{g}]$ e usando a Proposição 2.0.16 item (i) obtemos $\phi(E_{n(g)}(g)) = E_{n(\overline{g})}(\overline{g})$. Uma vez que N foi tomado arbitrariamente, o argumento vale para todo subgrupo normal aberto de G. Logo, concluímos que a imagem de $[Q, g]$, em qualquer quociente finito, está contida na imagem de $E_{n(g)}(g)$. Assim, para cada $N \lhd_o G$, temos

$$\frac{[Q, g]N}{N} = \phi([Q, g]) \leq \phi(E_{n(g)}(g)) = \frac{E_{n(g)}(g)N}{N}. \qquad (5.2.1)$$

Agora, como $E_{n(g)}(g)$ é fechado, pois é finito, tem-se pelo Teorema 4.4.5 item (i) que

$$[Q, g] \cong \varprojlim_{N \in I} \frac{[Q, g]}{[Q, g] \cap N} \quad \text{e} \quad E_{n(g)}(g) \cong \varprojlim_{N \in I} \frac{E_{n(g)}(g)}{E_{n(g)}(g) \cap N}, \qquad (5.2.2)$$

onde I é a base filtrada de todos os subgrupos normais abertos de G. Então, segue do segundo teorema do isomorfismo, aplicando o limite em (5.2.1) e substituindo por (5.2.2) temos que $[Q, g] \leq E_{n(g)}(g)$. Desde que $E_{n(g)}(g)$ é finito, obtemos que $[Q, g]$ é também finito.

Como $[Q, g]$ é normal em $F(G)$, seu fecho normal $\langle [Q, g]^G \rangle$ em G é um produto de uma quantidade finita de conjugados. Pois, desde que $[Q, g]$ é normal em $F(G)$, segue que $F(G) \leq N_G([Q, g]) \leq G$. Logo, o índice $[G : N_G([Q, g])]$ divide $[G : F(G)]$ e como $[G : F(G)]$ é finito, resulta que $[G : N_G([Q, g])]$ é finito. Portanto, concluímos que a ordem de $[Q, g]^G$ é finita. Consequentemente, por $[Q, g]^a$ ser finito, para cada $a \in G$, temos que o fecho normal $\langle [Q, g]^G \rangle$ em G é um produto de uma quantidade finita de conjugados. Logo, segue que $\langle [Q, g]^G \rangle$ também é finito.

Denotamos agora por R o produto dos fechos normais $\langle [Q,g]^G \rangle$ ao variar de Q entre todos os q-subgrupos de Sylow de $F(G)$ para $q \neq p$. Sabendo que $[Q,g] \leq E_{n(g)}(g)$, obtemos que existe somente uma quantidade finita de primos q tal que $[Q,g] \neq 1$ para o correspondente q-subgrupo de Sylow Q de $F(G)$. De fato, suponhamos que para todo primo $q \neq p$ tivéssemos $[Q,g] \neq 1$. Então, teríamos que $\prod_{q \neq p} [Q,g] \leq E_{n(g)}(g)$ uma vez que $[Q,g] \leq E_{n(g)}(g)$ e por $E_{n(g)}(g)$ ser finito, isso seria um absurdo. Lembrando que todo fecho normal $\langle [Q,g]^G \rangle$ em G é finito, concluímos que R é também finito.

Sendo o nosso objetivo mostrar que $\gamma_\infty(G)$ é finito, é suficiente mostrar que $\gamma_\infty(G/R)$ é finito. De fato, pelo Lema 4.7.3 item (ii), temos que

$$\gamma_\infty(G/R) = \frac{\gamma_\infty(G)R}{R} \cong \frac{\gamma_\infty(G)}{\gamma_\infty(G) \cap R}.$$

Então, se mostrarmos que $\gamma_\infty(G/R)$ é finito, segue pelo isomorfismo que $\gamma_\infty(G)/(\gamma_\infty(G) \cap R)$ é finito. Assim, como $1 \leq \gamma_\infty(G) \cap R \leq R$, e R é finito, obtemos que $\gamma_\infty(G) \cap R$ é finito. Agora, combinando as duas informações, concluímos que $\gamma_\infty(G)$ é finito. Então, sem perda de generalidade, como podemos trabalhar em G/R, vamos assumir que $R = 1$. Sob esta hipótese e pela definição de R, sabemos que $[Q, g^a] \leq R$ para qualquer conjugado g^a de g e qualquer q-subgrupo de Sylow Q de $F(G)$ para $q \neq p$, e portanto segue que $[Q, g^a] = 1$.

Escolhamos agora, um transversal $\{t_1, \ldots, t_k\}$ de $F(G)$ em G, onde $k = |G/F(G)|$. Seja $G_1 = \langle g^{t_1}, \ldots, g^{t_k} \rangle$. Note que $G_1F(G)/F(G)$ é gerado pela classe de conjugação da imagem de g em $G/F(G)$. Isto implica que $G_1F(G)/F(G)$ é um subgrupo normal de $G/F(G)$, pois o mesmo é gerado por um conjunto normal. Agora, vejamos que $G_1F(G)/F(G)$ é não trivial. Com efeito, se fosse trivial, teríamos que $G_1 \leq F(G)$, o que é uma contradição, pois $G_1 = \langle g^{t_1}, \ldots, g^{t_k} \rangle$ com $g \in G \backslash F(G)$. Deste modo, como $G/F(G)$ é simples, concluímos que $G_1F(G)/F(G) = G/F(G)$, e em particular, segue que $G = G_1F(G)$.

Seja T o produto Cartesiano de todos os q-subgrupos de Sylow de $F(G)$ com $q \neq p$. Temos que T é centralizado por todos os elementos g^{t_i}, uma vez que $[Q, g^a] = 1$ para qualquer conjugado g^a de g e qualquer q-subgrupo de Sylow Q de $F(G)$ com $q \neq p$. Assim, como $G_1 = \langle g^{t_1}, \ldots, g^{t_k} \rangle$ e sabendo que cada um dos geradores g^{t_i} centraliza T, obtemos que $[G_1, T] = 1$. Seja P o p-subgrupo de Sylow de $F(G)$, possivelmente trivial. Notemos que $[P,T] = 1$. De fato, como os elementos de P e T possuem ordens coprima e $F(G)$ é pronilponte, tem-se que $[P,T] = 1$.

Agora vamos provar que $\gamma_\infty(G) \cap T$ é finito. De fato, consideremos o grupo quociente $G/P = \overline{G}$. Como $G = G_1F(G)$, temos que a imagem de T tem índice finito em $\overline{G}$, uma vez que $G/F(G)$ é finito. Então, quocientando por P, podemos assumir que T possui agora índice finito em G, pois assumimos que $P = 1$. Assim, como $[G_1, T] = 1$, temos que $T \cap G_1 \leq Z(G_1)$ e sabendo que $[G : T]$ é finito, concluímos que $[G_1 : T \cap G_1]$ é finito. Isto implica que $[G_1 : Z(G_1)]$ é finito. Logo, pelo Teorema 1.2.3, resulta que G_1' é finito. Agora, como G_1' é normalizado por G_1 e por T e lembrando que $G = G_1T$, segue que $G_1' \lhd G$. Por ser G_1' finito, podemos considerar o quociente sobre ele. Assim, podemos assumir que G_1 é abeliano. Por outro lado, note que G_1 é um p-grupo abeliano, uma vez que G_1 é gerado por p-elementos e usando que $[G_1, T] = 1$, obtemos que G_1 é um subgrupo normal pronilpotente. Desde que T é pronilpotente e sabendo que $G = G_1T$ segue, pelo Lema 4.7.4, que G é pronilpotente e portanto, pelo Lema 4.7.3 item (iii), tem-se $\gamma_\infty(G) = 1$. Pela construção feita temos que $\gamma_\infty(G) \leq G_1'$ que foi provado ser finito, o que implica que $\gamma_\infty(G) \cap T$ é finito, como queríamos.

Deste modo, para mostrarmos que $\gamma_\infty(G)$ é finito, é suficiente ver que $\gamma_\infty(G/T)$ é finito. De fato, temos pelo Lema 4.7.3 item (ii), que

$$\gamma_\infty(G/T) = \frac{\gamma_\infty(G)T}{T} \cong \frac{\gamma_\infty(G)}{\gamma_\infty(G) \cap T}.$$

Então, se $\gamma_\infty(G/T)$ é finito segue que $\gamma_\infty(G)/(\gamma_\infty(G) \cap T)$ é finito. Assim, sabendo que $\gamma_\infty(G) \cap T$ e $\gamma_\infty(G)/(\gamma_\infty(G) \cap T)$ são ambos finitos, obtemos que $\gamma_\infty(G)$ é finito. Vamos mostrar que $\gamma_\infty(G/T)$ é finito. Sem perda de generalidade, podemos assumir que $T = 1$. Logo, podemos assumir que $F(G)$ é um p-grupo, uma vez que $F(G) \cong T \times P$.

Lembrando que estamos no caso em que $G/F(G)$ é um grupo finito simples, chegamos a um ponto em que precisamos distinguir dois subcasos. Primeiramente, se $G/F(G)$ é um grupo finito abeliano simples, então $|G/F(G)| = p$ e como $F(G)$ é um p-grupo segue que G é um grupo pro-p. Logo, G é pronilpotente, consequentemente $\gamma_\infty(G) = 1$ e o resultado segue. Agora, suponhamos que $G/F(G)$ seja um grupo finito simples não abeliano e lembramos que, nas nossas hipóteses, estamos considerando $F(G)$ um p-grupo. Então, escolhemos outro primo $r \neq p$ dividindo $|G/F(G)|$ e podemos repetir todos os mesmos argumentos, como acima, com r no lugar de p. Observe que podemos repetir esta ideia todas as vezes que for necessário e vamos reduzir a prova ao caso em que $F(G) = 1$. Neste caso, $G/F(G) = G$ é finito. Portanto, $\gamma_\infty(G)$ é finito e o resultado segue.

Isto conclui a prova do passo base da indução e, pelo explicado ao começo da demonstração, conclui também a demonstração. □

O próximo corolário segue combinado o Teorema 3.2.1 e o Teorema 5.2.2.

Corolário 5.2.3. *Suponha que G é um grupo profinito e existe um inteiro positivo m tal que para cada $g \in G$ existe $n = n(g)$ tal que $|E_n(g)| \leq m$. Então G possui um subgrupo normal finito N de ordem limitada em termos de m tal que G/N é localmente nilpotente.*

Demonstração. Com efeito, como por hipótese existe um inteiro positivo m tal que para cada $g \in G$ existe $n = n(g)$ tal que $|E_n(g)| \leq m$, então temos que $E_n(g)$ é finito para todo $g \in G$. Assim, aplicando o Teorema 5.2.2, concluímos que G possui um subgrupo normal finito N tal que G/N é localmente nilpotente. Segue da demonstração do Teorema 5.2.2 que este subgrupo N é o subgrupo residual pronilpotente $\gamma_\infty(G)$ de G. Desta forma, resta mostrarmos que $\gamma_\infty(G)$ possui ordem limitada em termos de m. De fato, seja $N \lhd_\circ G$ e consideremos o quociente finito G/N. Como G/N é uma seção de G, usando a Proposição 2.0.16 item (iv), vemos que $|E_n(\overline{g})| \leq m$ para todo $\overline{g} \in G/N$. Disto segue que $|E(\overline{g})| \leq m$ para todo $\overline{g} \in G/N$ e como G/N é finito, obtemos pelo Teorema 3.2.1, que a ordem do residual nilpotente $\gamma_\infty(G/N)$ é m-limitada. Agora, pelo Lema 4.7.3 item (ii) tem-se

$$\gamma_\infty(G/N) = \frac{\gamma_\infty(G)N}{N} \cong \frac{\gamma_\infty(G)}{\gamma_\infty(G) \cap N}. \tag{5.2.3}$$

Logo, temos que a ordem de $\gamma_\infty(G)/(\gamma_\infty(G) \cap N)$ é m-limitada. Como o subgrupo N foi tomado arbitrariamente segue, para qualquer subgrupo normal aberto de G, que (5.2.3) vale. Assim, como $\gamma_\infty(G)$ é finito, obtemos pelo Lema 4.5.7 que existe um subgrupo normal aberto M de G tal que $\gamma_\infty(G) \cap M = 1$. Então, concluímos por (5.2.3) que a ordem de $\gamma_\infty(G)$ é limitada em termos de m, e o resultado segue.

□

Referências Bibliográficas

[1] M. Aschbacher, *Finite Group Theory*, Cambridge University Press, 1988.

[2] D. Gorenstein, *Finite Groups*, 2nd Ed., Chelsea, New York, 1980.

[3] D. Gorenstein, *Finite Simple Groups-An Introduction to their Classification*, Springer, 1982.

[4] O. Grün, Beitrge zur Gruppentheorie. I, *J. Reine Angew. Math.* **174** (1935), 1-14.

[5] P. Hall and G. Higman, The p-length of a p-soluble group and reduction theorems for Burnside's problem, *Proc. London Math. Soc. (3)*, **6** (1956), 1-42.

[6] P. Hall, Some sufficient conditions for a group to be nilpotent, *Illinois J. Math.*, **2** (1958), 787-801.

[7] B. Huppert, *Endliche Gruppen I*, Springer, Berlin, 1967.

[8] M. I. Kargopolov and Ju. I. Merzljakov, *Fundamentals of the Theory of Groups*, Springer, Berlin, 1979.

[9] J. L. Kelley, *General Topology*, Springer, Berlin, 1975.

[10] E. I. Khukhro, *Nilpotent Groups and their Automorphisms*, Berlin-New York, 1993.

[11] E. I. Khukhro, *p-Automorphisms of Finite p-Groups*, Cambridge University Press, 1998.

[12] E. I. Khukhro and V. D. Mazurov, Finite groups with an automorphism of prime order whose centralizer has small rank, *J. Algebra*, **301** (2006), 474-492.

[13] E. I. Khukhro and P. Shumyatsky, Almost Engel finite and profinite groups, *Int. J. Algebra Comput.*, **5** (2016), 973-983.

[14] E. I. Khukhro and P. Shumyatsky, Engel-type subgroups and length parameters of finite groups, *Israel Journal of Mathematics* (2017), to appear.

[15] I. M. Isaacs, *Finite Group Theory*, Amer. Math. Soc., 2008.

[16] I. M. Isaacs, *Algebra. A Graduate Course*, Amer. Math. Soc., 2009.

[17] S. A. Morris, *Topology Without Tears*, 2016, http://www.topologywithouttears.net/topbook.pdf.

[18] B. H. Neumann, A problem of Paul Erdös on groups, *J. Aust. Math. Soc.*, **21** (1976), no. 04, 467-472.

[19] L. Ribes and P. Zalesskii, *Profinite Groups*, 2nd Edition, Springer, 2010.

[20] D. J. S. Robinson, *Finiteness Conditions and Generalized Soluble Groups*, Springer-Verlag, 1972.

[21] D. J. S. Robinson, *A Course in the Theory of Groups*, 2nd Ed., Springer-Verlag, 1996.

[22] J. S. Rose, *A Course on Group Theory*, Cambridge University Press, 1978.

[23] J. J. Rotman, *An Introduction to the Theory of Groups*, 4th Edition, Springer-Verlag, 1994.

[24] A. Shalev, Profinite groups with restricted centralizers, *Proc. Amer. Math. Soc.*, **122** (1994), 1279-1284.

[25] J. S. Wilson, *Profinite Groups*, Clarendon Press, Oxford, 1998.

[26] J. S. Wilson and E. I. Zelmanov, Identites for Lie algebras of pro-p groups, *J. Pure Appl. Algebra*, **81** (1992), 103-109.