Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

Involuções e seus Centralizadores em Grupos Finitos

por

Jéssyca Cristine Lima de Souza

Orientador: Cristina Acciarri

Brasília
2016

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

Souza, Jéssyca Cristine
S SO719 Involuções e seus Centralizadores em Grupos
i Finitos / Jéssyca Cristine Souza; orientador
Cristina Acciarri. -- Brasília, 2016.
76 p.

Dissertação (Mestrado - Mestrado em Matemática) --
Universidade de Brasília, 2016.

1. Involuções e seus centralizadores em grupos
finitos.. I. Acciarri, Cristina , orient. II. Título.

Ao Rafael

Agradecimentos

Gostaria de agradecer ao meu marido, Rafael Silva Franco, por todo amor e companheirismo. Obrigada por estar ao meu lado em todos os momentos, por cuidar de mim sempre, por me cobrir de noite e pelo apoio incondicional. Agradeço por ter me acolhido quando eu mais precisava e por ter sido parte fundamental em todas as minhas conquistas.

À minha irmã, Jacqueline Cristina Lima de Souza, por todos os filmes (bons e ruins), pela ótima companhia em qualquer momento e pela amizade e amor incondicionais. À minha mãe, Simone Gomes, pelo amor durante todos esses anos.

À minha orientadora, Cristina Acciarri, pela extrema eficiência e dedicação ao trabalho. Obrigada pelo apoio, paciência e por não me deixar desistir em nenhum momento.

Aos professores e trabalhadores do Departamento de Matemática. Em particular, à Professora Aline Pinto, por estar presente desde a graduação ministrando cursos excepcionais e sendo um exemplo e inspiração para mim. Ao Professor Luís Henrique de Miranda pela matéria mais difícil que fiz até hoje, graças a ele sei como é chorar de felicidade ao receber uma nota. Ao professor José Antônio de Freitas pela primeira matéria da matemática e primeira matéria de Álgebra que fiz na UnB. Aos professores que ministraram as matérias de introdução no mestrado, Cátia Regina Gonçalves, Cristina Acciarri, Luciana Maria Rodrigues e Ricardo Ruviaro; pelas excelentes aulas que me prepararam para os exames.

À Rebeca Chuffi, por ter me acompanhado desde o primeiro semestre de gradução, pelo apoio e amizade incondicionais. Obrigada por me acompanhar nos semestres malucos (e entender que não tinha como não fazer todas aquelas matérias), por me fazer sempre ter certeza de que eu sou louca, burra, esquisita e me visto mal. Obrigada por ter sido parte de mim por todo esse tempo e não ter me deixado desistir nunca. Ao Victor Jatobá por entender que a Rebeca é parte de mim, por fazer ela feliz e pelo apoio durante esse anos (ainda não te perdoei por ter levado ela para Chicago!).

À Angélica Felix, pela amizade desde o primeiro semestre de graduação. Obrigada por ser essa amiga engraçada, divertida, sincera e leal. Sei que posso sempre contar com você e sei que serei corrigida se estiver errada. Obrigada pelo apoio em todos

os momentos, amiga. Ao Bruno Xavier por me contar que o cubo é uma variedade diferencial, pelas caronas e partidas de LOL.

Aos membros do PET e do PIBID, em especial ao Leandro Chiarini e à Carol Lafetá, pelas partidas de AVALON e todas as brincadeiras durante esses anos de UnB.

Ao CNPq/CAPES pelo apoio financeiro concedido durante a elaboração deste trabalho.

Resumo

Seja ϕ um automorfismo de ordem prima p de um grupo finito G. A estrutura do subgrupo de pontos fixos $C_G(\phi)$ de ϕ em G tem forte influência sobre a estrutura de G. Por exemplo, sabemos que se $C_G(\phi) = 1$, então G é nilpotente com classe de nilpotência limitada em termos de p [[10] e [25]].

É natural considerar que o centralizador $C_G(\phi)$ satisfaz algumas condições, como ter posto finito r, e analisar quais são as consequências sobre a estrutura de G.

Em [16] é apresentada a questão de determinar se é verdade que, dado um grupo finito nilpotente G admitindo um automorfismo ϕ de ordem prima p tal que $C_G(\phi)$ tem posto r, G sempre possui um subgrupo normal N tal que o posto de G/N é limitado em termos de p e r somente e N possui classe de nilpotência limitada em função de p.

Em [24], que é a referência principal deste trabalho, Shumyatsky mostra que a questão posta antes possui resposta afirmativa no caso particular em que $p = 2$, ou seja, quando ϕ é uma involução.

Também se prova que, se eliminarmos a hipótese de G ser nilpotente, o posto do centralizador $C_G(\phi)$ da involução ϕ continua tendo forte impacto sobre a estrutura de um grupo G de ordem ímpar. Além disso, em algumas situações é até possível limitar o comprimento derivado de G em termos do posto de $C_G(\phi)$.

Palavras-chave: Grupos Finitos, Automorfismos, Centralizadores.

Abstract

Let G be a finite group admitting an automorphism ϕ of prime order p. The structure of the centralizer $C_G(\phi)$ of ϕ in G has strong influence on the structure of G. For instance, it is well-know that if $C_G(\phi) = 1$, then G is nilpotent of nilpotency class bounded from above by a function of p [[10] and [25]].

It is natural to consider the situation when the centralizer $C_G(\phi)$ satisfies some conditions, as being of finite rank r, and ask what kind of consequences we get on the structure of G.

In [16], the following problem is raised: given a finite nilpotent group G admitting an automorphism ϕ of prime order p such that $C_G(\phi)$ is of rank r, does this imply that the group G possess a normal subgroup N such that the rank of G/N is bounded in terms of p and r, and N has nilpotency class bounded from above by a fuction of p?

In [24], the main reference of this essay, Shumyatsky shows that the question above has an affirmative answer in the particular case when $p = 2$, that is, when ϕ is an involutory automorphism.

It is also proved that even if G is not nilpotent, the rank of the centralizer $C_G(\phi)$ of an involutory automorphism ϕ still has a strong impact on the structure of a group G of odd order. Moreover, in some situations it is also possible to bound the derived length of G in terms of the rank of $C_G(\phi)$.

Keywords: Finite Groups, Automorphisms, Centralizers.

Sumário

Introdução

Seja G um grupo finito e considere ϕ um automorfismo de G de ordem prima p. Existem muitos resultados na literatura que mostram como a estrutura do subgrupo de pontos fixos $C_G(\phi)$ de ϕ em G exerce forte influência sobre a estrutura do grupo G. Por exemplo, se ϕ tem ordem dois, ou seja, se ϕ é uma involução de G, e sabemos que $C_G(\phi) = 1$, então G é abeliano. Esse é um resultado elementar que já ilustra bem o fenômeno.

Outro exemplo clássico é o famoso resultado, combinação dos trabalhos de J. G. Thompson [25] e G. Higman [10], que nos fornece que se G é um grupo finito admitindo um automorfismo ϕ de ordem prima p tal que $C_G(\phi) = 1$, então G é nilpotente com classe de nilpotência limitada por uma função que depende apenas de p.

Impondo condições sobre a ordem de $C_G(\phi)$, também é possível obter importantes consequências sobre a estrutura de G. A combinação dos trabalhos de Khukhro [13], Fong [4] e Hartley e Meixner [9] leva ao seguinte resultado: se G é um grupo finito admitindo um automorfismo ϕ de ordem prima p tal que $|C_G(\phi)| \leq m$, então G possui um subgrupo normal nilpotente N tal que o índice $|G : N|$ é limitado por uma função que depende apenas de m e de p e, além disso, a classe de nilpotência de N é limitada por uma função dependendo apenas de p. Mais em concreto, o trabalho de Fong [4] mostra que o índice do radical solúvel é limitado "módulo" a classificação dos grupos finitos simples, no artigo de Hartley e Meixner [9] se limita o índice do subgrupo de Fitting no caso de um grupo solúvel e em [13] Khukhro considera o caso particular dos grupos nilpotentes. Notemos, também, que se ϕ for tomado de ordem $p = 2$, então em [8] Hartley e Meixner mostram que, de fato, o subgrupo nilpotente N pode ser escolhido como tendo classe de nilpotência, no máximo, 2.

É natural pensar em impor outros tipos de restrições sobre o centralizador $C_G(\phi)$ e analisar quais são as consequências disso sobre a estrutura de G. Por exemplo, substituindo a condição de $C_G(\phi)$ ter ordem limitada pela de $C_G(\phi)$ ter o posto limitado, podemos nos perguntar se existem resultados análogos aos enunciados anteriormente para um grupo finito G admitindo um automorfismo ϕ de ordem prima. Assim, em [16] Khukhro considera a seguinte questão: dado um grupo finito nilpotente G admitindo um automorfismo ϕ de ordem prima p tal que $C_G(\phi)$ tem posto r, é verdade que G

sempre possui um subgrupo normal N tal que o posto de G/N é limitado em termos de p e de r e N possui classe de nilpotência limitada por uma função de p?

Dado um conjunto $\{a, b, c, ...\}$ de parâmetros, dizemos que um número k é $\{a, b, c, ...\}$-limitado se existe uma função f que depende apenas de $\{a, b, c, ...\}$ tal que $k \leq f$.

No artigo *Involutory automorphisms of finite groups and their centralizers* [24], que é a principal referência deste trabalho, Shumyatsky mostra que a questão posta anteriormente possui resposta afirmativa quando ϕ é uma involução, ou seja, quando $p = 2$, obtendo o seguinte resultado.

Teorema A. *Seja G um grupo finito nilpotente admitindo uma involução ϕ tal que $C_G(\phi)$ tem posto r. Então G possui um subgrupo normal ϕ-invariante N com classe de nipotência, no máximo, 2 tal que o quociente G/N tem posto r-limitado.*

Veremos que a teoria dos p-grupos powerful, introduzida pela primeira vez em [21] por A. Lubotsky e A. Mann, desempenha um papel fundamental na demonstração deste resultado. A ideia para demonstrar o Teorema A é, de fato, fazer uma redução ao caso em que G seja um p-grupo finito. Em seguida, se considera separadamente dois casos, quando $p = 2$ e quando p é ímpar. Nesse último caso, a teoria de p-grupos powerful será essencial para provar que se P é um p-grupo finito admitindo uma involução ϕ tal que $P = [P, \phi]$ e o posto $rk(C_P(\phi)) \leq r$, então o posto de P é limitado em função de r. A partir desse resultado, usando um argumento técnico, se chega a provar que G possui as propriedades enunciadas no Teorema A.

Em [12], E. I. Khukhro e V. D. Mazurov observam que, em geral, dado um grupo finito admitindo um automorfismo ϕ de ordem prima p tal que o posto $rk(C_G(\phi)) \leq r$, existem exemplos em que é impossível limitar o posto do grupo quociente $G/S(G)$, onde $S(G)$ é o radical solúvel de G, ou seja, não é possível obter um resultado análogo ao resultado de Fong [4] no caso em que se considera que $C_G(\phi)$ tem posto limitado e as ordens de G e de ϕ não são coprimas. Além disso, no mesmo artigo, os autores provam um análogo ao resultado de Fong no caso em que as ordens de G e de ϕ são coprimas, limitando o posto do quociente $G/S(G)$ em função do posto de $C_G(\phi)$ e da ordem p do automorfismo ϕ.

Agora, se considerarmos grupos finitos de ordem ímpar e, portanto, solúveis por Feit-Thompson, em [24] Shumyatsky também fornece uma resposta completa mostrando como o centralizador $C_G(\phi)$ de uma involução ϕ continua tendo um forte impacto na estrutura de G. O seguinte resultado é provado.

Teorema B. *Seja G um grupo de ordem ímpar admitindo uma involução ϕ tal que $rk(C_G(\phi)) \leq r$. Então $rk([G, \phi]')$ é r-limitado.*

Com esse resultado vemos que, se G é como nas hipóteses acima, então G possui uma série normal $1 \leq G_1 \leq G_2 \leq G$ tal que $rk(G_1)$ é r-limitado, G_2/G_1 é abeliano e $rk(G/G_2) \leq r$, o que nos fornece uma estrutura bem detalhada do posto de G.

Mais tarde, em [12], E. I. Khukhro e V. D. Mazurov consideram o caso de um grupo solúvel com um automorfismo ϕ de ordem p, onde p é um primo arbitrário, provando um resultado análogo ao Teorema B, ou seja, que se G é um grupo finito solúvel admitindo um automorfismo ϕ de ordem prima p tal que $C_G(\phi)$ tem posto r, então G possui dois subgrupos característicos $R \leq N \leq G$ tais que N/R é nilpotente e G/N e R possuem, ambos, posto $\{p, r\}$-limitado. Os autores também observam que nessa situação mais geral, onde p é um primo qualquer, existem exemplos que mostram que é impossível limitar o posto do grupo quociente $G/F(G)$, ou seja, que um resultado completamente análogo ao teorema de Hartley-Meixner sobre a ordem de $C_G(\phi)$ é impossível de se obter no caso em que se limita o posto de $C_G(\phi)$.

Notamos que, nas condições do Teorema B, em geral não é possível limitar o comprimento derivado de G em termos do posto do centralizador $C_G(\phi)$. De fato, em [18], Kovács e Wall nos fornecem um exemplo de um grupo finito G de ordem ímpar que admite uma involução ϕ tal que seu centralizador $C_G(\phi)$ é cíclico, mas G possui comprimento derivado arbitrariamente grande. Em vista desse exemplo é interessante ver que, como consequência do Teorema B, em [24], Shumyatsky também mostra um resultado que, em algumas codições específicas, permite limitar o comprimento derivado de G em termos do posto de $C_G(\phi)$. Mais em concreto, é mostrado o seguinte resultado.

Corolário C. *Seja G um grupo finito admitindo um 2-automorfismo livre de pontos fixos ψ. Seja ϕ a involução de $\langle\psi\rangle$ e assuma que $rk(C_G(\phi)) = r$. Então, o comprimento derivado de G é r-limitado.*

Concluímos observando que este trabalho está dividido em cinco capítulos. No Capítulo 1, daremos algumas definições e resultados preliminares que serão utilizados ao longo da dissertação. Ele está dividido em quatro tópicos principais: grupos solúveis, grupos nilpotentes, automorfismos e ação coprima e, por último, geradores e postos de um grupo. No Capítulo 2, iremos apresentar a teoria de p-grupos finitos powerful. No Capítulo 3, usando a teoria de p-grupos powerful, vamos desenvolver os fundamentos técnicos para provar que se G é um p-grupo finito admitindo uma involução ϕ tal que $G = [G, \phi]$ e $rk(C_G(\phi)) \leq r$, então o posto de G' é r-limitado. O material apresentado nesse capítulo será fundamental para a prova do Teorema A, portanto nosso interesse será focalizado sobre grupos finitos nilpotentes. No Capítulo 4 iremos desenvolver uma teoria análoga à apresentada no Capítulo 3 para grupos finitos de ordem ímpar admitindo uma involução. Essa teoria será usada mais tarde para demonstrar o Teorema B. Por fim, no Capítulo 5, apresentaremos os principais resultados desta dissertação, dando os detalhes das demonstrações dos Teorema A, Teorema B e Corolário C.

Capítulo 1

Preliminares

O objetivo deste capítulo é apresentar resultados e definições de Teoria de Grupos que servirão de base para o trabalho. Assumiremos como conhecidos alguns resultados como os Teoremas do Isomorfismo, o Teorema de Sylow, o Teorema da Correspondência, entre outros, assim como definições básicas como as definições de grupo, subgrupo, subgrupo normal, índice, entre outras. As principais referências utilizadas aqui serão os livros de D. Gorenstein [6] e de I. M. Isaacs [11]. É possível encontrar nessas referências todas as provas que serão omitidas neste capítulo.

Iremos denotar por G um grupo finito, por $|G|$ a ordem de G e, dado um elemento x em G, $o(g)$ será a ordem de g. Além disso, dada uma aplicação ϕ, usaremos na maioria dos casos a "notação exponencial" x^{ϕ} para indicar a imagem do elemento x pela aplicação ϕ. Outras notações serão introduzidas ao longo do trabalho, quando necessário.

1.1 Grupos Solúveis

Dado um primo p, temos que um grupo G é dito um *p-grupo* se para todo elemento g em G temos que a ordem de g é p^{α}, para algum número natural α. Observe que, se G é finito, então G é um p-grupo se, e somente se, $|G| = p^m$, para algum $m \in \mathbb{N}$.

Denotaremos por $\pi(G)$ o conjunto finito de todos os divisores primos da ordem de um grupo finito G, ou seja

$$\pi(G) = \{p \in \mathbb{P} \mid p \text{ divide } |G|\},$$

onde $\mathbb{P}$ é o conjunto de todos os primos.

Seja π um conjunto de primos e $n \in \mathbb{N}$. Dizemos que n é um π-número se dado qualquer primo p que divide n temos que $p \in \pi$. Denotamos por π' o conjunto complementar de π em $\mathbb{P}$, ou seja, $\pi' = \mathbb{P} \setminus \pi$.

Definição 1.1. *Seja G um grupo finito e π um conjunto 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-subgrupo e $|G : H|$ é um π'-número.*

Definição 1.2. *Seja H um subgrupo de um grupo G. Definimos o "core" de H em G como sendo o subrgupo de G dado por*

$$core_G(H) = \bigcap_{x \in G} H^x,$$

onde, para todo $x \in G$, indicamos com H^x a imagem de H com respeito ao automorfismo interno de G induzido pela conjugação por x, ou seja $H^x = \{x^{-1}hx \mid h \in H\}$.

Note que $core_G(H)$ é o maior subgrupo normal de G contido em H. Além disso, se H é normal em G, então temos que $core_G(H) = H$.

Se considerarmos um qualquer p-subgrupo de Sylow de G e seu *core* em G, podemos dar a seguinte definição.

Definição 1.3. *Seja G um grupo finito e P um qualquer p-subgrupo de Sylow de G. Definimos o p-core de G como sendo o subgrupo dado por*

$$O_p(G) = core_G(P) = \bigcap_{x \in G} P^x = \bigcap_{Q \in Syl_p(G)} Q.$$

Temos que $O_p(G)$ é o maior p-subgrupo normal de G. Observe que $O_p(G)$ é característico em G. Uma outra maneira, equivalente, de definir o subgrupo $O_p(G)$ é a seguinte

$$O_p(G) = \langle K \lhd G \mid K \text{ é } p\text{-subgrupo } \rangle.$$

Observamos que para qualquer conjunto de primos π é possível generalizar a definição acima, denotando por $O_\pi(G)$ o maior π-subgrupo normal de G. O subgrupo $O_\pi(G)$ é característico em G e, pela definição, segue que

$$O_\pi(G/O_\pi(G)) = 1.$$

Em particular, para qualquer primo p, temos que

$$O_p(G/O_p(G)) = 1.$$

Lema 1.4. *Seja G um grupo finito e N um p-subgrupo normal de G. Temos que*

$$O_p(G/N) = O_p(G)/N.$$

Demonstração: Considere o homomorfismo canônico $\varphi : G \to G/N$. Temos que $\varphi(O_p(G)) = O_p(G)/N$. Dado K um p-subgrupo normal de G, pelo Teorema da Correspondência, temos que $KN/N \triangleleft G/N$ e, como K e N são p-grupos, KN/N é um p-subgrupo de G/N, logo, $KN/N \leq O_p(G/N)$. Por outro lado, dado L/N um p-subgrupo normal de G/N, pelo Teorema da Correspondência, segue que $L \triangleleft G$ e, como N é um p-subgrupo de G, L é um p-subgrupo de G, portanto $L \leq O_p(G)$ e, assim, $L/N \leq O_p(G)/N$.

■

Definição 1.5. *Dado G um grupo finito, definimos o subgrupo de Fitting de G por*

$$F(G) = \prod_{p \in \pi(G)} O_p(G).$$

Note que $F(G)$ é característico em G. Observaremos logo outras propriedades importantes do subgrupo $F(G)$.

Dizemos que um subgrupo próprio M de um grupo G é maximal se sempre que $M \leq H \leq G$, ou $M = H$ ou $H = G$ e denotamos por $M \; max \; G$.

Se considerarmos a interseção de todos os subgrupos maximais em G obtemos o seguinte subgrupo.

Definição 1.6. *Seja G um grupo. Definimos o subgrupo de Frattini de G como*

$$\Phi(G) = \bigcap_{M \; max \; G} M.$$

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

Temos que $\Phi(G)$ é um subgrupo característico em G e que $\Phi(G)$ está contido em $F(G)$. Notemos também que, em um grupo finito G, qualquer subgrupo próprio de G está sempre contido em um subgrupo maximal.

Definição 1.7. *Seja G um grupo. Um elemento g de 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.*

É possível mostrar que podemos definir, de maneira equivalente, o subgrupo de Frattini de G como sendo

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

Lembramos que, dados quaisquer dois elementos x e y em G, o *comutador* de x e y é o elemento de G definido por

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

No lema a seguir serão apresentadas as principais propriedades dos comutadores de um grupo, que serão muito usadas durante este trabalho.

Lema 1.8. *(Propriedades dos Comutadores) Seja G um grupo. Dados $x, y, z \in G$, são verdadeiras as seguintes afirmações:*

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

(ii) $[xy, z] = [x, z]^y[y, z]$.

(iii) $[x, yz] = [x, z][x, y]^z$.

(iv) $[x, y^{-1}, z]^y[y, z^{-1}, x]^z[z, x^{-1}, y]^x = 1$.

(v) $[x, z]^y = [x, z][x, z, y]$.

(vi) $yx = xy[y, x]$.

(vii) *Para todo inteiro $n \geq 1$, temos que*

$$[x^n, y] = [x, y]^{x^{n-1}}[x, y]^{x^{n-2}} \cdots [x, y]^x[x, y],$$
$$[x, y^n] = [x, y][x, y]^y \cdots [x, y]^{y^{n-2}}[x, y]^{y^{n-1}}.$$

Sejam A e B dois subgrupos de um grupo G. Podemos definir o comutador de A e B como sendo o seguinte subgrupo de G:

$$[A, B] = \langle [a, b] \mid a \in A,\ b \in B \rangle,$$

gerado por todos os comutadores de elementos de A com elementos de B. Além disso, podemos definir recursivamente comutadores de mais elementos da seguinte maneira: defina $[x_1] = x_1$ por convenção e

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

para todos $x_1, ..., x_n \in G$ e $n \geq 2$. Analogamente, se $A_1, ..., A_n$ são subgrupos de G, definimos o subgrupo $[A_1, \cdots, A_n]$ como sendo

$$[A_1, \cdots, A_n] = [[A_1, \cdots, A_{n-1}], A_n],$$

para todo $n \geq 2$.

Seja G um grupo. Uma *série normal* de G é dada por

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

onde cada N_i é normal em G.

Definição 1.9. *Seja G um grupo. Dizemos que G é solúvel se G possui uma série normal*

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

onde cada quociente N_i/N_{i-1} é abeliano, para todo $1 \leq i \leq s$.

Um caso particular de subgrupo comutador em G é obtido quando consideramos $A = B = G$, obtendo o *subgrupo derivado* ou *subgrupo comutador* de G

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

Assim, dado um grupo G, podemos definir a *série derivada* de G, recursivamente, como sendo

$$G^{(0)} = G,\ G^{(1)} = G' = [G, G] \text{ e } G^{(i)} = [G^{(i-1)}, G^{(i-1)}],$$

para todo $i \geq 2$. Note que cada termo dessa série é o subgrupo derivado do termo anterior, logo todos os $G^{(i)}$ são subgrupos característicos em G e que cada quociente $G^{(i)}/G^{(i+1)}$ é abeliano, para todo $i \geq 0$. Em particular, a série derivada de G é uma série normal de G com todos os fatores abelianos.

Podemos provar que G é solúvel se, e somente se, existe um número m tal que o m-ésimo termo da série derivada de G é 1, ou seja, $G^{(m)} = 1$. Além disso, se G é um grupo solúvel, então, usando a série derivada, podemos ver que todo subgrupo H de G é solúvel, que qualquer imagem homomórfica de G é solúvel e que extensões de grupos solúveis são solúveis.

Definição 1.10. *Seja G um grupo solúvel. Definimos o comprimento derivado de G como o menor inteiro m tal que o m-ésimo termo da série derivada de G é trivial, ou seja, $G^{(m)} = 1$. Denotaremos o comprimeto derivado de G por $dl(G)$.*

Alguns resultados importantes para grupos solúveis, que usaremos neste trabalho, podem ser vistos no teorema a seguir. Os resultados apresentados são semelhantes aos vistos nos Teoremas de Sylow, mas neste novo contexto os subgrupos de Sylow são substituídos pelos π-subgrupos de Hall. Esse teorema é considerado como uma "extensão" dos teoremas de Sylow para grupos solúveis.

Teorema 1.11. *(P. Hall) Seja G um grupo solúvel finito. Então, são válidas as seguintes afirmações:*

(i) *Para todo conjunto de primos π, existe um π-subgrupo de Hall de G.*

(ii) *Fixado um conjunto de primos π, todos os π-subgrupos de Hall de G são conjugados.*

(iii) *Se L é um π-subrgupo de G, para algum conjunto de primos π, então existe um π-subgrupo de Hall S de G tal que $L \leq S$.*

A demonstração do teorema acima pode ser vista em [Theorem 2.1, [6]].

Como já observamos, dados um primo p e um grupo G, denotamos por $O_p(G)$ o único maior p-subgrupo normal de G. Dado um grupo G e um número primo p que divide a ordem de G, podemos definir a *p-série descendente* de G como sendo a série

$$1 \leq O_{p'}(G) \leq O_{p',p}(G) \leq O_{p',p,p'}(G) \leq \cdots,$$

onde cada termo é definido, recursivamente, de modo que $O_{p'}(G)$ é o maior p'-subgrupo normal de G, $O_{p',p}(G)$ é a imagem inversa de $O_p(G/O_{p'}(G))$ em G com respeito ao homomorfismo canônico $G \to G/O_{p'}(G)$. Assim, temos que

$$O_p(G/O_{p'}(G)) = O_{p',p}(G)/O_{p'}(G).$$

De forma semelhante, $O_{p',p,p'}(G)$ será a imagem inversa de $O_{p'}(G/O_{p',p}(G))$ em G e assim por diante. Note que os termos dessa série são característicos em G e cada fator é um p-grupo ou um p'-grupo.

Se G é um grupo finito solúvel, temos que, para todo p primo que divide a ordem de G, o último termo da p-série descendente será igual a G. Com isso, podemos dar a seguinte definição.

Definição 1.12. *Seja G um grupo finito solúvel. Definimos o p-comprimento de G como sendo o número de fatores da p-série descendente de G que são p-subgrupos. Denotaremos o p-comprimento de G por $l_p(G)$.*

Terminamos esta seção dedicada a grupos solúveis enunciando o Teorema de Feit-Thompson [2] que será várias vezes usado ao longo deste trabalho, sem dar referência explícita.

Teorema 1.13. *Todo grupo finito de ordem ímpar é solúvel.*

1.2 Grupos Nilpotentes

Lembramos que, dado um grupo G, uma série normal

$$1 = N_0 \leq N_1 \leq \cdots \leq N_s = G$$

de G é dita *central* se $N_i/N_{i-1} \leq Z(G/N_{i-1})$, para todo $1 \leq i \leq s$.

Definição 1.14. *Um grupo G é dito nilpotente se G possui uma série central.*

Dado um grupo G, é possível definir algumas séries específicas que nos ajudam a determinar se um grupo é nilpotente. A primeira série que veremos é chamada de *série central ascendente* de um grupo G e é definida, recursivamente, como $Z_0(G) = 1$, $Z_1(G) = Z(G)$ e $Z_i(G)$ é o único subgrupo normal em G tal que

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

para todo $i \geq 2$.

Note que todos os termos dessa série são característicos em G. Por definição, é fácil ver que a série central ascendente é uma série central, mas nem sempre G será um termo dessa série. Podemos mostrar que um grupo G é nilpotente se, e somente se, existe um inteiro s tal que $Z_s(G) = G$.

O resultado a seguir nos fornece uma caracterização dos termos da série central ascendente de um grupo G que, muitas vezes, será usada em demonstrações, pois através dela podemos ter uma ideia melhor de algumas propriedades específicas dos elementos dos termos $Z_i(G)$ da série.

Teorema 1.15. *Seja G um grupo. Para todo $n \geq 1$, o n-ésimo termo da série central ascendente de G é dado por*

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

Demonstração: A prova é feita por indução sobre n. Para $n = 1$, temos que $Z_1(G) = Z(G)$. Considere, então, que $n > 1$ e que para todo $k < n$ temos que $Z_k(G) = \{x \in G | [x, g_1, ..., g_k] = 1, \ \forall \ g_1, ..., g_k \in G\}$. Agora, $Z_n(G)$ é o único subgrupo normal de G tal que $Z_n(G)/Z_{n-1}(G) = Z(G/Z_{n-1}(G))$, logo, dado $x \in Z_n(G)$ e $g \in G$ temos que $[x, g] \in Z_{n-1}(G)$, assim, por hipótese de indução, temos que

$$[[x, g], g_1, ..., g_{n-1}] = [x, g, g_1, ..., g_{n-1}] = 1,$$

para quaisquer elementos $g_1, ..., g_n$ de G. Como vale para todo $x \in Z_n(G)$ e para todo $g \in G$, segue que

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

como queríamos.

■

Definição 1.16. *Seja G um grupo nilpotente. O menor natural s tal que $Z_s(G) = G$ é chamado de classe de nilpotência de G e é denotado por $cl(G)$.*

Usando novamente subgrupos comutadores, podemos definir uma segunda série importante para o estudo de grupo nilpotentes que é chamada de *série central descendente*. Mais precisamente, se define:

$$\gamma_1(G) = G,\ \gamma_2(G) = G' = [G, G] \text{ e } \gamma_{i+1}(G) = [\gamma_i(G), G],$$

para todo $i \geq 2$.

Da mesma maneira, temos que todos os termos $\gamma_i(G)$ da série central descendente são característicos em G. Além disso, podemos mostrar que um grupo G é nilpotente se, e somente se, existe um número m tal que $\gamma_{m+1}(G) = 1$. O menor m com essa propriedade coincide com a classe de nilpotência de G, assim, as duas séries, central ascendente e descendente, de um grupo nilpotente possuem o mesmo comprimento.

Teorema 1.17. *Seja G um grupo. Para todo $n \geq 1$, o n-ésimo termo da série central descendente de G é dado por*

$$\gamma_n(G) = \langle [g_1, ..., g_n] \mid g_1, ..., g_n \in G \rangle.$$

O teorema acima é provado de forma análoga ao Teorema 1.15, usando indução sobre n.

Corolário 1.18. *Seja G um grupo. Para todo $i \in \mathbb{N}$, temos que $[Z_i(G), \gamma_i(G)] = 1$.*

A demonstração do Corolário 1.18 segue diretamente, por indução sobre i, das caracterizações dadas nos Teorema 1.15 e Teorema 1.17.

Observamos que subgrupos e imagens homomórficas de grupos nilpotentes são também nilpotentes. A seguir veremos uma caracterização dos grupos finitos nilpotentes.

Teorema 1.19. *Seja G um grupo finito. As seguintes afirmações são equivalentes:*

(i) *G é nilpotente.*

(ii) *Se H é um subgrupo próprio de G, então H está contido propriamente em $N_G(H)$.*

(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.*

Uma propriedade muito útil de p-grupos finitos pode ser vista no seguinte resultado.

Lema 1.20. *Sejam P um p-grupo finito e $1 \neq N \triangleleft P$. Então $N \cap Z(P) \neq 1$. Em particular, se $P \neq 1$, então $Z(P) \neq 1$.*

Do lema acima é fácil provar que todo p-grupo finito é nilpotente.

Lembrando que o subgrupo de Fitting de um grupo finito G é dado por

$$F(G) = \prod_{p \in \pi(G)} O_p(G),$$

vemos que $F(G)$ é o maior subgrupo normal nilpotente em G.

A demonstração do resultado que veremos a seguir será omitida, mas sua prova pode ser vista em [Corollary 3.13, [15]].

Lema 1.21. *Suponha que G é um grupo nilpotente de classe c. Então, para todo g em G, a classe de nilpotência do subgrupo $\langle g, [G,G] \rangle$ é, no máximo, $c-1$.*

Obviamente os grupos nilpotentes de classe 1 são exatamente os grupos abelianos. Os grupos nilpotentes de classe 2 possuem várias propriedades semelhantes com as dos grupos abelianos. Por exemplo, em um grupo abeliano G, dados x e y em G, temos que

$$(xy)^n = x^n y^n,$$

para todo $n \geq 1$. Nos grupos nilpotentes de classe 2 temos a seguinte análoga propriedade.

Teorema 1.22. *Seja G um grupo nilpotente com classe de nilpotência 2, então*

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

para todo $n \geq 1$.

Demonstração: Faremos a prova por indução sobre n. Sejam x e y elementos quaisquer de G. Para $n = 1$ o resultado é trivial. Suponha, então, que $n \geq 2$ e que para todo $k < n$ vale que

$$(xy)^k = x^k y^k [y,x]^{\frac{k(k-1)}{2}}.$$

Temos que $(xy)^n = (xy)^{n-1}(xy)$, mas, por hipótese de indução, segue que

$$(xy)^n = x^{n-1} y^{n-1} [y,x]^{\frac{(n-1)(n-2)}{2}} (xy).$$

Como G tem classe de nilpotência 2, temos que $[G',G] = [G,G,G] = 1$, logo obtemos que $G' \leq Z(G)$. Assim,

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

pelo Lema 1.8 (vi). Agora, pelo item (vii) desse mesmo lema, segue que

$$(xy)^n = x^n y^n [y,x]^{y^{n-2}} \cdots [y,x]^{y} [y,x] [y,x]^{\frac{(n-1)(n-2)}{2}}.$$

Portanto, como G' está em $Z(G)$, temos, por fim, que

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

como queríamos.

■

1.3 Automorfismos e Ação Coprima

Dados um grupo G e um conjunto não vazio Ω, uma *ação* de G sobre Ω está definida quando, para cada $g \in G$ e $\alpha \in \Omega$, existe um único elemento $\alpha^g \in \Omega$ tal que as seguintes condições são satisfeitas:

(i) $\forall\ \alpha \in \Omega$, $\alpha^1 = \alpha$;

(ii) $\forall\ \alpha \in \Omega$ e $\forall\ g, h \in G$, $(\alpha^g)^h = \alpha^{gh}$.

Nesse caso, dizemos que G age em Ω. Dizemos que a ação é fiel, ou que G age fielmente em Ω, se a identidade de G é o único elemento $g \in G$ tal que $\alpha^g = \alpha\ \forall\ \alpha \in \Omega$.

Dada uma ação de um grupo G em um conjunto não vazio Ω, podemos definir, para todo $\alpha \in \Omega$, o estabilizador de α em G por

$$G_\alpha = \{g \in G | \alpha^g = \alpha\},$$

que é um subgrupo de G, e a órbita de α é definida como sendo o subconjunto de Ω dado por

$$O_\alpha = \{\alpha^g | g \in G\}.$$

Dizemos que um elemento $g \in G$ fixa α se $\alpha^g = \alpha$ e consideramos o núcleo da ação como sendo o subconjunto de G composto pelos elementos que fixam todo α em Ω.

Para cada $g \in G$ podemos definir $\pi_g : \Omega \to \Omega$ por $\alpha \longmapsto \alpha^g$, onde α^g é o resultado da ação de g em α. Observe que $\pi_g \in Sym(\Omega)$ e a aplicação $\varphi : G \to Sym(\Omega)$ dada por $g \longmapsto \pi_g$ é um homomorfismo onde o kernel é igual ao núcleo da ação. Assim, se K é o núcleo da ação de G em Ω, temos que $K \lhd G$ e G/K é isomorfo a um subgrupo de $Sym(\Omega)$.

Teorema 1.23. *Seja G um grupo agindo sobre um conjunto Ω e considere O uma órbita dessa ação. Tome $\alpha \in O$ e $H = G_\alpha$. Então existe uma bijeção entre O e $\{Hx | x \in G\}$. Em particular, temos que*

$$|O| = |G : G_\alpha|.$$

Se G é finito temos que

$$|O| = \frac{|G|}{|G_\alpha|}.$$

Por exemplo, se considerarmos a ação por conjugação de um grupo G nele mesmo, dado x em G, temos que o estabilizador G_x de x é o centralizador $C_G(x)$ de x em G e a órbita de x coincide com sua classe de conjugação K. Assim, obtemos que

$$|K| = |G : C_G(x)|.$$

Sejam, agora, H e N dois grupos e considere que H age sobre N como conjunto. Sendo N um grupo, é natural pedir que, para todo h em H a aplicação $\pi_h : N \to N$ que define a ação do elemento h em N seja de fato um automorfismo de N, ou seja, que

$$\pi_h(n_1n_2) = \pi_h(n_1)\pi_h(n_2),$$

para todo $n_1, n_2 \in N$. Portanto, dizemos que H *age por automorfismos* sobre N se a ação for determinada por um homomorfismo $\varphi : H \to Aut(N)$. Note que cada homomorfismo $\varphi : H \to Aut(N)$ define obviamente uma ação via automorfismos de H sobre N.

Suponha que G é o produto $G = NH$ de um subgrupo normal N por um subgrupo H, onde $H \cap N = 1$. Então, G é dito o *produto semidireto interno* de N por H. Nesse caso, cada elemento g de G possui uma única representação da forma $g = nh$, com n em N e h em H. Além disso, como N é normal em G, cada elemento h de H age em N por conjugação induzindo, assim, um automorfismo $\varphi(h)$ de N. Assim, temos que a aplicação $\varphi : H \to AutN$ que leva cada $h \in H$ no automorfismo $\varphi(h)$ é um homomorfismo.

Reciprocamente, suponha que um grupo H age por automorfismos sobre N, então existe um homomorfismo $\varphi : H \to AutN$. Assim, podemos formar o *produto semidireto externo* de H e N, que denotamos por $N \rtimes H$, que é composto pelo conjunto $N \rtimes H = \{(n, h) \mid n \in N,\ h \in H\}$ com a multiplicação definida da seguinte forma

$$(n_1, h_1)(n_2, h_2) = (n_1 n_2^{\varphi(h_1^{-1})}, h_1h_2).$$

Temos que $N \rtimes H$ é um grupo com a operação definida acima. A estrutura do grupo $N \rtimes H$ depende de N, H e do homomorfismo φ.

Temos que o subconjunto $\hat{N} = \{(n, 1) \mid n \in N\}$ é um subgrupo normal de $G = N \rtimes H$ isomorfo a N e $\hat{H} = \{(1, h) \mid h \in H\}$ é um subgrupo de G isomorfo a H. Temos, também, que $G = \hat{N}\hat{H}$ e $\hat{N} \cap \hat{H} = 1$. Logo, $N \rtimes H$ é o produto semidireto interno de $\hat{N}$ e $\hat{H}$. Com isso, é natural identificar $\hat{N}$ por N e $\hat{H}$ por H e considerar H e N como subgrupos de $N \rtimes H$. Sob essa identificação, a ação de conjugação de $h \in H$ sobre N coincide com o automorfismo $\varphi(h)$, ou seja, para todo n em N, temos que

$$h^{-1}nh = (1, h^{-1})(n, 1)(1, h) = (n^{\varphi(h)}, h^{-1})(1, h) = (n^{\varphi(h)}, 1) = n^{\varphi(h)},$$

o que justifica denotarmos por n^h o elemento $n^{\varphi(h)}$.

Assim, qualquer produto semidireto externo pode ser visto como um produto semidireto interno. O inverso vale também e esse "equivalência" entre produto semidireto interno e externo é "livremente" usada.

Em particular, o grupo $Aut(G)$ é considerado como um subgrupo de $G \rtimes Aut(G)$ e, mais em geral, se um grupo A age por automorfismos sobre um grupo G, consideramos A como um subgrupo do produto semidireto $G \rtimes A$.

Lembramos que se A é um grupo que age por automorfismos em um grupo G, a ação é dita *coprima* se $(|A|, |G|) = 1$.

Dado um grupo G e um automorfismo ϕ de G, definimos o *subgrupo de pontos fixos* de ϕ em G como sendo o subgrupo dado por

$$C_G(\phi) = \{g \in G | g^\phi = g\}.$$

Além disso, usaremos $[G, \phi]$ para denotar o subgrupo

$$[G, \phi] = \langle x^{-1}x^\phi | x \in G \rangle$$

e, por consequência, se A é um grupo que age por automorfismos sobre G, definimos

$$[G, A] = \langle [G, \phi] \mid \phi \in A \rangle.$$

Dado um automorfismo ϕ de G, um subgrupo H de G é dito *ϕ-invariante* se $H^\phi = H$ ou, em outras palavras, se $[H, \phi] \leq H$.

Dados um grupo G, ϕ um automorfismo de G e N um subgrupo normal ϕ-invariante de G, podemos considerar a aplicação $\bar{\phi}$ induzida por ϕ sobre o quociente G/N, definida por

$$(gN)^{\bar{\phi}} = Ng^\phi.$$

Sendo N ϕ-invariante, temos que $\bar{\phi}$ é bem definido e é, de fato, um automorfismo de G/N. Chamamos $\bar{\phi}$ de automorfismo induzido e usaremos um abuso de notação denotando $\bar{\phi}$ apenas por ϕ, na maioria das vezes.

O próximo resultado nos fornece uma estimativa de número de pontos fixos de $\bar{\phi}$ com respeito ao número de pontos fixos de ϕ. Veremos mais a frente que, no caso em que a ordem de ϕ é coprima à ordem de N, então é possível dar ainda mais informações.

Teorema 1.24. *Sejam G um grupo finito, φ um automorfismo de G e N um subgrupo normal φ-invariante de G. Então*

$$|C_{G/N}(\varphi)| \leq |C_G(\varphi)|.$$

Demonstração: Note que, para qualquer grupo H e qualquer auomorfismo $\psi \in Aut(H)$, temos que o número de elementos da forma $x^{-1}x^\psi$, com $x \in H$, é igual a $|H : C_H(\psi)|$. Mais precisamente, a função $xC_H(\psi) \longmapsto x^{-1}x^\psi$ é uma correspondência injetiva entre o conjunto $\{x^{-1}x^\psi | x \in H\}$ e o conjunto de classes laterais à esquerda de $C_H(\psi)$. Note que essa correspondência é bem definida e injetiva, pois $x^{-1}x^\psi = y^{-1}y^\psi$ e isso acontece se, e somente se, $yx^{-1} = y^\psi(x^\psi)^{-1} = (yx^{-1})^\psi$ e isso vale se, e só se,

$$yx^{-1} \in C_H(\psi).$$

Agora, elementos da forma $\bar{g}^{-1}\bar{g}^{\psi}$ com $\bar{g} = gN \in G/N$ são imagens de elementos da forma $g^{-1}g^{\psi}$ de G pelo homomorfismo canônico de G em G/N. Cada classe lateral $\bar{g}^{-1}\bar{g}^{\psi}$ de N contém, no máximo, $|N|$ elementos da forma $g^{-1}g^{\psi}$ e cada elemento dessa forma está contido na classe lateral $\bar{g}^{-1}\bar{g}^{\psi}$. Então

$$|\{g^{-1}g^{\psi}|g \in G\}| \leq |N||\{\bar{g}^{-1}\bar{g}^{\psi}|\bar{g} \in G/N\}|.$$

Mas

$$|G/N : C_{G/N}(\psi)| = |\{\bar{g}^{-1}\bar{g}^{\psi}|\bar{g} \in G/N\}| \text{ e } |G : C_G(\psi)| = |\{g^{-1}g^{\psi}|g \in G\}|.$$

Logo,

$$|G : C_G(\psi)| = \frac{|G|}{|C_G(\psi)|} \leq |N|\frac{|G/N|}{|C_{G/N}(\psi)|} = |N|\frac{|G|}{|N||C_{G/N}(\psi)|}$$

e, assim,

$$\frac{|G|}{|C_G(\psi)|} \leq \frac{|G|}{|C_{G/N(\psi)|}},$$

portanto

$$|C_{G/N}(\psi)| \leq |C_G(\psi)|,$$

como queríamos.

■

Para os próximos resultados precisaremos da seguinte definição

Definição 1.25. *Um automorfismo ϕ de um grupo G é dito livre de pontos fixos se*

$$C_G(\phi) = 1.$$

Similarmente, um grupo de automorfismos A de G é dito livre de pontos fixos se $C_G(A) = 1$.

Observe que um automorfismo ϕ é livre de pontos fixos se, e somente se, $\langle\phi\rangle$ é um grupo de automorfismos livres de pontos fixos.

Os resultados a seguir têm como objetivo dar várias propriedades dos automorfismos livres de pontos fixos de um grupo G em relação aos elementos de G.

Lema 1.26. *Sejam n um inteiro, com $n \geq 1$, e ϕ um automorfismo livre de pontos fixos de G de ordem n. Então, temos que:*

(i) *Todo elemento de G pode ser expresso na forma $x^{-1}x^{\phi}$ e na forma $x^{\phi}x^{-1}$ para algum x em G adequado.*

(ii) *Para todo $x \in G$, temos que*

$$xx^{\phi}\cdots x^{\phi^{n-1}} = x^{\phi^{n-1}}\cdots x^{\phi}x = 1.$$

Demonstração: Se $x^{-1}x^{\phi} = y^{-1}y^{\phi}$ para $x, y \in G$, então $x^{\phi} = xy^{-1}y^{\phi}$, assim $x^{\phi}(y^{\phi})^{-1} = xy^{-1}$ e disso segue que

$$xy^{-1} = (xy^{-1})^{\phi}.$$

Logo, como ϕ é um automorfismo livre de pontos fixos de G, temos que $xy^{-1} = 1$, assim $x = y$. Portanto, o número de elementos em G da forma $x^{-1}x^{\phi}$ é igual à ordem de G, logo, todos os elementos de G podem ser expressos nessa forma. De maneira análoga, provamos que todo elemento de G pode ser expresso na forma $x^{\phi}x^{-1}$, o que conclui a prova do item (i).

Agora, dado $x \in G$, temos que $x = y^{-1}y^{\phi}$ para algum y em G, então

$$xx^{\phi}\cdots x^{\phi^{n-1}} = y^{-1}y^{\phi}(y^{-1}y^{\phi})^{\phi}\cdots(y^{-1}y^{\phi})^{\phi^{n-1}} =$$
$$y^{-1}y^{\phi}(y^{\phi})^{-1}y^{\phi^2}(y^{\phi^2})^{-1}\cdots y^{\phi^{n-1}}(y^{\phi^{n-1}})^{-1}y^{\phi^n} = y^{-1}y^{\phi^n} = y^{-1}y = 1,$$

pois ϕ tem ordem n. Provamos de forma análoga que $x^{\phi^{n-1}}\cdots x^{\phi}x = 1$, concluindo a prova de (ii).

■

Definição 1.27. *Dizemos que ϕ é uma involução de um grupo G se ϕ é um automorfismo de G de ordem dois.*

Teorema 1.28. *Se ϕ é uma involução de G livre de pontos fixos, então G é abeliano e $x^{\phi} = x^{-1}$ para todo x em G.*

Demonstração: Pelo Lema 1.26 (ii), como ϕ tem ordem 2, temos que $xx^{\phi} = 1$, então $x^{\phi} = x^{-1}$ para todo $x \in G$. Agora, dados x e y elementos arbitrários em G temos que

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

assim

$$y^{-1}x^{-1} = x^{-1}y^{-1},$$

portanto, G é abeliano, como queríamos.

■

Teorema 1.29. *Se A é um p-grupo de automorfismos de G tal que $C_G(A) = 1$, então G é um p'-grupo.*

Demonstração: Considere G^* o produto semidireto de G por A e seja P^* um p-subgrupo de Sylow de G^* que contém A. Temos que $P = P^* \cap G$ é um p-subgrupo de Sylow de G, já que G é normal em G^*. Suponha que $P \neq 1$.

Como P é normal em P^*, pelo Lema 1.20, temos que $P \cap Z(P^*) \neq 1$. Mas A centraliza $P \cap Z(P^*)$, o que é uma contradição com a hipótese de que $C_G(A) = 1$. Portanto, temos que, necessariamente, $P = 1$ e disso segue que G é um p'-grupo.

■

A demonstração do teorema a seguir será omitida, mas pode ser vista em [Theorem 5.2.3, [6]].

Teorema 1.30. *Seja A um p'-grupo de automorfismos de um grupo abeliano P. Então*

$$P = C_P(A) \times [P, A].$$

Nosso próximo objetivo será dar uma versão análoga ao Teorema 1.30 no caso em que P seja um p-grupo arbitrário (não necessariamente abeliano).

Sejam G um grupo, A um subgrupo de $Aut(G)$ e

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

uma série normal de G. Dizemos que A *estabiliza* a série dada se todos os termos G_i são A-invariantes e A age trivialmente em cada fator G_{i-1}/G_i, para todo $1 \leq i \leq n$.

É imediato da definição acima o seguinte lema.

Lema 1.31. *Um subgrupo A de $Aut(G)$ estabiliza a série normal*

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

se, e somente se, A normaliza cada G_i e $[G_i, A] \leq G_{i+1}$, para todo $0 \leq i \leq n-1$.

Demonstração: Denotaremos por $\bar{G}_i = G_i/G_{i+1}$ e por $\bar{x}$ a imagem em $\bar{G}_i$ do elemento x pertencente a G_i. Temos que A estabiliza a série dada se A normaliza cada G_i e $(\bar{x})^\phi = \bar{x}$, para todo $\bar{x}$ em $\bar{G}_i$ e ϕ em A, onde $0 \leq i \leq n-1$. Logo, $(\bar{x})^\phi = \bar{x}$ é quivalente a ter $\bar{x}^{-1}(\bar{x})^\phi = \bar{1}$, para todo $\bar{x} \in \bar{G}_i$, ou seja, que $[x, \phi]$ está em G_{i+1} e, assim, o lema segue.

■

Teorema 1.32. *Seja A um p'-grupo de automorfismos de um p-grupo P que estabiliza alguma série normal de P. Então $A = 1$.*

Demonstração: Seja

$$P = P_0 \geq P_1 \geq \cdots \geq P_n = 1$$

a série normal de P que é estabilizada por A. Faremos indução sobre n. Se $n = 1$, temos a série $P = P_0 \geq P_1 = 1$, assim, como A estabiliza essa série, obtemos que $[P, A] = 1$ e A age trivialmente sobre P. Mas A é um p'-subgrupo de $Aut(P)$, então temos que $A = 1$. Suponha, então, que $n > 1$ e que para toda $k < n$ o resultado é verdadeiro.

Como A estabiliza a série dada, temos que cada termo P_i da série é A-invariante, logo A induz um grupo de automorfismos em P_1 e estabiliza a série normal $P_1 \geq P_2 \geq \cdots \geq P_n = 1$ de P_1 e, assim, por hipótese de indução, A age trivialmente em P_1. Mas, temos que A age trivialmente em P/P_1, por hipótese. Logo, $[x, \phi] \in P_1$, para todo x em P e ϕ em A, o que nos fornece que $x^\phi = xz$, para algum z em P_1. Portanto, como ϕ age trivialmente em P_1, obtemos que

$$x^{\phi^2} = (xz)^\phi = x^\phi z^\phi = (xz)z = xz^2$$

e concluímos facilmente, por indução sobre i, que $x^{\phi^i} = xz^i$, para todo $i \geq 1$. Em particular, isso vale para $i = m$, onde m é a ordem de ϕ, assim

$$x = x^{\phi^m} = xz^m,$$

o que nos fornece que $z^m = 1$. Agora, $(m, p) = 1$, pois A é um p'-grupo, logo $z = 1$, já que z é um p-elemento. Portanto, $x^\phi = x$, para todo x em P e para todo ϕ em A e, assim, segue que $[P, A] = 1$, ou seja, A age trivialmente sobre P e temos que $A = 1$, como queríamos.

■

Teorema 1.33. *Se A é um p'-grupo de automorfismos de um p-grupo P, então $P = CH$, onde $C = C_P(A)$ e $H = [P, A]$. Em particular, se $H \leq \Phi(P)$, então $A = 1$.*

Demonstração: Considere, primeiro, o caso em que $H \leq Z(P)$ e, dado ϕ em A, defina a função α_ϕ de P em P como sendo $\alpha_\phi(x) = x^{-1}x^\phi$, para todo x em P. Para x e y elementos arbitrários em P, temos que

$$\alpha_\phi(xy) = (xy)^{-1}(xy)^\phi = y^{-1}(x^{-1}x^\phi)y^\phi = x^{-1}x^\phi y^{-1}y^\phi,$$

pois $x^{-1}x^\phi$ está em H que estamos suponto está contido em $Z(P)$. Então, $\alpha_\phi(xy) = \alpha_\phi(x)\alpha_\phi(y)$ e disso segue que α_ϕ é um endomorfismo de P, para todo ϕ em A. Note que, o núcleo de α_ϕ é precisamente $C_P(\phi)$ e sua imagem está contida em H. Como $H \leq Z(P)$, obtemos que α_ϕ é uma função de P em um grupo abeliano, pois

$$Im(\alpha_\phi) = \{x^{-1}x^\phi \mid x \in P\} \leq [P, A] = H \leq Z(P)$$

e $P' = [P, P]$ está contido no núcleo de α_ϕ. Disso segue que P' está contido em $C_P(\phi)$, para todo ϕ em A e, assim, concluímos que $P' \leq C$.

Agora, sejam $\bar{P} = P/P'$, $\bar{C} = C_{\bar{P}}(A)$ e $\bar{H} = [\bar{P}, A]$. Como $\bar{P}$ é abeliano, pelo Teorema 1.30, temos que $\bar{P} = \bar{C} \times \bar{H}$. Note que $\bar{H}$ é a imagem de H em $\bar{P}$. Logo, $P = C_1 H$, onde C_1 denota a imagem inversa de $\bar{C}$ em P. Mas, A age trivialmente em P' e em $\bar{C}$, logo A estabiliza a série $C_1 \geq P' \geq 1$ e, pelo Teorema 1.32, segue que A age trivialmente em C_1. Portanto, $C_1 \leq C$ e, assim, $P = CH$.

Suponha, então, que H não está contido em $Z(P)$, logo, certamente, temos que $H \neq 1$. Como H é normal em P, já que $[P, A] \lhd \langle P, A\rangle = P \rtimes A$, e P é um p-grupo, pelo Lema 1.20, temos que $K = H \cap Z(P) \neq 1$. Note que K é A-invariante, já que H é A-invariante. Defina

$$D = \langle x \in P \mid [x, A] \leq K \rangle.$$

Claramente $C_P(A) \leq D$. Sejam $\bar{P} = P/K$, $\bar{C} = C_{\bar{P}}(A)$ e $\bar{H} = [\bar{P}, A]$. Se x está em P e $[x, A] \leq K$, entã A centraliza a imagem de x em $\bar{P}$. Logo, pela definição de D, obtemos que D é levado em $\bar{C}$ pelo homomorfismo canônico de P em $\bar{P}$. Reciprocamente, se $\bar{x} \in \bar{C}$, então $[\bar{x}, A] = \bar{1}$ e $[x, A] \leq K$ para todo representante x de $\bar{x}$ em P. Então, x está em D e concluímos que $\bar{C}$ é a imagem de D em $\bar{P}$. Por outro lado, também temos que $\bar{H}$ é a imagem de H em $\bar{P}$.

Como $K \neq 1$, temos que $|\bar{P}| < |P|$, assim, por hipótese de indução sobre $|P|$, obtemos que $\bar{P} = \bar{C}\bar{H}$. Logo, pelo visto no parágrafo anterior, temos que $P = DH$. Se $[x, A] \leq K$, para todo x em P, ou seja, se $P = D$, então $H \leq K \leq Z(P)$, o que é uma contradição. Assim, D está contido propriamente em P. Observe que D é A-invariante, pois K e $\bar{C}$ são ambos A-invariantes. Portanto, por hipótese de indução e usando o fato de que $C \leq D$, obtemos que $D = C[D, A]$. Com isso, como $[D, A] \leq H = [P, A]$ e $P = DH$, concluímos a prova para o caso em que H não está contido em $Z(P)$.

Finalmente, se H está em $\Phi(P)$, então $P = C\Phi(P) = C$ e disso segue que $A = 1$.

■

Do Teorema 1.33 obtemos a seguinte propriedade que será bastante útil nas demonstrações futuras.

Corolário 1.34. *Se A é um p'-grupo de automorfismos de um p-grupo P, então*

$$[P, A, A] = [P, A].$$

Em particular, se $[P, A, A] = 1$, então $A = 1$.

Demonstração: Sejam $H = [P, A]$, $H_1 = [H, A] = [P, A, A]$ e $C = C_P(A)$. Temos que H, H_1 e C são todos A-invariantes. Aplicando o Teorema 1.33 em P e em H, obtemos que $P = CH$ e $H = (H \cap C)H_1$, logo $P = CH_1$. Assim, para todo x em P, podemos escrever $x = yz$, onde $y \in C$ e $z \in H_1$ e disso segue que

$$x^{-1}x^{\phi} = z^{-1}y^{-1}y^{\phi}z^{\phi} = z^{-1}z^{\phi},$$

para todo ϕ em A. Mas, $z^{-1}z^{\phi}$ está em H_1, já que $z \in H_1$ e H_1 é A-invariante. Disso concluímos, pela definição de H, que $H \leq H_1$. Por outro lado, $H_1 = [H, A] \leq [P, A] = H$, logo $H = H_1$.

Finalmente, se $H_1 = 1$, então $H = 1$, assim, A age trivialmente em P e obtemos que $A = 1$.

■

Lembramos que, dado um subgrupo normal N de um grupo G, dizemos que um subgrupo H de G é um *complemento* de N em G se $NH = G$ e $N \cap H = 1$.

O próximo resultado, conhecido como Teorema de Schur-Zassenhaus, garante que, em um grupo finito, um subgrupo de Hall normal sempre possui um complemento.

Teorema 1.35. *Sejam G um grupo finito, π um conjunto de primos e H um π-subgrupo de Hall normal de G. Então, são verdadeiras as seguintes afirmações:*

(i) *G possui um π'-subgrupo de Hall K que é um complemento de H em G.*

(ii) *Se H ou G/H é solúvel, então quaisquer dois π'-subgrupos de Hall de G são conjugados em G.*

Notemos que a hipótese em (ii) de H ou G/H ser solúvel de fato não é necessária em vista do Teorema 1.13 de Feit-Thompson.

Agora, combinando o Teorema 1.35 com o Teorema 1.11 é possível obter o seguinte importante resultado sobre ação coprima.

Teorema 1.36. *Sejam A e G grupos tais que A age sobre G e $(|A|, |G|) = 1$. Se A ou G é solúvel, então, para todo conjunto de primos π, temos que:*

(i) *A deixa invariante algum π-subgrupo de Hall de G.*

(ii) *Dois quaisquer A-invariantes π-subgrupos de Hall de G são conjugados por um elemento de $C_G(A)$.*

(iii) *Todo π-subgrupo A-invariante de G está contido em um π-subgrupo de Hall A-invariante de G.*

A demonstração do teorema anterior pode ser vista em [Theorem 8.2.6, [19]].

1.4 Geradores e Posto de um Grupo

Dado um grupo G e um número natural d, dizemos que G é d-gerado se existe um subconjuto X de G tal que $|X| = d$ e $\langle X\rangle = G$. Se G é um grupo finito, definimos o *número minimal de geradores* de G como sendo

$$d(G) = \min\{|S| \mid S \subseteq G \text{ e } \langle S\rangle = G\}.$$

Um subconjunto X de um grupo G é dito um conjunto minimal de geradores de G se $G = \langle X\rangle$ e, para todo $Y \subset X$, temos que $\langle Y\rangle < G$. Observe que o conceito de cardinalidade de um conjunto minimal de geradores não coincide com a definição de $d(G)$. Temos, por exemplo, que o no grupo Simétrico S_n de ordem $n \geq 3$, o conjunto $X = \{(1\ 2), (2\ 3), ..., (n-1\ n)\}$ é um conjunto minimal de geradores de S_n de cardinalidade $n-1$, mas, claramente, $d(S_n) = 2$, já que $S_n = \langle (1\ 2), (1\ 2\ ...\ n)\rangle$.

Um problema que nos deparamos ao estudar o número minimal de geradores de um grupo G é que se H é um subgrupo próprio de G nem sempre temos que $d(H) \leq d(G)$, ou seja, a função $d : G \mapsto d(G)$ pode ter um comportamento ruim com respeito aos subgrupos de G. O exemplo clássico disso é dado considerando o grupo simétrico S_n, com $n \geq 3$, onde temos que $S_n = \langle (1\ 2), (1\ 2\ ...\ n)\rangle$ e, assim, $d(S_n) = 2$, já que S_n não é cíclico. Agora, tomando o subgrupo próprio H de S_n definido por $H = \langle (1\ 2), (3\ 4), ..., (2i-1\ 2i), ...\rangle$, obtemos que $d(H) = [n/2]$, onde $[x]$ de um número real x denota a parte inteira de x. Logo, se considerarmos $n = 6$, temos que $d(S_6) = 2$, mas $d(H) = 3$, onde $H = \langle (1\ 2), (3\ 4), (5\ 6)\rangle$.

Até na família dos p-grupos finitos podemos dar exemplos desse fenômeno. Para dar os exemplos, vamos precisar primeiro lembrar a construção de produto entrelaçado de dois grupos.

Considere, agora, dois grupos G e H e um conjunto Ω tal que G age sobre Ω. Defina B como sendo o conjunto de todas as funções de Ω em H e defina, em B, o produto de dois elementos $f, g \in B$ da seguinte forma:

$$(fg)(\alpha) = f(\alpha)g(\alpha), \text{ para todo } \alpha \in \Omega.$$

Temos que B é um grupo com o produto definido acima e, além disso, B é, de fato, o produto direto de $|\Omega|$ cópias de H.

A ação de G em Ω induz uma ação por automorfismos de G em B dada por

$$\begin{aligned} G \times B &\to B \\ (x, f) &\longmapsto f^x, \end{aligned}$$

onde $f^x \in B$ é a função de Ω em H definida da seguinte forma:

$$\begin{aligned} f^x : \Omega &\longrightarrow H \\ \alpha &\longmapsto f^x(\alpha) = f(\alpha^{x^{-1}}) \end{aligned}$$

onde $\alpha^{x^{-1}}$ é a imagem da ação do elemento x^{-1} de G sobre o elemento α de Ω. Assim, em particular, temos que

$$f^x(\alpha^x) = f(\alpha),$$

para todo x em G, α em Ω e f em B.

Como temos uma ação por automorfismos bem definida de G em B, temos que existe um homomorfismo $\varphi : G \to Aut(B)$ e, portanto, podemos considerar o produto semidireto $W = B \rtimes G$ definido usando φ como vimos na Seção 1.3. Dizemos que W é o *produto entrelaçado* de H por G. Além disso, B, visto como um subgrupo de W, é chamado de *grupo base* do produto entrelaçado. É comum denotar o produto entrelaçado de H por G como $W = H \wr G$, mas essa notação é defeituosa, já que não especifica o conjunto Ω e nem a ação de G sobre Ω. Se G é um grupo abstrato e o conjunto Ω não é especificado, então, usualmente, consideramos $H \wr G$ construído usando $\Omega = G$ e a ação de multiplicação à direita de G em G. Muitas vezes, chamamos o produto entrelaçado construído dessa maneira de *produto entrelaçado regular* de H por G.

Agora, voltando ao exemplo, considere o produto entrelaçado $G = C_2 \wr C_4$, temos que $\Omega = C_4$ e ação de C_4 em C_4 é a multiplicação à direita dada por

$$\begin{aligned} C_4 \times C_4 &\longrightarrow C_4 \\ (x, \alpha) &\longmapsto x\alpha. \end{aligned}$$

Então, temos que o subgrupo base B do produto entrelaçado G é tal que $B \cong C_2 \times C_2 \times C_2 \times C_2$. Assim, $G = B \rtimes C_4$ e temos que $d(G) = 2$ e $d(B) = 4$.

Generalizando o exemplo anterior, podemos considerar o produto entrelaçado dado por $G = C_p \wr C_{p^n}$, com $n \geq 2$ se $p = 2$, e $n \geq 1$ se p é ímpar. Também nesse caso temos que $d(G) = 2$, mas $B \cong C_p \times \cdots \times C_p$, isomorfo ao produto de p^n cópias de C_p, é um subgrupo próprio de G e $d(B) = p^n$. Nesse caso vemos, também, que $d(G) = 2$, mas B é um subgrupo próprio de G e $d(B) = p^n$.

O resultado que veremos a seguir será muito usado neste trabalho. Nele encontramos uma forma mais eficiente de calcular o número minimal de geradores de um p-grupo finito. Além disso, o resultado mostra que para p-grupos finitos a cardinalidade de um conjunto minimal de geradores de G coincide com $d(G)$, coisa que em geral não é certa, como observamos com o exemplo de S_n.

Teorema 1.37. *(Teorema de Bases de Burnside) Seja G um p-grupo finito. São verdadeiras as seguintes afirmações:*

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

(ii) *Se $|G : \Phi(G)| = p^d$, para algum $d \geq 1$, então, dado X um conjunto de geradores de G, existe um subconjunto Y de X tal que $G = \langle Y \rangle$ e $|Y| = d$.*

Como vimos antes, a função que associa $d(G)$ a um grupo G não tem um comportamento bom com respeito aos subgrupos próprios de G, já que pode existir $H < G$ tal que $d(H) > d(G)$. Para contornar esse problema vamos introduzir um novo conceito.

Definição 1.38. *O posto de um grupo finito G é definido como sendo*

$$rk(G) = sup\{d(H)|H \leq G\}.$$

Observe que, pela definição de posto, dado um subgrupo H de um grupo G, sempre temos que $rk(H) \leq rk(G)$, o que não ocorria com o número minimal de geradores de um grupo. Notamos, também, que em geral temos que $d(G) \neq rk(G)$.

Lema 1.39. *Sejam G um grupo finito, N um subgrupo normal de G e n e k inteiros ≥ 1. Se N é n-gerado e G/N é k-gerado, então G é $(n+k)$-gerado.*

Demonstração: Como N é um subgrupo normal de G, podemos considerar o homomorfismo canônico $\pi : G \to G/N$. Agora, G/N é k-gerado, logo existem $g_1, ..., g_k \in G$ tais que $\{Ng_1, ..., Ng_k\}$ gera G/N. Assim, dado g em G, temos que $Ng = N(y_1 \cdots y_r)$, onde $y_i \in \{g_1, ..., g_k\} \cup \{g_1^{-1}, ..., g_k^{-1}\}$, com $1 \leq i \leq r$, logo, $g = my_1 \cdots y_r$, para algum m em N. Mas N é n-gerado, logo existem $m_1, ..., m_n \in N$ tais que $\{m_1, ..., m_n\}$ gera N e disso segue que $m = l_1 \cdots l_t$, onde $l_i \in \{m_1, ..., m_n\} \cup \{m_1^{-1}, ..., m_n^{-1}\}$. Portanto, obtemos que

$$g = l_1 \cdots l_t y_1 \cdots y_r$$

e, assim, G é $(n+k)$-gerado, como queríamos.

■

Como consequência temos o seguinte resultado.

Corolário 1.40. *Sejam G um grupo finito e N um subgrupo normal de G. Então*

$$rk(G) \leq rk(G/N) + rk(N).$$

Lema 1.41. *Seja G um grupo abeliano finito e $d(G) = s$. Então, o posto de G é limitado por uma função que depende apenas de s.*

Demonstração: Como G é abeliano e $G = \langle x_1, ..., x_s \rangle$, temos que G é produto direto de seus subgrupos cíclicos

$$G = \langle x_1 \rangle \cdots \langle x_s \rangle.$$

Assim, dado $H \leq G$, temos que H também é abeliano e finitamente gerado, logo

$$H = \langle y_1 \rangle \cdots \langle y_k \rangle,$$

onde $k \leq s$. Assim, $d(H) \leq d(G)$ e, portanto, o posto de G é limitado por uma função que depende apenas de s.

■

O resultado a seguir apresenta uma limitação do posto de um grupo nilpotente G através do número minimal de geradores de G e da classe de nilpotência de G. Como, neste trabalho, estamos interessados em estudar postos de alguns grupos, o teorema a seguir será uma ferramenta chave para várias demonstrações que faremos nos capítulos seguintes.

Teorema 1.42. *Seja G um grupo nilpotente finito. Então o posto $rk(G)$ de G é limitado em termos da classe de nilpotência de G e do número minimal de geradores de G.*

Demonstração: Como G é nilpotente, existe $c \geq 1$ tal que a série central descendente de G é dada por

$$\gamma_1(G) = G \geq \gamma_2(G) = G' \geq \cdots \geq \gamma_c(G) \geq \gamma_{c+1}(G) = 1,$$

com a classe de nilpotência de G sendo $cl(G) = c$. Faremos a prova por indução sobre c. Se $c = 1$, então G é abeliano, pois $\gamma_2(G) = G' = 1$, assim, o resultado segue pelo Lema 1.41. Suponhamos, então, $c \geq 2$ e que o resultado é verdadeiro para todo grupo H tal que $cl(H) < c$.

Note que que a classe de nilpotência de $G/\gamma_c(G)$ é $cl(G/\gamma_c(G)) \leq c - 1$. Logo, como $d(G/\gamma_c(G))$ é $d(G)$-limitado, por hipótese de indução, temos que $rk(G/\gamma_c(G))$ é $\{d(G), c\}$-limitado.

Agora, $\gamma_c(G)$ é abeliano e $d(\gamma_c(G))$ é $\{d(G), c\}$-limitado, pois, como os comutadores de comprimentos a partir de $c + 1$ são todos iguais a 1, pelo [Lemma 3.6, [15]], temos que

$$\gamma_c(G) = \langle [t_{i_1}, \cdots, t_{i_c}] \mid t_{i_j} \in \{g_1, ..., g_{d(G)}\} \cup \{g_1^{-1}, ..., g_{d(G)}^{-1}\} \rangle,$$

onde $\{g_1, ..., g_{d(G)}\}$ é um conjunto de geradores de G. Assim, pelo Lema 1.41, temos que $rk(\gamma_c(G))$ é $\{d(G), c\}$-limitado.

Portanto, como pelo Corolário 1.40, temos que

$$rk(G) \leq rk(G/\gamma_c(G)) + rk(\gamma_c(G)),$$

segue que o posto de G $rk(G)$ é limitado em termos da classe de nilpotência de G e do número minimal de geradores de G, como queríamos.

■

Capítulo 2

p-Grupos Powerful

Os principais resultados deste trabalho nos fornecem limites para os postos de alguns grupos em situações especiais. Neste capítulo iremos estudar uma classe de p-grupos finitos, chamados powerful. A família dos p-grupos powerful foi introduzida pela primeira vez em [21] por A. Lubotsky e A. Mann. Os p-grupos finitos powerful possuem a propriedade de ter o número minimal de geradores igual ao seu posto, sendo, assim, importantes ferramentas para o desenvolvimento de provas no estudo de p-grupos finitos. Para tornar essa ferramenta viável, iremos mostrar que em um p-grupo finito de posto limitado sempre existe um subgrupo característico powerful que possui o índice limitado por uma função que depende apenas de p e do posto do p-grupo.

As principais referências biliográficas para a teoria de p-grupos powerful que usamos neste capítulo são os livros "Analytic Pro-p groups" [1], "The Structure of Groups of Prime Power Order" [20] e o artigo "Powerful p-groups. I: finite groups" [21].

Denotaremos como p um número primo qualquer e, dado um grupo G, G^p será o subgrupo de G dado por $G^p = \langle g^p \mid g \in G \rangle$.

Definição 2.1. (i) *Um p-grupo finito G é powerful se p é ímpar e G/G^p é abeliano; ou se $p = 2$ e G/G^4 é abeliano.*

(ii) *Um subgrupo N de um p-grupo finito G é powerfully embedded em G, e escrevemos N p.e. G, se p é ímpar e $[N, G] \leq N^p$; ou se $p = 2$ e $[N, G] \leq N^4$.*

Os termos *powerful* e *powerfully embedded* não serão traduzidos para seus respectivos termos em português *potente* e *potentemente imerso*, porque na literatura existem outras definições de "potent group" não relacionadas com o tópico deste capítulo (veja, por exemplo, [3] pg. 181) e definições de "potent group" relacionadas com o tópico apresentado (veja, por exemplo, [5]), mas com significado distinto. Portanto, a tradução para o português poderia gerar confusão ao leitor e preferimos deixar o termo original em inglês.

Note que, pela definição acima, um p-grupo finito é powerful se p é ímpar e $G' \leq G^p$ ou se $p = 2$ e $G' \leq G^4$. Observe, também, que quando G é um 2-grupo, G/G^2 tem expoente 2, logo é abeliano. Assim, a definição de grupos powerful para $p = 2$ precisa ser diferente.

Temos, por exemplo, que todo p-grupo abeliano é powerful e seus subgrupos são todos powerfully embedded. Para p ímpar, p-grupos não abelianos de expoente p não são powerful, pois $1 \neq G' \not\leq G^p = 1$. Lembrando que, para $n \geq 2$, o grupo Diedral de ordem $2n$, D_n, é definido por $D_n = \langle \rho, \tau \mid \rho^n = 1 = \tau^2, \rho^\tau = \rho^{-1} \rangle$, temos que D_4 é um 2-grupo que não é powerful, pois $D_4' = D_4^2 = \langle \rho^2 \rangle > D_4^4 = 1$. Com o exemplo de D_4 podemos ver, também, que nem todo p-grupo com classe de nilpotência 2 é powerful. Além disso, a partir do mesmo exemplo podemos exibir um grupo powerful que contém propriamente uma cópia isomorfa de D_4, mostrando, assim, que nem todo subgrupo de um p-grupo powerful é powerful. Para construir esse exemplo, considere o produto direto $D_4 \times C$, onde $D_4 = \langle \rho, \tau \mid \rho^4 = \tau^2 = 1, \rho^\tau = \rho^{-1} \rangle$ e $C \cong C_8 = \langle z \rangle$ é o cíclico de ordem 8, e defina

$$N = \langle [\rho, \tau]^{-1} z^4 \rangle = \langle \rho^2 z^4 \rangle \leq D_4 \times C.$$

Observe que N é normal em $D_4 \times C$, pois $Z(D_4 \times C) \cong Z(D_4) \times Z(C) = \langle \rho^2 \rangle \times C$, logo $N \leq Z(D_4 \times C)$. Considere, então, $G = (D_4 \times C)/N$. Temos que G é um 2-grupo powerful, pois

$$G' = \langle \rho^2 N \rangle = \langle z^4 N \rangle \leq G^4.$$

Agora, tome $H = \langle \rho N, \tau N \rangle$. Temos que $\delta : D_4 \to H$ dado por $\delta(\rho) = \rho N$ e $\delta(\tau) = \tau N$ é um isomorfismo, logo, como D_4 não é powerful, temos que H não é powerful. Assim, G é um 2-grupo powerful que possui um subgrupo próprio H que não é powerful, como queríamos.

O lema a seguir descreve as principais propriedades dos grupos powerful.

Lema 2.2. *Seja G um p-grupo finito e sejam N, K e W subgrupos normais de G com $N \leq W$. Então:*

(i) *G é powerful se, e somente se, G p.e. G.*

(ii) *Se N p.e. G, então $N \lhd G$ e N é powerful.*

(iii) *Seja p ímpar. Então, G é powerful se, e somente se, $G^p = \Phi(G)$.*

(iv) *Se N p.e. G, então NK/K p.e. G/K. Em particular, quocientes de grupos powerful são powerful.*

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

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

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

- *se p é ímpar,*

$$N^p[N,W,W] \leq J < N^p[N,W] \text{ e } |N^p[N,W] : J| = p;$$

- *se $p = 2$,*

$$N^4[N,W]^2[N,W,W] \leq J < N^4[N,W] \text{ e } |N^4[N,W] : J| = 2.$$

Demonstração:

(i) Suponhamos inicialmente que G é powerful. Se p é ímpar, então G/G^p é abeliano, logo $G' = [G,G] \leq G^p$ e temos que G p.e. G. Agora, se $p = 2$, temos que G/G^4 é abeliano, assim, $G' = [G,G] \leq G^4$ e, portanto, G p.e. G. Reciprocamente, suponhamos que G p.e. G. Se p é ímpar temos que $[G,G] \leq G^p$, logo G/G^p é abeliano. Analogamente, se $p = 2$, então $[G,G] \leq G^4$ e, portanto, G/G^4 é abeliano. Logo, G é powerful.

(ii) Considere p ímpar. Se N p.e. G, então $[N,G] \leq N^p \leq N$. Observe que $N \triangleleft G$ se, e somente se, $[N,G] \leq N$. Portanto, $N \triangleleft G$. Agora, queremos mostrar que N é powerful, ou seja, N/N^p é abeliano. Como N p.e. G temos que $[N,N] \leq [N,G] \leq N^p$ e o resultado segue. Se $p = 2$ o argumento é análogo.

(iii) Como G é um p-grupo finito, pelo Teorema de Bases de Burnside, Teorema 1.37, temos que $\Phi(G) = G'G^p$. Como p é ímpar, se G é powerful, então G/G^p é abeliano, logo $G' \leq G^p$ e o resultado segue. Reciprocamente, se $\Phi(G) = G^p$, com p ímpar, então $G' \leq G^p$ e, portanto, G é powerful.

(iv) Faremos a prova para p ímpar, pois a prova para $p = 2$ é análoga. Temos que N p.e. G, ou seja, que $[N,G] \leq N^p$. Como $K \triangleleft G$ podemos considerar o homomorfismo canônico $\pi : G \to G/K$, onde $\pi(N) = NK/K$. Observe inicialmente que $\pi(N^p) = \{\pi(m) \mid m \in N^P\}$ e $N^p = \langle n^p \mid n \in N\rangle$, logo $\pi(N^p) = \langle \pi(n^p) \mid n \in N\rangle$. Além disso, $\pi(N)^p = \langle \pi(n)^p \mid n \in N\rangle$. Assim,

$$\pi(N^p) = N^pK/K = (NK/K)^p = (\pi(N))^p,$$

pois π é um homomorfismo. Agora, como $[N,G] \leq N^p$, pelo Teorema da Correspondência, $\pi([N,G]) \leq \pi(N^p)$. Mas $\pi([N,G]) = [\pi(N), \pi(G)] = [NK/K, G/K]$, logo $[NK/K, G/K] \leq N^pK/K = (NK/K)^p$. Portanto, NK/K p.e. G/K.

(v) Considere p ímpar e $K \leq N^p$. Suponhamos primeiro que N p.e. G. Temos pelo item (iv) que NK/K p.e. G/K, mas $K \leq N^p$, assim,

$$[N/K, G/K] \leq N^p/K = (N/K)^p$$

e, portanto, N/K p.e. G/K. Reciprocamente, suponhamos que N/K p.e. G/K, logo,

$$[N, G]/K = [N/K, G/K] \leq (N/K)^p = (NK/K)^p = N^pK/K = N^p/K,$$

já que $K \leq N^p$. Assim, pelo Teorema da Correspondência, $[N, G] \leq N^p$ e, portanto, N p.e. G. A prova para $p = 2$ é análoga.

(vi) Denote por $H = \langle N, x\rangle$. Como $N \lhd G$, é fácil ver que todo elemento $h \in H$ pode ser escrito como $h = nx^i$, para algum $n \in N$ e $0 \leq i \leq o(x) - 1$. Agora, é suficiente mostrar que $[H, H] = [N, H]$, pois, por hipótese, N p.e. G, assim, se p é ímpar, $[N, H] \leq [N, G] \leq N^p \leq H^p$ e, se $p = 2$, $[N, H] \leq [N, G] \leq N^4 \leq H^4$, logo H p.e H e, portanto, H é powerful. Já temos que $[N, H] \leq [H, H]$. Para provar que $[H, H] \leq [N, H]$, tome $nx^i, mx^j \in H$. Pelas propriedades dos comutadores e usando que $N \lhd H$, temos que,

$$[nx^i, mx^j] = [n, mx^j]^{x^i}[x^i, mx^j] = ([n, x^j][n, m]^{x^j})^{x^i}[x^i, x^j][x^i, m]^{x^j} = [n^{x^i}, x^j][n^{x^{j+i}}, m^{x^{j+i}}][x^i, m^{x^j}] \in [N, H],$$

onde a soma $j + i$ é feita módulo a ordem de x. E, assim, o resultado segue.

(vii) Faremos a prova somente para p ímpar, pois o argumento é análogo quando $p = 2$. Suponhamos que $[N, W] \nleq N^p$, ou seja, que N não é powerfully embedded em W. Temos que $N^P < N^p[N, W] = M$. Como G é um p-grupo e M e N são subgrupos normais em G, existe $J \lhd G$ tal que $N^p \leq J < M$ e $|M : J| = p$. Agora, G/J é um p-grupo e, pelo Teorema da Correspondência, $M/J \lhd G/J$, logo $Z(G/J) \cap M/J \neq 1$. Como $|M/J| = p$, temos que $M/J \leq Z(G/J)$, ou seja, M/J é central em G/J; logo $[M, G] \leq J$. Note que $[N, W, W] \leq [M, G] = [N^p[N, W], G]$ e como já tínhamos que $N^p \leq J$, o resultado segue.

■

O ponto principal do item (vii) do lema anterior é estabelecer uma técnica para provar que N p.e. W, onde $N \leq W$ são subgrupos normais de um p-grupo G. Esta técnica consiste em supor, por contradição, que N não é powerfully embedded em W, assim existirá um $J \lhd G$ apropriado para fazermos um corte em G e reduzir ao caso em que $N^p = 1$, se p é ímpar, ou ao caso $N^4 = 1$, se $p = 2$. Além disso, podemos supor que $[N, W]$ tem ordem p. Note que nesse caso $[N, W]$ será central em G. Um exemplo deste método pode ser visto na prova do seguinte resultado.

Proposição 2.3. *Sejam G um p-grupo finito e $N \leq G$. Se N p.e. G, então N^p p.e. G.*

Demonstração: Suponhamos, primeiro, que p é ímpar. Temos que $[N, G] \leq N^p$ e queremos mostrar que $[N^p, G] \leq (N^p)^p$. Para isso, suponhamos por contradição que N^p não é powerfully embedded em G, assim, pelo Lema 2.2 (vii), podemos assumir que

$$(N^p)^p = 1 = [N^p, G, G]$$

e vamos mostrar que $[N^p, G] = 1$. Note que, $[N, G, G, G] \leq [N^p, G, G] = 1$, logo $[N, G, G] \leq Z(G)$ e, assim, para quaisquer $x \in N$ e $g \in G$, a função $w \longmapsto [x, g, w]$ é um homomorfismo de G em $Z(G)$. Então,

$$\prod_{j=0}^{p-1} [x, g, x^j] = \prod_{j=0}^{p-1} [x, g, x]^j = [x, g, x]^{p(p-1)/2}. \tag{2.1}$$

Assim,

$$\begin{aligned} [x^p, g] &= [x, g]^{x^{p-1}} [x, g]^{x^{p-2}} \cdots [x, g] \\ &= \prod_{j=p-1}^{0} [x, g][x, g, x^j] \\ &= [x, g]^p \prod_{j=0}^{p-1} [x, g, x^j] \\ &= [x, g]^p [x, g, x]^{p(p-1)/2} = 1, \end{aligned}$$

onde as duas primeiras igualdades seguem das propriedades dos comutadores, a terceira igualdade segue do fato de que $[x, g, x^j]$ está em $Z(G)$ para todo $j \in \mathbb{N}$, a quarta igualdade segue de (2.1) e a última igualdade segue do fato de que $[N, G]^p = 1$, já que $[N, G] \leq N^p$ e estamos supondo que $(N^p)^p = 1$. Logo, $[N^p, G] = 1$ como queríamos.

Agora, considere que $p = 2$. Análogo ao feito anteriormente, suponhamos por contradição que N^p não é powerfully embedded em G, assim, pelo Lema 2.2, podemos assumir que $[N, G] \leq N^4$ e que

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

Note que para todo $x \in N$ e $g \in G$ temos pelas propriedades dos comutadores que

$$[x^4, g] = [x^2, g]^{x^2} [x^2, g] = [x^2, g][x^2, g, x^2][x^2, g] = [x^2, g]^2 = 1,$$

então $N^4 \leq Z(G)$. Como N tem expoente divisor de 8, N^4 é gerado por elementos de ordem 2, então $(N^4)^2 = 1$. Portanto, dados $x \in N$ e $g \in G$ temos

$$[x^2, g] = [x, g]^x[x, g] = [x, g][x, g, x][x, g] = [x, g]^2 = 1,$$

já que $[x, g, x] \in [N, G, G] \leq [N^4, G] = 1$ e $[x, g] \in [N, G] \leq N^4$. Então, $[N^2, G] = 1$ e o resultado segue.

■

Definição 2.4. *Seja G um p-grupo finito. Definimos*

$$P_1(G) = G \text{ e } P_{i+1}(G) = P_i(G)^p[P_i(G), G] \text{ para todo } i \geq 1.$$

Para simplificar a notação, usaremos

$$G_i = P_i(G).$$

Observe que, como G é um p-grupo finito, pelo Teorema de Bases de Burnside, $\Phi(G) = G^pG'$, assim $G_2 = G^p[G, G] = \Phi(G)$. Além disso, $\Phi(G_i) = G_i^pG_i' \leq G_i^p[G_i, G] = G_{i+1}$. Temos também que os termos da Definição 2.4 acima formam uma série

$$G = G_1 \geq G_2 = \Phi(G) \geq G_3 \geq \cdots \geq G_n \geq \cdots$$

onde cada termo é característico no termo anterior e, assim, todos os termos são característicos em G. Esta série é às vezes chamada de *série p-descedente* de G.

O resultado a seguir nos fornece algumas propriedades para a série definida acima quando G é um p-grupo powerful.

Lema 2.5. *Seja G um p-grupo powerful.*

(i) *Para todo $i \geq 1$ temos que G_i p.e. G e $G_{i+1} = G_i^p = \Phi(G_i)$.*

(ii) *Para todo $i \geq 1$, o mapa $x \longmapsto x^p$ induz um homomorfismo sobrejetivo de G_i/G_{i+1} em G_{i+1}/G_{i+2}.*

Demonstração: Faremos a prova do item (i) por indução sobre i. Temos que $G_1 = G$ é powerful, logo G_1 p.e. G. Além disso, já vimos que $G_2 = \Phi(G) = \Phi(G_1)$ e, como G é powerful, temos que $G' \leq G^p$, logo, pelo Teorema de Bases de Burnside, $G_2 = \Phi(G_1) = G_1^p$. Suponhamos, agora, que $i > 1$ e que para todo $j < i$ temos que G_j p.e. G e $G_{j+1} = G_j^p = \Phi(G_j)$. Note que $G_i = G_{i-1}^p[G_{i-1}, G]$, mas, por hipótese de indução, temos que $G_i = G_{i-1}^p$ e G_{i-1} p.e. G, então, pela Proposição 2.3, segue que $G_i = G_{i-1}^p$ p.e. G. Por outro lado, temos que $G_{i+1} = G_i^p[G_i, G]$ e pelo Teorema de Bases de Burnside, $\Phi(G_i) = G_i^p[G_i, G_i]$ e $[G_i, G_i] \leq [G_i, G] \leq G_i^p$. Assim, segue que

$$G_{i+1} = G_i^p = \Phi(G_i),$$

o que completa a prova do item (i).

Por (i) e pelo Lema 2.2 (ii) temos que G_i é powerful para todo $i \geq 1$. Note que $G_{i+1} = P_2(G_i)$ e $G_{i+2} = P_3(G_i)$. Então, mudando a notação, podemos assumir que $i = 1$; e substituindo G por G/G_3, podemos assumir que $G_3 = 1$. Agora, como $[G_2, G] \leq G_3 = 1$ temos que $[G, G] \leq G_2 \leq Z(G)$ e, assim, $[G, G, G] = 1$, logo segue que G tem classe de nilpotência 2. Portanto, dados $x, y \in G$ temos que $(xy)^p = x^p y^p [y, x]^{p(p-1)/2}$. Se p é ímpar, temos que p divide $p(p-1)/2$ e, assim, $[y, x]^{p(p-1)/2}$ está em $G_2^p = G_3 = 1$. E, se $p = 2$, $[G, G] \leq G^4 \leq G_3 = 1$. Em ambos os casos temos que

$$(xy)^p = x^p y^p.$$

Então, como $G_2^p = G_3 = 1$ e $G^p = G_2$, mostramos que $x \mapsto x^p$ induz um homomorfismo sobrejetivo de G/G_2 em G_2/G_3, o que completa a prova de (ii).

■

Os próximos dois resultados mostram como propriedades óbvias para grupos abelianos também são válidas para p-grupos powerful.

Lema 2.6. *Se $G = \langle a_1, ..., a_d \rangle$ é um p-grupo powerful, então $G^p = \langle a_1^p, ..., a_d^p \rangle$.*

Demonstração: Seja $\theta : G/G_2 \to G_2/G_3$ o homomorfismo sobrejetivo considerado no Lema 2.5. Então, G_2/G_3 é gerado por $\{\theta(a_1 G_2), ..., \theta(a_d G_2)\}$, assim, $G_2 = \langle a_1^p, ..., a_d^p \rangle G_3$. Agora, como $G_3 = \Phi(G_2)$, que é o conjunto de não geradores de G_2, e, pelo Lema 2.5, $G_2 = G^p$, temos que $G^p = \langle a_1^p, ..., a_d^p \rangle$.

■

Vamos introduzir uma definição que é necessária para estudar potências de elementos nos grupos powerful.

Definição 2.7. *Seja G um p-grupo. Um elemento $g \in G$ é dito uma p-potência em G se existe $x \in G$ tal que $g = x^p$. Se $H \leq G$, dizemos que H é pth power em G se para todo $y \in H$ existe um $x \in G$ tal que $y = x^p$, ou seja, todo elemento em H é uma p-potência em G.*

Proposição 2.8. *Se G é um p-grupo powerful, então G^p é pth power em G, ou seja, $G^p = \{g^p \mid g \in G\}$.*

Demonstração: Faremos a prova por indução sobre $|G|$. Se $|G| = 1$ o resultado é trivial. Suponhamos, então, que $|G| > 1$ e que o resultado vale para todo p-grupo powerful de ordem menor que $|G|$. Tome g em G^p. Pelo Lema 2.5 (ii), existem x em G e y em G_3 tais que $g = x^p y$. Considere $H = \langle G^p, x \rangle$. Agora, pelo Lema 2.5 (i), $G^p = G_2$

p.e. G, assim, pelo Lema 2.2 (vi), H é powerful. Além disso, $g \in H^p$, já que y está em $G_3 = G_2^p$. Se $H \neq G$, então, por hipótese de indução, g é p-potência em H e, em particular, g é p-potência em G. Se $G = H$, pelo Lema 2.5 (i), temos que $G^p = \Phi(G)$ e, portanto, $G = \langle \Phi(G), x \rangle = \langle x \rangle$, ou seja, G é cíclico e o resultado é trivial.

■

No teorema a seguir descreveremos as principais propriedades da p-lower série para p-grupos powerful. Lembramos que para todo $i \geq 1$ denotamos $G_i = P_i(G)$.

Teorema 2.9. *Seja $G = \langle a_1, ..., a_d \rangle$ um p-grupo powerful. Para todo $i \geq 1$ temos:*

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

(ii) *$G_{i+k} = P_{k+1}(G_i) = G_i^{p^k}$ para todo $k \geq 0$.*

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

(iv) *A função $x \longmapsto x^{p^k}$ induz um homomorfismo sobrejetivo de G_i/G_{i+1} em G_{i+k}/G_{i+k+1} para todo $i \geq 1$ e para todo $k \geq 0$.*

Demonstração: O item (i) já foi provado no Lema 2.5 (i). Para o item (iii) faremos indução sobre i. Temos que $G_1 = G = G^{p^0} = G^1 = \langle a_1, ..., a_d \rangle$. Suponhamos, então, que $i > 1$ e que para todo $j < i$ temos que

$$G_j = G^{p^{j-1}} = \{x^{p^{j-1}} \mid x \in G\} = \langle a_1^{p^{j-1}}, ..., a_d^{p^{j-1}} \rangle.$$

Observe que, pelo item (i) e pelo Lema 2.2 (ii), G_i é powerful. Note, também, que pelo Lema 2.5 (i), temos que $G_i = G_{i-1}^p = P_2(G_{i-1})$ e, pela Proposição 2.8, $G_i = \{x^p \mid x \in G_{i-1}\}$. Além disso, por hipótese de indução, temos que $G_{i-1} = G^{p^{i-2}} = \{x^{p^{i-2}} \mid x \in G\} = \langle a_1^{p^{i-2}}, ..., a_d^{p^{i-2}} \rangle$. Assim,

$$G_i = (G_{i-1})^p = (G^{p^{i-2}})^p = G^{p^{i-1}} = \{x^{p^{i-1}} \mid x \in G\} = \langle a_1^{p^{i-1}}, ..., a_d^{p^{i-1}} \rangle,$$

como queríamos. Assim, tomando G_i no lugar de G e $k+1$ no lugar de i no item (iii), temos que

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

o que completa a prova do item (ii). E o item (iv) segue do Lema 2.5 (ii).

■

Corolário 2.10. *Se $G = \langle a_1, ..., a_d \rangle$ é um p-grupo powerful, então*

$$G = \langle a_1 \rangle \cdots \langle a_d \rangle,$$

isto é, G é o produto de seus subgrupos cíclicos $\langle a_i\rangle$, $1 \leq i \leq d$.

Demonstração: Assuma que $G_e > G_{e+1} = 1$. Queremos mostrar, inicialmente, que $G = \langle a_1\rangle \cdots \langle a_d\rangle G_e$, para isso, faremos indução sobre e. Se $e = 1$ o resultado é trivial. Suponhamos, então, que o resultado é válido para $e-1$, ou seja, $G = \langle a_1\rangle \cdots \langle a_d\rangle G_{e-1}$. Agora, note que G_{e-1}/G_e é abeliano, logo, usando Teorema 2.9 (iii), temos

$$\begin{aligned} G/G_e &= \langle a_1\rangle \cdots \langle a_d\rangle G_{e-1}/G_e \\ &= \langle a_1\rangle \cdots \langle a_d\rangle \langle a_1^{p^{e-1}}, ..., a_d^{p^{e-1}}\rangle/G_e \\ &= \langle a_1\rangle \cdots \langle a_d\rangle \langle a_1^{p^{e-1}}\rangle \cdots \langle a_d^{p^{e-1}}\rangle/G_e \\ &= \langle a_1\rangle \cdots \langle a_d\rangle/G_e. \end{aligned}$$

Portanto, podemos supor que $G = \langle a_1\rangle \cdots \langle a_d\rangle G_e$, como queríamos. Pelo Teorema 2.9 (iii), $G_e = \langle a_1^{p^{e-1}}, ..., a_d^{p^{e-1}}\rangle$ e, além disso, temos que G_e p.e. G logo $[G_e, G] \leq G_e^p$, mas $G_e^p = G_{e+1} = 1$. Segue que G_e é central em G e o resultado é claro.

■

Lembramos que dado um p-grupo finito G, denotamos por $d(G)$ a cardinalidade de um conjunto minimal de geradores de G. O teorema que veremos a seguir é um dos principais resultados desse capítulo, pois retrata a propriedade dos p-grupos powerful de que se H é um subgrupo de um p-grupo powerful G, então podemos sempre limitar $d(H)$ em função de $d(G)$, que é mais uma propriedade compartilhada pelos grupos abelianos. Esse resultado será fundamental em provas futuras.

Já vimos na Seção 1.4 que para p-grupos finitos todo conjunto minimal de geradores possui a mesma cardinalidade, além disso, se G é um p-grupo finito, $d(G)$ é também a dimensão de $G/\Phi(G)$ visto como um espaço vetorial sobre um corpo de p elementos. Denotaremos por $\dim V$ a dimensão de V como espaço vetorial sobre um corpo de p elementos.

Teorema 2.11. *Se G é um p-grupo powerful e $H \leq G$, então $d(H) \leq d(G)$.*

Demonstração: A prova será por indução sobre $|G|$. Se $|G| = 1$ o resultado é trivial. Suponhamos, então que $|G| > 1$ e que o resultado vale para qualquer p-grupo powerful com cardinalidade menor que $|G|$. Seja $d = d(G)$ e considere $m = d(G_2)$. No Lema 2.5 mostramos que G_2 é powerful, então, por hipótese de indução, podemos supor que o subgrupo $K = H \cap G_2$ satisfaz $d(K) \leq m$. Agora, pelo Lema 2.5 (ii), temos que a função $x \longmapsto x^p$ induz um homomorfismo sobrejetivo $\pi : G/G_2 \to G_2/G_3$, assim $\dim(ker\pi) = d - m$. Então, $\dim(ker\pi \cap HG_2/G_2) \leq d - m$ e temos

$$\dim(\pi(HG_2/G_2)) \geq \dim(HG_2/G_2) - (d-m) = m - (d-e),$$

onde $e = \dim(HG_2/G_2)$. Sejam $h_1, ..., h_e \in H$ tais que $HG_2 = \langle h_1, ..., h_e\rangle G_2$. Como $\Phi(K) \leq K^p \leq G_3$, o subespaço de $K/\Phi(K)$ gerado pelas classes laterais de $h_1^p, ..., h_e^p$ tem dimensão, no mínimo, $\dim(\pi(HG_2/G_2)) \geq m-(d-e)$. Como $d(K) \leq m$, podemos achar $d-e$ elementos $y_1, ..., y_{d-e}$ em K tais que $K = \langle h_1^p, ..., h_e^p, y_1, ..., y_{d-e}\rangle\Phi(K)$, então $K = \langle h_1, ..., h_e, y_1, ..., y_{d-e}\rangle$ e, assim, usando a Regra de Dedekind, temos

$$\begin{aligned} H = H \cap HG_2 &= H \cap \langle h_1, ..., h_e\rangle G_2 = \langle h_1, ..., h_e\rangle(H \cap G_2) \\ &= \langle h_1, ..., h_e\rangle K = \langle h_1, ..., h_e, y_1, ..., y_{d-e}\rangle. \end{aligned}$$

Portanto, $d(H) \leq d$, como queríamos.

■

O teorema anterior nos diz que se G é um p-grupo powerful, então $rk(G) = d(G)$, o que já vimos na Seção 1.4 não ser válido para todo p-grupo finito. No geral, a volta desse teorema não é válida, pois já vimos que D_4 não é powerful, mas $rk(D_4) = d(D_4) = 2$. Uma volta parcial consiste em mostrar que em qualquer p-grupo finito G existe um subgrupo powerful normal cujo índice em G é delimitado por uma função em termos de $rk(G)$. Este resultado, Teorema 2.18, é o segundo ponto principal do capítulo.

Iremos agora construir um subgrupo que será, mais tarde, usado como uma ferramenta chave na prova do Teorema 2.18.

Definição 2.12. *Sejam G um p-grupo finito e r um inteiro positivo. Definimos $V(G, r)$ como sendo a interseção dos núcleos de todos os homomorfismos de G em $GL_r(\mathbb{F}_p)$.*

Como a imagem de qualquer homomorfismo de um p-grupo G em $GL_r(\mathbb{F}_p)$ é um p-grupo e qualquer p-subgrupo de $GL_r(\mathbb{F}_p)$ é conjugado de um subgrupo do grupo $U_r(\mathbb{F}_p)$, pois $U_r(\mathbb{F}_p)$ é um p-subgrupo de Sylow de $GL_r(\mathbb{F}_p)$, poderíamos definir $V(G, r)$, de forma análoga, como sendo a interseção dos núcleos de todos os homomorfismos de G em $U_r(\mathbb{F}_p)$.

Nosso próximo resultado nos fornece uma caracterização para os elementos de $V(G, r)$. Para demonstrar esse resultado precisamos da seguinte definição.

Definição 2.13. *Sejam G um p-grupo finito e $\mathbb{F}_p$ o corpo finito com p elementos. Uma $\mathbb{F}_p$-representação de G é dada por um $\mathbb{F}_p$-espaço vetorial V e um homomorfismo $\rho : G \to GL(V)$, onde $GL(V)$ é o grupo de todos os $\mathbb{F}_p$-automorfismos de V.*

Note que, se $V \cong \mathbb{F}_p^n$, para algum $n \geq 1$, então o grupo $GL(V)$ é isomorfo ao grupo $GL_n(\mathbb{F}_p)$ de todas as matrizes invertíveis $n \times n$ sobre $\mathbb{F}_p$.

Lema 2.14. *Dado G um p-grupo finito. Um elemento $g \in G$ pertence a $V(G, r)$ se, e somente se, g age trivialmente em qualquer representação linear de G sobre qualquer $\mathbb{F}_p$-espaço vetorial de dimensão até r.*

Demonstração: Suponha que $g \in V(G,r)$ e considere $\varphi : G \to GL_r(\mathbb{F}_p)$ uma representação de G. Como $g \in V(G,r)$, temos que $g \in ker\varphi$ e, assim, $\varphi(g) = I_r$, onde I_r é a matriz identidade em $GL_r(\mathbb{F}_p)$. Observe que $\varphi(G) \leq GL_r(\mathbb{F}_p)$ e age por conjugação em $GL_r(\mathbb{F}_p)$, logo, g age trivialmente sobre $GL_r(\mathbb{F}_p)$. Considere agora $k < r$ e $\phi : G \to GL_k(\mathbb{F}_p)$ uma representação de G. Queremos ver que g age trivialmente sobre $GL_k(\mathbb{F}_p)$. Para isso, observe que para todo $k < r$ podemos considerar o homomorfismo

$$\theta : GL_k(\mathbb{F}_p) \to GL_r(\mathbb{F}_p)$$

definido por

$$A \longmapsto \begin{bmatrix} A & 0_{k\times(r-k)} \\ 0_{(r-k)\times k} & I_{r-k} \end{bmatrix},$$

onde 0_l é a matriz nula em $GL_l(\mathbb{F}_p)$ para qualque $l \in \mathbb{N}$. Assim, temos que

$$\theta \circ \phi : G \to GL_r(\mathbb{F}_p)$$

é um homomorfismo. Como $g \in V(G,r)$, obtemos que

$$(\theta \circ \phi)(g) = I_r = \begin{bmatrix} \varphi(g) & 0_{k\times(r-k)} \\ 0_{(r-k)\times k} & I_{r-k} \end{bmatrix}.$$

Portanto,

$$\phi(g) = \begin{bmatrix} I_k & 0_{k\times(r-k)} \\ 0_{(r-k)\times k} & I_{r-k} \end{bmatrix} = I_k.$$

Logo, g age trivialmente sobre $GL_k(\mathbb{F}_p)$ para todo $k \leq r$.

Reciprocamente, se g age trivialmente em qualquer representação linear de G sobre qualquer $\mathbb{F}_p$-espaço vetorial de dimensão até r, em particular, $g \in ker\varphi$ para todo homomorfismo $\varphi : G \to GL_r(\mathbb{F}_p)$ e, portanto, $g \in V(G,r)$.

■

Definição 2.15. *Dado $r \in \mathbb{N}$, definimos $\lambda(r)$ como sendo um inteiro que satisfaz*

$$2^{\lambda(r)-1} < r \leq 2^{\lambda(r)}.$$

Para o lema a seguir iremos usar a notação $[x]$ para indicar o maior inteiro menor ou igual a x.

Lema 2.16. (i) *O grupo $U_r(\mathbb{F}_p)$ possui uma série de comprimento $\lambda(r)$ de subgrupos normais com todos os fatores abelianos elementares.*

(ii) *Se G é um p-grupo finito, então $G/V(G,r)$ possui uma série com as mesmas propriedades enunciadas em* (i).

Demonstração: Faremos a prova do item (i) por indução sobre r. Se $r = 1$, então $U_1(\mathbb{F}_p) = \mathbb{F}_p$ que é abeliano elementar, assim $\lambda(1) = 0$ e $U_1(\mathbb{F}_p)$ possui uma série de subgrupos normais com fatores abelianos elementares e comprimento $\lambda(1)$. Suponha, então, que $r \geq 2$ e que o resultado é válido para $U_t(\mathbb{F}_p)$ para todo $t < r$. Considere $s = [r/2]$. Os elementos de $U_r(\mathbb{F}_p)$ são da forma

$$X = \begin{bmatrix} A & 0 \\ B & C \end{bmatrix}$$

com $A \in U_s(\mathbb{F}_p)$ e $C \in U_{r-s}(\mathbb{F}_p)$. A função ϕ que envia X em (A, C) é um homomorfismo de $U_r(\mathbb{F}_p)$ em $U_s(\mathbb{F}_p) \times U_{r-s}(\mathbb{F}_p)$. Note que se X está contido no núcleo de ϕ, então X é da forma

$$X = \begin{bmatrix} I_s & 0 \\ B & I_{r-s} \end{bmatrix},$$

logo, o núcleo de ϕ é um p-grupo abeliano elementar. Como $U_r(\mathbb{F}_p)/Ker\phi \cong Im\phi \leq U_s(\mathbb{F}_p) \times U_{r-s}(\mathbb{F}_p)$ e , por hipótese de indução, temos que $U_s(\mathbb{F}_p)$ e $U_{r-s}(\mathbb{F}_p)$ possuem uma série de comprimentos $\lambda(s)$ e $\lambda(r-s)$, respectivamente, de subgrupos normais com todos os fatores abelianos elementares, então o resultado segue pelo Teorema da Correspondência.

Para a prova de (ii) observe que se $\varphi : G \to U_r(\mathbb{F}_p)$ é um homomorfismo e $ker\varphi = N$, então

$$G/N \cong Im(\varphi) \leq U_r(\mathbb{F}_p).$$

Agora, $V(G, r)$ é a interseção dos núcleos de todos os homomorfismos de G em $U_r(\mathbb{F}_p)$. Note que, como G é um grupo finito, $V(G, r)$ é uma interseção de um número finito, k, de subgrupos. Seja, agora, $V(G, r) = N_1 \cap \cdots \cap N_k$, podemos considerar o homomorfismo sobrejetivo $\pi : G \to G/N_1 \times \cdots \times G/N_k$ definido por

$$\pi(g) = (gN_1, ..., gN_k).$$

Temos que o núcleo desse homomorfismo é $V(G, r)$, assim,

$$G/V(G, r) \cong G/N_1 \times \cdots \times G/N_k,$$

mas $G/N_1 \times \cdots \times G/N_k$ é isomorfo a um subgrupo de $U_r(\mathbb{F}_p)^k$. Portanto, o resultado segue de (i).

■

Proposição 2.17. *Sejam G um p-grupo finito e r um inteiro positivo. Considere $V = V(G, r)$ e denote $W = V$ se p é ímpar e $W = V^2$ se $p = 2$. Se $N \triangleleft G$, $d(N) \leq r$ e $N \leq W$, então N p.e. W.*

Demonstração: A prova é feita por indução sobre $|N|$. Se $|N| = 1$, já temos que N p.e. W. Suponha, então, que $|N| > 1$ e que o resultado é válido para todo subgrupo $K \triangleleft G$ que satisfaz as condições do enunciado com $|K| < |N|$.

Considere primeiro que p é ímpar e suponhamos por absurdo que $[N, V] \nleq N^p$, ou seja, que N não é powerfully embedded em V. Pelo Lema 2.2 (vii), podemos assumir que $N^p = 1$ e $|[N, V]| = p$. Como G é um p-grupo, existe $M \triangleleft G$ tal que $[N, V] \leq M < N$ e $|N : M| = p$. Note que M é maximal em N e $N/[N, V]$ é abeliano elementar, logo $N/[N, V]$ é gerado por seus subgrupos cíclicos e $M/[N, V]$ é maximal em $N/[N, V]$, assim, temos que

$$d(M/[N, V]) = d(N/[N, V]) - 1 \leq r - 1.$$

Temos ainda que $[N, V]$ é cíclico, logo $d(M) \leq r$. Assim, por hipótese indutiva, $[M, V] \leq M^p = 1$, então M é central em N e, como N/M é cíclico, temos que N é abeliano. Com isso e dado que $d(N) \leq r$ e $N^p = 1$ temos que N é abeliano elementar e, portanto, N é um $\mathbb{F}_p$-espaço vetorial de dimensão, no máximo, r. Logo, pelo Lema 2.14, a ação de conjugação de V em N é trivial. Assim, $[N, V] = 1$, o que é uma contradição. Portanto, N p.e. V.

Agora, considere o caso $p = 2$. Como antes, suponhamos por absurdo que $[N, V^2] \nleq N^4$, ou seja, que N não é powerfully embedded em V^2, assim podemos reduzir ao caso em que $N^4 = 1$ e $|[N, W]| = 2$. Como $N^4 = 1$ temos que N é nilpotente de classe 2, assim, pelo Teorema 1.22, temos que qualquer produto de quadrados em N é congruente a um quadrado módulo $[N, W]$, ou seja, para quaisquer $x, y \in N$ temos que,

$$(xy)^2[N, W] = x^2y^2[N, W].$$

Logo, como $N^4 = 1$, obtemos que $(N^2)^2 = 1$. Temos também que dados $a, b \in N$ e $[a, b] = c$,

$$b^{-1}ab = ac$$

e disso seugue que

$$b^{-1}a^2b = (b^{-1}ab)^2 = (ac)^2 = a^2c^2[c, a]$$

mas N é nilpotente de classe 2, assim $[c, a] = [[a, b], a] = 1$. Logo, temos que $b^{-1}a^2b = a^2c^2$ e, portanto, $a^{-2}b^{-1}a^2b = c^2$, ou seja,

$$[a^2, b] = [a, b]^2 \in [N, W]^2 = 1,$$

logo, $N^2 \leq Z(N)$. Agora, N/N^2 é um $\mathbb{F}_p$-espaço vetorial de dimensão, no máximo, r, então, pelo Lema 2.14, $[N, V] \leq N^2$. Logo, para todo $a \in N$ e para todo $v \in V$ temos que $[a, v] = b$, para algum b em N^2, assim $a^{-1}a^v = b$ e temos que $a^v = ab$. Logo, como $b \in N^2$, $(N^2)^2 = 1$ e $N^2 \leq Z(N)$, temos que

$$(a^2)^v = (a^v)^2 = (ab)^2 = a^2.$$

Portanto, $[N^2, V] = 1$. Assim, como $[N, V] \leq N^2$, temos que $[N, V, V] = 1$, logo

$$[N, W] = [N, V^2] \leq [N, V]^2[N, V, V] = 1,$$

o que é uma contradição. Portanto, N p.e. W.

■

Teorema 2.18. *Seja G um p-grupo finito com posto r. Então, G possui um subgrupo característico powerful com índice, no máximo, $p^{r\lambda(r)}$ se p é ímpar e, no máximo, $2^{r+r\lambda(r)}$ se $p = 2$.*

Demonstração: Considere $V = V(G, r)$. Note que, pela definição de V, temos que V é característico em G. Pelo Lema 2.16 (ii), existe uma série

$$G = N_0 \geq N_1 \geq \cdots \geq N_s = V$$

de subgrupos normais em G tais que $s \leq \lambda(r)$ e todos os fatores N_i/N_{i+1} são abelianos elementares, com $0 \leq i \leq s - 1$. Como G tem posto r, cada um desses fatores tem ordem, no máximo, p^r, então $|G : V| \leq p^{r\lambda(r)}$. Suponhamos que p é ímpar. Note que $V \triangleleft G$ e $d(V) \leq r$, pois G tem posto r, logo, pela Proposição 2.17, temos que V p.e. V e, assim, pelo Lema 2.2 (i), temos que V é powerful. Agora, seja $p = 2$. Note que V^2 é característico em V, pois, dado ϕ um automorfismo de V temos que $\phi(v^2) = \phi(v)^2$, para todo v em V, logo, V^2 é característico em G e, como G tem posto r, $d(V^2) \leq r$. Assim, novamente pela Proposição 2.17, temos que V^2 p.e. V^2 e, portanto, pelo Lema 2.2 (i), V^2 é powerful. Além disso, temos que $|V/V^2| \leq 2^r$, logo $|G : V^2| \leq 2^{r+r\lambda(r)}$, o que completa a prova.

■

Capítulo 3

Grupos Nilpotentes admitindo uma Involução

Neste capítulo estudaremos, principalmente, p-grupos finitos da forma $G = [G, \phi]$, onde ϕ é uma involução de G e $[G, \phi] = \langle x^{-1}x^{\phi} \mid x \in G \rangle$. Nosso principal objetivo é ver que, conhecendo o posto do subgrupo de pontos fixos de ϕ em G, ou seja, $rk(C_G(\phi))$, é sempre possível limitar o número de geradores dos termos da série central descendente de G e, sobre tudo, limitar o posto de G' em termos de $rk(C_G(\phi))$.

A principal referência usada neste capítulo é o artigo "Involutory automorphisms of finite groups and their centralizers" [24].

Os próximos resultados nos fornecem propriedades de um grupo G de ordem ímpar que admite uma involução.

Lema 3.1. *Seja G um grupo finito de ordem ímpar que admite uma involução ϕ. Seja $F = C_G(\phi)$ e considere I o subconjunto formado pelos elementos de G que são transformados em seus inversos por ϕ, ou seja, $I = \{x \in G \mid x^{\phi} = x^{-1}\}$. Então, são válidas as seguintes afirmações:*

(i) *$G = FI = IF$, $F \cap I = 1$ e $|I| = |G : F|$.*

(ii) *I é F-invariante.*

(iii) *Se H é um subconjunto de F tal que $H^x \subseteq F$ para $x \in I$, então x centraliza H.*

(iv) *Dois elementos de F conjugados em G são conjugados em F.*

(v) *Se H é um subgrupo de F, então $N_G(H) = C_G(H)N_F(H)$.*

(vi) *Se H é um subgrupo de I, então H é abeliano.*

Demonstração: Observe que I não é necessariamente um subgrupo de G. Em primeiro lugar, temos que se $y = x^{-1}x^{\phi}$, com $x \in G$, então

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

pois ϕ tem ordem 2. Assim, todo elemento y da forma $y = x^{-1}x^\phi$, com x em G, está em I. Agora, seja $\{x_i \mid 1 \leq i \leq n\}$ um cojunto completo de representantes de classes laterais à direita de F em G e sejam $y_i = x_i^{-1}x_i^\phi$, para todo $1 \leq i \leq n$. Temos que y_i está em I para todo i. Vamos provar que $\{y_i \mid 1 \leq i \leq n\}$ também é um conjunto completo de representantes de classes laterais à direita de F em G. Suponha por absurdo que isso não ocorre, assim devemos ter $y_j = zy_i$, para algum z em F e $i \neq j$. Aplicando ϕ obtemos

$$y_j^\phi = (zy_i)^\phi = z^\phi y_i^\phi.$$

Agora, como $z \in F = C_G(\phi)$ e $y_i, y_j \in I$, temos que $y_j^{-1} = zy_i^{-1}$, ou seja $y_j = y_i z^{-1}$, logo $zy_i = y_i z^{-1}$ e disso segue que $z^{y_i} = z^{-1}$, portanto,

$$z^{y_i^2} = z.$$

Logo, y_i^2 centraliza z. Como $|G|$ é ímpar, temos que y_i centraliza z, assim $z^{y_i} = z = z^{-1}$ e, portanto, $z^{-1} = z$. Agora, $o(z)$ é ímpar, assim $z = 1$, logo $y_i = y_j$. Portanto, $x_j^{-1}x_j^\phi = x_i^{-1}x_i^\phi$ e disso segue que $x_i x_j^{-1} = (x_i x_j^{-1})^\phi$, ou seja, $x_i x_j^{-1}$ está em F, logo

$$Fx_i = Fx_j,$$

ou seja, x_i e x_j representam a mesma classe lateral à direita de F em G, o que é uma contradição, pois $i \neq j$. Portanto, $\{y_i \mid 1 \leq i \leq n\}$ é um conjunto completo de representantes de classes laterais à direita de F em G, como queríamos.

Suponha, agora, que $u = zy_i \in I$ para algum $z \in F$ e algum $i \in \{1, ..., n\}$. Então

$$u^{-1} = u^\phi = (zy_i)^\phi = z^\phi y_i^\phi = zy_i^{-1},$$

assim, $u^{-1} = y_i^{-1}z^{-1} = zy_i^{-1}$, logo $z^{-1}y_i = y_i z$ e disso segue que

$$y_i z^{-1} = zy_i.$$

Portanto, usando um argumento análogo ao que vimos anteriormente, concluímos que $z = 1$. Logo, $I = \{y_i \mid 1 \leq i \leq n\}$ e, consequentemente, $G = FI$ e $|I| = |G : F|$. Usando as classes laterais à esquerda de F em G obtemos, de forma análoga, que $G = IF$. Finalmente, se $z \in F \cap I$, então $z = z^\phi = z^{-1}$, logo $z = 1$. Assim, $F \cap I = 1$ e finalizamos a prova de (i).

Tome x em I e z em F. Temos que

$$(x^z)^\phi = (z^{-1}xz)^\phi = (z^{-1})^\phi x^\phi z^\phi = z^{-1}x^{-1}z = (x^z)^{-1},$$

assim x^z está em I. Portanto, I é F-invariante, o que prova o item (ii).

Suponha, agora, que $H^x \subseteq F$, onde H é um subconjunto de F e x está em I. Tome z em H e $u = z^x$, então $u \in F$, pois $H^x \subseteq F$. Aplicando ϕ, obtemos

$$u = u^\phi = (z^x)^\phi = (x^{-1}zx)^\phi = (x^{-1})^\phi z^\phi x^\phi = xzx^{-1},$$

assim, temos que $x^{-1}zx = xzx^{-1}$ e disso segue que

$$z^{x^2} = x^{-1}x^{-1}zxx = x^{-1}xzx^{-1}x = z.$$

Logo, x^2 centraliza z e, como $o(x)$ é ímpar, x centraliza z. Como z é um elemento arbitrário em H, provamos (iii).

Suponhamos que $z_1, z_2 \in F$ e $z_2 = z_1^x$, para algum x em G. Pelo item (i), temos que $x = yz$ para algum y em I e z em F, logo

$$z_2 = z_1^x = z_1^{yz} = (yz)^{-1}z_1(yz) = z^{-1}y^{-1}z_1yz$$

e disso segue que

$$z_1^y = z_2^{z^{-1}} \in F.$$

Mas, pelo item (iii), y centraliza z_1, assim $z_1^y = z_1 = z_2^{z^{-1}}$, logo $z^{-1}z_1z = z_2$ e disso segue que

$$z_2 = z_1^z$$

e, portanto z_1 e z_2 são conjugados em F, o que prova o item (iv).

Para demonstrar o item (v), dado $H \leq F$, considere $N = N_G(H)$. Temos que H é ϕ-invariante, pois $H \subseteq F = C_G(\phi)$, então N também é ϕ-invariante e, consequentemente, pelo item (i), temos que

$$N = (N \cap I)(N \cap F).$$

Mas, $H^{(N\cap I)} = H \subseteq F$, assim pelo item (iii) temos que $N \cap I$ centraliza H. Como $N \cap F = N_F(H)$, temos que

$$N_G(H) = C_G(H)N_F(H),$$

como queríamos.

Se H é um subgrupo de I, como $I = \{x \in G \mid x^\phi = x^{-1}\}$, temos que $C_H(\phi) = 1$, logo ϕ induz um automorfismo livre de pontos fixos em H de ordem 2, então H é abeliano pelo Teorema 1.28, demonstrando o item (vi).

■

Lema 3.2. *Sejam G um grupo finito de ordem ímpar e ϕ uma involução de G. Considere $F = C_G(\phi)$ e $I = \{x \in G \mid x^\phi = x^{-1}\}$. Então, as seguintes afirmações são válidas:*

(i) *O subgrupo gerado por I é exatamente $[G, \phi]$;*

(ii) *Se N é um subgrupo normal ϕ-invariante de G, então $C_{G/N}(\phi) = FN/N$;*

(iii) *Se N é um subgrupo normal ϕ-invariante de G tal que $C_N(\phi) = 1$, então temos que $[N, I] = 1$ e $N \leq Z([G, \phi])$.*

Demonstração: Observe que na demonstração do item (i) do Lema 3.1 mostramos que todo elemento da forma $y = x^{-1}x^{\phi}$, com x em G, está em I, logo, $[G, \phi] \leq \langle I \rangle$. Assim, para ver que $[G, \phi] = \langle I \rangle$, resta mostrar que I está contido em $[G, \phi]$. Tome x em I, temos que $x^{\phi} = x^{-1}$, assim, como ϕ tem ordem 2, temos que $x = (x^{-1})^{\phi}$ e disso segue que

$$x^2 = x(x^{-1})^{\phi} = (x^{-1})^{-1}(x^{-1})^{\phi},$$

logo, x^2 está em $[G, \phi]$. Portanto, temos que $\langle x^2 \rangle$ está contido em $[G, \phi]$, mas G tem ordem ímpar, assim, $\langle x^2 \rangle = \langle x \rangle$ e, portanto, temos que x está em $[G, \phi]$ para todo x em I, como queríamos. Logo, temos que $[G, \phi] = \langle I \rangle$, o que demonstra o item (i).

Para o item (ii) note que, como G tem ordem ímpar, temos que N também tem ordem ímpar, logo, como a ordem de ϕ é 2, segue que $(|N|, o(\phi)) = 1$. Note que, como N é um subgrupo ϕ-invariante de G, temos que $C_G(\phi)N/N \leq C_{G/N}(\phi)$, assim, basta mostrar que dado qualquer gN em $C_{G/N}(\phi)$ temos que gN contém um elemento de $C_G(\phi)$ que é equivalente a mostrar que $C_{G/N}(\phi) = C_G(\phi)N/N$. Observe que ϕ tem ordem 2 e considere a ação de $\langle \phi \rangle$ no conjunto gN. Temos que as $\langle \phi \rangle$-órbitas que formam uma partição de gN têm tamanhos 2 ou 1. Agora, se todas as órbitas possuem tamanho 2 temos que 2 divide $|gN| = |N|$, o que é uma contradição pela hipótese de que $(|N|, o(\phi)) = 1$. Assim, existe pelo menos uma $\langle \phi \rangle$-órbita de tamanho 1 que nos fornece o elemento desejado de $C_G(\phi)$, o que conclui a prova do item (ii).

Assuma, agora, que N é um subgrupo normal ϕ-invariante de G tal que $C_N(\phi) = 1$. Como $C_N(\phi) = 1$, pelo Teorema 1.28, temos que todo n em N é tal que $n^{\phi} = n^{-1}$, pois ϕ tem ordem 2, logo, $N \subseteq I$. Temos, também, que $N \lhd G$, assim, n^i está em N para todo n em N e i em I. Disso segue que $(n^i)^{\phi} = (n^i)^{-1}$, mas temos também que $(n^i)^{\phi} = (i^{-1})^{\phi}n^{\phi}i^{\phi} = in^{-1}i^{-1}$. Logo, temos que $n^{-1} = (i^{-1})^2n^{-1}i^2 = (i^2)^{-1}n^{-1}i^2$, assim, i^2 comuta com n^{-1} e, portanto, i^2 comuta com n para todo i em I e n em N. Note que, pela definição de I, obtemos que $I^2 \subseteq I$ e, como G tem ordem ímpar, temos que $I^2 = I$. Portanto, n comuta com i para todo n em N e i em I e disso segue que $[N, I] = 1$.

Por fim, note que, como $[N, I]$ é ϕ-invariante, temos $[N, I] = ([N, I] \cap F)([N, I] \cap I)$, mas $C_N(\phi) = 1$, assim, $([N, I] \cap F) = 1$ e temos que $[N, I] = [N, I] \cap I$. Portanto, $[N, I] \subseteq I$. Como o subgrupo gerado por I é exatamente $[G, \phi]$ e $[N, I] = 1$ temos que $N \leq Z([G, \phi])$, como queríamos.

■

Lembramos que um grupo G tem expoente n, onde $n \geq 1$, se n é o menor inteiro tal que para todo g em G temos que $g^n = 1$. Observe que se G tem expoente p, então G é um p-grupo.

Lema 3.3. *Seja G um grupo finito com expoente p e posto r. Então $|G| \leq p^s$, onde $s = s(r)$ é um número que depende apenas de r.*

Demonstração: Pelo Teorema 2.18 temos que G possui um subgrupo powerful e característico N com índice, no máximo, $p^{\mu(r)}$, onde $\mu(r)$ é um número que depende apenas de r. Agora, como G tem posto r, temos que N é gerado por, no máximo, r elementos, assim, pelo Corolário 2.10, temos que N é o produto de, no máximo, r subgrupos cíclicos. Todos os subgrupos cíclicos de N possuem ordem p, pois G tem expoente p, logo N possui ordem, no máximo, p^r. Portanto,

$$|G| = |N||G : N| \leq p^r p^{\mu(r)} = p^{r+\mu(r)} = p^s,$$

onde $s = s(r)$ é um número que depende apenas de r.

■

Na demonstração anterior vimos como é possível deduzir resultados sobre um p-grupo de posto limitado G usando as propriedades do p-subgrupo powerful contido em G. Essa técnica é usada fortemente neste trabalho, pois reduz problemas de um p-grupo de posto limitado para um subgrupo powerful contido nele, visto que em p-grupos powerful temos propriedades de linearidade muito especiais que ajudam a controlar melhor o número de geradores e o posto.

Lema 3.4. *Sejam G um p-grupo de classe de nilpotência, no máximo, c e $x \in G$. Assuma que $|G : C_G(x)| = p^n$. Então, o posto de $\langle x^G \rangle$ é $\{n, c\}$-limitado.*

Demonstração: Faremos a prova por indução sobre n. Considere $n = 0$, assim temos que $|G : C_G(x)| = 1$, então $G = C_G(x)$ e, portanto, para todo $g \in G$, $x^g = x$. Assim, $\langle x^G \rangle = \langle x \rangle$ que tem posto 1 e o resultado vale trivialmente. Suponhamos, então, que $n > 0$ e que o resultado vale para qualquer grupo H que satisfaz as hipóteses do lema e para todo todo y em H tal que $|H : C_H(y)| = p^l$ com $l < n$.

Seja $M = \langle x^G \rangle$. Temos, pelo Lema 1.21, que M possui classe de nilpotência, no máximo, $c - 1$, assim, pelo Teorema 1.42, é suficiente mostrar que $d(M)$ é $\{n, c\}$-limitado. Pelo Teorema de Bases de Burnside, $d(M)$ coincide com o posto de $M/\Phi(M)$. Assim, passando ao quociente $G/\Phi(M)$, se necessário, podemos assumir, sem perda de generalidade, que M é abeliano elementar.

Tome N como sendo um subgrupo maximal de G contendo M. Observe que N existe, pois G é finito. Considere $L = \langle x^N \rangle$. Por hipótese de indução, temos que $rk(L) = d$ é $\{n, c\}$-limitado. Usaremos, agora, indução sobre d. Tome $a \in L \cap Z(N)$ e

$b \in G \setminus N$. Note que G é nilpotente, logo todo subgrupo maximal é normal e, portanto, $N \lhd G$. Além disso, $G = \langle N, b\rangle$, pois N é maximal e $b \notin N$.

Vamos provar agora que $K = \langle a^G\rangle$ é gerado por $\{a, [a,b], [a,b,b], ...\}$. Observe que dado $S = \{a, [a,b], [a,b,b], ...\}$ temos que $S \subseteq K$, logo $\langle S\rangle \leq K$. Assim, basta mostrar que qualquer elemento de a^G está em $\langle S\rangle$. Disso segue que $K \leq \langle S\rangle$ e, portanto, temos a igualdade. Como $N \lhd G$, dado $g \in G$, temos que $g = nb^i$ para algum $n \in N$ e algum $0 \leq i \leq o(b) - 1$. Temos que $a^{nb^0} = a^n = a$, pois $a \in Z(N)$. Note que, como a está em $Z(N)$, obtemos que

$$a^{nb^i} = (a^n)^{b^i} = a^{b^i},$$

para qualquer n em N e todo $0 \leq i \leq o(b) - 1$. Assim, usando as propriedades dos comutadores, temos que

$$a^{nb} = a^b = a[a,b] \in \langle S\rangle.$$

Suponha, por indução, que para todo $k < i$ temos que a^{nb^k} está em $\langle S\rangle$. Assim, existem $x_1, ..., x_t \in S \cup S^{-1}$, tais que $a^{nb^{i-1}} = a^{b^{i-1}} = x_1 \cdots x_t$ e disso segue que

$$a^{nb^i} = a^{b^i} = (a^{b^{i-1}})^b = (x_1 \cdots x_t)^b = x_1^b \cdots x_t^b.$$

Note que, para todo $1 \leq j \leq t$, temos que se x_j está em S, então, $x_j^b = x_j[x_j, b]$ que está em $\langle S\rangle$ e, se x_j está em S^{-1}, então, temos que $x_j^b = (l^b)^{-1} = (l[l,b])^{-1}$, para algum $l \in S$, que também está em $\langle S\rangle$. Portanto, $K \leq \langle S\rangle$, como queríamos.

Observe que o número de geradores de K é, no máximo, c, pois G tem classe de nilpotência, no máximo, c, então o posto de K é menor ou igual a c. Note que $K \lhd G$ e $K \neq 1$. Aplicando a hipótese indutiva em G/K obtemos que o posto de M/K é $\{n, c\}$-limitado. Portanto, como o posto de K é $\{c\}$-limitado, pelo Corolário 1.40, temos que o posto de M é $\{n, c\}$-limitado, como queríamos.

■

Lema 3.5. *Sejam p um número primo ímpar e G um p-grupo com uma involução ϕ tal que $G = [G, \phi]$. Considere M um subgrupo normal ϕ-invariante de G e assuma que $|C_M(\phi)| = p^n$, onde $n \in \mathbb{N}$. Então, $M \leq Z_{2n+1}(G)$.*

Demonstração: Faremos a prova por indução sobre n. Se $n = 0$, temos que $C_M(\phi) = 1$, assim, pelo Lema 3.2 (iii), $M \leq Z([G, \phi]) = Z(G) = Z_1(G)$. Suponhamos, então, que $n > 0$ e que o resultado é verdadeiro para qualquer grupo H que satisfaz as hipóteses do lema e para todo subgrupo K normal ϕ-invariante de H tal que $|C_K(\phi)| = p^l$ com $l < n$. Seja $N = M \cap Z_2(G)$.

Se $N \not\leq Z(G)$, então, pelo Lema 3.2 (iii), temos que $C_N(\phi) \neq 1$. Pelo Lema 3.2 (ii), temos que

$$|C_{M/N}(\phi)| = |C_M(\phi)N/N| = |C_M(\phi)|/|C_M(\phi) \cap N|,$$

mas, $1 \neq C_N(\phi) \leq C_M(\phi) \cap N$ e $|C_M(\phi)| = p^n$, logo $|C_{M/N}(\phi)| < p^n$. Note que $G/N = [G/N, \phi]$ é um p-grupo e M/N é subgrupo normal ϕ-invariante de G/N com $|C_{M/N}(\phi)| = p^k < p^n$, assim, por hipótese de indução, onde G e M são substituídos por G/N e M/N respectivamente, temos que

$$M/N \leq Z_{2k+1}(G/N) \leq Z_{2(n-1)+1}(G/N) \leq Z_{2n-1}(G/N).$$

Agora, pelo Teorema 1.15, temos que

$$Z_{2n-1}(G/N) = \{xN \in G/N \mid [xN, g_1N, ..., g_{2n-1}N] = 1, \ \forall \ g_1, ..., g_{2n-1} \in G\},$$

assim, $xN \in Z_{2n-1}(G/N)$ se, e somente se

$$[x, g_1, ..., g_{2n-1}] \in N = M \cap Z_2(G).$$

Mas, se $[x, g_1, ..., g_{2n-1}]$ está em $Z_2(G)$, então, pelo Teorema 1.15, temos que

$$[[x, g_1, ..., g_{2n-1}], g_{2n}, g_{2n+1}] = [x, g_1, ..., g_{2n+1}] = 1.$$

Note que, dado $m \in M$, temos que $mN \in M/N \leq Z_{2n-1}(G/N)$, então $[m, g_1, ..., g_{2n+1}] = 1$ para todo $g_1, ..., g_{2n+1} \in G$, logo $M \leq Z_{2n+1}(G)$.

Considere, agora, o caso $N \leq Z(G)$. Temos que $N = M \cap Z_2(G) \leq M \cap Z(G) \leq M \cap Z_2(G)$. Logo, $M \cap Z(G) = M \cap Z_2(G)$. Vamos provar por indução sobre i que $M \cap Z(G) = M \cap Z_i(G)$ para todo $i \geq 2$. Já temos que $M \cap Z(G) = M \cap Z_2(G)$. Suponha, então, que $i > 2$ e que para todo $k < i$ temos que $M \cap Z(G) = M \cap Z_k(G)$. Lembramos que

$$Z_i(G) = \{x \in G \mid [x, g] \in Z_{i-1}(G), \ \forall \ g \in G\}.$$

Por um lado é óbvio que $M \cap Z(G) \leq M \cap Z_i(G)$. Para provar que $M \cap Z_i(G) \leq M \cap Z(G) = M \cap Z_{i-1}(G)$ tome m em $M \cap Z_i(G)$. Temos que para todo $g \in G$, $[m, g] \in Z_{i-1}(G)$ e $[m, g] \in M$, pois M é normal em G, logo, o comutador $[m, g]$ está em $M \cap Z_{i-1}(G) = M \cap Z_{i-2}(G)$. Note que, como $[m, g]$ está em $Z_{i-2}(G)$ para todo g em G, então $m \in Z_{i-1}(G)$. Portanto,

$$M \cap Z(G) = M \cap Z_i(G),$$

para todo $i \geq 2$. Como G é nilpotente temos que $G = Z_s(G)$ para algum s, assim, em particular, segue que $M \cap Z(G) = M \cap G = M$, assim $M \leq Z(G) \leq Z_{2n+1}(G)$, como queríamos. Isso conclui a demonstração.

■

Lema 3.6. *Seja G um p-grupo, com p ímpar, admitindo uma involução ϕ tal que $|C_G(\phi)| = p^m$. Então G contém um subgrupo ϕ-invariante J com classe de nilpotência, no máximo, dois e índice, no máximo, $p^{f_1(m)}$, onde $f_1(m) = 1^2 + 2^2 + \cdots + m^2$.*

O Lema 3.6 será usado para demonstrar o resultado seguinte. Sua prova será omitida, mas pode ser vista em [Lemma 2.3, [8]].

Lema 3.7. *Sejam p um primo ímpar e G um p-grupo admitindo uma involução ϕ tal que $G = [G, \phi]$. Assuma que $C_G(\phi)$ é r-gerado. Então, existe um número m, r-limitado, tal que G' é m-gerado.*

Demonstração: Pelo Teorema de Bases de Burnside, o número minimal de geradores de G' é igual ao posto de $G'/\Phi(G')$, assim, passando ao quociente $G/\Phi(G')$, se necessário, podemos assumir, sem perda de generalidade, que G' é abeliano elementar. Vamos mostrar inicialmente que $C_G(\phi) \leq G'$. Considerando o quociente G/G' é suficiente mostrar que $C_{G/G'}(\phi) = 1$. De fato, como G' é um subgrupo característico de G, em particular é um subgrupo normal ϕ-invariante de G, pelo Lema 3.2 (ii), temos que

$$C_{G/G'}(\phi) = C_G(\phi)G'/G'.$$

Logo, se $C_{G/G'}(\phi)$ for 1 segue que $C_G(\phi) \leq G'$. Temos que G/G' é um p-grupo abeliano, com p ímpar, e possui um automorfismo ϕ de ordem 2, então, pelo Teorema 1.30, temos que

$$G/G' = [G/G', \phi] \times C_{G/G'}(\phi).$$

Mas, $G = [G, \phi]$, assim, $G/G' = [G/G', \phi]$ e, portanto, $C_{G/G'}(\phi) = 1$, como queríamos.

Como $C_G(\phi) \leq G'$ e estamos supondo que G' é abeliano elementar, temos que $C_G(\phi)$ é abeliano elementar, assim, sendo $C_G(\phi)$ r-gerado, segue que $|C_G(\phi)| = p^k$ para algum $k \leq r$.

Faremos indução sobre k. Se $k = 0$ temos que $|C_G(\phi)| = 1$, assim, G possui um automorfismo livre de pontos fixos de ordem 2, logo, pelo Teorema 1.28, temos que G é abeliano e disso segue que $G' = 1$ completando o resultado. Suponha, então, que $k > 0$ e que para qualquer grupo que satisfaz as condições do lema com $|C_G(\phi)| = p^l$, onde $l < k$, o resultado é verdadeiro. Considere $N = \langle x^G \rangle$, o fecho normal em G de algum elemento não trivial x em $C_G(\phi)$. Observe que $N \triangleleft G$ e, como x está em $C_G(\phi)$, $N \leq C_G(\phi)$, logo N é um subgrupo normal ϕ-invariante de G. Como $G = [G, \phi]$ segue que $G/N = [G/N, \phi]$. Além disso, pelo Lema 3.2 (ii), temos que

$$C_{G/N}(\phi) = C_G(\phi)N/N = C_G(\phi)/N,$$

assim,

$$|C_{G/N}(\phi)| = \tfrac{|C_G(\phi)|}{|N|}.$$

Note que, como x é um elemento não trivial de $C_G(\phi)$, então $|N| \neq 1$, assim, $|C_{G/N}(\phi)| < |C_G(\phi)|$. Considere, então, que $|C_{G/N}(\phi)| = p^s$, com $s < k$. Como G' é abeliano elementar, segue que $C_{G/N}(\phi)$ é s-gerado, assim, por hipótese de indução aplicada ao quociente G/N, temos que $(G/N)' = G'/N$ é m_1-gerado, onde m_1 é um número que depende somente de k. Em particular, temos que $|G'/N| \leq p^{m_1}$. Então, é suficiente mostrar que existem uma função $t(k)$ dependendo somente de k e um elemento $x \in C_G(\phi)$ tais que $\langle x^G \rangle$ tem posto, no máximo, $t(k)$. De fato, como G' é abeliano elementar, sendo G'/N m_1-gerado e N de posto, no máximo $t(k)$, segue que G' é m-gerado, onde m é uma função que depende apenas de k. O resultado segue lembrando que $k \leq r$.

Agora, pelo Lema 3.5, aplicado com $M = G$, como $|C_G(\phi)| = p^k$, temos que $G \leq Z_{2k+1}(G)$. Em outras palavras, temos que G tem classe de nilpotência, no máximo, $2k+1$. Pelo Lema 3.4, o posto de $\langle x^G \rangle$ é k-limitado sempre que $|G : C_G(x)| \leq p^f$ para algum número f k-limitado. Mostraremos a seguir que sempre existem um elemento x em $C_G(\phi)$ e um número f que satisfazem as condições acima.

Pelo Lema 3.6, G contém um subgrupo ϕ-invariante J com classe de nilpotência, no máximo, dois e índice, no máximo, p^{f_1} para algum número f_1 k-limitado. Seja $H = [J, \phi]$. Pelo Teorema 1.34, temos que $[J, \phi, \phi] = [J, \phi]$, logo $H = [H, \phi]$ e, por um argumento análogo ao feito anteriormente, $C_H(\phi) \leq H'$. Como J tem classe de nilpotência, no máximo, dois temos que H tem classe de nilpotência, no máximo, dois, logo

$$[C_H(\phi), H] \leq [H', H] = \gamma_3(H) = 1$$

e, portanto, $C_H(\phi)$ é central em H. Note que $H/C_H(\phi)$ possui uma involução ϕ agindo livre de pontos fixos, logo, pelo Teorema 1.28, temos que $H/C_H(\phi)$ é abeliano, assim, $H' \leq C_H(\phi)$ e disso segue que $H' = C_H(\phi)$. Logo, $H' \leq C_G(\phi)$. Note que, como $|C_G(\phi)| = p^k$, então $|C_G(\phi) : H'| \leq p^k$. Temos, também, que

$$\frac{|HC_G(\phi)|}{|H|} = \frac{|C_G(\phi)|}{|C_G(\phi) \cap H|} = \frac{|C_G(\phi)|}{|C_H(\phi)|} = \frac{|C_G(\phi)|}{|H'|} \leq p^k,$$

Mas, J é um subgrupo ϕ-invariante de G, assim ϕ é um automorfismo de J que age de forma coprima, logo, pelo Teorema 1.30, temos que

$$J = C_J(\phi)[J, \phi] = C_J(\phi)H,$$

assim, como $C_J(\phi) \leq C_G(\phi)$, temos que $H \leq J \leq HC_G(\phi)$, portanto, usando o fato de que $|HC_G(\phi) : H| \leq p^k$, temos que $|J : H| \leq p^k$, logo

$$|G : H| = |G : J||J : H| \leq p^{f_1}p^k = p^{f_1+k}$$

e disso segue que o índice de H em G é, no máximo, p^{f_2}, onde $f_2 = k + f_1$.

Se $H' \neq 1$, podemos escolher $1 \neq x \in H'$. Note que, como $C_H(\phi) = H' \leq Z(H)$, temos que $H \leq C_G(x)$, assim, como o índice de H em G é, no máximo, p^{f_2}, segue que o índice $|G : C_G(x)| \leq p^{f_2}$, o que completa a prova no caso em que H é não abeliano.

Agora, suponha que $H' = 1$, ou seja, que H é abeliano. Como $H' = C_H(\phi)$, temos que ϕ é uma involução livre de pontos fixos em H, logo, pelo Teorema 1.28, temos que $h^\phi = h^{-1}$ para todo h em H.

Se H é normal em G, pelo Lema 3.2 (iii), $H \leq Z([G,\phi]) = Z(G)$, logo $H \leq C_G(x)$ para todo x em G e, assim, $|G : C_G(x)| \leq p^{f_2}$ para todo x em G.

Considere, então, o caso em que H não é normal em G. Temos que $G = [G,\phi]$ e, pelo Lema 3.2 (i), $\langle I \rangle = [G,\phi]$, onde $I = \{x \in G \mid x^\phi = x^{-1}\}$. Assim, existe um elemento y em G tal que y não normaliza H e $y^\phi = y^{-1}$. Escolha h em H tal que $h^y \notin H$. Pelo Lema 3.2, como $G = IC_G(\phi)$, podemos escrever $h^y = ab$, onde $a^\phi = a^{-1}$ e $b \in C_G(\phi)$. Se $b = 1$, teríamos que $h^y = a$ e aplicando ϕ em ambos os lados obteríamos que

$$(h^y)^\phi = yh^{-1}y^{-1} = y^{-1}h^{-1}y = a^\phi,$$

e disso seguiria que h e y comutam, o que seria uma contradição, assim podemos assumir que $b \neq 1$. Considere $K = H^y$ e $L = K^\phi \cap K$. Note que K é abeliano, pois H é abeliano, logo ab centraliza L. Dado x em L temos que x está em K^ϕ, logo $x = k^\phi$, para algum k em K, assim, como ϕ tem ordem 2, obtemos que $x^\phi = (k^\phi)^\phi = k$ que está em K. Por outro lado, x está K, logo x^ϕ está em K^ϕ e, portanto, temos que $x^\phi \in L$, logo L é ϕ-invariante. Assim, como ab está em $C_G(L)$, segue que $(ab)^\phi = a^{-1}b$ pertence à $C_G(L)$, pois para todo $x \in L$ temos que

$$[x^\phi, (ab)^\phi] = [x, ab]^\phi = 1^\phi = 1.$$

Logo $(a^{-1}b)(ab)^{-1} \in C_G(L)$ e, portanto, $(a^{-1})^2$ está em $C_G(L)$. Como G tem ordem ímpar, obtemos que a está em $C_G(L)$ e, consequentemente, temos que b pertence à $C_G(L)$. Logo, $L \leq C_G(b)$ e, com isso, temos que $|G : C_G(b)| \leq |G : L|$. Agora, note que $|G : L| \leq |G : K||G : K^\phi| \leq p^{2f_2}$, logo

$$|G : C_G(b)| \leq p^{2f_2},$$

obtendo o elemento $x = b$ e a função desejados para este caso. Com isso, concluímos a prova do lema.

■

Note que, pelo Lema 3.7, temos que para um p-grupo G, dentro das hipóteses do enunciado, podemos limitar o número de geradores do subgrupo derivado de G a partir do número de geradores do subgrupo de pontos fixos de ϕ em G.

O próximo resultado será a ferramenta chave para a prova do teorema principal deste capítulo, Teorema 3.10, que consiste em limitar o posto do subgrupo derivado de um grupo $G = [G,\phi]$, onde ϕ é uma involução de G, a partir do posto do subgrupo de pontos fixos de ϕ em G.

Lema 3.8. *Sejam p um primo ímpar e G um p-grupo admitindo uma involução ϕ tal que $G = [G, \phi]$ e $C_G(\phi)$ tem posto r. Considere $s(r) = s$ dado como no Lema 3.3. Então, $\gamma_{2s+1}(G)$ é powerful.*

Demonstração: Seja $N = \gamma_{2s+1}(G)$. Temos que mostrar que N/N^p é abeliano, ou seja, que $N' \leq N^p$. Sem perda de generalidade, podemos passar ao quociente N/N^p e, assim, assumir que N tem expoente p. Logo, vamos provar que N é abeliano. Note que $C_N(\phi) \leq N$ tem expoente p, além disso, $C_G(\phi)$ tem posto r, logo, como $C_N(\phi) \leq C_G(\phi)$, temos que $rk(C_N(\phi)) \leq rk(C_G(\phi)) = r$. Assim, pelo Lema 3.3, temos que $|C_N(\phi)| \leq p^s$. Observe que, como N é característico em G, N é um subgrupo normal ϕ-invariante de G. Como $|C_N(\phi)| \leq p^s$, pelo Lema 3.5, temos que $N \leq Z_{2s+1}(G)$. Agora, dados $n_1, n_2 \in N$, temos que $N = \gamma_{2s+1}(G)$ e $N \leq Z_{2s+1}(G)$, assim pelo Corolário 1.18, temos que $[n_1, n_2] \in [\gamma_{2s+1}(G), Z_{2s+1}(G)] = 1$ e, portanto, $N' = 1$. Logo N é abeliano, como queríamos e o resultado segue.

■

O resultado a seguir, nas hipóteses do lema anterior, nos fornece informações sobre o número de geradores dos termos $\gamma_i(G)$ da série central descendente de G quando $i \geq 2$.

Lema 3.9. *Sejam p um primo ímpar e G um p-grupo admitindo uma involução ϕ tal que $G = [G, \phi]$ e $C_G(\phi)$ tem posto r. Então, para qualquer inteiro $i \geq 2$, existe um número m_i dependendo somente de i e r tal que $\gamma_i(G)$ é m_i-gerado.*

Demonstração: Sejam $i \geq 2$ e $N = \gamma_i(G)$. Pelo Teorema de Base de Burnside, o número minimal de geradores de N coincide com o posto de $N/\Phi(N)$, assim, passando ao quociente $G/\Phi(N)$, se necessário, podemos supor, sem perda de generalidade, que N é abeliano elementar. Em particular, $C_N(\phi)$ é abeliano elementar e, como o posto de $C_G(\phi)$ é igual a r, temos que $|C_N(\phi)| \leq p^r$. Assim, pelo Lema 3.5, temos que $N \leq Z_{2r+1}(G)$. Note que dados $y_1, ..., y_{2r+i}$ elementos de G, temos que $[y_1, ..., y_i] \in \gamma_i(G) = N \leq Z_{2r+1}(G)$, logo, pelas propriedades de $Z_{2r+1}(G)$, segue que

$$[[y_1, ..., y_i], y_{i+1}, ..., y_{i+2r}] = [y_1, ..., y_{i+2r}] = 1.$$

Portanto, $\gamma_{2r+i+1}(G) = 1$ e, assim, G tem classe de nilpotência, no máximo, $2r + i$.

Agora, pelo Lema 3.7, temos que o número minimal de geradores de G' é r-limitado. Além disso, G' tem classe de nilpotência $\{i, r\}$-limitada, assim, pelo Teorema 1.42, o posto de G' é $\{i, r\}$-limitado. Mas, $N = \gamma_i(G) \leq \gamma_2(G) = G'$ e, assim, pela definição de posto de G' temos que N é m_i-gerado para algum número m_i limitado em termos de i e de r.

■

O teorema a seguir tem como objetivo limitar o posto do subgrupo derivado de um p-grupo G, admitindo uma involução ϕ tal que $G = [G, \phi]$, a partir do posto do subgrupo de pontos fixos de ϕ em G. Para demonstrar esse resultado iremos usar um subgrupo powerful, N, que é um dos termos da série central descendente de G dado no Lema 3.8. Estimamos o posto de G' a partir do posto de N e do posto de G'/N. Para limitar o posto de N, aplicaremos primeiro o Lema 3.9 que nos fornece um limite para o número minimal de geradores de N e, em seguida, usaremos o fato de que, como N é powerful, $d(N) = rk(N)$.

Teorema 3.10. *Seja G um p-grupo finito admitindo uma involução ϕ tal que $G = [G, \phi]$ e $rk(C_G(\phi)) \leq r$. Então, o posto de G' é r-limitado.*

Demonstração: Como $G = [G, \phi] = \langle x^{-1}x^{\phi} | x \in G \rangle$ e ϕ tem ordem 2, então p é ímpar. Sejam $s = s(r)$ dado no Lema 3.3 e $N = \gamma_{2s+1}(G)$. Considere d o número minimal de geradores de N. Pelo Lema 3.9, temos que d é r-limitado. Além disso, pelo Lema 3.8, N é powerful, logo, aplicando o Teorema 2.11, temos que $rk(N) = d$. Mas, pelo Lema 3.7, temos que G' é m-gerado, onde m é r-limitado. Observe que para todo $i \geq 1$ temos que

$$\gamma_i(G'/N) = \gamma_i(G')N/N,$$

assim, $\gamma_{2s+1}(G'/N) = \gamma_{2s+1}(G')N/N$, mas $\gamma_{2s+1}(G') \leq \gamma_{2s+1}(G) = N$, logo, obtemos que $\gamma_{2s+1}(G'/N) = 1$ e, como $s = s(r)$, temos que a classe de nilpotência de G'/N também é r-limitada. Agora, como G'/N é nilpotente com número minimal de geradores e classe de nilpotência r-limitados, pelo Teorema 1.42, temos que o posto de G'/N é r-limitado.

Pelo Corolário 1.40, sabemos que

$$rk(G') \leq rk(G'/N) + rk(N).$$

Portanto, como $rk(G'/N)$ e $rk(N)$ são r-limitados, concluímos que $rk(G')$ é r-limitado.

■

Capítulo 4

Grupos de Ordem Ímpar admitindo uma Involução

Neste capítulo iremos considerar p um primo ímpar fixado. Dado um grupo finito solúvel G, denotaremos por $r_p(G)$ e $l_p(G)$ o posto de um p-subgrupo de Sylow e o p-comprimento de G, respectivamente. Lembramos que o p-comprimento $l_p(G)$ é definido como o número de p-fatores da p-série descendente de G

$$1 \leq O_{p'}(G) \leq O_{p',p}(G) \leq O_{p',p,p'}(G) \leq \cdots.$$

Nosso objetivo principal aqui é provar uma generalização para a Teorema 3.10 do capítulo anterior, que diz que dado um grupo G de ordem ímpar admitindo uma involução ϕ tal que $G = [G, \phi]$ e $r_p(C_G(\phi)) \leq r$, então temos que $r_p(G')$ é r-limitado. Veremos, também, que em muitos dos resultados do capítulo anterior a hipótese de G ser um p-grupo finito não é essencial.

Os teoremas a seguir não serão demonstrados, mas suas provas podem ser vistas em [Theorem 3.2, [6]] e em [Theorem 3.23, [22]].

Teorema 4.1. *Se um p-grupo abeliano elementar H é visto como um espaço vetorial sobre $\mathbb{F}_p$, então $AutH$ é isomorfo ao grupo de transformações lineares não singulares de H.*

Teorema 4.2. *(Zassenhaus) Seja G um grupo linear de grau n sobre um corpo arbitrário. Se G é solúvel, então o comprimento derivado de G é n-limitado.*

O resultado a seguir relaciona $l_p(G)$ e $r_p(G)$ quando G é um grupo finito solúvel, mostrando que $l_p(G)$ é limitado em função de $r_p(G)$.

Lema 4.3. *Se G é um grupo finito solúvel, então $l_p(G)$ é $r_p(G)$-limitado.*

Demonstração: Observe que $O_{p'}(G)$ é o maior p'-subgrupo normal de G e $l_p(G)$ é definido como sendo o número de p-fatores da p-série descendente, assim temos que

$l_p(G) = l_p(G/O_{p'}(G))$ e, portanto, podemos assumir, sem perda de generalidade, que $O_{p'}(G) = 1$. Sejam $M = O_p(G)/\Phi(O_p(G))$ e $A = G/\Phi(O_p(G))$. Temos que M é normal em A, assim A/M age sobre M, pois basta considerar a ação dada por $(aM, x) \mapsto x^{(aM)} := x^a$, onde (aM, x) está em $A/M \times M$. Note que, como $\Phi(O_p(G)) \leq F(O_p(G))$ e estamos supondo que $O_{p'}(G) = 1$, temos que

$$F(A) = F(G/\Phi(O_p(G))) = F(G)/\Phi(O_p(G)) = O_p(G)/\Phi(O_p(G)) = M.$$

Além disso, como G é solúvel, temos $C_A(F(A)) \leq F(A)$ e disso segue que $C_A(M) \leq M$, logo, A/M age fielmente sobre M. Agora, $G/O_p(G) \cong A/M$, assim, concluímos que $G/O_p(G)$ age fielmente sobre M. Logo, temos que $G/O_p(G)$ é isomorfo a um subgrupo de $AutM$.

Pelo Teorema 4.1, como M é um p-grupo abeliano elementar que pode ser visto como um espaço vetorial sobre $\mathbb{F}_p$, temos que $AutM$ é isomorfo ao grupo de transformações lineares não singulares de M. Assim, pelo Teorema 4.2 de Zassenhaus, temos que o comprimento derivado de $G/O_p(G)$ é limitado em termos de $\dim M$, que é, no máximo, $r_p(G)$, o que conclui a prova do lema.

■

O lema seguinte é uma extensão do Lema 3.5 visto no capítulo anterior.

Lema 4.4. *Seja G um grupo de ordem ímpar admitindo uma involução ϕ tal que $G = [G, \phi]$. Considere M um p-subgrupo normal ϕ-invariante de G tal que $|C_M(\phi)| \leq p^n$. Então $M \leq Z_{2n+1}(O_p(G))$.*

Demonstração: A prova é praticamente idêntica à prova do Lema 3.5. Lembramos que

$$O_p(G) = \langle K \leq G \mid K \text{ é um } p\text{-subgrupo normal de } G \rangle,$$

então $M \leq O_p(G)$. Assim, é natural esperar que o papel que G desempenhava na demonstração do Lema 3.5 seja desempenhado aqui por $O_p(G)$. Faremos a prova por indução sobre n. Se $n = 0$, temos que $|C_M(\phi)| = 1$, logo, pelo Lema 3.2 (iii), temos que $M \leq Z([G, \phi]) = Z(G) \leq Z(O_p(G)) = Z_1(O_p(G))$. Suponha, então, que $n \geq 1$ e que o resultado é válido para todo grupo H de ordem ímpar que admite uma involução ψ tal que $H = [H, \psi]$ e todo p-subgrupo normal ψ-invariante L de H com $|C_L(\psi)| = p^k$, onde $k < n$. Seja $N = M \cap Z_2(O_p(G))$.

Se $N \not\leq Z(O_p(G))$, então $N \not\leq Z(G)$ e temos, pelo Lema 3.2 (iii), que $C_N(\phi) \neq 1$, assim, pelo Teorema 1.24, $|C_{M/N}(\phi)| < |C_M(\phi)|$. Logo, por hipótese de indução, temos que

$$M/N \leq Z_{2n-1}(O_p(G/N)),$$

pois M/N é um p-subgrupo normal ϕ-invariante de G/N tal que $|C_{M/N}(\phi)| < p^n$.

Pelo Lema 1.4, como N é um p-subgrupo normal de G, temos que $O_p(G/N) = O_p(G)/N$. Além disso,

$$Z_{2n-1}(O_p(G)/N) = \{xN \in O_p(G)/N | [xN, g_1N, ..., g_{2n-1}N] = 1 \forall g_1, ..., g_{2n-1} \in O_p(G)\},$$

logo

$$Z_{2n-1}(O_p(G)/N) = \{xN \in O_p(G)/N \mid [x, g_1, ..., g_{2n-1}] \in N \ \forall \ g_1, ..., g_{2n-1} \in O_p(G)\},$$

assim, se $xN \in Z_{2n-1}(O_p(G))$, temos que $[x, g_1, ..., g_{2n-1}]$ está em $Z_2(O_p(G))$ para todos $g_1, ..., g_{2n-1}$ em $O_p(G)$. Disso segue que

$$[x, g_1, ..., g_{2n+1}] = 1 \ \forall \ g_1, ..., g_{2n+1} \in O_p(G),$$

portanto, $x \in Z_{2n+1}(O_p(G))$. Assim, dado $m \in M$, como $M/N \leq Z_{2n-1}(O_p(G/N))$, temos que $m \in Z_{2n+1}(O_p(G))$, logo $M \leq Z_{2n+1}(O_p(G))$, como queríamos.

Se $N \leq Z(O_p(G))$, temos que

$$N = M \cap Z_2(O_p(G)) \leq M \cap Z(O_p(G)) \leq M \cap Z_2(O_p(G)),$$

logo

$$M \cap Z_2(O_p(G)) = M \cap Z(O_p(G))$$

e disso segue que

$$M \cap Z(O_p(G)) = M \cap Z_i(O_p(G)) \ \forall \ i \in \mathbb{N}.$$

Portanto, $M \cap Z(O_p(G)) = M \cap O_p(G) = M$ e, assim, $M \leq Z(O_p(G)) \leq Z_{2n+1}(O_p(G))$, o que completa a prova.

■

O teorema a seguir é o principal resultado deste capítulo que fornece uma generalização do Teorema 3.10 visto no capítulo anterior.

Teorema 4.5. *Seja G um grupo de ordem ímpar admitindo uma involução ϕ tal que $G = [G, \phi]$ e $r_p(C_G(\phi)) \leq r$. Então $r_p(G')$ é r-limitado.*

Demonstração: Seja $l = l_p(G)$ o p-comprimento de G. Por um resultado de Thompson [26], l é limitado em termos de $l_p(C_G(\phi))$ e, pelo Lema 4.3, $l_p(C_G(\phi))$ é limitado em termos de $r_p(C_G(\phi))$, logo $l_p(C_G(\phi))$ é r-limitado. Assim, temos que l é r-limitado. Usaremos indução sobre l para mostrar que $r_p(G')$ é $\{l, r\}$-limitado.

Se $l = 1$, então, temos que

$$1 \leq O_{p'}(G) \leq O_{p',p}(G) = G$$

Agora, $O_{p',p}(G)$ é o único subgrupo normal de G tal que $O_p(G/O_{p'}(G)) = O_{p',p}(G)/O_{p'}(G)$ que é um p-grupo, logo $G/O_{p'}(G)$ é um p-grupo. Como $G = [G, \phi]$ e $O_{p'}(G)$ é ϕ-invariante, temos que $G/O_{p'}(G) = [G/O_{p'}(G), \phi]$. Além disso, pelo Lema 3.2 (ii),

$$C_{G/O_{p'}(G)}(\phi) = C_G(\phi)O_{p'}(G)/O_{p'}(G),$$

assim, obtemos que o posto de $C_{G/O_{p'}(G)}(\phi)$ é, no máximo, $r_p(C_G(\phi)) \leq r$. Do Teorema 3.10 segue que o posto de $(G/O_{p'}(G))'$ é r-limitado. Lembrando, por fim, que $G/O_{p'}(G) = O_p(G/O_{p'}(G))$, obtemos que $r_p(G')$ é r-limitado.

Suponha, então, que $l \geq 2$ e que o resultado é verdadeiro para todo grupo H de ordem ímpar satisfazendo as hipóteses com p-comprimento menor que l. Note que, podemos assumir que $O_{p'}(G) = 1$, pois, $l_p(G) = l_p(G/O_{p'}(G))$. Sejam $T = O_p(G)$ e $P = T \cap G'$.

Notemos que o grupo quociente G/P é tal que $l_p(G/P) = l - 1$, assim, por hipótese indutiva sobre l, sabemos que $r_p((G/P)')$ é $\{l, r\}$-limitado, ou seja, $r_p(G'/P)$ é $\{l, r\}$-limitado. O nosso objetivo é provar que $r_p(G')$ é $\{l, r\}$-limitado, mas como temos que, pelo Corolário 1.40

$$r_p(G') \leq rk(P) + r_p(G'/P),$$

é suficiente mostrar que

$$\textit{o posto de } P \textit{ é } \{l, r\}\textit{-limitado.} \quad (**)$$

A seguir vamos desenvolver o argumento teórico para mostrar que a afirmação $(**)$ é verdadeira e, para isso, vamos considerar a seguinte hipótese que resume as condições com as quais iremos trabalhar daqui para frente.

Hipótese 4.6. *Seja G um grupo de ordem ímpar admitindo uma involução ϕ tal que $G = [G, \phi]$ e $r_p(C_G(\phi)) \leq r$. Assuma que $l_p(G) = l \geq 2$, $O_{p'}(G) = 1$ e que para todo grupo H que satisfaz as condições acima com p-comprimento, no máximo, $l - 1$ temos que $r_p(H')$ é r-limitado. Denote por $T = O_p(G)$ e $P = T \cap G'$.*

Lema 4.7. *Assuma a Hipótese 4.6 e suponha que P é abeliano elementar. Então, temos que $|P| \leq p^m$, para algum número m r-limitado.*

Demonstração: Sejam $Q = O_{p,p'}(G)$ e S um p'-subgrupo de Hall ϕ-invariante de Q. Considere, também, $R = [P, S]$. Note que $[T, G]$ está contido em $P = T \cap G'$, pois T é normal em G. Assim, temos que $[S, G, P]$ está em $[S, G, T] \leq [S, P] = R$ e $[G, P, S]$ está contido em $[G, T, S] \leq [P, S] = R$. Logo, pelas propriedades dos comutadores, temos que $[P, S, G] = [R, G]$ está em R e disso segue que R é normal em G.

Note que, como P é um p-grupo e S é um p'-grupo, pelo Teorema 1.34, temos que $R = [P, S] = [R, S]$, logo G/R possui um p'-subgrupo de Hall normal que é a imagem

de S em G/R. Portanto, o quociente G/R tem p-comprimento, no máximo, $l-1$, logo, por hipótese, temos que $r_p(G'/R)$ é r-limitado. Observe que P é um p-subgrupo de G', logo está contido em um p-subgrupo de Sylow de G', assim, $rk(P) \leq r_p(G')$. Agora, pelo Corolário 1.40, para provar que $r_p(G')$ é r-limitado, precisamos mostrar apenas que o posto de R é r-limitado. Por outro lado, se provarmos que o posto de P é r-limitado, como P é abeliano elementar, teremos o resultado. Assim, resta mostrar que o posto de R é r-limitado.

Temos que $C_R(\phi) \leq R$ que está em P que é abeliano elementar, então, se o posto de $C_R(\phi)$ é k, obtemos que $|C_R(\phi)| = p^k$, para algum k que é r-limitado, já que $r_p(C_G(\phi)) \leq r$. Faremos indução sobre k para mostrar que o posto de R é r-limitado. Se $k = 0$, temos que $C_R(\phi) = 1$, logo, pelo Lema 3.2 (iii), obtemos que $R \leq Z(G)$ e disso segue que $R = [P, S] = [R, S] \leq [R, G] = 1$. Portanto, $R = 1$ e o resultado segue. Suponha, então que $k > 0$ e que para qualquer H dentro das hipóteses dadas tal que $|C_H(\phi)| = p^l$, com $l < k$, temos que o posto de H é r-limitado. Como $k > 0$, existe um elemento não trivial x em $C_R(\phi)$. Considere $N = \langle x^G \rangle$. Temos que N é normal em R e x está em $C_R(\phi)$, logo N está em $C_R(\phi)$, assim, N é um subgrupo normal ϕ-invariante de R. Pelo Lema 3.2 (ii), temos que

$$C_{R/N}(\phi) = C_R(\phi)N/N = C_R(\phi)/N,$$

mas x é um elemento não trivial de $C_R(\phi)$, logo $|N| \neq 1$. Assim, $|C_{R/N}(\phi)| \leq |C_R(\phi)|$ e, por hipótese de indução, temos que o posto de R/N é r-limitado. Portanto, basta mostrar que existe um elemento não trivial x em $C_R(\phi)$ tal que o posto de $\langle x^G \rangle$ é r-limitado.

Tome M um subgrupo normal ϕ-invariante minimal de G contido em R e considere $H = G/C_G(M)$. Note que, por construção, H age fielmente sobre M. Se $C_M(\phi) = 1$, pelo Lema 3.2 (iii), temos que $M \leq Z(G)$. Por outro lado, temos que $R = [P, S] = [R, S]$ e disso segue que $C_R(S) = 1$, o que é uma contradição, pois $M \leq C_R(S)$ e M é não trivial. Assim, obtemos que necessariamente $C_M(\phi) \neq 1$.

Observe que podemos ver M como um $H\langle\phi\rangle$-módulo sobre um corpo com p elementos. Logo, pelo Teorema B de Hartley-Isaacs [7], temos que $\dim M$ é limitada em termos da dimensão de $C_M(\phi)$. Disso segue que $|M| \leq p^d$ para algum número d r-limitado e, como M está contido em R, o resultado segue tomando qualquer elemento não trivial de $C_M(\phi)$.

■

Lema 4.8. *Assuma a Hipótese 4.6 e seja m o número dado pelo Lema 4.7. Então P é m-gerado.*

Demonstração: Vamos mostrar, inicialmente, que $O_{p'}(G/\Phi(P)) = O_{p'}(G)\Phi(P)/\Phi(P)$. Considere $\beta : G \to G/\Phi(P)$ o homomorfismo canônico. Note que $\beta(O_{p'}(G)) =$

$O_{p'}(G)\Phi(P)/\Phi(P)$. Como $O_{p'}(G)$ é um p'-subgrupo normal de G, pelo Teorema da Correspondência, temos que $O_{p'}(G)\Phi(P)/\Phi(P)$ é um p'-subgrupo normal de $G/\Phi(P)$, logo, como $O_{p'}(G/\Phi(P))$ é o maior p'-subgrupo normal de $G/\Phi(p)$ e qualquer p'-subgrupo subnormal de $G/\Phi(P)$ está em $O_{p'}(G/\Phi(P))$, temos que

$$O_{p'}(G)\Phi(P)/\Phi(P) \leq O_{p'}(G/\Phi(P)).$$

Agora, $O_{p'}(G/\Phi(P)) = H/\Phi(P)$ para algum $H \triangleleft G$ tal que $\Phi(P) \leq H$. Observe que $|\Phi(P)|$ é um p-número, pois $\Phi(P)$ está em P que é um p-grupo, e $|H : \Phi(P)|$ é um p'-número já que $O_{p'}(G/\Phi(P)) = H/\Phi(P)$. Assim, $\Phi(P) \triangleleft H$ e $(|\Phi(P)|, |H : \Phi(P)|) = 1$, logo, pelo Teorema 1.35 de Schur-Zassenhaus, existe um subgrupo K de H tal que K é um complemento de $\Phi(P)$ em H, ou seja, $H = K\Phi(P)$ e $K \cap \Phi(P) = 1$. Como K é um complemento de $\Phi(P)$ em H, temos que $|K| = |H : \Phi(P)|$ que é um p'-número, logo K é um p'-subgrupo de G e disso segue que $K \leq O_{p'}(G)$, assim, temos que $H = K\Phi(P) \leq O_{p'}(G)\Phi(P)$ e, portanto,

$$O_{p'}(G/\Phi(P)) = H/\Phi(P) \leq O_{p'}(G)\Phi(P)/\Phi(P).$$

Logo, $O_{p'}(G/\Phi(P)) = O_{p'}(G)\Phi(P)/\Phi(P)$.

Com isso, temos que

$$O_{p'}(G/\Phi(P)) = O_{p'}(G)\Phi(P)/\Phi(P) = 1,$$

pois, pela Hipótese 4.6, temos que $O_{p'}(G) = 1$. Lembramos que, pelo Teorema de Bases de Burnside, temos que $P/\Phi(P)$ é m-gerado se, e somente se, P é m-gerado. Assim, sem perda de generalidade, podemos passar ao quociente $G/\Phi(P)$ e supor que P é abeliano elementar. Do Lema 4.7, obtemos que $|P| \leq p^m$, para algum m r-limitado e, portanto, P é m-gerado, como queríamos.

■

Lema 4.9. *Seja $i \geq 2$ e assuma a Hipótese 4.6. Então existe um número m_i que é $\{i, r\}$-limitado tal que $\gamma_i(T)$ é m_i-gerado.*

Demonstração: Seja $N = \gamma_i(T)$. Pelo Teorema de Bases de Burnside, passando ao quociente $G/\Phi(N)$, se necessário, podemos assumir, sem perda de generalidade, que N é abeliano elementar. Temos que $T = O_p(G)$ é um p-subgrupo de G e $C_N(\phi) \leq N \leq T$. Por outro lado, $C_N(\phi)$ está contido em $C_G(\phi)$, logo $C_N(\phi)$ está contido em algum p-subgrupo de Sylow de $C_G(\phi)$. Como $r_p(C_G(\phi)) \leq r$ e N é abeliano elementar, temos que $|C_N(\phi)| \leq p^r$, assim, lembrando que N é caracteríatico, logo é ϕ-invariante, pelo Lema 4.4, segue que

$$\gamma_i(T) = N \leq Z_{2r+1}(T).$$

Logo, temos que $P = T \cap G' \leq T$ tem classe de nilpotência $\{i, r\}$-limitada. Agora, pelo Lema 4.8, temos que o número minimal de geradores de P é r-limitado, assim, pelo Teorema 1.42, o posto de P também é $\{i, r\}$-limitado. Note que $N \leq G'$, sendo $i \geq 2$, logo $N \leq P$ e, portanto, N é m_i-gerado, para algum número m_i $\{i, r\}$-limitado, como queríamos.

■

Lema 4.10. *Assuma a Hipótese 4.6 e seja $s = s(r)$ dado pelo Lema 3.3. Então, $\gamma_{2s+1}(T)$ é powerful.*

Demonstração: Seja $N = \gamma_{2s+1}(T)$. Temos que mostrar que $N' \leq N^p$. Para isso, vamos assumir que N tem expoente p e provar que N é abeliano, que é o mesmo de considerar o quociente N/N^p e ver que N/N^p é abeliano, logo $N' \leq N^p$. Temos que N está em T que é um p-subgrupo de G e $C_N(\phi)$ está em N. Por outro lado, $C_N(\phi)$ está em $C_G(\phi)$, assim, temos que $C_N(\phi)$ está contido em algum p-subgrupo de Sylow de $C_G(\phi)$, logo, temos que

$$rk(C_N(\phi)) \leq r_p(C_G(\phi)) \leq r.$$

Assim, pelo Lema 3.3, como $C_N(\phi)$ tem expoente p, temos que $|C_N(\phi)| \leq p^s$, onde s é um número que depende de r. Note que N é um p-subgrupo ϕ-invariante de G, logo, pelo Lema 4.4, temos que

$$N \leq Z_{2s+1}(T).$$

Portanto, pelo Corolário 1.18, temos que

$$N' = [N, N] \leq [\gamma_{2s+1}(T), Z_{2s+1}(T)] = 1,$$

logo, N é abeliano, como queríamos.

■

Lema 4.11. *Assuma a Hipótese 4.6. Então o posto de P é r-limitado.*

Demonstração: Seja $N = \gamma_{2s+1}(T)$ como na demonstração do Lema 4.10. Pelo Lema 4.9, temos que o número minimal de geradores de N é $\{s, r\}$-limitado e, como $s = s(r)$, temos que o número minimal de geradores de N é r-limitado. Como N é powerful, pelo Teorema 2.11, temos que o posto de N também é r-limitado. Observe que, pelo Lema 4.8, o número minimal de geradores de P/N é r-limitado. Além disso, temos que, para todo $j \geq 1$, $\gamma_j(P/N) = \gamma_j(P)N/N$ e, como P está em T, $\gamma_j(P) \leq \gamma_j(T)$. Logo, em particular, temos que

$$\gamma_{2s+1}(P/N) = \gamma_{2s+1}(P)\gamma_{2s+1}(T)/\gamma_{2s+1}(T) = 1,$$

pois $\gamma_{2s+1}(P) \leq \gamma_{2s+1}(T)$ e, assim, vemos que a classe de nilpotência de P/N também é r-limitada, logo, pelo Teorema 1.42, o posto de P/N é r-limitado. Agora,

$$rk(P) \leq rk(P/N) + rk(N),$$

portanto, o posto de P é r-limitado, como queríamos.

■

Com isso mostramos que a afirmação $(**)$ considerada na página 52 é verdadeira, ou seja, P possui posto $\{l, r\}$-limitado e concluímos a prova do Teorema 4.5.

Capítulo 5

Resultados Principais

Seja G um grupo admitindo um automorfismo ϕ de ordem prima p. Existem vários resultados que mostram como a estrutura de $C_G(\phi)$ exerce um forte impacto na estrutura de G. Um exemplo disso são os resultados de Higman [10] e Thompson [25], que, juntos, nos fornecem que se $C_G(\phi) = 1$, então G é nilpotente com classe de nilpotência p-limitada.

Os trabalhos de Khukhro [13], Fong [4] e Hartley and Meixner [9] mostraram que se a ordem de $C_G(\phi)$ é pequena, digamos $|C_G(\phi)| \leq m$, então G possui um subgrupo normal nilpotente N tal que o índice $|G : N|$ é $\{m, p\}$-limitado e a classe de nilpotência de N é p-limitada. Assim, é natural considerar que tipo de relação existe entre o posto de $C_G(\phi)$ e a estrutura de G. Por exemplo, em vista do resultado de Khukhro [13] para grupos nilpotentes, uma questão que surge é determinar se, dado um grupo finito nilpotente G admitindo um automorfismo ϕ de ordem prima p tal que $C_G(\phi)$ tem posto r, G sempre possui um subgrupo normal N ϕ-invariante tal que o posto de G/N é $\{p, r\}$-limitado e N possui classe de nilpotência p-limitada. Um dos resultados principais deste capítulo traz uma resposta afirmativa para essa questão quando ϕ tem ordem 2.

Estudamos, anteriormente, o impacto que o posto de $C_G(\phi)$ exerce sobre o grupo G, quando ϕ é uma involução. No Teorema 3.10 vimos que se G é um p-grupo admitindo uma involução ϕ tal que $G = [G, \phi]$ e $rk(C_G(\phi)) \leq r$, então o posto de G' é r-limitado. Usando este resultado, na primeira seção do capítulo mostraremos que em um grupo finito nilpotente G admitindo uma involução ϕ tal que $C_G(\phi)$ tem posto r, sempre existe um subgrupo normal ϕ-invariante N com classe de nilpotência, no máximo, 2 e tal que G/N tem posto r-limitado.

Outro resultado que mostra o impacto de $C_G(\phi)$ sobre a estrutura de G foi considerado no Teorema 4.5, onde vimos que se G é um grupo finito de ordem ímpar admitindo uma involução ϕ tal que $G = [G, \phi]$ e $r_p(C_G(\phi)) \leq r$, então $r_p(G')$ é r-limitado. Agora, na segunda seção do capítulo, usando o Teorema 4.5, veremos que até quando G não

é nilpotente, o posto de $C_G(\phi)$ pode ter um impacto forte sobre a estrutura de G. Mais em concreto, será provado que se G é um grupo de ordem ímpar admitindo uma involução ϕ tal que o posto de $C_G(\phi)$ é r-limitado, então o posto de $[G,\phi]'$ é r-limitado. Em seguida veremos quais são as consequências disso sobre a estrutura do posto de G.

Além disso, veremos como consequência que é até possível deduzir informações sobre o comprimento derivado de G a partir do posto de $C_G(\phi)$ impondo algumas condições adicionais às anteriores sobre o grupo G.

5.1 Sobre involuções em grupos finitos nilpotentes

Os dois resultados que veremos a seguir serão usados para demonstar o Lema 5.3. Eles não serão demonstrados, mas suas provas podem ser encontradas em [Corollary 1.7.4, [14]] e [Lemma 7.44, [22]], respectivamente.

Proposição 5.1. *Seja p um número primo e ϕ um automorfismo de ordem p^k de um p-grupo abeliano V, onde $|C_V(\phi)| = p^n$. Então, o posto de V é, no máximo, $p^k n$.*

Lema 5.2. *Seja G um p-grupo abeliano com posto finito r. Então os p-subgrupos de Sylow de $AutG$ são finitos e possuem posto, no máximo, $\frac{1}{2}r(5r-1)$.*

Para demonstrar o resultado principal dessa seção precisaremos dos seguintes lemas.

Lema 5.3. *Seja G um p-grupo finito que possui um elemento ϕ de ordem p tal que $C_G(\phi)$ tem posto r. Então, G tem posto r-limitado.*

Demonstração: Seja N um subgrupo normal abeliano maximal de G. Note que N existe, pois G é finito, e, como G é um p-grupo, temos que $Z(G) \neq 1$, logo N é não trivial.

Como N é normal em G, podemos considerar um automorfismo φ em N tal que para todo n em N temos que $n^\varphi = n^\phi$, ou seja, o automorfismo dado pela conjugação pelo elemento ϕ. Consideramos, como é usual, os subgrupos $\langle\varphi\rangle$ e N como subgrupos do produto semidireto $N \rtimes \langle\varphi\rangle$.

Observe que, como ϕ tem ordem p como elemento de G, o automorfismo φ tem ordem p. Além disso, $C_G(\phi)$ tem posto r e $C_N(\varphi) = C_N(\phi) \leq C_G(\phi)$, logo o posto de $C_N(\varphi)$ é r-limitado. Assim, pela Proposição 5.1, temos que N possui posto r-limitado. Então, como N é um p-grupo abeliano com posto finito r-limitado, pelo Lema 5.2 , todo p-subgrupo de $AutN$ possui posto r-limitado.

Agora, como N é abeliano, temos que $C_G(N)$ é um subgrupo normal abeliano de G e $N \leq C_G(N)$, mas N é maximal entre os normais abelianos em G, logo $N = C_G(N)$. Assim, como

$$\tfrac{N_G(N)}{C_G(N)} \cong H \leq AutN,$$

temos que G/N é isomorfo a um p-subgrupo de $AutN$. Disso segue que G/N tem posto r-limitado. Portanto, pelo Corolário 1.40, o resultado segue.

■

Lema 5.4. *Sejam A e B p-grupos finitos para algum primo p. Assuma que A age fielmente sobre B e seja $r = rk(B)$. Então, $rk(A)$ é r-limitado.*

Demonstração: Seja G a extensão natural de B por A, ou seja, $G \cong B \rtimes A$. Tome N um subgrupo normal abeliano maximal de G e considere $P = \Omega_1(N)$ o subgrupo de N gerado por todos os elementos de N de ordem prima, ou seja, de ordem p. Note que P é um p-grupo abeliano elementar. Como N é abeliano, temos que N está contido em $C_G(N)$, que é um subgrupo normal abeliano de G. Mas, N é maximal entre os normais abelianos em G, logo $N = C_G(N)$. Assim, como $N_G(N)/C_G(N)$ é isomorfo a um subgrupo de $AutN$, obtemos que G/N é isomorfo a um subgrupo de $AutN$. Observe que, se provarmos que N tem posto r-limitado, então, pelo Lema 5.2, como N é um p-grupo abeliano, teremos que todo p-subgrupo de $AutN$ possui posto r-limitado. Portanto, teremos que N e G/N possuem postos r-limitados e, assim, pelo Corolário 1.40, G terá posto r-imitado e, como $A \leq G$, o resultado segue. Logo, é suficiente mostrar que o posto de N é r-limitado.

Tome $\{b_1, b_2, ..., b_r\}$ um conjunto de geradores de B. Note que, como B é normal em G, temos que $[P, b_i] \leq B$, para todo $1 \leq i \leq r$, assim, $rk([P, b_i]) \leq r$. Mas, $[P, b_i] \leq P$, pois P é característico em N que é normal em G, e P é abeliano elementar, logo, temos que $|[P, b_i]| \leq p^r$. Considerando a ação de conjugação de P sobre B, obtemos que

$$|P : C_P(b_i)| = |O(b_i)| = |\{b_i^x \mid x \in P\}| \leq |\langle b_i^{-1} b_i^x \mid x \in P\rangle| = |[P, b_i]| \leq p^r,$$

para todo $1 \leq i \leq r$ e $O(b_i)$ representa a órbita de b_i com respeito à ação de P sobre B.

Considere $S = \bigcap_{i=1}^{r} C_P(b_i)$. Temos que

$$|P : S| \leq \prod_{i=1}^{r} |P : C_P(b_i)| \leq p^{r^2}.$$

É claro que S centraliza $B = \langle b_i \mid 1 \leq i \leq r\rangle$ e, como A age fielmente sobre B, temos que $S \leq B$. Logo, como $rk(B) = r$ e $S \leq P$ que é abeliano elementar, temos que $|S| \leq p^r$. Agora, $|P : S| \leq p^{r^2}$, assim, obtemos que $|P| \leq p^{r^2+r}$.

Por fim, note que, pelo Teorema de Bases de Burnside, o posto de N é o maior número r tal que existe um subgrupo abeliano elementar de ordem p^r. Mas P é o maior subgrupo abeliano elementar de N, pois é gerado por todos os elementos de ordem p. Logo, temos que $rk(N) \leq rk(P)$ e, como já tínhamos que $rk(P) \leq rk(N)$ por P ser um subgrupo de N, concluímos que

$$rk(N) = rk(P) \leq r^2 + r.$$

O que demonstra o lema.

■

Agora temos todas as ferramentas necessárias para provar o resultado principal desta seção.

Teorema 5.5. *Seja G um grupo nilpotente finito admitindo uma involução ϕ tal que $C_G(\phi)$ tem posto r. Então G possui um subgrupo normal ϕ-invariante N com classe de nilpotência, no máximo, 2 tal que o quociente G/N tem posto r-limitado.*

Demonstração: Como G é um grupo finito nilpotente, temos que G é o produto direto de seus subgrupos de Sylow, digamos $G = S_1 \times S_2 \times \cdots \times S_k$. Assim, dado H um subgrupo de G, H é da forma $H = H_1 \times H_2 \times \cdots \times H_k$, onde H_i é um subgrupo de S_i, para todo $1 \leq i \leq k$. Considere d_i o posto de S_i, para todo $1 \leq i \leq k$. Temos que, por definição de posto de S_i, $d(H_i) \leq d_i$, para todo $1 \leq i \leq k$. Agora, H é um produto direto dos H_i, assim, $d(H) = \max_i\{d(H_i)\} \leq \max_i\{d_i\}$. Portanto, o posto de G é igual ao máximo dos postos dos subgrupos de Sylow de G, logo, podemos assumir, sem perda de generalidade, que G é um p-grupo para algum primo p.

Se $p = 2$, pelo Lema 5.3, o posto de G é r-limitado. Assim, tomando $N = 1$, temos que N é um subgrupo normal ϕ-invariante, com classe de nilpotência menor do que 2 e tal que $G/N \cong G$ tem posto r-limitado. Com isso temos o resultado.

Considere, então, o caso em que $p \neq 2$. Seja $N = [G, \phi] \cap C_G([G, \phi]')$. Note que $[G, \phi]'$ é normal em $[G, \phi]$ e $C_{[G,\phi]}([G, \phi]') = N$, logo $[G, \phi]/N$ age fielmente sobre $[G, \phi]'$. Observe que $C_{[G,\phi]}(\phi)$ está em $C_G(\phi)$ que tem posto r, logo $rk(C_{[G,\phi]}(\phi)) \leq r$ e temos, pelo Teorema 3.10, que $[G, \phi]'$ possui posto r-limitado. Assim, aplicando o Lema 5.4 com $A = [G, \phi]/N$ e $B = [G, \phi]'$, obtemos que o posto r_1 de $[G, \phi]/N$ é r-limitado. Pelo Teorema 1.30, $G = C_G(\phi)[G, \phi]$ e, por hipótese, $C_G(\phi)$ tem posto r, logo, pelo Corolário 1.40, G/N tem posto, no máximo, $r + r_1$ que é r-limitado.

Por fim, observe que $N = [G, \phi] \cap C_G([G, \phi]') \leq C_G([G, \phi]')$, logo $[G, \phi]'$ está em $C_G(N)$. Assim, $N' \leq [G, \phi]' \leq C_G(N)$ e disso segue que

$$\gamma_3(N) = [N', N] \leq [C_G(N), N] = 1.$$

Portanto, N tem classe de nilpotência, no máximo, 2. Além disso, pela definição de N, N é um subgrupo normal ϕ-invariante de G e, assim, o resultado segue.

■

5.2 Sobre involuções em grupos finitos de ordem ímpar

O teorema a seguir é usada para demonstrar o Teorema 5.7, que é o resultado principal desta seção. Ela não será demonstrada, mas sua prova pode ser vista em [Theorem 2, [17]].

Teorema 5.6. *Se cada subgrupo de Sylow de um grupo finito solúvel G pode ser gerado por d elementos, então G pode ser gerado por $d+1$ elementos.*

Note que, do Teorema 5.6 vemos que o número de geradores de um grupo finito solúvel pode ser determinado pelo número máximo de geradores de seus subgrupos de Sylow. Tendo em conta a definição de posto, segue que para todo grupo solúvel H

$$rk(H) \leq \max\{r_p(H) \mid p \in \pi(H)\} + 1,$$

onde $\pi(H)$ é o conjunto de todos os primos que dividem a ordem de H.

Teorema 5.7. *Seja G um grupo de ordem ímpar admitindo uma involução ϕ tal que $rk(C_G(\phi)) \leq r$. Então $rk([G,\phi]')$ é r-limitado.*

Demonstração: Note que $[G,\phi]$ está contido G, logo $C_{[G,\phi]}(\phi) \leq C_G(\phi)$ e, como por hipótese $rk(C_G(\phi)) \leq r$, obtemos que $rk(C_{[G,\phi]}(\phi)) \leq r$. Logo, podemos assumir que $G = [G,\phi]$. Pela Proposição 5.6, temos que, para todo grupo finito solúvel H, $rk(H) \leq \max\{r_p(H) \mid p \in \pi(H)\} + 1$. Assim, como G é solúvel e, consequentemente G' é solúvel, para limitar o posto de G' é suficiente mostrar que $r_p(G')$ é limitado em termos de r, para todo p em $\pi(G')$. Note que, o posto de $C_G(\phi)$ é r-limitado, logo $r_p(C_G(\phi))$ é r-limitado. Portanto, como G é um grupo de ordem ímpar admitindo uma involução ϕ e estamos assumindo que $G = [G,\phi]$, pelo Teorema 4.5, temos que $r_p(G')$ é r-limitado e, assim, o resultado segue.

■

Observamos que o resultado acima mostra que, como também no caso de um grupo que não é nilpotente, o posto do centralizador de uma involução tem uma influência forte sobre a estrutura de G. Mais em concreto, nas hipóteses do Teorema 5.7, denotando $G_1 = [G,\phi]'$ e $G_2 = [G,\phi]$, podemos construir uma série normal para G dada por

$$1 \leq G_1 \leq G_2 \leq G.$$

Note que G_2 é um subgrupo ϕ-invariante de G, logo, pelo Lema 3.2 (ii), temos que

$$C_{G/G_2}(\phi) = \frac{C_G(\phi)G_2}{G_2} \cong \frac{C_G(\phi)}{C_G(\phi)\cap G_2}.$$

Por outro lado, dado gG_2 em G/G_2, a imagem de gG_2 pelo automorfismo induzido ϕ de G/G_2 é $g^\phi G_2$. Mas, pela definição de G_2, temos que $g^{-1}g^\phi$ está em G_2 e disso segue que gG_2 determina a mesma classe lateral de $g^\phi G_2$. Com isso concluímos que $C_{G/G_2}(\phi) = G/G_2$. Portanto,

$$\frac{G}{G_2} \cong \frac{C_G(\phi)}{C_G(\phi) \cap G_2}$$

e, assim, como por hipótese no Teorema 5.7 $rk(C_G(\phi)) \leq r$, segue que $rk(G/G_2) \leq r$. Logo, na série normal acima temos que $rk(G_1)$ é r-limitado, G_2/G_1 é abeliano e $rk(G/G_2) \leq r$. Obtendo, assim, uma estrutura bem detalhada do posto de G.

A partir do Teorema 5.7 podemos provar, como corolário, que se G é um grupo finito admitindo um 2-automorfismo livre de pontos fixos ψ e ϕ é a involução de $\langle\psi\rangle$ que satisfaz $rk(C_G(\phi)) = r$, então o comprimento derivado de G é r-limitado. Para demonstrar esse corolário precisaremos da seguinte proposição.

Proposição 5.8. *Seja G um grupo finito de posto r admitindo um automorfismo livre de pontos fixos com ordem coprima com a ordem de G. Então, o comprimento derivado de G satisfaz*

$$dl(G) \leq 2^{r+1} - r + \lceil \log_2 r \rceil + 5\log_9(r/8) + 4,$$

onde $\lceil x \rceil$ denota o menor inteiro maior ou igual que o número real x.

O resultado acima, devido a Shalev, não será provado, mas sua demonstração pode ser encontrada em [Theorem 4.7, [23]].

Note que, nas hipóteses do Teorema 5.7, G pode ter um comprimento derivado arbitrário, que não é necessariamente limitado. Em [18], Kovács e Wall nos fornecem um exemplo de um grupo finito G de ordem ímpar que admite uma involução ϕ tal que $C_G(\phi)$ é cíclico, mas G possui comprimento derivado ilimitado. Tendo isso em vista, o resultado a seguir é bastante interessante, já que nos fornece uma situação em que podemos limitar o comprimento derivado do grupo.

Corolário 5.9. *Seja G um grupo finito admitindo um 2-automorfismo livre de pontos fixos ψ. Seja ϕ a involução de $\langle\psi\rangle$ e assuma que $rk(C_G(\phi)) = r$. Então, o comprimento derivado de G é r-limitado.*

Demonstração: Pelo Teorema 1.29, temos que G tem ordem ímpar. Note que $C_G(\phi)$ é ψ-invariante, pois, dado g em $C_G(\phi)$, como $\phi \in \langle\psi\rangle$, temos que

$$(g^\psi)^\phi = (g^\phi)^\psi = g^\psi$$

e, assim, g^ψ está em $C_G(\phi)$. Logo, $C_G(\phi)$ admite um automorfismo livre de pontos fixos. Como $C_G(\phi)$ é um grupo finito com posto r admitindo um automorfismo livre de pontos fixos, pela Proposição 5.8, temos que o comprimento derivado de $C_G(\phi)$ é r-limitado. Além disso, pelo Teorema 5.7, o posto de $[G,\phi]'$ é r-limitado. Observe que $[G,\phi]$ é ψ-invariante, pois, dado um gerador $x^{-1}x^\phi$ de $[G,\phi]$, com x em G, temos que

$$(x^{-1}x^{\phi})^{\psi} = (x^{\psi})^{-1}(x^{\psi})^{\phi} \in [G, \phi].$$

Como $[G, \phi]'$ é característico em $[G, \phi]$, obtemos que $[G, \phi]'$ é ψ-invariante e disso segue que $[G, \phi]'$ possui um automorfismo livre de pontos fixos. Assim, pela Proposição 5.8, temos que o comprimento derivado de $[G, \phi]'$ também é r-limitado. Agora, pelo Teorema 1.30, sabemos que $G = [G, \phi]C_G(\phi)$ e, assim, o resultado segue.

■

Referências Bibliográficas

[1] J. D. Dixon, M. P. F. du Sautoy, A. Mann e D. Segal, *Analytic Pro-p groups.* Cambridge 1991.

[2] W. Feit e J. Thompson, *Solvability of groups of odd order.* Pacific J. Math. **13,** 773-1029 (1963).

[3] B. Fine, A. Gaglione e F. C. Y. Tang, *Combinatorial Group Theory.* American Mathematical Society. Providence Rhode Island 1964.

[4] P. Fong, *On orders of finite groups and centralizers of p-elements.* Osaka J. Math. **13,** 483-489 (1976).

[5] J. González-Sánchez e A. Jaikin-Zapirain, *On the structure of normal subgroups of potent p-groups.* J. Algebra **276,** 193-209 (2002).

[6] D. Gorenstein, *Finite groups.* New York-Evanston-London 1968.

[7] B. Hartley e I. M. Isaacs, *On characters and fixed points of coprime operator groups.* J. Algebra **131,** 342-358 (1990).

[8] B. Hartley e T. Meixner, *Periodic groups in which the centralizer of an involution has bounded order.* J. Algebra **64,** 285-291 (1980).

[9] B. Hartley e T. Meixner, *Finite soluble groups in which the centralizer of an element of prime order is small.* Arch. Math. **36,** 211-213 (1981).

[10] G. Higman, *Groups and rings which have automorphisms without non-trivial fixed elements.* J. London Math. Soc. (2) **32,** 321-334 (1957).

[11] I. M. Isaacs, *Finite groups theory.* American Math. Soc. 2008.

[12] E. I. Khukhro e V. D. Mazurov, *Finite groups with an automorphism of prime order whose centralizer has small rank.* J. Algebra **301,** 474-492 (2006).

[13] E. I. Khukhro, *Groups an Lie rings admitting almost regular automorphisms of prime order.* In: Proc. Int. Conf. Theory Groups. Rend. Circ. Mat. Palermo (2) Suppl. 183-192 (1990).

[14] E. I. Khukhro, *Nilpotent groups and their automorphisms.* Berlin-New York 1993.

[15] E. I. Khukhro, *p-Automorphisms of Finite p-Groups.* Cambridge 1998.

[16] *The Kourovka Notebook. Unsolved problems in group theory.* 13th augm. ed. E. I. Khukhro (ed.) e V.D Mazurov (ed.), Sobolev Inst. Mat., Novosybirsk (1995).

[17] L. G. Kovács, *On finite soluble groups.* Math. Z. **103,** 37-39 (1967).

[18] L. G. Kovács e G. E. Wall, *Involutory automorphisms of groups of odd order and their fixed point groups.* Nagoya Math. J. **27,** 113-120 (1966).

[19] H. Kurzweil e B. Stellmacher, *The Theory of Finite Groups: An Introduction.* Springer 2004.

[20] C. R. Leedham-Green e S. McKay, *The structure of groups of prime power order.* Oxford 2002.

[21] A. Lubotzky e A. Mann, *Powerful p-groups. I: finite groups.* J. Algebra **105,** 484-505 (1987).

[22] D. J. S. Robinson, *Finiteness conditions and generalized soluble groups.* Berlin 1972.

[23] A. Shalev, *Automorphisms of finite groups of bounded rank.* Israel J. Math. **82,** 395-404 (1993).

[24] P. Shumyatsky, *Involutory automorphisms of finite groups and their centralizers.* Arch. Math. **71,** 425-432 (1998).

[25] J. G. Thompson, *Finite groups with fixed-point-free automorphisms of prime order.* Proc. Nat. Acad. Sci. U.S.A. **45,** 578-581 (1959).

[26] J. G. Thompson, *Automorphisms of solvable groups.* J. Algebra **1,** 259-267 (1964).