Universidade de Brasília

Sobre grupos finitos nos quais os comutadores têm ordens potência de primo

Mateus Figueiredo de Souza

Orientador: Dr. Pavel Shumyatsky

Departamento de Matemática
Universidade de Brasília

28 de março de 2024

Agradecimentos

É com grande prazer que dedico este espaço para prestar meus agradecimentos a algumas pessoas e instituições que contribuíram direta ou indiretamente na construção deste trabalho.

Primeiramente gostaria de agradecer ao meu orientador, o Prof. Dr. Pavel Shumyatsky. Agradeço por sua incansável dedicação ao nosso trabalho, pela prontidão na resolução dos problemas, pelos conselhos que levarei para a vida e pelo aprendizado que adquiri observando seu modo de pensar matemática. Principalmente, agradeço pela paciência que teve comigo em momentos de pandemia, quando eu mesmo pensei em desistir e o senhor me incentivou a continuar. Torço que todos tenham a sorte de ter um orientador como o senhor. Muito obrigado.

Agradeço à minha companheira Maria Gabriela. Muitas coisas vivemos nestes quase 10 anos juntos e durante toda minha trajetória na pós-graduação, e mesmo em parte da graduação, você esteve presente me dando amor e abrigo. Você me deu forças e permanece lutando até hoje para me fazer acreditar em mim. Agradeço por tudo. ♡

Agradeço à Dona Figueiredo, mais conhecida como mamãe, e a Seu Nonato, mais conhecido como papai, pelo amor e por me incentivar mesmo de longe. Aos meus irmãos Alcemira, Alcymara e Tiago pelo amor e por ser meu alicerce.

Agradeço ao Marcio e à Raquel pela amizade e carinho. Me senti em família nos momentos que compartilhamos no Ed. Hyara Center. Muito obrigado mesmo.

Ao meu amigo Geovane, meu maior fã, pela amizade e pelas conversas enriquecedoras nas caminhadas que fazíamos pela manhã na época do mestrado. Você se tornou um irmão para mim.

À Maria que mesmo após 4 anos de doutorado permaneceu com o status de subamiga. Também permanece a melhor subamiga que uma pessoa pode ter. Muito obrigado pela amizade e apoio, pelas fofocas principalmente, e pela paciência em me ouvir falar tantas vezes sobre os problemas da pesquisa.

À Ayana e à Maristela pelas conversas matinais e por poder compartilhar abertamente nossas frustrações com a vida na pós-graduação.

Ao Jônatas (PP-P), meu parceiro de cantoria e segundo maior fã, e ao Ismael, responsável por discordar de mim e me fazer pensar e também pela paciência em me ouvir falar de matemática nas nossas caminhadas.

Aos meus ex-alunos: Caio, Gabriel, Gabriela e Ismael. Vocês talvez não saibam mas me deram forças para enfrentar os desafios. Eu me esforcei para que pudesse dizer "se eu consegui, vocês também conseguem". Foi uma honra ter vocês como colegas do doutorado e uma honra maior ainda foi ter sido professor de vocês, eu sempre pensei isso.

Ao Tharles que teve paciência para se tornar meu amigo. Muito obrigado.

Aos membros da banca Prof. Dr. Danilo Silveira, Prof. Dr. Jhone Caldeira e Prof. Dr. Raimundo Bastos pelas valiosas considerações para a melhoria deste trabalho.

A muitos amigos que fiz nesta jornada em Brasília, dentre os quais posso destacar: Claudia, Dal Berto, Julia, Rodolfo, Deyfila, Talita, Thiago (O James), Flávia, Xiaofang Gao, Katianny, Sharmenya, Rômulo, Zaban, Felipe e Kobayashi.

Aos muitos professores com os quais aprendi muito sobre matemática e sobre a vida, dentre os quais destaco os professores Sergio Brazil, Aline Pinto, Liliane Maia, José Teruel, Tarcísio Castro, Irina Sviridova, Alex Cazarredo. Um agradecimento especial à professora Cristina Acciarri, minha orientadora de mestrado.

Expresso minha sincera gratidão ao estado brasileiro que por meio das políticas de cotas raciais me permitiu ingressar na Universidade Federal do Acre e iniciar minha trajetória acadêmica. Desde a graduação até o doutorado, as bolsas de estudo foram essenciais durante minha jornada. Como uma pessoa de origem humilde, sem essas bolsas, eu não teria condições financeiras para prosseguir meus estudos. Sou profundamente grato pelo apoio que recebi, que foi fundamental para poder ter dedicação plena à pesquisa e à vida na pós graduação. Obrigado por investir em oportunidades educacionais que possibilitam o desenvolvimento pessoal e profissional de indivíduos como eu.

À CNPq pelo suporte financeiro que, além de tudo já comentado, me possibilitou a realização de algumas colaborações científicas, principalmente em visitas ao Amazonas, Rio de Janeiro e Minas Gerais.

Resumo

O estudo de grupos nos quais cada elemento tem ordem potência de primo (EPPO-grupos) foi iniciado em trabalhos pioneiros de G. Higman e M. Suzuki. Hoje em dia os EPPO-grupos finitos são bem conhecidos. Por exemplo, é conhecido que se G é um EPPO-grupo finito solúvel, então a altura de Fitting de G é no máximo 3 e $|\pi(G)| \leqslant 2$. Mais do que isto, se G é não solúvel, então o radical solúvel $R(G)$ de G é um 2-grupo e o grupo quociente $G/R(G)$ pertence a uma lista de exatamente 9 grupos determinada por Suzuki.

No presente trabalho nos concentramos em grupos nos quais todo comutador tem ordem potência de primo (CPPO-grupos). Mostramos que se G é um CPPO-grupo finito, então a estrutura de G' é similar à de um EPPO-grupo. Em particular, mostramos que qualquer CPPO-grupo finito solúvel G tem altura de Fitting no máximo 3 e que $|\pi(G')| \leqslant 3$. Mais do que isto, se G é não solúvel, então $R(G')$ é um 2-grupo e $G'/R(G')$ é isomorfo a um EPPO-grupo simples.

Palavras chave: Altura de Fitting, Grupos Finitos, Torres de Turull.

Abstract

The study of finite groups in which every element has prime power order (EPPO-groups) was initiated in pioneering works of G. Higman and M. Suzuki. Nowadays EPPO-groups are fairly well understood. For instance, it is known that if G is a finite soluble EPPO-group, then the Fitting height of G is at most 3 and $|\pi(G)| \leqslant 2$. Moreover, if G is insoluble, then the soluble radical $R(G)$ of G is a 2-group and the quotient group $G/R(G)$ belongs to a list of exactly 9 groups determined by Suzuki.

In the present work we concentrate on finite groups in which every commutator has prime power order (CPPO-groups). Roughly, we show that if G is a finite CPPO-group, then the structure of G' is similar to that of an EPPO-group. In particular, we show that the Fitting height of any finite soluble CPPO-group is at most 3 and $|\pi(G')| \leqslant 3$. Moreover, if G is insoluble, then $R(G')$ is a 2-group and $G'/R(G')$ is isomorphic to a simple EPPO-group.

Keywords: Fitting Height, Finite Groups, Turull Towers.

Conteúdo

Introdução

Uma classe de grupos que atrai atenção de matemáticos há algumas décadas é a classe dos EPPO-grupos (às vezes chamados de CP-grupos). Um grupo é chamado de EPPO-grupo se cada um de seus elementos tem ordem potência de primo. O primeiro a estudar esta classe de grupos foi G. Higman em [8], onde o mesmo descreveu a estrutura dos EPPO-grupos finitos solúveis provando o seguinte resultado.

Teorema 0.1 (Higman)**.** *Seja G um EPPO-grupo finito e solúvel e seja p um primo tal que G possui um p-subgrupo normal não trivial. Seja P o maior p-subgrupo normal de G. Nestas condições, o quociente G/P é ou um q-grupo cíclico com $q \neq p$, ou um grupo quaternion generalizado, ou um grupo de ordem $p^a q^b$ com subgrupos de Sylow cíclicos, onde q é um número primo da forma $kp^r + 1$.*

Decorre do resultado acima que em um EPPO-grupo finito não solúvel qualquer subgrupo solúvel tem ordem divisível por no máximo 2 primos. Usando isto, Higman verificou em [8] que um EPPO-grupo finito não solúvel tem um único fator de composição não abeliano que em muito determina sua estrutura.

Posteriormente, em [22] M. Suzuki estudou uma classe de grupos duplo-transitivos com a propriedade que só a identidade fixa 3 elementos, generalizando um trabalho anterior de Zassenhaus. Como parte de seu trabalho, Suzuki descobriu uma nova família de grupos simples não abelianos com a propriedade exclusiva que nenhum destes grupos tem ordem divisível pelo primo 3. Estes são chamados de grupos de Suzuki, denotados por $Sz(q)$ com $q \geqslant 8$ potência de 2. Ainda, Suzuki conseguiu classificar os EPPO-grupos finitos simples não abelianos neste mesmo trabalho.

Teorema 0.2 (Suzuki)**.** *Seja G um EPPO-grupo finito simples não abeliano. Então G é isomorfo a um dos seguintes grupos:* $\mathrm{PSL}(2,q)$*,* $q \in \{4,7,8,9,17\}$*,* $\mathrm{PSL}(3,4)$*,* $Sz(8)$ *e* $Sz(32)$*.*

Acima, $\mathrm{PSL}(n,q)$ denota o grupo Projetivo Especial Linear de grau n sobre um corpo com q elementos.

R. Brandl continuou em [2] a investigação de Suzuki em EPPO-grupos não solúveis. Então, a descrição da estrutura dos EPPO-grupos finitos foi finalmente obtida em [1] por W. Bannuscher e G. Tiedt.

Foi após a obtenção da descrição dos EPPO-grupos finitos que em [7] H. Heineken considerou os EPPO-grupos localmente finitos. Um grupo G é dito ser localmente finito se todo subgrupo finitamente gerado de G for finito. Uma descrição completa dos EPPO-grupos localmente finitos foi posteriormente obtida por A. L. Delgado e Yu-Fen Wu em [5].

Os EPPO-grupos topológicos também têm sido estudados. Por exemplo, em [20], P. Shumyatsky verificou que um EPPO-grupo profinito G é virtualmente um grupo *pro-p*, para algum primo p. Ademais, se G é infinito e P é o maior *pro-p* subgrupo normal aberto de G, então o quociente G/P admite uma descrição detalhada.

Investigações mais recentes têm focado em grupos nos quais um conjunto específico de elementos têm ordem potência de primo. Por exemplo, em [13] M. Lewis considera grupos finitos G que possuem um subgrupo normal N tal que todos os elementos do conjunto $G \setminus N$ têm ordens potência de primo. Neste artigo, Lewis verifica, por exemplo, que se os elementos do conjunto $G \setminus N$ têm ordens divisíveis por primos p e q, então G é um $\{p,q\}$-grupo e ou G é um grupo de Frobenius ou G é um grupo 2-Frobenius.

Neste trabalho, iremos estudar uma classe de grupos mais geral que a classe dos EPPO-grupos. Precisamente, iremos estudar a classe dos grupos nos quais todos os comutadores têm ordens potência de primo, que aqui serão chamados de CPPO-grupos. Baseado no resultado de Higman sobre EPPO-grupos solúveis, nosso primeiro interesse é em obter informações sobre a altura de Fitting de um CPPO-grupo solúvel.

Para um grupo finito G, denotamos por $F(G)$ o produto de todos os subgrupos normais nilpotentes de G. O subgrupo $F(G)$ é chamado o subgrupo de Fitting de G e o usamos como ponto de partida para definir a *série de Fitting superior* de G indutivamente sob as regras

$$F_0(G) = 1 \text{ e } F_i(G)/F_{i-1}(G) = F(G/F_{i-1}(G)),\ i \geqslant 1.$$

Ocorre que para todo grupo finito solúvel não trivial G vale $F(G) \neq 1$. Como consequência, existe um inteiro não negativo h para o qual $F_h(G) = G$ e o menor inteiro não negativo com esta propriedade é chamado de altura de Fitting de G, denotada por $h(G)$.

O Teorema 0.1 mostra que se G é um EPPO-grupo finito e solúvel, então a altura de Fitting de G é no máximo 3. Adicionalmente, denotando por $\pi(G)$ o conjunto de fatores primos da ordem de um grupo finito G, decorre do Teorema 0.1 que se G é um EPPO-grupo finito e solúvel, então $|\pi(G)| \leqslant 2$.

Os resultados expostos neste trabalho são essencialmente semelhantes aos obtidos por Higman em [8], embora as provas sigam caminhos distintos. Provaremos primeiramente que,

assim como para EPPO-grupos, os CPPO-grupo finitos e solúveis têm altura de Fitting no máximo 3.

Por sua vez, não é verdade que $|\pi(G)| \leqslant 2$ para CPPO-grupos finitos e solúveis. Isto ocorre pois os grupos abelianos são CPPO-grupos. Contudo, conseguimos verificar que o subgrupo derivado de um CPPO-grupo finito e solúvel tem ordem divisível por no máximo 3 primos.

Melhorando o que fora obtido por Higman sobre EPPO-grupos não solúveis, Suzuki provou em [21] que $R(G)$ é um 2-grupo para todo EPPO-grupo finito e não solúvel, onde $R(G)$ denota o radical solúvel de G. Mais do que isto, juntando os resultados em [21] e [22], Suzuki descreveu a estrutura do quociente $G/R(G)$. Iremos fazer o mesmo para CPPO-grupos finitos e não solúveis.

Dadas estas considerações enunciamos abaixo o principal resultado deste trabalho.

Teorema 0.3. *Seja G um CPPO-grupo finito.*

(a) Se G é solúvel, então a altura de Fitting de G é no máximo 3;

(b) Se G é solúvel, então no máximo 3 primos dividem a ordem de G';

(c) Se G é não solúvel, então $R(G') = [G', R(G)]$ é um 2-grupo e $G'/R(G')$ é isomorfo a um dos seguintes grupos: $\mathrm{PSL}(2,q)$, $q \in \{4,7,8,9,17\}$, $\mathrm{PSL}(3,4)$, $Sz(8)$, $Sz(32)$.

A principal ferramenta que utilizamos para provar a parte do Teorema 0.3 que trata sobre grupos solúveis advém do artigo [24] de A. Turull. Neste artigo, Turull introduziu a noção de *torres* em grupos finitos e provou que um grupo solúvel finito G tem altura de Fitting igual a maior altura de uma torre de G, o que será de fundamental importância em nossos cálculos.

Nas linhas que se seguem iremos descrever a estrutura deste trabalho. No primeiro capítulo deste trabalho iremos expor algumas definições, notações e resultados elementares que serão utilizados ao longo do trabalho, possivelmente sem menção explícita.

Os Capítulos 2 e 3 têm como objetivo principal provar o Teorema 0.3. Dividimos a prova deste Teorema em 3 partes, chamadas de Teoremas A, B e C. O conteúdo do Teorema A é o conteúdo do item (a) do Teorema 0.3 e assim sucessivamente.

No Capítulo 2 iremos introduzir os CPPO-grupos e provar os Teoremas A e B. Na primeira seção iremos definir e provar alguns resultados elementares sobre CPPO-grupos. Após isto iremos introduzir a noção de torres de Turull. Provaremos alguns resultados que permitem entender melhor esta ferramenta e posteriormente estabeleceremos alguns resultados auxiliares sobre torres em CPPO-grupos. Iremos concluir o Capítulo 2 com as provas dos Teoremas A e B.

No Capítulo 3 estabeleceremos o Teorema C. Iniciaremos o capítulo estudando CPPO-grupos com radical solúvel trivial. Na seção seguinte introduziremos os grupos que constam na classificação dos EPPO-grupos finitos simples. Também determinaremos os CPPO-grupos quase-simples. Um grupo não trivial e finito G é chamado quase-simples se possui um subgrupo normal simples H tal que $C_G(H) = 1$. O ponto chave para provar o resultado sobre CPPO-grupos não solúveis será verificar que um tal grupo tem subgrupo derivado perfeito e, após fazer isto, provaremos o Teorema C.

Capítulo 1

Preliminares

Neste capítulo iremos apresentar as notações, definições e alguns resultados básicos que iremos utilizar ao longo do trabalho, possivelmente sem menção prévia. Resultados como os Teoremas do Isomorfismo, da Correspondência e de Sylow são assumidos como conhecidos. Quando X e Y forem conjuntos e $f : X \longrightarrow Y$ for uma função, iremos denotar por x^f a imagem segundo f do elemento $x \in X$. Para um grupo finito G e um elemento $g \in G$, denotamos por $|G|$ e $|g|$ as ordens de G e g, respectivamente. As principais referências aqui utilizadas são os livros de D. Gorenstein [6], H. Kurzweil e B. Stellmacher [12] e H. E. Rose [18].

1.1 Noções elementares

Iniciamos este capítulo com a seguinte lista de notações que serão usadas ao longo do trabalho.

Sejam G um grupo, H e K subgrupos de G e sejam a e b elementos de G. Escrevemos

1. $a^b = b^{-1}ab$ para o conjugado de a por b;
2. $[a,b] = a^{-1}a^b$ para o comutador de a e b, nesta ordem;
3. $C_G(a) = \{c \in G;\ a^c = a\}$ para o centralizador de a em G;
4. $C_G(H) = \{g \in G;\ h^g = h,\ \text{para todo } h \in H\}$ para o centralizador de H em G;
5. $[H,K]$ para o subgrupo de G gerado pelos elementos $[h,k]$ com $h \in H$ e $k \in K$;
6. $G' = [G,G]$ para o subgrupo derivado de G;
7. $N_G(H) = \{g \in G;\ H^g = H\}$ para o normalizador de H em G;

8. $Z(G)$ para o centro de G.

A seguinte lista de propriedades de comutadores pode ser verificada diretamente, ou ainda, é possível encontrar suas demonstrações em [6, Capítulo 2].

Lema 1.1. *Seja G um grupo e sejam $x,y,z \in G$. Então*

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

O seguinte resultado é conhecido como Lema dos Três Subgrupos e uma prova pode ser encontrada em [6, Teorema 2.3].

Lema 1.2 (Lema dos Três subgrupos)**.** *Sejam G um grupo e sejam $H,K,L \leq G$. Suponha que $[[H,K],L] = 1 = [[K,L],H]$. Então $[[L,H],K] = 1$.*

Definição 1.3. O subgrupo de Frattini de um grupo finito G é definido como a intersecção de todos os subgrupos maximais de G e é denotado por $\Phi(G)$.

Comentamos que uma vez que automorfismos preservam maximalidade em subgrupos, o subgrupo de Frattini é sempre característico.

Lema 1.4. *Seja G um grupo finito e seja $H \leq G$. Se $G = H\Phi(G)$, então $G = H$.*

Demonstração. Pois se H fosse um subgrupo próprio de G, então H estaria contido em um subgrupo maximal, digamos M, de G, o qual por definição também contém $\Phi(G)$. Neste caso obteríamos o absurdo $G = H\Phi(G) \leq M$. □

O seguinte resultado, conhecido como Lema de Dedekind (ou Lei Modular de Dedekind), é bem conhecido e pode ser provado diretamente.

Lema 1.5. *Sejam G um grupo e sejam H,K,L subgrupos de G com $K \leq H$. Então $H \cap LK = (H \cap L)K$.*

Lema 1.6. *Seja G um grupo finito e seja N um subgrupo normal de G. Então $\Phi(N) \leq \Phi(G)$.*

Demonstração. Assuma falso. Então existe um subgrupo maximal M de G que não contém $\Phi(N)$. Pela maximalidade de M temos que $G = M\Phi(N)$ e, portanto, usando o Lema de Dedekind, obtemos $N = N \cap G = N \cap M\Phi(N) = (N \cap M)\Phi(N)$. Segue do Lema 1.4 que $N = N \cap M$. Mas isto significa que $N \leq M$, o que contradiz a escolha de M. □

Seja π um conjunto de números primos. Denotamos por π' o conjunto de todos os números primos que não estão em π. Para um grupo G, denotamos por $\pi(G)$ o conjunto de fatores primos da ordem de G. Dizemos, então, que G é um π-grupo se $\pi(G) \subseteq \pi$.

Seja G um grupo. Não é difícil verificar que o produto de dois π-subgrupos normais de G é também um π-subgrupo normal de G. Podemos, portanto, definir $O_\pi(G)$ como sendo o maior π-subgrupo normal de G. No caso em que $\pi = \{p\}$ contém um único primo, escrevemos $O_p(G)$ e $O_{p'}(G)$ para $O_\pi(G)$ e $O_{\pi'}(G)$, respectivamente.

Para um grupo finito arbitrário G, pode ser difícil determinar $\Phi(G)$. Entretanto, no caso em que G é um p-grupo finito, pode-se encontrar uma prova em [12, Teorema 5.2.8] que $\Phi(G)$ é o menor subgrupo normal de G cujo grupo quociente induzido é abeliano elementar. Lembre que um p-grupo G é dito abeliano elementar se G é abeliano e $G^p = \langle g^p;\ g \in G\rangle$ é trivial. Usando esta informação, podemos deduzir a seguinte descrição do subgrupo de Frattini de p-grupos finitos.

Lema 1.7. *Seja G um p-grupo finito. Então $\Phi(G) = G'G^p$.*

Demonstração. Se N é um subgrupo maximal de G então N é normal e tem índice p em G (veja [18, Teorema 6.6]). Então G/N tem ordem p e por isto $G'G^p \leq N$. Da arbitrariedade da escolha de N decorre que $G'G^p \leq \Phi(G)$. Por outro lado, claramente o grupo quociente $G/G'G^p$ é abeliano elementar. Segue que $\Phi(G) \leq G'G^p$. □

Definição 1.8. Dizemos que um grupo G é solúvel se G possui uma série normal

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

tal que G_{i+1}/G_i é abeliano para cada i.

Dado um grupo G, iremos agora usar o subgrupo derivado como ponto de partida para definir uma série de subgrupos de G que é suficiente para determinar solubilidade. Esta série é a chamada série derivada de G e seus termos são definidos indutivamente por

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

Definida desta maneira, a série derivada de um grupo G é uma cadeia descendente de subgrupos característicos de G cujos fatores $G^{(i)}/G^{(i+1)}$ são abelianos.

Como sabemos, se N é um subgrupo normal de um grupo G, então G/N é abeliano se, e somente se, $G' \leq N$. Usando isto, pode-se verificar que G é solúvel se, e somente se, $G^{(n)} = 1$ para algum inteiro positivo n. Também a classe de todos os grupos solúveis é fechada para subgrupos, imagens epimórficas e produtos diretos finitos. Ainda, não é muito difícil verificar que se $N \trianglelefteq G$ é solúvel e também G/N é solúvel, então G é solúvel. Veja [18, Capítulo 11] para a prova destes fatos.

Lema 1.9. *Seja G um grupo. O produto de dois subgrupos normais solúveis de G é solúvel.*

Demonstração. Em verdade, se M e N são subgrupos normais solúveis de G, então como N e $MN/N \cong M/M \cap N$ são solúveis, temos que MN é solúvel. □

Pelo Lema 1.9, podemos definir para um grupo finito G o maior subgrupo normal solúvel de G como sendo o produto de todos os subgrupos normais solúveis de G, o qual denotamos por $R(G)$. Este subgrupo é chamado o radical solúvel de G e será de grande importância neste trabalho.

Outra classe muito importante de grupos é a classe dos grupos nilpotentes, que definimos a seguir.

Definição 1.10. Dizemos que um grupo G é nilpotente se G possui uma *série central*, isto é, G possui uma série de subgrupos

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

tal que

$$G_{i+1}/G_i \leq Z(G/G_i) \text{ para todo } i.$$

Segue da própria definição que todo grupo nilpotente é solúvel, e assim como a classe dos grupos solúveis, a classe dos grupos nilpotentes é fechada para subgrupos, imagens epimórficas e produtos diretos finitos, veja [18, Capítulo 10] para as provas destes fatos. Entretanto, esta classe não é fechada para extensões, diferentemente da classe dos grupos solúveis. Por exemplo, o grupo simétrico S_3 possui um subgrupo normal cíclico que induz também quociente cíclico, logo S_3 é solúvel, mas S_3 não é nilpotente.

Exemplo 1.11. Se G é um p-grupo finito não trivial, pode-se verificar que $Z(G) \neq 1$ (veja [18, Lema 5.21]). Como consequência, pode-se provar por indução em $|G|$ que G é nilpotente.

Análogo ao caso de solubilidade, iremos expor uma série de subgrupos normais capaz de responder a questão se um grupo G é ou não nilpotente.

Definição 1.12. A *série central inferior* de um grupo G é a série cujos termos são definidos sob as regras

$$\gamma_1(G) = G \text{ e } \gamma_{i+1}(G) = [\gamma_i(G), G] \text{ para todo } i \geqslant 1.$$

Adcionalmente,

$$\gamma_\infty(G) = \bigcap_{i \geqslant 1} \gamma_i(G).$$

Definida como acima, todos os termos da série central de um grupo G, incluindo $\gamma_\infty(G)$, são subgrupos característicos de G.

A série central de um grupo G determina nilpotência em G no sentido que G é nilpotente se, e somente se, $\gamma_n(G) = 1$ para algum inteiro positivo n.

O seguinte lema pode ser verificado diretamente.

Lema 1.13. *Seja G um grupo e seja n um inteiro positivo. Para um subgrupo normal N de G, temos $\gamma_n(G/N) = \gamma_n(G)N/N$. Em particular, se G é finito, então $\gamma_\infty(G)$ é o menor subgrupo normal N de G tal que G/N é nilpotente.*

Abaixo citamos um resultado que coleta definições equivalentes para nilpotência em grupos finitos, as quais utilizaremos nos próximos capítulos sem menção explícita.

Teorema 1.14 ([18], Teorema 10.9)**.** *Seja G um grupo finito. As seguintes condições são equivalentes:*

1. *G é nilpotente;*
2. *$\gamma_n(G) = 1$ para algum inteiro positivo n;*
3. *$\gamma_\infty(G) = 1$;*
4. *Se $H < G$, então $H < N_G(H)$;*
5. *Todos os subgrupos maximais de G são normais em G;*
6. *Todos os subgrupos de Sylow de G são normais em G;*
7. *G é isomorfo ao produto direto de seus subgrupos de Sylow;*
8. *Se $a, b \in G$ têm ordens coprimas, então a e b comutam.*

Exemplo 1.15. Seja G um grupo finito. Seja P um p-subgrupo de Sylow de $\Phi(G)$, p um número primo. Pelo Argumento de Frattini (veja a seção 1.3), $G = N_G(P)\Phi(G)$ e por isso $G = N_G(P)$. Isto significa que $P \trianglelefteq G$ e, por maior razão, $P \trianglelefteq \Phi(G)$. Segue do Teorema 1.14 que $\Phi(G)$ é nilpotente.

Análogo à definição do radical solúvel de um grupo G temos a definição de um maior subgrupo normal nilpotente de G, que se baseia no seguinte resultado devido a H. Fitting.

Lema 1.16 ([18], Teorema 10.22)**.** *Sejam M e N subgrupos normais nilpotentes de um grupo G. Então MN é nilpotente.*

Definição 1.17. Seja G um grupo finito. O produto de todos os subgrupos normais nilpotentes de G é chamado o subgrupo de Fitting de G e é denotado por $F(G)$.

Um grupo finito, mesmo não simples, pode ter subgrupo de Fitting trivial, como por exemplo é o caso do grupo simétrico S_5. Contudo, argumentaremos a seguir que $F(G)$ é não trivial para todo grupo finito solúvel e não trivial G.

Um grupo finito e não trivial G é chamado de caracteristicamente simples se G não possui subgrupo característico próprio não trivial.

Lema 1.18 ([6], Teorema 1.4)**.** *Um grupo caracteristicamente simples é um produto direto de um número finito de grupos simples mutuamente isomorfos.*

Usamos agora o lema anterior para estudar subgrupos normais minimais de grupos finitos, com atenção especial a grupos solúveis.

Lema 1.19. *Um subgrupo normal minimal de um grupo finito não trivial G é caracteristicamente simples. Se G é solúvel, tal subgrupo é p-abeliano elementar para algum primo p e, em particular, $F(G) \neq 1$.*

Demonstração. Seja N um subgrupo normal minimal de G. Um subgrupo característico de N é normal em G. Logo, a minimalidade de N implica que N é caracteristicamente simples. No caso em que G é solúvel, N é produto direto de um número finito de grupos simples solúveis e mutuamente isomorfos. Mas um grupo solúvel simples não trivial tem ordem prima. Logo, N é p-abeliano elementar para algum primo p. □

Uma propriedade importante do subgrupo de Fitting de um grupo finito solúvel G é que seu centralizador em G coincide com o seu centro. Este é o conteúdo do próximo resultado.

Lema 1.20. *Seja G um grupo finito solúvel. Então $C_G(F(G)) \leq F(G)$.*

Demonstração. Deixe-nos escrever $C = C_G(F(G))$. Assuma por contradição que $C \not\leq F(G)$. Então $H = C \cap F(G)$ é um subgrupo próprio de C e por isto o quociente C/H é não trivial. Seja B/H o último termo não trivial da série derivada de C/H. Então $B' \leq H$ e, como $H \leq Z(C)$, obtemos que $[B,B,B] = 1$, isto é, B é nilpotente. Mas por definição temos também que B é característico em G. Portanto, $B \leq F(G)$ e assim $B \leq H$, o que contradiz a escolha de B. Isto prova que $C \leq F(G)$. □

A seguir definiremos uma classe de p-grupos que será de grande importância em nossos cálculos.

Definição 1.21. Um p-grupo finito G é chamado extraespecial se $|Z(G)| = p$ e $G/Z(G)$ é p-abeliano elementar.

Exemplo 1.22. Um grupo *quaternion* é um grupo da forma

$$Q_{2^n} = \langle a, b;\ a^{2^{n-1}} = 1,\ b^2 = a^{2^{n-2}},\ a^b = a^{-1} \rangle,$$

onde $n \geqslant 3$. Veja que de $a^b = a^{-1}$ temos que $[a,b] = a^{-2}$. Como $Q'_{2^n} = \langle [a,b]^g;\ g \in Q_{2^n} \rangle$, segue que $Q'_{2^n} = \langle a^2 \rangle$. Por sua vez, Q_{2^n} é não abeliano e então $Z(Q_{2^n}) \leq \langle a \rangle$. Mas se i é um inteiro positivo, $(a^i)^b = a^{-i}$ e assim $a^i \in Z(Q_{2^n})$ se, e somente se, $2^{n-2} \mid i$. Portanto, $Z(Q_{2^n}) = \langle a^{2^{n-2}} \rangle$ tem ordem 2. Disto decorre que Q_{2^n} é extraespecial se, e somente se, $n = 3$.

Para encerrar esta seção de noções elementares, provaremos o seguinte resultado.

Teorema 1.23 (Baer-Suzuki)**.** *Seja G um grupo finito e seja x um elemento de G. Então $x \in O_p(G)$ se, e somente se, todo par de conjugados de x gera um p-subgrupo de G.*

Demonstração. Seja $C = Cl_G(x)$ a classe de conjugação de x em G e note que C é um subconjunto normal de G. Então $x \in O_p(G)$ se, e somente se, $\langle C \rangle$ é um p-grupo. Em particular, se $x \in O_p(G)$, então todo par de conjugados de x gera um p-subgrupo de G.

Assuma, reciprocamente, que todo par de conjugados de x gera um p-subgrupo de G e que $x \notin O_p(G)$. Neste caso, podemos achar p-subgrupos de Sylow de G, digamos P e Q, para os quais $C \cap P \neq C \cap Q$. Como C é normal e P e Q são conjugados, temos que $|C \cap P| = |C \cap Q|$. Logo, temos que $C \cap P \nsubseteq Q$ e $C \cap Q \nsubseteq P$. Considere adicionalmente P e Q de modo que $|C \cap P \cap Q|$ é maximal.

Seja $H = \langle C \cap P \cap Q \rangle$. Então H é um subgrupo próprio de ambos P e Q e podemos considerar uma série ascendente $H = H_0 < H_1 \leq \cdots \leq H_n = P$ de subgrupos de P tais que $[H_{i+1} : H_i] = p$ para cada $i < n$. Como $C \cap P \nsubseteq Q$, temos que $C \cap P \nsubseteq H$ e então existe um menor $0 < i \leqslant n$ para o qual $C \cap H_i \nsubseteq C \cap H$. Tomemos um elemento $g \in C \cap H_i \setminus H$. Como $[H_i : H_{i-1}] = p$ e C é normal em G, temos que g normaliza $C \cap H_{i-1}$. Por minimalidade temos que $C \cap H_{i-1} = C \cap H$, isto é, g normaliza $C \cap H$. Desde que $C \cap P \cap Q \subseteq C \cap H$ obtemos que g normaliza $\langle C \cap H \rangle = H$. Analogamente podemos achar um elemento $h \in C \cap Q \setminus H$ que normaliza H.

Considere o subgrupo $L_0 = \langle g, h, H \rangle$. Ambos g e h são conjugados a x e por isto geram um p-subgrupo de G. Mais do que isto, g e h normalizam H. Segue que L_0 é um p-subgrupo de G. Seja, agora, L um p-subgrupo de Sylow de G contendo L_0. Veja que

$\{g\} \cup (H \cap C) \leq C \cap P \cap L$, logo $|C \cap P \cap L| > |H \cap C|$. Mais do que isto, $H \cap C \supseteq C \cap P \cap Q$, por isto obtemos $|C \cap P \cap L| > |C \cap P \cap Q|$. Analogamente obtemos $|C \cap Q \cap L| > |C \cap P \cap Q|$. Pela escolha de P e Q concluímos que $P \cap C = L \cap C = Q \cap C$, uma contradição.

□

1.2 Altura de Fitting

Definição 1.24. Seja G um grupo. Uma série de Fitting de G é uma série de subgrupos normais

$$1 = G_0 \leq G_1 \leq \cdots \leq G_h = G$$

tal que G_i/G_{i-1} é um grupo nilpotente, para todo i. No caso em que G possui uma série de Fitting, o menor comprimento de uma série de Fitting de G é chamado de altura de Fitting de G, a qual será denotada por $h(G)$.

Observe que para que um grupo G possua uma série de Fitting é necessário, e suficiente, que G seja solúvel. De fato, se G é solúvel então G possui uma série solúvel, a qual é também uma série de Fitting de G. Reciprocamente, se G possui uma série de Fitting obtemos que G é solúvel lembrando que grupos nilpotentes são solúveis e que a classe dos grupos solúveis é fechada para extensões.

Lema 1.25. *Sejam G e Q grupos solúveis e sejam $H, N \leq G$ com $N \trianglelefteq G$. Então*

1. $h(H) \leq h(G)$;
2. $h(G/N) \leq h(G)$;
3. $h(G) \leq h(N) + h(G/N)$;
4. $h(G \times Q) = max\{h(G), h(Q)\}$.

Demonstração. No decorrer da prova assumimos que $1 = G_0 \leq G_1 \leq \cdots \leq G_h = G$ é uma série de Fitting de G.

1. Considere a seguinte série de subgrupos normais de H

$$1 = H \cap G_0 \leq H \cap G_1 \leq \cdots \leq H \cap G_h = H.$$

Para cada $i = 1, \ldots, h$, temos que

$$\frac{H \cap G_i}{H \cap G_{i-1}} = \frac{H \cap G_i}{H \cap G_i \cap G_{i-1}} \cong \frac{(H \cap G_i)G_{i-1}}{G_{i-1}} \leq \frac{G_i}{G_{i-1}}$$

é nilpotente. Isto significa que $1 = H \cap G_0 \leq H \cap G_1 \leq \cdots \leq H \cap G_h = H$ é uma série de Fitting de H. Pela arbitrariedade da escolha da série de Fitting de G, concluímos que $h(H) \leq h(G)$.

2. Analogamente ao caso anterior, a série

$$1 = G_0N/N \leq G_1N/N \leq \cdots \leq G_hN/N = G/N$$

é uma série de Fitting de G/N, uma vez que para todo $i = 1, \ldots, h$ temos que o grupo

$$\frac{G_iN/N}{G_{i-1}N/N} \cong \frac{G_iN}{G_{i-1}N} \cong \frac{G_i}{G_i \cap G_{i-1}N} = \frac{G_i}{G_{i-1}(G_i \cap N)} \cong \frac{G_i/G_{i-1}}{(G_i \cap N)G_{i-1}/G_{i-1}}$$

é nilpotente. Portanto $h(G/N) \leq h(G)$.

3. Considere séries de Fitting

$$1 = N_0 \leq N_1 \leq \cdots \leq N_{h_1} = N \text{ e } 1 = K_0 \leq K_1 \leq \cdots \leq K_{h_2} = G/N$$

de N e G/N, respectivamente. Para cada $i = 0, \ldots, h_2$, existe um único $N_{h_1+i} \trianglelefteq G$, tal que $N \leq N_{h_1+i}$ e $N_{h_1+i}/N = K_i$. Agora, a série normal

$$1 = N_0 \leq N_1 \leq \cdots \leq N_{h_1} = N \leq N_{h_1+1} \leq \cdots \leq N_{h_1+h_2} = G$$

é uma série de Fitting de G. Segue que, $h(G) \leq h(N) + h(G/N)$.

4. De fato, qualquer que seja

$$1 = Q_0 \leq Q_1 \leq \cdots \leq Q_r = Q$$

uma série de Fitting de Q, assumindo sem perda de generalidade que $h \leqslant r$, a série

$$1 \leq G_1 \times Q_1 \leq \cdots \leq G_h \times Q_h \leq G_h \times Q_{h+1} \leq \cdots \leq G_h \times Q_r = G \times Q$$

é uma série de Fitting de $G \times Q$. Então, $h(G \times Q) \leqslant max\{h(G), h(Q)\}$. Mas pelo item 1, obtemos que $max\{h(G), h(Q)\} \leqslant h(G \times Q)$. Isto conclui a prova do item 4 e, portanto, deste lema. □

No que segue, definimos duas séries de subgrupos normais de um grupo finito que, em caso de grupo solúveis, determinam altura de Fitting.

Definição 1.26. Seja G um grupo finito. Definimos o n-ésimo termo da série de Fitting superior de G indutivamente por

$$F_0(G) = 1,\ \frac{F_n(G)}{F_{n-1}(G)} = F\left(\frac{G}{F_{n-1}(G)}\right),\ n \geqslant 1.$$

Similarmente, o n-ésimo termo da série de Fitting inferior de G é definido indutivamente por

$$T_0(G) = G,\ T_n(G) = \gamma_\infty(T_{n-1}(G)),\ n \geqslant 1.$$

Quando não houver ambiguidade sobre qual grupo estamos fazendo considerações, escrevemos F_i em vez de $F_i(G)$ para denotar o i-ésimo termo da série de Fitting superior de G. Faremos o mesmo com a série $T_i(G)$.

Lema 1.27. *A altura de Fitting de um grupo solúvel G é o menor inteiro não negativo h para o qual temos $F_h(G) = G$ e $T_h(G) = 1$.*

Demonstração. É suficiente verificar que para toda série de Fitting

$$1 = G_0 \leq G_1 \leq \cdots \leq G_h = G$$

de G temos $G_i \leq F_i(G)$ e $T_i(G) \leq G_{h-i}$ para todo $i = 0, \ldots, h$, fato que checaremos por indução em i. Claramente, o resultado em ambos os casos vale para $i = 0$. Se assumimos que $G_{i-1} \leq F_{i-1}$, temos que

$$\frac{G_i F_{i-1}}{F_{i-1}} \cong \frac{G_i}{G_i \cap F_{i-1}} \cong \frac{G_i/G_{i-1}}{(G_i \cap F_{i-1})/G_{i-1}},$$

isto é, $G_i F_{i-1}/F_{i-1}$ é um subgrupo normal nilpotente de G/F_{i-1}. Logo, $G_i \leq F_i$. Analogamente, se supomos $T_{i-1} \leq G_{h-i+1}$, temos que $T_i = \gamma_\infty(T_{i-1}) \leq \gamma_\infty(G_{h-i+1}) \leq G_{h-i}$. Portanto, o resultado segue por indução.

Lema 1.28. *Seja G um grupo finito solúvel não trivial. Então*

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

Demonstração. Primeiramente, decorre do Lema 1.27 que $h(G/F(G)) \leq h(G) - 1$. Por outro lado, pelo Lema 1.25 temos que $h(G) \leq h(G/F(G)) + h(F(G)) = h(G/F(G)) + 1$.

Lema 1.29. *Seja G um grupo solúvel finito. Então*

$$h(G) = h(G/\Phi(G)).$$

Demonstração. O resultado é óbvio se $G = 1$. Assumindo que G é não trivial, é suficiente mostrar que $F(G/\Phi(G)) = F(G)/\Phi(G)$. De fato, neste caso pelo Lema 1.28 obteremos

$$h(G/\Phi(G)) = h\left(\frac{G/\Phi(G)}{F(G)/\Phi(G)}\right) + 1 = h(G/F(G)) + 1 = h(G),$$

como afirmado. Para verificar que $F(G)/\Phi(G) = F(G/\Phi(G))$, assuma que $N/\Phi(G) \trianglelefteq G/\Phi(G)$ é um subgrupo nilpotente. Dado p um primo e P um p-subgrupo de Sylow de N, temos que $P\Phi(G) \trianglelefteq G$. Segue do Argumento de Frattini que $G = \Phi(G)PN_G(P)$. Mas pelo Lema 1.4 isto mostra que $G = N_G(P)$, isto é, P é normal em G. O Teorema 1.14 agora nos mostra que N é nilpotente. Concluímos, então, que $F(G)/\Phi(G) = F(G/\Phi(G))$. A prova está completa. □

1.3 Ações de grupo

Definição 1.30. Dizemos que um grupo G age em um conjunto X se para quaisquer elementos $g \in G$ e $x \in X$ existe um elemento bem determinado $x^g \in X$ de forma que para dados $g, h \in G$ e $x \in X$ sempre vale:

1. $x^1 = x$;
2. $x^{gh} = (x^g)^h$.

Se assumimos que um grupo G age sobre um conjunto X, fixado um elemento $g \in G$, a correspondência que associa $x \in X$ a x^g é uma bijeção de X. De fato, ela é invertível pois para cada $x \in X$ temos que $x = x^1 = x^{gg^{-1}} = (x^g)^{g^{-1}}$. Mais do que isto, a correspondência

$$\begin{aligned} \rho : G &\longrightarrow Sym(X) \\ g &\longmapsto \quad g^\rho : X \longrightarrow X \\ &\qquad\qquad x \longmapsto x^g \end{aligned}$$

é um homomorfismo, onde $Sym(X)$ é o grupo das bijeções do conjunto X. Reciprocamente, se nos é dado um homomorfismo $\rho : G \longrightarrow Sym(X)$, obtemos uma ação de G sobre X definindo $x^g := x^{g^\rho}$ para cada $g \in G$ e cada $x \in X$. Em resumo, uma ação de um grupo G sobre um conjunto X determina e é determinada por um homomorfismo $\rho : G \longrightarrow Sym(X)$. O núcleo de ρ é chamado o núcleo da ação e é denotado por $C_G(X)$.

Lema 1.31. *Seja G um grupo agindo sobre um conjunto X, com homomorfismo associado $\rho : G \longrightarrow Sym(X)$. Então, a ação de G em X induz naturalmente uma ação de $G/C_G(X)$ em X.*

Demonstração. Observe que dados $g_1, g_2 \in G$, se $g_1 C_G(X) = g_2 C_G(X)$, para qualquer $x \in X$ temos $x^{g_1 g_2^{-1}} = x$ e então $x^{g_1} = x^{g_2}$. A correspondência

$$\begin{aligned} \overline{\rho} : G/C_G(X) &\longrightarrow \quad Sym(X) \\ gC_G(X) &\longmapsto (gC_G(X))^{\overline{\rho}} : X \longrightarrow X \\ & \qquad\qquad x \longmapsto x^{gC_G(X)} := x^g \end{aligned}$$

é então um homomorfismo bem definido. □

Não é difícil verificar que a ação obtida no Lema 1.31 acima tem núcleo trivial.

Definição 1.32. Dizemos que o grupo G age fielmente sobre X se $C_G(X) = 1$.

Quando consideramos um grupo G agindo sobre um conjunto X podemos definir uma relação de equivalência em X do seguinte modo: $x \sim y$ se existe $g \in G$ tal que $y = x^g$. A classe de equivalência de $x \in X$ é chamada a órbita de x e o conjunto $stab_G(x) = \{g \in G;\ x^g = x\}$ é um subgrupo de G, chamado de estabilizador de x em G. Uma situação particular ao considerarmos uma ação de um grupo G sobre um conjunto X é a de termos uma única órbita. Nomearemos esta situação abaixo.

Definição 1.33. Dizemos que o grupo G age transitivamente sobre o conjunto X se para quaisquer $x, y \in X$ existe $g \in G$ tal que $x^g = y$.

Lema 1.34 (Argumento de Frattini)**.** *Seja G um grupo agindo sobre um conjunto X e suponha que $N \trianglelefteq G$ age transitivamente sobre X. Nestas condições, dado $x \in X$, temos que $G = stab_G(x)N$.*

Demonstração. Dado $g \in G$, usamos a transitividade de N para tomar $n \in N$ de modo que $x^g = x^n$. Mas então $gn^{-1} \in stab_G(x)$. Segue que $g \in stab_G(x)N$. □

Corolário 1.35. *Seja G um grupo finito e $N \trianglelefteq G$. Seja P um p-subgrupo de Sylow de G. Então $G = N_G(P)N$.*

Demonstração. Seja $\Gamma_p(N)$ o conjunto dos p-subgrupos de Sylow de N. Então G age sobre $\Gamma_p(N)$ por conjugação. Adicionalmente, a ação de N sobre $\Gamma_p(N)$ é transitiva. Basta, portanto, aplicar o Lema 1.34. □

Seja G um grupo agindo sobre o conjunto subjacente a um grupo H. Dizemos, neste caso, que G age por automorfismos sobre o grupo H se para quaisquer $g \in G$ e $a, b \in H$ valer $(ab)^g = a^g b^g$. Em outras palavras, sendo $\rho : G \longrightarrow Sym(H)$ o homomorfismo associado à

ação do grupo G sobre o conjunto subjacente de H, então G age por automorfismos em H se, e somente se, $G^{\rho} \leq Aut(H)$.

Nas considerações que se seguem iremos assumir que G e H são grupos e que G age por automorfismos sobre H.

Definição 1.36. Definimos:

1. $C_H(g) = \{h \in H;\ h^g = h\}$ com $g \in G$;
2. $C_H(G) = \{h \in H;\ h \in C_H(g)$ para todo $g \in G\}$;
3. $[h,g] = h^{-1}h^g$ para $g \in G$ e $h \in H$;
4. $[H,G] = \langle [h,g];\ h \in H,\ g \in G \rangle$.

Dizemos que $K \leq H$ é G-invariante se $k^g \in K$ para todos $k \in K$ e $g \in G$. Claramente o subgrupo dos pontos fixos $C_H(G)$ é um subgrupo G-invariante de H. Pode-se mostrar também que $[G,H]$ é um subgrupo normal G-invariante de H.

Quando N é um subgrupo normal G-invariante de H, a ação de G sobre H induz naturalmente uma ação de G no quociente H/N segundo o homomorfismo

$$\begin{aligned} \overline{\rho} : G &\longrightarrow Aut(H/N) \\ g \longmapsto\ g^{\overline{\rho}} &: H/N \longrightarrow H/N \\ hN &\longmapsto (hN)^g := h^g N \end{aligned}$$

e então é razoável nos questionar sobre o subgrupo dos pontos fixos de H/N. De fato, nem sempre ocorre a igualdade $C_H(G)N/N = C_{H/N}(G)$. Esse não é o caso se a ação for coprima, isto é, se G e H tiverem ordens coprimas, como ficará claro no Lema 1.38 a seguir. Antes disto, iremos enunciar um famoso resultado conhecido como Teorema de Schur-Zassenhaus.

Teorema 1.37 ([12], Teorema 6.2.1)**.** *Seja G um grupo finito possuindo um subgrupo normal N que satisfaz $mdc(|N|,[G:N]) = 1$. Então N é complementável, isto é, existe $H \leq G$ tal que $G = NH$ e $N \cap H = 1$. Ainda, todos os complementos de N são conjugados.*

Lema 1.38. *Suponha que G e H sejam finitos e de ordens coprimas e que N é um subgrupo normal G-invariante de H. Então*

(a) $C_{H/N}(G) = C_H(G)N/N$;

(b) Se G age trivialmente em N e em H/N, então G age trivialmente em H;

(c) $H = [H,G]C_H(G)$;

(d) $[H,G] = [H,G,G]$;

(e) Se H *é abeliano, então* $H = [H,G] \times C_H(G)$.

Demonstração. Iremos provar aqui o item (a), as provas dos demais itens podem ser encontradas no Capítulo 8 de [12].

É suficiente mostrar que toda classe $Nh \in C_{H/N}(G)$ contém um elemento de $C_H(G)$. Seja, então, $Nh \in C_{H/N}(G)$. Para cada $g \in G$, temos que $h^g h^{-1} \in N$. Isto significa que no produto semidireto $H \rtimes G$ vale $G^{h^{-1}} \leq GN$. Portanto, ambos G e $G^{h^{-1}}$ são complementos para N em GN. Pelo Teorema 1.37, podemos considerar $n \in N$ para o qual vale $G^n = G^{h^{-1}}$. Defina $c = nh$. Então $c \in N_{HG}(G) \cap Nh$ e também $[G,c] \leq G \cap H = 1$, isto é, $c \in C_H(G)$. □

Corolário 1.39. *Suponha que* G *e* H *sejam finitos e de ordens coprimas. Se* G *age trivialmente sobre* $H/\Phi(H)$*, então* G *age trivialmente sobre* H.

Demonstração. De fato, pelo Lema 1.38 temos que

$$H/\Phi(H) = C_{H/\Phi(H)}(G) = C_H(G)\Phi(H)/\Phi(H),$$

isto é, $H = C_H(G)\Phi(H)$. Segue do Lema 1.4 que $H = C_H(G)$. □

Mesmo quando a ação não é coprima, em condições especiais temos informações sobre o subgrupo dos pontos fixos. Este é o conteúdo do próximo resultado.

Lema 1.40. *Seja* G *um* p*-grupo finito agindo sobre um* p*-grupo finito* Q*. Então* $C_Q(G) \neq 1$.

Demonstração. Admita inicialmente que H é um grupo finito nilpotente e $N \trianglelefteq H$. Afirmamos que $N \cap Z(H) \neq 1$. Sem perda de generalidade podemos supor que N é um subgrupo normal minimal de H. Neste caso, se N não for central em H temos $N = [N,H]$. Mas então $N \leq \gamma_\infty(H)$ e H não é nilpotente, uma contradição.

Agora, nas hipóteses deste lema, consideramos $A = Q \rtimes G$. Então A é um p-grupo finito, logo nilpotente. Temos $Q \trianglelefteq A$ e assim $Q \cap Z(A) \neq 1$. Em particular $C_Q(G) \neq 1$. □

Se G é um grupo agindo sobre um grupo H, vários resultados na literatura mostram que impor condições sobre o subgrupo dos pontos fixos $C_H(G)$ pode nos retornar informações sobre o grupo G. Um dos melhores exemplos é o seguinte resultado, provado por J.G. Thompson em [23].

Teorema 1.41. *Seja* G *um grupo finito possuindo um automorfismo* φ *de ordem prima tal que* $C_G(\varphi) = 1$. *Então* G *é nilpotente.*

Um outro exemplo onde impor condições sobre os centralizadores retorna informações sobre o grupo que age é o seguinte resultado.

Teorema 1.42 ([12], Teorema 8.3.2)**.** *Seja G um grupo finito agindo em um grupo abeliano finito e não trivial V. Suponha que*

$$C_V(g) = 1, \text{ para todo } 1 \neq g \in G.$$

Se G satisfaz uma das seguintes propriedades:

1. *G é abeliano;*
2. *G é um p-grupo, p um primo ímpar;*
3. *G é um 2-grupo não quaternion;*

então G é cíclico.

Dizemos que a ação do grupo G sobre o grupo H é irredutível se os únicos subgrupos G-invariantes de H forem o subgrupo trivial e o próprio grupo H.

Corolário 1.43. *Seja G um grupo finito agindo fielmente e irredutivamente sobre um grupo abeliano V. Então $Z(G)$ é cíclico.*

Demonstração. Dado $g \in Z(G)$, temos que $C_V(g)$ é um subgrupo G-invariante de V. Pela irredutibilidade da ação temos que $C_V(g) = 1$ ou $C_V(g) = V$. Mas se $C_V(g) = V$, então $g = 1$, já que a ação é fiel. O resultado segue do Teorema 1.42. □

Para encerrar este capítulo provaremos a seguinte consequência do Teorema 1.42.

Lema 1.44. *Seja G um grupo finito abeliano não cíclico agindo em um grupo finito abeliano V. Se $mdc(|G|, |V|) = 1$, então*

$$\bigcap_{1 \neq g \in G} [V, g] = 1.$$

Demonstração. Nossa prova é por indução sobre $|V|$. O resultado é óbvio se V é trivial. Assuma que V é não trivial. Neste caso, pelo Teorema 1.42 podemos encontrar $1 \neq h \in G$ para o qual $C_V(h) \neq 1$. Observe que $C_V(h)$ é um subgrupo normal de V, que também é G-invariante, uma vez que G é abeliano. Por isto, podemos considerar a ação induzida de G sobre o quociente $V/C_V(h)$. Por indução, temos que

$$\bigcap_{1 \neq g \in G} \big[V/C_V(h), g\big] = \bigcap_{1 \neq g \in G} [V, g]C_V(h)/C_V(h) = 1.$$

Disto, podemos concluir que $C_V(h)$ contém o subgrupo

$$\bigcap_{1\neq g\in G} [V,g],$$

que também está contido em $[V,h]$. Mas pelo Teorema 1.38, temos que $C_V(h)\cap[V,h]=1$. Então, obtemos

$$\bigcap_{1\neq g\in G} [V,g]=1,$$

como afirmado. □

Capítulo 2

CPPO-grupos solúveis

Neste capítulo temos como objetivo principal provar os resultados obtidos sobre CPPO-grupos solúveis, a saber os Teoremas A e B (veja a Seção 2.1). Na primeira seção deste capítulo iremos introduzir os CPPO-grupos, enunciar os Teoremas A e B e também estabelecer alguns resultados elementares sobre CPPO-grupos. Após isto, na segunda seção, iremos introduzir o conceito de torres de Turull. Iremos verificar alguns resultados que permitem compreender de maneira geral este tipo de ferramenta e posteriormente provaremos alguns resultados auxiliares sobre torres em CPPO-grupos. Concluiremos este capítulo com as provas dos Teoremas A e B.

2.1 CPPO-grupos

Definição 2.1. Um grupo G é chamado um EPPO-grupo se cada elemento de G tem ordem potência de primo.

Existem algumas formas equivalentes de caracterizar os EPPO-grupos, a seguir apresentamos uma que nos será útil.

Proposição 2.2. *Seja G um grupo. Então G é um EPPO-grupo se, e somente se, o centralizador de cada elemento não trivial $g \in G$ é um p-grupo para algum primo $p = p(g)$.*

Demonstração. Primeiramente, assuma que G é um EPPO-grupo e tome $1 \neq g \in G$. Então existe um primo p tal que $|g|$ é potência de p. Agora, como G é EPPO-grupo, qualquer que seja $h \in C_G(g)$, temos que $|gh| = mmc(|g|,|h|)$ é potência de primo. Segue que $|h|$ é potência de p e por razão maior $C_G(g)$ é um p-grupo.

Para a recíproca basta lembrar que $g \in C_G(g)$ para cada $g \in G$. □

Foi G. Higman o primeiro a estudar os EPPO-grupos em seu artigo [8]. Higman classificou os EPPO-grupos finitos solúveis e, no que segue, damos uma ideia da prova desta classificação.

Se G é um EPPO-grupo finito e solúvel, pela Proposição 2.2, $F = F(G)$ é um p-grupo para algum primo p. Se G não for nilpotente, então podemos tomar um número primo $q \in \pi(G) \setminus \{p\}$ e um q-subgrupo Q de G tal que $QF/F = F(G/F)$. Considerando a ação de Q sobre um subgrupo normal minimal de G obtemos da Proposição 2.2 e do Teorema 1.42 que Q não contém subgrupos abelianos elementares de ordem q^2. Portanto, Q é cíclico se $q \neq 2$ e ou Q é cíclico ou *quaternion* generalizado, se $q = 2$. Em qualquer caso, Q contém um subgrupo característico Z de ordem q. Como $QF/F = C_{G/F}(ZF/F)$, segue-se que G/QF é isomorfo a um subgrupo do grupo de autormorfismos de Z. Por isto, G/QF é cíclico de ordem dividindo $q-1$. Tal ordem é potência de um primo r, visto que G é um EPPO-grupo. Mas certamente r não pode ser um terceiro primo, visto que neste caso o grupo não nilpotente QF possuiria um automorfismo de ordem prima livre de pontos fixos, o que contradiria o Teorema 1.41. Então $r = p$. Podemos, enfim, enunciar o resultado de Higman como segue.

Teorema 2.3. *Seja G um EPPO-grupo finito solúvel e seja p um primo tal que $P = O_p(G) \neq 1$. Então G/P tem uma das seguintes estruturas:*

1. *G/P é cíclico de ordem uma potência de um primo diferente de p;*
2. *G/P é um grupo quaternion generalizado e p é ímpar;*
3. *G/P tem ordem $p^a q^b$, q sendo um primo da forma $kp^r + 1$, e os subgrupos de Sylow de G/P são cíclicos.*

Em qualquer caso, $h(G) \leqslant 3$ e no máximo dois primos dividem a ordem de G.

Os EPPO-grupos têm sido fonte de estudo desde o artigo prioneiro de Higman [8]. Em 1962, M. Suzuki ([22]) estudou uma classe de grupos duplo-transitivos com a propriedade que só a identidade deixa fixados 3 ou mais letras e, como consequência deste estudo, classificou os EPPO-grupos finitos simples. Anos depois, R. Brandl em [2] continuou esta investigação em EPPO-grupos não solúveis e, finalmente, em [1] W. Bannuscher e G. Tiedt descreveram a estrutura de todos os EPPO-grupos finitos. Vale aqui comentar que, em 1989, M. Deaconescu ([4]) classificou completamente os grupos finitos nos quais todos os elementos têm ordens primas.

Após trabalhos de W. Yang e Z. Zhang [26] e H. Heineken [7], A.L. Delgado e Yu-Fen Wu conseguiram em [5] descrever a estrutura dos EPPO-grupos localmente finitos. Comentamos aqui também que P. Shumyatsky em [20] considerou EPPO-grupos profinitos mostrando que um tal grupo é virtualmente *pro-p* para algum primo p.

Neste trabalho temos como objetivo estudar uma classe de grupos consideravelmente mais geral que a dos EPPO-grupos, que aqui chamaremos de CPPO-grupos.

Definição 2.4. Um grupo G é chamado um CPPO-grupo se todo comutador de G tem ordem potência de primo.

Evidentemente todo EPPO-grupo é também um CPPO-grupo, mas a recíproca não é verdadeira. Por exemplo, qualquer grupo abeliano é um CPPO-grupo, o que certamente não vale para EPPO-grupos, como mostra a Proposição 2.2.

O Teorema 2.3 mostra que o subgrupo de Fitting de um EPPO-grupo finito é sempre um p-grupo para algum primo p. Isto não é verdade para os CPPO-grupos. Por exemplo, o grupo diedral D_{12} é um CPPO-grupo cujo subgrupo de Fitting tem ordem 6. O Teorema 2.3 ainda estabelece que a altura de Fitting de um EPPO-grupo finito solúvel é no máximo 3. Estabeleceremos esta mesma cota para os CPPO-grupos.

Teorema A. *Um CPPO-grupo finito e solúvel G tem altura de Fitting no máximo 3.*

Dado que todo grupo abeliano é um CPPO-grupo, não é possível limitar o número de primos dividindo a ordem de um CPPO-grupo solúvel finito. Contudo, usando o Teorema A provaremos o seguinte resultado.

Teorema B. *Se G é um CPPO-grupo finito e solúvel, então $|\pi(G')| \leqslant 3$.*

Higman em seu artigo [8] também estudou EPPO-grupos finitos não solúveis e conseguiu verificar que um grupo nestas condições possui um único fator de composição não abeliano que em muito determina a estrutura do grupo. No Capítulo 3 iremos estudar os CPPO-grupos finitos não solúveis utilizando a classificação dada por Suzuki aos EPPO-grupos finitos simples.

Uma vez definida uma nova classe de grupos, algumas questões surgem naturalmente e as primeiras delas são se a classe de grupos é fechada para subgrupos, imagens epimórficas, extensões e produtos diretos. No que segue, iremos responder estas questões.

O seguinte resultado é de simples verificação e por isto omitiremos sua prova.

Lema 2.5. *Subgrupos e quocientes de CPPO-grupos são CPPO-grupos.*

É um exercício prazeroso verificar que todo grupo com ordem no máximo 23 é um CPPO-grupo. Por sua vez o grupo diedral D_{24} não é um CPPO-grupo, o que em particular prova que a classe dos CPPO-grupos não é fechada para extensões. Abaixo, estabelecemos uma condição necessária e suficiente para um grupo diedral ser um CPPO-grupo.

Proposição 2.6. *Seja $G = D_{2n}$ o grupo diedral de ordem $2n$, com $n \geqslant 3$. Então G é um CPPO-grupo se, e somente se, vale uma das seguintes afirmações:*

(a) n é potência de primo.

(b) $2 \mid n$ e $\dfrac{n}{2} > 1$ é potência de um primo ímpar.

Demonstração. Escrevamos $G = \langle a, b;\ a^n = b^2 = 1,\ a^b = a^{-1} \rangle$. Então $G' = \langle a^2 \rangle$. Assuma primeiramente que G é um CPPO-grupo. Então $a^2 = [b,a]$ tem ordem p^k para algum primo p e algum inteiro positivo k. Se n é ímpar, então a e a^2 têm a mesma ordem, isto é, $n = p^k$ é potência de primo. Se n é par, então $n = 2|a^2|$ e então ou (a) ou (b) vale.

Reciprocamente, assuma que (a) ou (b) vale. Em ambas as possibilidades a^2 tem ordem potência de primo e como $G' = \langle a^2 \rangle$ obtemos que G é um CPPO-grupo. □

É simples observar que se G é qualquer CPPO-grupo e H é um grupo abeliano, então $G \times H$ é novamente um CPPO-grupo. Entretanto, verificaremos que não é possível decompor um CPPO-grupo finito não solúvel como produto direto de fatores não abelianos (Lema 2.8 a seguir). Antes, provamos o seguinte resultado.

Lema 2.7 ([19], Lema 3.2)**.** *Seja π um conjunto de primos e seja G um grupo finito. Se todo comutador de G é um π-elemento, então G' é um π-grupo.*

Demonstração. Assuma que o resultado é falso e considere um contraexemplo G de ordem minimal. Pela minimalidade de G devemos ter $O_\pi(G) = 1$. Claramente G não é um π-grupo e podemos tomar $p \in \pi(G) \setminus \pi$. Seja P um p-subgrupo de Sylow de G. Como todo comutador de G é um π-elemento e $[N_G(P), P] \leq P$, temos que P é abeliano e $N_G(P) = C_G(P)$. Podemos então usar o Teorema do Complemento Normal de Burnside (veja [12, Teorema 7.2.1]) para encontrar um p-complemento normal N de P em G. Temos que $O_\pi(N) = 1$ e então a minimalidade de G implica que N é abeliano. A decomposição $N = O_\pi(N) \times O_{\pi'}(N)$ agora mostra que $N = O_{\pi'}(N)$ é um π'-grupo. Concluímos de $G = N \rtimes P$ que G é um π'-grupo. A condição em G agora resulta que $G' = 1$ é um π-grupo, uma contradição. □

Lema 2.8. *Seja $Q = G \times H$ um CPPO-grupo finito. Se ambos G e H são grupos não abelianos, então Q' é um p-grupo, para algum primo p. Em particular, Q é solúvel e $h(Q) \leqslant 2$.*

Demonstração. Tomemos elementos $g_1, g_2 \in G$ tais que $[g_1, g_2] \neq 1$. Como Q é um CPPO-grupo, $|[g_1, g_2]|$ é potência de p, para algum número primo p. Quaisquer que sejam $h_1, h_2 \in H$ tais que $[h_1, h_2] \neq 1$, a igualdade

$$[h_1 g_1, h_2 g_2] = [h_1, h_2][g_1, g_2] \tag{2.1}$$

mostra que $[h_1, h_2]$ tem ordem potência de p. Repetindo o argumento agora com $[h_1, h_2]$ no lugar de $[g_1, g_2]$ obtemos que todo comutador de G tem ordem potência de p. A igualdade

em (2.1) agora mostra que todo comutador de Q é um p-elemento. Concluímos usando o Lema 2.7 que Q' é um p-grupo. □

Como uma consequência da prova do Lema 2.8 temos a seguinte caracterização dos CPPO-grupos finitos nilpotentes.

Corolário 2.9. *Seja G um grupo finito nilpotente. Então G é um CPPO-grupo se, e somente se, $O_{p'}(G) \leq Z(G)$ para algum número primo p.*

No que segue, iremos mostrar que um subgrupo finito normal e nilpotente de um CPPO-grupo G é próximo de ser central em G, em um sentido que ficará claro no Lema 2.10 abaixo. Antes disto, lembramos que se um grupo G admite uma decomposição $G = H \cup K$, com H e K subgrupos de G, então ou $G = H$ ou $G = K$.

Lema 2.10. *Seja N um subgrupo finito, normal e nilpotente de um CPPO-grupo G. Então $O_{p'}(N) \leq Z(G)$ para algum número primo p.*

Demonstração. Se N é central em G, nada temos a provar. Suponha que N não é central. Então existe um primo p tal que o p-subgrupo de Sylow P de N não é central em G. Escrevamos $N = P \times O_{p'}(N)$. Afirmamos que $G = C_G(P) \cup C_G(O_{p'}(N))$. De fato, em caso contrário, existem $a \in P$, $b \in O_{p'}(N)$ e $g \in G$ para os quais $[a,g] \neq 1$ e $[b,g] \neq 1$. Mas então o elemento $[ab,g] = [a,g][b,g] \in N$ tem ordem divisível por primos distintos, um absurdo. Isto mostra que $G = C_G(P) \cup C_G(O_{p'}(N))$. Mas P não é central em G, isto é, $C_G(P) < G$. Então $G = C_G(O_{p'}(N))$ e $O_{p'}(N) \leq Z(G)$. □

2.2 Torres de Turull

Nesta seção iremos introduzir as torres de Turull, ferramenta principal para estabelecer as provas dos Teoremas A e B. Adicionalmente, provaremos lemas técnicos para auxiliar o entendimento destas ferramentas e também estabeleceremos alguns resultados sobre torres em CPPO-grupos.

Para auxiliar o compreendimento da definição das torres de Turull iremos provar o seguinte lema.

Lema 2.11. *Sejam H, K e L grupos. Suponha que H aja sobre K e KH aja sobre L. Dado um subgrupo normal KH-invariante N de L temos que $C_K(L/N)$ é H-invariante.*

Demonstração. De fato, para quaisquer $h \in H$, $k \in C_K(L/N)$ e $l \in L$ vale

$$(lN)^{k^h} = l^{k^h}N = ((l^{h^{-1}})^k)^h N = ((l^{h^{-1}}N)^k)^h = lN,$$

de modo que $k^h \in C_K(L/N)$. □

Definição 2.12. Seja G um grupo finito. Dizemos que uma sequência $(P_i)_{i=1,\ldots,h}$ de subgrupos de G é uma torre de G de altura h se valem as seguintes condições:

(a) P_i é um p_i-grupo para cada $i = 1, \ldots, h$.

(b) $[P_i, P_j] \leq P_j$ sempre que $i < j$.

(c) Pondo $\overline{P_h} = P_h$ e

$$\overline{P_i} = {}^{P_i}\!/_{C_{P_i}(\overline{P_{i+1}})},\ i = 1, \ldots, h-1,$$

então $\overline{P_i}$ é não trivial para todo i.

(d) $p_i \neq p_{i+1}$ para todo $i = 1, \ldots, h-1$.

Exemplo 2.13. Seja $G = S_4$ o grupo simétrico de grau 4. Seu subgrupo de Fitting é o subgrupo $V = \langle (12)(34), (13)(24) \rangle$. Considere os subgrupos $\langle (12) \rangle$ e $\langle (123) \rangle$ e veja que $(123)^{(12)} = (132) = (123)^{-1}$. Como V contém seu centralizador em G (Lema 1.20), a sequência $(\langle (12) \rangle, \langle (123) \rangle, V)$ é uma torre de G.

Notação. Quando estivermos considerando uma torre $(P_i)_{i=1,\ldots,h}$ de um grupo finito G, iremos sempre escrever p_i para denotar o primo que divide a ordem do subgrupo correspondente P_i. Ainda, sendo H um subgrupo de P_i, iremos sempre denotar por $\overline{H}$ a imagem de H no correspondente grupo quociente $\overline{P_i}$ da Definição 2.12.

Na seção seguinte iremos utilizar sem menção prévia o fato de que se $(P_1, \ldots, P_h)$ é uma torre de um grupo finito G, então $(P_1, \ldots, P_i)$ é uma torre de G para todo $i \leqslant h$. Este fato é justificado nas linhas que se seguem. Abaixo, estabelecemos uma versão mais forte do Lema 3.6 de [3].

Lema 2.14. *Seja G um grupo finito e seja $(P_i)_{i=1,\ldots,h}$ uma torre de G. Para quaisquer $1 \leqslant i < j \leqslant h$ vale $C_{P_i}(P_j) \leq C_{P_i}(\overline{P_{i+1}})$.*

Demonstração. Fixado $1 < j \leqslant h$, argumentamos por indução sobre $j - i$ que

$$C_{P_i}(P_j) \leq C_{P_i}(\overline{P_{i+1}}).$$

Isto claramente vale se $j - i = 1$. Assuma $j - i > 1$ e observe que

$$[C_{P_i}(P_j), P_j, P_{i+1}] = 1 = [P_j, P_{i+1}, C_{P_i}(P_j)].$$

Pelo Lema dos Três Subgrupos temos que $[P_{i+1}, C_{P_i}(P_j), P_j] = 1$. Isto significa que

$$[C_{P_i}(P_j), P_{i+1}] \leq C_{P_{i+1}}(P_j),$$

e segue da hipótese de indução que

$$[C_{P_i}(P_j), P_{i+1}] \leq C_{P_{i+1}}(P_j) \leq C_{P_{i+1}}(\overline{P_{i+2}}).$$

Obtemos pois que $C_{P_i}(P_j) \leq C_{P_i}(\overline{P_{i+1}})$, o que nos dá o resultado. □

Como corolário imediato do Lema 2.14 temos o seguinte resultado.

Corolário 2.15. *Se $(P_i)_{i=1,\ldots,h}$ é uma torre de um grupo finito G, então $(P_i)_{i=1,\ldots,k}$ é uma torre de G para todo $1 \leqslant k \leqslant h$.*

A definição de torre evidencia que as imagens dos termos de uma torre em um quociente não necessariamente formará uma torre neste quociente. O seguinte lema dá uma condição suficiente para que este incômodo não ocorra.

Lema 2.16 ([3], Lema 3.6)**.** *Seja $(P_i)_{i=1,\ldots,h}$ uma torre de um grupo finito G com $h \geqslant 2$. Seja $N \trianglelefteq G$ tal que $N \cap P_i \leqslant C_{P_i}(P_h)$, $i = 1, \ldots, h-1$. Então $(P_iN/N)_{i=1,\ldots,h-1}$ é uma torre de G/N.*

Demonstração. Observe que é suficiente verificar o item (c) da Definição 2.12 para a sequência $(Q_i)_{i=1,\ldots,h-1}$, onde $Q_i := P_iN/N$. Sejam $(\overline{P_i})$ e $(\overline{Q_i})$ as sequências associadas a (P_i) e (Q_i), respectivamente, como na Definição 2.12. Então, é suficiente mostrar que o grupo $\overline{Q_i}$ tem um quociente isomorfo a $\overline{P_i}$ para cada $i < h$.

Considere para cada $i \leqslant h-2$ um subgrupo L_i de P_i de modo que $L_iN/N = C_{Q_i}(\overline{Q_{i+1}})$ e defina $L_{h-1} = 1$. Pelas considerações do primeiro parágrafo, a prova estára completa se mostrarmos que $L_i \leq R_i$, para todo $i < h$, onde $R_i = C_{P_i}(\overline{P_{i+1}})$. De fato, pelo Lema 2.14 sabemos que $P_i \cap N = R_i \cap N$, e por isto

$$\overline{Q_i} \cong P_iN/L_iN \cong P_i/P_i \cap L_iN = P_i/L_i(P_i \cap N) = P_i/L_i(R_i \cap N).$$

Portanto, se $L_i \leq R_i$ então $\overline{Q_i}$ tem $\overline{P_i}$ por quociente, como requerido no primeiro parágrafo.

Nas linhas que se seguem, argumentaremos por indução em $h - i > 0$ que $L_i \leq R_i$, o que é óbvio para $h - i = 1$. Se $h - i = 2$, temos por definição de L_{h-2} que $[L_{h-2}N/N, Q_{h-1}] = 1$. Isto é,

$$[L_{h-2}, P_{h-1}] \leq P_{h-1} \cap N = R_{h-1} \cap N \leq R_{h-1},$$

o que significa que L_{h-2} age trivialmente sobre $\overline{P_{h-1}}$ e, portanto, $L_{h-2} \leq R_{h-2}$. Assuma $h-i>2$. Por definição de L_i e L_{i+1} temos que $[L_iN/N, Q_{i+1}] \leq L_{i+1}N/N$. Agora, a hipótese de indução nos dá que $L_{i+1} \leq R_{i+1}$. Segue-se que

$$[L_i, P_{i+1}] \leq P_{i+1} \cap R_{i+1}N = R_{i+1}(P_{i+1} \cap N) = R_{i+1}(R_{i+1} \cap N) = R_{i+1},$$

ou seja, L_i age trivialmente no grupo $\overline{P_{i+1}}$ e então $L_i \leq R_i$. O passo indutivo está verificado e portanto a prova está completa. □

Um fato bem conhecido é que o grupo de automorfismos de um grupo cíclico G de ordem finita n é um grupo abeliano de ordem $\phi(n)$, onde ϕ denota a função Totiente de Euler. Em particular, se $n = 2^k$, então $Aut(G)$ é abeliano de ordem 2^{k-1}.

Lema 2.17. *Seja (P_i) uma torre de altura $h \geqslant 3$ em um grupo finito G. Então P_i é não cíclico para cada $i \geqslant 3$. Se $p_2 = 2$, então também P_2 é não cíclico.*

Demonstração. Suponha por contradição que P_i é cíclico para algum $i \geqslant 3$. Então para quaisquer $a \in P_{i-2}$ e $b \in P_{i-1}$, os automorfismos de P_i induzidos por a e b comutam. Isto significa que $[a,b] \in C_{P_{i-1}}(P_i) \leq C_{P_{i-1}}(\overline{P_i})$. Pela escolha arbitrária de a e b, obtemos que $\overline{P_{i-2}} = 1$, o que contradiz a definição de torre. Ainda, se $p_2 = 2$ e P_2 é cíclico, então temos que $\overline{P_1} \leq Aut(P_2)$ é trivial, uma nova contradição. □

Para os cálculos que iremos fazer será necessário ter em mãos mais informações sobre os termos P_i de uma torre de um grupo finito G do que se encontra na Definição 2.12. Felizmente, o tipo específico de torre que definimos abaixo contém informações descritivas de seus termos.

Definição 2.18. Seja G um grupo finito e seja (P_i) uma torre de G de altura h. Dizemos que a torre é irredutível se valem as seguintes condições:

(a) $\Phi(\overline{P_i}) \leq Z(\overline{P_i})$, $\Phi(\Phi(\overline{P_i})) = 1$ e se $p_i \neq 2$, então $exp(\overline{P_i}) = p_i$ para $i = 1, \ldots, h$ e P_{i-1} centraliza $\Phi(\overline{P_i})$ para cada $i = 2, \ldots, h$.

(b) P_1 é cíclico e $\overline{P_1}$ tem ordem prima.

(c) Existe um subgrupo abeliano elementar H_i de $\overline{P_{i-1}}$ tal que $[H_i, \overline{P_i}] = \overline{P_i}$, para cada $i = 2, \ldots, h$.

(d) Se $Q \leq P_i$ é $P_1 \cdots P_{i-1}$-invariante e $\overline{Q} \not\leq \Phi(\overline{P_i})$, então $Q = P_i$.

O leitor pode notar que nossa definição de torre irredutível difere da definição dada por A. Turull em [24] somente no item (b). Contudo, se $(P_1,\dots,P_h)$ é qualquer torre de um grupo finito G, podemos tomar $a \in P_1 \setminus C_{P_1}(\overline{P_2})$, de modo que a sequência $(\langle a\rangle, P_2,\dots,P_h)$ é uma torre de G. Então o Lema 1.4 de [24] permite-nos encontrar uma torre irredutível de mesma altura a qual por sua vez satisfaz todos os itens da Definição 2.18.

Exemplo 2.19. A sequência $(\langle(12)\rangle, \langle(123)\rangle, V)$ é uma torre irredutível de S_4.

A seguinte proposição explica o termo "*irredutível*" na Definição 2.18.

Proposição 2.20. *Suponha que $(P_i)_{i=1,\dots,h}$ seja uma torre irredutível de um grupo G. Para cada $1 < i \leqslant h$, a ação de $P_1\cdots P_{i-1}$ sobre $\overline{P_i}/\Phi(\overline{P_i})$ é irredutível e, portanto, o grupo $P_1\cdots P_{i-1}/C_{P_1\cdots P_{i-1}}(\overline{P_i}/\Phi(\overline{P_i}))$ tem centro cíclico.*

Demonstração. Seja V um subgrupo $P_1\cdots P_{i-1}$-invariante de $\overline{P_i}/\Phi(\overline{P_i})$. Podemos, então, achar um subgrupo $P_1\cdots P_i$-invariante Q de P_i para o qual vale $\overline{Q}\Phi(\overline{P_i})/\Phi(\overline{P_i}) = V$. Agora, se $V \neq 1$, então $\overline{Q} \not\leq \Phi(\overline{P_i})$ e pela Definição 2.18 obtemos $Q = P_i$. Segue que $V = \overline{P_i}/\Phi(\overline{P_i})$. Portanto, a ação é irredutível. O grupo $P_1\cdots P_{i-1}/C_{P_1\cdots P_{i-1}}(\overline{P_i}/\Phi(\overline{P_i}))$ consequentemente tem centro cíclico, como estabelece o Corolário 1.43. □

É razoável esperar que, se (P_i) é uma torre de um grupo finito G, seja possível encontrar uma torre irredutível de G que seja, de alguma forma, relacionada com (P_i). No que segue mostramos que de uma tal torre é possível encontrar uma torre irredutível de G de mesma altura.

Definição 2.21. Dadas duas torres $(P_i^{(1)})$ e $(P_i^{(2)})$ de um grupo finito G, de alturas h_1 e h_2, respectivamente, dizemos que $(P_i^{(1)})$ está contida em $(P_i^{(2)})$ se existe uma função crescente $f : \{1,\dots,h_1\} \longrightarrow \{1,\dots,h_2\}$ tal que $P_i^{(1)} \subseteq P_{f(i)}^{(2)}$ para cada $i = 1,\dots,h_1$.

Lema 2.22 ([24], Lema 1.4)**.** *Seja (P_i) uma torre de um grupo finito G. Então (P_i) contém uma torre irredutível de mesma altura.*

Demonstração. Assuma que o resultado não seja válido. Então podemos considerar um grupo G possuindo uma torre (P_i) que não contém torre irredutível e com h sendo menor possível. Claramente $h > 1$.

Observe que qualquer torre propriamente contida em (P_i) e de mesma altura não pode conter uma torre irredutível de mesma altura, então sem perda de generalidade podemos supor que (P_i) não contém propriamente uma torre de mesma altura. Podemos também supor $G = P_1\cdots P_h$.

Podemos trocar o item (d) da Definição 2.18 pela seguinte condição mais fraca

$$(d'). \quad \overline{P_i}/\Phi(\overline{P_i}) \text{ é } P_1\cdots P_{i-1}\text{-irredutível.}$$

De fato, se (d') é assumido e $Q \leq P_i$ é $P_1\cdots P_{i-1}$-invariante, se $\overline{Q} \not\leq \Phi(\overline{P_i})$, por (d') e a minimalidade de (P_i) obtemos $Q = P_i$.

Como $P_h \trianglelefteq G$, temos $N = C_G(P_h) \trianglelefteq G$. O Lema 2.16 nos dá que $(P_iN/N)_{i=1,\ldots,h-1}$ é uma torre de G/N, que é minimal pela minimalidade de (P_i). Por isto, os itens da Definição 2.18 valem, com (d) trocado por (d'), para $i = 1,\ldots,h-1$.

Considere $Q \subseteq P_h$ normal em G e minimal com a propriedade que $C_{\overline{P_{h-1}}}(Q) \neq \overline{P_{h-1}}$. Por (d') temos que $C_{\overline{P_{h-1}}}(Q) \leq \Phi(\overline{P_{h-1}})$. Assim, se $h > 2$ temos que

$$C_{P_{h-2}}(\overline{P_{h-1}}) = C_{P_{h-2}}(\overline{P_{h-1}}/C_{\overline{P_{h-1}}}(Q)),$$

de modo que $(P_1,\ldots,P_{h-1},Q)$ é uma torre. A minimalidade de (P_i) agora mostra que $Q = P_h$.

Agora, $\Phi(P_h)$ é um subgrupo normal de G propriamente contido em P_h. Pelas considerações do último parágrafo, obtemos que P_{h-1} centraliza $\Phi(P_h)$. Em particular, como $P_h = [P_h,P_{h-1}]$ obtemos $P_h \leq [P_h,C_G(\Phi(P_h))]$, isto é, $\Phi(P_h) \leq Z(P_h)$.

Por sua vez, P_{h-1} não centraliza $\Omega_1(P_h/P_h')$ e obtemos pela minimalidade que $\Phi(P_h) \leq P_h'$. Em particular, dados elementos $g,h \in P_h$ temos $[g,h]^{p_h} = [g,h^{p_h}] = 1$, de modo que $\Phi(P_h)$ é um grupo abeliano gerado por elementos de ordem p_h. Isto significa que $\Phi(\Phi(P_h)) = 1$.

Para concluir a prova, é suficiente observar que como P_{h-1} é irredutível sobre $P_h/\Phi(P_h)$ temos que $P_1\cdots P_{h-1}$ é irredutível sobre $P_h/\Phi(P_h)$. O item (c) agora segue de (d'). □

Lema 2.23 ([24], Lema 1.6)**.** *Seja G um grupo finito e seja $N \trianglelefteq G$. Suponha que $(Q_i)_{i=1,\ldots,h}$ é uma torre do grupo G/N. Então existe uma torre $(P_i)_{i=1,\ldots,h}$ de G tal que para cada $i = 1,\ldots,h$ vale $P_iN/N = Q_i$.*

O ponto chave que permite-nos estudar a altura de Fitting de um grupo finito solúvel através de suas torres de Turull é o seguinte resultado.

Lema 2.24 ([24], Lema 1.9)**.** *Seja G um grupo finito solúvel. Então*

$$h(G) = max\{h;\ G \textit{ contém uma torre de altura } h\}.$$

Demonstração. Inicialmente, afirmamos que se G possui uma torre de altura h, digamos $(P_1,\ldots,P_h)$, então $h \leqslant h(G)$. De fato, sem perda de generalidade podemos supor que esta torre é irredutível. Neste caso, para $i = 2,\ldots,h-1$ podemos escrever $P_i = [P_i,P_{i-1}]C_{P_i}(\overline{P_{i+1}})$.

Recursivamente, obtemos a igualdade

$$P_i = [P_i, \ldots, [P_3, [P_2, P_1]] \ldots] C_{P_i}(\overline{P_{i+1}}),\ i = 2, \ldots, h-1.$$

Agora como $p_1 \neq p_2$, pelo Lema 1.38, temos que $[P_2, P_1] = [P_2, P_1, P_1]$, o que significa que $[P_2, P_1] \leq T_1(G)$. Analogamente, $[P_3, [P_2, P_1]] = [P_3, [P_2, P_1], [P_2, P_1]]$ e, consequentemente, $[P_3, [P_2, P_1]] \leq T_2(G)$. Repetindo este argumento obteremos que

$$[P_{h-1}, \ldots, [P_3, [P_2, P_1]] \ldots] \leq T_{h-2}(G).$$

Concluímos pois que

$$P_h = [P_h, [P_{h-1}, \ldots, [P_3, [P_2, P_1]] \ldots]] \leq T_{h-1}(G),$$

isto é, $h \leqslant h(G)$, como afirmado.

Suponha, agora, que o resultado seja falso e seja G um contraexemplo de ordem minimal. Para cada $1 \neq M \trianglelefteq G$ temos que $h(G/M) < h(G)$ e então $F(G) = O_p(G)$ para algum número primo p. Considere $(H_1, \ldots, H_{h-1})$ uma torre irredutível de $G/F(G)$, onde $h = h(G)$. Pelas considerações do parágrafo acima temos

$$H_{h-1} \leq T_{h-2}(G)F(G)/F(G) \leq F_2(G)/F(G),$$

isto é, $p_{h-1} \neq p$. Por fim, seja $(P_1, \ldots, P_{h-1})$ uma torre de G tal que $P_iF(G)/F(G) = H_i$, para $i = 1, \ldots, h-1$. O Lema 1.20 agora nos permite concluir que, pondo $P_h = F(G)$, a sequência $(P_1, \ldots, P_h)$ é uma torre de G, o que contradiz a escolha de G. □

No que segue iremos provar alguns resultados sobre torres em CPPO-grupos que serão de fundamental importância na prova do Teorema A. Antes provamos o seguinte lema.

Lema 2.25. *Seja $G = V\langle a \rangle$ um grupo finito com $V \trianglelefteq G$ e $mcd(|a|, |V|) = 1$. Se $v \in V$ é tal que o elemento av tem ordem coprima com $|V|$, então $v \in [V, a]$.*

Demonstração. Trabalhamos no grupo quociente $G/[V, a]$, onde a e V comutam, então sem perda de generalidade podemos supor $[V, a] = 1$. Neste caso, escrevendo $m = |av|$, temos $1 = a^m = v^m$. Portanto, $v = 1$. □

O Lema 2.26 e o Lema 2.28, que estabeleceremos a seguir, são os passos cruciais presentes na argumentação da prova do Teorema A.

Lema 2.26. *Seja G um grupo finito e suponha que G contém uma torre $(P_i)_{i=1,2,3}$ de subgrupos abelianos. Suponha que P_1 seja cíclico e que $P_2 = [P_2, P_1]$ seja não cíclico. Então G não é um CPPO-grupo.*

Demonstração. Assuma por contradição que G é um CPPO-grupo. Sem perda de generalidade podemos assumir $G = P_1P_2P_3$ e então $P_3 \trianglelefteq G$. Escreva $P_1 = \langle a \rangle$. Pelo Lema 1.38, note que $C_{P_2}(a) = 1$. Dados quaisquer $1 \neq b \in P_2$ e $c \in P_3$, o elemento $[c,a][a,b] = [cb^{-1},a]^b$ tem ordem potência de primo. Sua ordem então é uma potência de p_2. O Lema 2.25 agora nos mostra que $[c,a] \in [P_3,[a,b]]$ e, pela escolha arbitrária de $c \in P_3$ e $1 \neq b \in P_2$, concluimos que

$$[P_3,P_1] = [P_3,a] \leq \bigcap_{1 \neq b \in P_2} [P_3,[a,b]] = \bigcap_{1 \neq b \in P_2} [P_3,b].$$

Mas P_2 é um grupo abeliano não cíclico. Segue do Lema 1.44 que $[P_3,P_1] = 1$, isto é, $C_{P_1}(P_3) = P_1$. Usando o Lema 2.14, concluimos que $C_{P_1}(\overline{P_2}) = P_1$, isto é, $\overline{P_1} = 1$, o que contradiz a definição de torre. Esta contradição prova o resultado. □

A seguir estabelecemos um lema técnico para simplificação da prova do Lema 2.28.

Lema 2.27. *Seja φ um automorfismo coprimo de um p-grupo finito extraespecial P tal que $C_P(\varphi) = \Phi(P)$. Então todo elemento de $P \setminus \Phi(P)$ é conjugado a um elemento da forma $[x,\varphi]$ para uma conveniente escolha de $x \in P$.*

Demonstração. Note que a correspondência $\overline{b} \mapsto [\overline{b},\varphi]$ é um automorfismo de $\overline{P} = P/\Phi(P)$. Dado um elemento $b \in P \setminus \Phi(P)$, achemos elementos $x \in P$ e $k \in \Phi(P)$ tais que possamos escrever $b = [x,\varphi]k$. Claramente $[x,\varphi] \notin \Phi(P)$ e existe $y \in P$ de modo que $[x,\varphi,y] \neq 1$. Então $[x,\varphi,y]$ é um gerador de $\Phi(P)$ e para algum $r \in \mathbb{Z}$ temos que $[x,\varphi,y]^r = k^{-1}$. Finalmente, obtemos

$$b^{y^r} = ([x,\varphi]k)^{y^r} = [x,\varphi][x,\varphi,y^r]k = [x,\varphi][x,\varphi,y]^r k = [x,\varphi],$$

como afirmado. □

Lema 2.28. *Seja $(P_i)_{i=1,2,3}$ uma torre de um grupo finito G satisfazendo as seguintes condições:*

(a) P_1 é cíclico;

(b) P_2 é extraespecial e $C_{P_2}(P_1) = \Phi(P_2)$;

(c) P_3 é abeliano e $P_3 = [P_3,\Phi(P_2)]$.

Se G é um CPPO grupo, então $p_2 = 2$ e P_2 é isomorfo a Q_8.

Demonstração. Seja $P_1 = \langle a \rangle$. Para quaisquer $b \in P_2 \setminus \Phi(P_2)$ e $c \in P_3$, veja que o elemento $[c,a][a,b] = [cb^{-1},a]^b$ tem ordem potência de primo e, por isto, usando o Lema 2.25 obtemos $[c,a] \in [P_3,[a,b]]$. Adicionalmente, sendo $1 \neq z \in \Phi(P_2)$, veja que o elemento $[c,z][c,a]^z[a,b] = [cb^{-1},az]^b$ tem ordem potência de primo e usando novamente o Lema 2.25 obtemos $[c,z][c,a]^z \in [P_3,[a,b]]$. Mas como $[P_3,[a,b]]$ é $\Phi(P_2)$-invariante, segue que $[c,z] \in [P_3,[a,b]]$. A arbitrariedade da escolha de $c \in P_3$ nos permite concluir que

$$P_3 = [P_3,\Phi(P_2)] = [P_3,z] \leq [P_3,[a,b]],$$

isto é, usando agora a arbitrariedade da escolha de b, temos

$$P_3 = [P_3,[a,b]], \text{ para todo } b \in P_2 \setminus \Phi(P_2).$$

Ora, pelo Lema 2.27 cada elemento de $P_2 \setminus \Phi(P_2)$ é conjugado a um elemento da forma $[x,a]$ para uma conveniente escolha de $x \in P_2$. Concluimos portanto que $P_3 = [P_3,b]$, e assim $C_{P_3}(b) = 1$, para todo $1 \neq b \in P_2$. O Teorema 1.42 agora nos permite concluir que $p_2 = 2$ e que P_2 é um grupo *quaternion*. Uma vez que Q_8 é o único grupo *quaternion* extraespecial, segue finalmente que $P_2 \cong Q_8$. □

Provaremos agora dois lemas técnicos sobre torres de altura 4 em CPPO-grupos com intuito de simplificar a prova do Teorema A.

Lema 2.29. *Seja G um CPPO-grupo finito e seja (P_1,P_2,P_3,P_4) uma torre irredutível de G tal que*

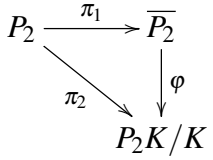
1. $C_{P_3}(P_4) = 1$;
2. P_4 *é abeliano elementar.*

Nestas condições, o grupo $\overline{P_i}$ é ou abeliano ou extraespecial, com $i \in \{2,3\}$.

Demonstração. Inicialmente, note que, como a torre é irredutível, é suficiente verificar que $\Phi(\overline{P_i})$ é cíclico. De fato, seja Q a imagem inversa de $Z(\overline{P_i})$ em P_i. Assim definido, Q é um subgrupo $P_1 \cdots P_{i-1}$-invariante de P_i. O item (d) da Definição 2.18 mostra agora que se $Z(\overline{P_i}) \not\leq \Phi(\overline{P_i})$, então $Q = P_i$, isto é, $\overline{P_i} = Z(\overline{P_i})$ é abeliano. Mas pelo item (a) da Definição 2.18 já sabemos que $\Phi(\overline{P_i}) \leq Z(\overline{P_i})$ e que $\Phi(\Phi(\overline{P_i})) = 1$. Então $\Phi(\overline{P_i})$ é abeliano elementar e ou $\Phi(\overline{P_i}) = Z(\overline{P_i})$ ou $\overline{P_i}$ é abeliano.

Mostraremos primeiramente que $\Phi(\overline{P_2})$ é cíclico. Para isto, seja K o núcleo da ação de P_1P_2 sobre $P_3/\Phi(P_3)$. Como $C_{P_3}(P_4) = 1$, $P_3 = \overline{P_3}$ e usando a Proposição 2.20 obtemos que P_1P_2/K tem centro cíclico. Portanto, é suficiente verificar que $\Phi(\overline{P_2})$ é isomorfo a um

subgrupo central de P_1P_2/K. Observe que como $p_2 \neq p_3$, segue do Corolário 1.39 que $P_2 \cap K = C_{P_2}(P_3)$. Logo, a correspondência $\varphi : \overline{P_2} \longrightarrow P_2K/K$ dada por $bC_{P_2}(P_3) \mapsto bK$ é um isomorfismo que torna comutativo o diagrama



onde π_1 e π_2 são as projeções canônicas. Pondo

$$Q = \pi_2^{-1}(\Phi(P_2K/K)),$$

vem do item (a) da Definição 2.18 que $[Q, P_1P_2] \leq C_{P_2}(P_3) \leq K$ e, consequentemente,

$$[P_1P_2/K, \Phi(P_2K/K)] = 1.$$

Portanto, φ induz um isomorfismo de $\Phi(\overline{P_2})$ em um subgrupo central de P_1P_2/K.

Agora iremos mostrar que $\Phi(P_3)$ é cíclico. Para isto, seja $L = C_{P_1P_2P_3}(P_4)$. Pela Proposição 2.20 temos que $P_1P_2P_3/L$ tem centro cíclico. Então, como $C_{P_3}(P_4) = 1$ é suficiente mostrar que $\Phi(P_3) \leq Z(P_1P_2P_3)$. Já sabemos do item (a) da Definição 2.18 que $\Phi(P_3) \leq Z(P_2P_3)$. Então, se $\Phi(P_3) \not\leq Z(P_1P_2P_3)$, podemos tomar $a \in P_1$ e $c \in \Phi(P_3)$ tal que $[c,a] \neq 1$. Sendo P_1 cíclico, podemos assumir que $P_1 = \langle a \rangle$ e tomar $b \in P_2$ para o qual $[b,a] \neq 1$. Segue-se que o comutador $[cb,a] = [c,a][b,a]$ tem ordem divisível por 2 primos, um absurdo. Concluímos que $\Phi(P_3) \leq Z(P_1P_2P_3)$. □

Se adicionarmos ao resultado anterior a condição de $\overline{P_2}$ ser extraespecial, o Lema 2.28 nos permite conhecer o grupo $\overline{P_2}$.

Lema 2.30. *Seja (P_1, P_2, P_3, P_4) uma torre irredutível de um CPPO-grupo finito G tal que*

1. *$\overline{P_2}$ é extraespecial;*
2. *$C_{P_3}(P_4) = 1$;*
3. *P_4 é abeliano elementar.*

Então $p_2 = 2$ e $\overline{P_2}$ é isomorfo ao grupo Q_8.

Demonstração. Considere $N = C_{P_2}(P_3)\Phi(P_3)$. Observe que

$$C_{P_2N/N}(P_3N/N) = \{gN;\ g \in P_2 \text{ e } [g, P_3] \leq N\} = 1.$$

Portanto, segue do Lema 2.16 que $(P_iN/N)_{i=1,2,3}$ é uma torre de $P_1P_2P_3/N$. Por um lado, temos que

$$P_2N/N = [P_2N/N, P_1N/N],$$

o que implica que

$$C_{P_2N/N}(P_1N/N) \leq \Phi(P_2N/N).$$

Por outro lado, a correspondência $bN \mapsto bC_{P_2}(P_3)$ define um isomorfismo ψ de P_2N/N em $\overline{P_2}$ tornando comutativo o seguinte diagrama

$$\begin{array}{ccc} P_2 & \xrightarrow{\pi_1} & P_2N/N \\ & \searrow^{\pi_2} & \downarrow \psi \\ & & \overline{P_2} \end{array}$$

onde π_1 e π_2 são as projeções canônicas. Seja $Q = \pi_1^{-1}(\Phi(P_2N/N))$. Pela irredutibilidade da torre (P_1, P_2, P_3, P_4) temos que $[Q, P_1] \leq C_{P_2}(P_3)$ e por isto vale que

$$[\Phi(P_2N/N), P_1N/N] = 1.$$

Concluímos pois que

$$C_{P_2N/N}(P_1N/N) = \Phi(P_2N/N).$$

Agora, note que $Q \trianglelefteq P_1P_2$ e assim $[P_3, Q]$ é um subgrupo P_1P_2-invariante de P_3. Sendo $p_2 \neq p_3$, não podemos ter $[P_3, Q] \leq \Phi(P_3)$, vide Corolário 1.39. Segue da irredutibilidade da torre (P_1, P_2, P_3, P_4) que $P_3 = [P_3, Q]$. Consequentemente,

$$[P_3N/N, \Phi(P_2N/N)] = P_3N/N.$$

Pelas considerações acima, a torre $(P_iN/N)_{i=1,2,3}$ está nas condições do Lema 2.28. Concluímos pois que $p_2 = 2$ e P_2N/N é isomorfo a Q_8. Lembrando que P_2N/N e $\overline{P_2}$ são isomorfos, segue que $\overline{P_2}$ é isomorfo a Q_8. □

2.3 Provas dos Teoremas A e B

Para provarmos os Teoremas A e B necessitamos de mais um lema técnico que provaremos a seguir.

Lema 2.31. *Seja φ um automorfismo involutivo de $G \cong Q_8$. Existe $u \in G$ tal que $[u, \varphi]$ é a involução de G.*

Demonstração. Assuma que o resultado seja falso. Pelo Lema 1.40 podemos tomar $u \in G \setminus \Phi(G)$ de modo que $(u\Phi(G))^{\varphi} = u\Phi(G)$. Assim, $[u,\varphi] \in \Phi(G)$ e a hipótese implica que $[u,\varphi] = 1$, isto é, $u \in C_G(\varphi)$. Ora, $[G : \langle u \rangle] = 2$ e $\varphi \neq 1$. Portanto $C_G(\varphi) = \langle u \rangle$. Seja agora $x \in G \setminus \langle u \rangle$. Então $x^{\varphi} \neq x$. Também temos $x^{\varphi} \neq x^{-1}$ pois em caso contrário teríamos $[x,\varphi] = x^{-2} \in \Phi(G) \setminus \{1\}$, uma contradição. Escrevamos $y = x^{\varphi}$. Como $\varphi^2 = 1$, temos que $y^{\varphi} = x$. Por um lado, temos que $(xy)^{\varphi} = x^{\varphi}y^{\varphi} = yx$ e, por outro lado, como $G = \langle u \rangle \cup \{x, x^{-1}, y, y^{-1}\}$ temos que $xy \in \langle u \rangle$ e assim $(xy)^{\varphi} = xy$. Mas então $x \in Z(G)$, um absurdo. □

Estamos, enfim, em condições de estabelecer as provas dos Teoremas A e B e, portanto, faremos isto nas linhas que se seguem. Para a comodidade do leitor iremos enunciar os resultados novamente abaixo.

Teorema A. *Um CPPO-grupo finito e solúvel G tem altura de Fitting no máximo 3.*

Demonstração. Assuma que o resultado seja falso e considere um contraexemplo G de ordem minimal. Pela minimalidade de G, todo subgrupo próprio de G e todo quociente de G por um subgrupo normal não trivial tem altura de Fitting no máximo 3. Pelo Lema 1.29 vemos que $\Phi(G) = 1$. Dado isto, pelo Lema 1.28 obtemos $4 \leqslant h(G) = h(G/F(G)) + 1 \leq 3 + 1 = 4$, isto é, $h(G) = 4$.

Usamos, agora, o Lema 2.22 e o Lema 2.24 para tomar uma torre irredutível (P_1, P_2, P_3, P_4) de subgrupos de G. Note que pela minimalidade de G e pelo Lema 2.24 temos $G = P_1P_2P_3P_4$.

Iremos agora fazer algumas considerações sobre os termos P_i da torre acima. Inicialmente, como $P_4 \trianglelefteq G$, temos que $\Phi(P_4) \leq \Phi(G) = 1$, isto é, P_4 é p_4-abeliano elementar. Seja agora $N = C_{P_3}(P_4)$ e note que $N \trianglelefteq G$. Temos

$$C_{P_3/N}(P_4N/N) = \{gN;\ g \in P_3 \text{ e } [g, P_4] \leq N\} = 1.$$

Sendo $N \leq C_G(P_4)$, segue do Lema 2.16 que $(P_iN/N)_{i=1,2,3,4}$ é uma torre de G/N e portanto $h(G/N) \geqslant 4$, como estabelece o Lema 2.24. A minimalidade de G agora resulta em $N = 1$. Isto significa que $P_3 = \overline{P_3}$. Adicionalmente, pelo Lema 2.29 temos que $\overline{P_i}$ é ou abeliano ou extraespecial, para $i \in \{2,3\}$, e $\Phi(P_3) \leq Z(P_1P_2P_3)$, como fica claro na prova do Lema 2.29.

Após estas considerações, iremos analisar separadamente as 3 seguintes possibilidades para o grupo $\overline{P_2}$: Ou $\overline{P_2}$ é cíclico, ou abeliano não cíclico ou extraespecial. A prova estará completa ao verificarmos que todas estas possibilidades resultam na existência de um comutador em G de ordem divisível por 2 primos distintos, um absurdo pois G é um CPPO-grupo.

Caso 1. Assuma primeiramente que $\overline{P_2}$ é cíclico. Escrevamos $\overline{P_2} = \langle \overline{b} \rangle$. De $[P_3, b] = P_3$ obtemos $C_{P_3}(b) = \Phi(P_3)$. Se P_3 fosse um grupo abeliano, a torre $(\langle b \rangle, P_3, P_4)$ estaria nas

condições do Lema 2.26, e por isto G possuiria um comutador de ordem divisível por 2 primos distintos, uma contradição. Então, P_3 é um p_3-grupo extraespecial. Mas, uma vez que $\Phi(P_3) \leq Z(P_1P_2P_3)$ e $C_{P_3}(P_4) = 1$, obtemos da irredutibilidade da torre (P_1, P_2, P_3, P_4) que $P_4 = [P_4, \Phi(P_3)]$ e consequentemente a torre $(\langle b\rangle, P_3, P_4)$ está nas condições do Lema 2.28. Como G é um CPPO-grupo, isto significa que $p_3 = 2$ e $P_3 \cong Q_8$. Ainda, segue que $p_2 = 3$ e $p_1 = 2$.

Escrevamos $K = C_{P_1P_2}(P_3)$. Como ambos P_1 e P_2 agem não trivialmente sobre P_3, o quociente P_1P_2/K é isomorfo a um subgrupo de ordem pelo menos 6 de S_4. Mas como P_1 é cíclico, devemos ter $|P_1P_2/K| = 6$ e, em particular, $(P_1)^2 \leq K$. Escrevendo $P_1 = \langle a\rangle$, o automorfismo de P_3 induzido pela conjugação por a é um automorfismo involutivo de P_3. O Lema 2.31 agora permite-nos encontrar $u \in P_3$ para o qual $[u,a]$ é a involução de P_3. Concluímos pois que $[ub,a] = [u,a][b,a]$ tem ordem divisível por 2 primos distintos, uma contradição.

Caso 2. Por sua vez, supomos agora que $\overline{P_2}$ é um grupo abeliano não cíclico e tomamos $M = C_{P_2}(P_3)\Phi(P_3)$. Observe que

$$C_{P_2M/M}(P_3M/M) = \{gM;\ g \in P_2 \text{ e } [g,P_3] \leq M\} = 1.$$

Portanto, pelo Lema 2.16, temos que $(P_iM/M)_{i=1,2,3}$ é uma torre de $P_1P_2P_3/M$. Uma vez que $[P_2M/M, P_1M/M] = P_2M/M$, segue do Lema 2.26 que $P_1P_2P_3/M$ tem um comutador cuja ordem não é potência de primo. Mas então G tem um comutador desta forma, uma contradição.

Caso 3. Para concluirmos a prova, nos resta considerar o caso em que $\overline{P_2}$ é um p_2-grupo extraespecial. O Lema 2.30 mostra-nos que $p_2 = 2$ e $\overline{P_2}$ é isomorfo a Q_8.

Por fim, seja $b \in P_2$ um elemento tal que $1 \neq \overline{b} \in \Phi(\overline{P_2})$. Como $[P_3,b] = P_3$, se P_3 é abeliano a torre $(\langle b\rangle, P_3, P_4)$ satisfaz as condiçoes do Lema 2.26, e então G tem um comutador cuja ordem não é potência de primo, uma contradição. Então P_3 é um p_3-grupo extraespecial. Neste caso temos $P_4 = [P_4, \Phi(P_3)]$ e assim a torre $(\langle b\rangle, P_3, P_4)$ satisfaz as condições do Lema 2.28. Como p_3 é ímpar, o Lema 2.28 mostra que G tem um comutador cuja ordem não é potência de primo, uma contradição.

A prova está completa. □

Teorema B. *Se G é um CPPO-grupo finito e solúvel, então $|\pi(G')| \leqslant 3$.*

Demonstração. Suponha inicialmente que $h(G) = 1$. Pelo Lema 2.10, podemos escrever $G = P \times O_{p'}(G)$, para algum primo p, onde P é um subgrupo de Sylow de G e $O_{p'}(G) \leq Z(G)$. Então $G' \leq P$ é um p-grupo.

Assuma agora que $h(G) = 2$. Então $\gamma_\infty(G)$ é um subgrupo normal nilpotente e não trivial de G e usando o Lema 2.10 podemos escrever $\gamma_\infty(G) = P \times O_{p'}(\gamma_\infty(G))$ onde p é um número primo, P é um p-subgrupo de Sylow de $\gamma_\infty(G)$ e $O_{p'}(\gamma_\infty(G)) \leq Z(G)$. Temos, então,

$$\gamma_\infty(G) = [\gamma_\infty(G), G] \leq P,$$

isto é, $\gamma_\infty(G)$ é um p-grupo. Adicionalmente, $G/\gamma_\infty(G)$ é um grupo nilpotente e o argumento do primeiro parágrafo mostra que

$$G'/\gamma_\infty(G) = (G/\gamma_\infty(G))'$$

é um q-grupo para algum primo q. Segue que G' é um $\{p,q\}$-grupo.

O caso $h(G) = 3$ verifica-se aplicando duas vezes o caso anterior. De fato, neste caso $h(\gamma_\infty(G)) = 2$ e o último parágrafo mostra que $\gamma_\infty(\gamma_\infty(G))$ é um p-grupo para algum primo p. Mas também $h(G/\gamma_\infty(\gamma_\infty(G))) = 2$ e novamente o caso anterior mostra que $G'/\gamma_\infty(\gamma_\infty(G))$ tem ordem divisível por no máximo 2 primos. O resultado segue. □

Comentamos, para encerrar este capítulo, que o Teorema A expõe a melhor cota possível pois o grupo simétrico S_4 é um CPPO-grupo solúvel tal que $h(S_4) = 3$. Contudo, não sabemos se a cota dada pelo Teorema B pode ser alcançada. É possível que para todo CPPO-grupo finito solúvel G ocorra $|\pi(G')| \leqslant 2$, mas não conseguimos confirmar esta hipótese.

Capítulo 3

CPPO-grupos não solúveis

O principal objetivo deste capítulo é estudar os CPPO-grupos não solúveis e provar o Teorema C (veja a seção 3.3). A primeira seção deste capítulo contém algumas considerações sobre CPPO-grupos finitos nos quais o radical solúvel é trivial. Provaremos que cada tal grupo é *quase-simples*, isto é, possui um subgrupo normal simples com centralizador trivial. Na segunda seção exporemos a classificação de Suzuki dos EPPO-grupos finitos simples e mostraremos que o subgrupo derivado de um CPPO-grupo finito quase-simples é simples. O passo crucial para demonstrar o Teorema C é verificar que um CPPO-grupo finito não solúvel tem subgrupo derivado perfeito. Após isto fazer, concluiremos a prova do Teorema 0.3 provando o Teorema C.

3.1 Grupos com radical solúvel trivial

Vimos no Capítulo 1 deste trabalho que subgrupos normais minimais de grupos finitos são caracteristicamente simples e, consequentemente, são produtos diretos de grupos simples mutuamente isomorfos. Os grupos que podem ser escritos como produto direto de grupos simples têm interesse próprio na literatura. Contudo, aqui nos interessa o seguinte resultado.

Lema 3.1 ([11], pg. 205)**.** *Sejam H e K subgrupos normais de um grupo finito G que podem ser escritos como produto direto de grupos simples não abelianos. Então HK tem centro trivial.*

Pelo resultado acima, dado um grupo finito G existe um subgrupo normal $K(G)$ de G que pode ser escrito como produto direto de grupos simples, tem centro trivial e contém todos os demais com estas duas propriedades.

Não é difícil encontrar grupos finitos com $K(G) = 1$. É claro, por exemplo, que todo grupo abeliano finito G tem $K(G) = 1$. Um exemplo de grupo não abeliano G com $K(G) = 1$ é $G \cong S_3$, o grupo simétrico de grau 3.

Lembre que para um grupo finito G denotamos por $R(G)$ o radical solúvel de G. Na literatura, não encontramos um consenso em como nomear os grupos finitos com radical solúvel trivial, por isto aqui não iremos nomear tais grupos.

Lema 3.2 ([11], pp. 205-206)**.** *Seja G um grupo finito não trivial com radical solúvel trivial. Então $K(G) \neq 1$ e $C_G(K(G)) = 1$.*

Usando o resultado acima podemos descrever a estrutura de $K(G)$ quando G é um CPPO-grupo finito com $R(G) = 1$.

Proposição 3.3. *Seja G um CPPO-grupo finito não trivial com radical solúvel trivial. Então $K(G)$ é um grupo simples não abeliano.*

Demonstração. De fato, pelo Lema 3.2, temos que $K(G) \neq 1$. Por definição, $K(G)$ é isomorfo a um produto direto de grupos simples não abelianos. Mas o Lema 2.8 mostra que uma tal decomposição possui um único fator. Logo $K(G)$ é um grupo simples não abeliano. □

Definição 3.4. Dizemos que um grupo finito não trivial G é *quase-simples* se G possui um subgrupo normal simples H tal que $C_G(H) = 1$.

A nomenclatura aqui é bem sugestiva. Primeiramente, H neste caso é um grupo simples não abeliano, pois tem centro trivial. Adicionalmente, o mergulho canônico $G \hookrightarrow Aut(H)$ tem núcleo trivial, isto é, G pode ser visto como um grupo de automorfismos de H que contém todos os automorfismos internos de H.

A Proposição 3.3 e o Lema 3.2 mostram-nos que um CPPO-grupo finito não trivial G com $R(G) = 1$ é, na verdade, quase-simples. Na seção a seguir iremos mostrar que se G é um CPPO-grupo finito com $R(G) = 1$, então o quociente $G/K(G)$ tem estrutura conhecida.

3.2 CPPO-grupos de automorfismos

Sejam F um corpo e $n \geqslant 2$ um número inteiro. Denotamos por $\mathrm{GL}(n,F)$ o grupo das matrizes invertíveis $n \times n$ com entradas em F. No caso em que F é um corpo finito com q elementos, escrevemos $\mathrm{GL}(n,q)$ em vez de $\mathrm{GL}(n,F)$. Esta notação não gera ambiguidade pois corpos finitos com mesma ordem são isomorfos (veja Seção 3.2 de [25]). O grupo $\mathrm{GL}(n,F)$ é chamado o Grupo Geral Linear de grau n sobre F.

Podemos observar $\mathrm{GL}(n,F)$ também como sendo o grupo das transformações lineares invertíveis de um espaço vetorial n-dimensional V sobre o corpo F. De fato, fixada uma base ordenada $\alpha = \{v_1, \ldots, v_n\}$, a cada operador linear T sobre V podemos associar a matriz do operador T com respeito à base α, denotada por $[T]_\alpha$. Assim sendo, dados operadores T_1 e T_2 sobre V, pode-se verificar que $[T_1T_2]_\alpha = [T_1]_\alpha[T_2]_\alpha$ e, assim, T é invertível se, e somente se, $[T]_\alpha$ é uma matriz invertível. Disto, segue que a correspondência $T \mapsto [T]_\alpha$ é um isomorfismo entre o grupo dos operadores lineares invertíveis sobre V e o grupo $\mathrm{GL}(n,F)$.

Esta identificação de $\mathrm{GL}(n,F)$ como grupo de operadores invertíveis sobre um espaço n-dimensional V é muito útil para determinar algumas informações sobre o grupo $\mathrm{GL}(n,F)$. Como exemplo podemos determinar o centro $Z(\mathrm{GL}(n,F))$. Dados $Z \in Z(\mathrm{GL}(n,F))$ e $v \in V$ tomamos $T \in \mathrm{GL}(n,F)$ de modo que $F \cdot x$ é o único autoespaço de T. Então

$$T(Z(x)) = TZ(x) = ZT(x) = Z(T(x)) \in F \cdot Z(x),$$

isto é, $Z(x) \in F \cdot x$ e x é um autovetor de Z. Pela arbitrariedade da escolha de $x \in V$ vemos que todo vetor de V é um autovetor de Z. Aplicando esta informação em uma base de V concluímos que Z é uma matriz diagonal. Em resumo, temos que

$$Z(\mathrm{GL}(n,F)) = \{\lambda I_n;\ \lambda \in F^*\},$$

onde I_n denota a matriz identidade $n \times n$.

Podemos, agora, definir o Grupo Projetivo Geral Linear de grau n sobre F como sendo o quociente

$$\mathrm{PGL}(n,F) = \frac{\mathrm{GL}(n,F)}{Z(\mathrm{GL}(n,F))}.$$

O nome projetivo aqui utilizado vem da Geometria. Definimos inicialmente uma relação de equivalência em $V \setminus \{0\}$ do seguinte modo: $x \sim y$ se, e somente se, existe $\lambda \in F$ tal que $x = \lambda y$. O conjunto $\mathbb{P}_{n-1}(V)$ das classes de equivalência com respeito à relação $\sim$ é chamado Espaço Projetivo de dimensão $n-1$ sobre F. Uma ação natural de $\mathrm{GL}(n,F)$ agora surge pondo $A \cdot [x] := [A(x)]$, com $A \in \mathrm{GL}(n,F)$ e $x \in V \setminus \{0\}$. O núcleo desta ação consiste das matrizes $Z \in \mathrm{GL}(n,F)$ das quais cada vetor de V é um autovetor. Isto é, o núcleo desta ação coincide com o centro de $\mathrm{GL}(n,F)$, razão a qual justifica o nome do grupo $\mathrm{PGL}(n,F)$.

O Grupo Especial Linear de grau n sobre o corpo F é o núcleo do homomorfismo $det : \mathrm{GL}(n,F) \longrightarrow F$ que associa a cada matriz de $\mathrm{GL}(n,F)$ o seu determinante. Denotamos este grupo por $\mathrm{SL}(n,F)$. Analogamente ao caso de $\mathrm{GL}(n,F)$ não é difícil verificar que

$$Z(\mathrm{SL}(n,F)) = \mathrm{SL}(n,F) \cap Z(\mathrm{GL}(n,F)) = \{\lambda I_n;\ \lambda \in F,\ \lambda^n = 1\}.$$

Podemos, então, definir o grupo Projetivo Especial Linear de grau n sobre F como sendo o quociente

$$\mathrm{PSL}(n,F) = \frac{\mathrm{SL}(n,F)}{Z(\mathrm{SL}(n,F))}.$$

No caso em que F é um corpo finito com q elementos, usando o Lema de Iwasawa([25, Teorema 3.1]) pode-se provar que $\mathrm{PSL}(n,q)$ é simples, exceto quando $n = 2$ e $q \in \{2,3\}$.

Vale comentar que existem alguns isomorfismos envolvendo grupos especiais. A seguinte lista de isomorfismos pode ser encontrada no Capítulo 2 de [25]:

1. $\mathrm{PSL}(2,2) \cong S_3$;
2. $\mathrm{PSL}(2,3) \cong A_4$;
3. $\mathrm{PSL}(2,4) \cong \mathrm{PSL}(2,5) \cong A_5$;
4. $\mathrm{PSL}(2,7) \cong \mathrm{PSL}(3,2)$;
5. $\mathrm{PSL}(2,9) \cong A_6$;
6. $\mathrm{PSL}(4,2) \cong A_8$.

No contexto da busca pela classificação dos grupos finitos simples, M. Suzuki estudou em [22] uma classe de grupos duplo transitivos com a propriedade que só a identidade fixa 3 ou mais elementos. Como parte deste trabalho, Suzuki descobriu uma nova família de grupos simples que leva seu nome. Não temos condições neste trabalho de expor as provas dos seus resultados. Contudo, iremos agora expor a definição dos grupos de Suzuki.

Seja F um corpo com $q = 2^{2n-1}$ elementos, $n \geqslant 2$. Temos $2q = 2^{2n} = (2^n)^2$. Pomos $r = 2^n$ e consideramos $\varphi : F \longrightarrow F$ dado por $x \mapsto x^r$. Escreva $\varphi^2 = \alpha$.

Dados elementos $x, y \in F$, definimos a matriz

$$A_{(x,y)} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ x & 1 & 0 & 0 \\ xx^{\varphi} + y & x^{\varphi} & 1 & 0 \\ x^{\alpha}x^{\varphi} + xy + y^{\varphi} & y & x & 1 \end{bmatrix} \in \mathrm{GL}(4,q).$$

Pode-se verificar que para quaisquer $x, y, z \in F$ vale

$$A_{(x,y)} \cdot A_{(z,w)} = A_{(x+z,\ xz^{\varphi}+y+w)},$$

e portanto o conjunto

$$L = \{A_{(x,y)} \in \mathrm{GL}(4,q);\ x, y \in F\}$$

é, na verdade, um subgrupo de $\mathrm{GL}(4,q)$ com q^2 elementos.

Por sua vez, para cada elemento não trivial $x \in F$, definimos uma matriz diagonal $B_x \in \mathrm{GL}(4,q)$ com a,b,c,d na diagonal principal, nesta ordem, onde estes elementos são dados pelas regras $a^\varphi = xx^\varphi$, $b^\varphi = x$, $c = b^{-1}$, $d = a^{-1}$. Logo, o conjunto $K = \{B_x;\ x \in F^*\}$ é um subgrupo de $\mathrm{GL}(4,q)$ isomorfo ao grupo cíclico $F^\times$.

Um cálculo direto mostra que para $x,y,z \in F$, $x \neq 0$, vale

$$(B_x)^{-1} A_{(y,z)} B_x = A_{(yx,\ zxx^\varphi)},$$

o que significa que K normaliza L. Em particular, $H = LK$ é um subgrupo de $\mathrm{GL}(4,q)$ de ordem $q^2(q-1)$. Mantendo estas construções em mente, podemos definir o grupo de Suzuki como segue.

Definição 3.5. Sob as considerações acima, o grupo de Suzuki $Sz(q)$ é definido como sendo o subgrupo de $\mathrm{GL}(4,q)$ gerado por H e a matriz X, onde X é a matriz contendo 1 na diagonal secundária e 0 nas outras entradas.

Suzuki em [22] classificou os EPPO-grupos finitos simples mostrando que somente 8 classes de isomorfismos de tais grupos existem. Mais precisamente, Suzuki provou o seguinte resultado.

Teorema 3.6 (M. Suzuki)**.** *Um EPPO-grupo finito simples é isomorfo a um dos seguintes grupos:* $\mathrm{PSL}(2,q)$*,* $q \in \{4,7,8,9,17\}$*,* $\mathrm{PSL}(3,4)$*,* $Sz(8)$ *ou* $Sz(32)$*.*

Agora, no nosso contexto, é natural questionar se existe um CPPO-grupo finito simples que não é um EPPO-grupo e, por isto, iremos fazer um comentário sobre este questionamento. Em [17], Oystein Ore provou que todo elemento do grupo Alternado A_n, $n \geqslant 5$, pode ser escrito como um comutador. Ore então conjecturou que seria possível provar o mesmo resultado para todos os grupos finitos simples não abelianos, problema que ficou conhecido como Conjectura de Ore. Foi só em 2010 que, usando o Teorema de Classificação dos Grupos Finitos Simples, Liebeck, O'Brien, Shalev e Tiep [14] responderam afirmativamente a Conjectura de Ore.

Teorema 3.7 (M.W. Liebeck, *et al*)**.** *Seja G um grupo finito simples não abeliano. Então cada elemento de G é um comutador.*

Uma consequência agora óbvia dos Teoremas 3.6 e 3.7 é enunciada a seguir

Corolário 3.8. *Um CPPO-grupo finito simples é isomorfo a um dos seguintes grupos:* $\mathrm{PSL}(2,q)$*,* $q \in \{4,7,8,9,17\}$*,* $\mathrm{PSL}(3,4)$*,* $Sz(8)$ *ou* $Sz(32)$*.*

Vale comentar que Liebeck *et al* provaram o mesmo resultado para grupos especiais lineares.

Teorema 3.9. *Seja $G = \mathrm{SL}(n,q)$ um grupo especial linear. Então todo elemento de G é um comutador, exceto quando $(n,q) \in \{(2,2),(2,3)\}$.*

Usando o Corolário 3.8 e o Teorema 3.9 podemos determinar quais grupos da forma $\mathrm{GL}(n,q)$ e $\mathrm{SL}(n,q)$ são CPPO-grupos. Isto é feito a seguir.

Proposição 3.10. *Seja G um grupo da forma $\mathrm{GL}(n,q)$ ou $\mathrm{SL}(n,q)$. Então G é um CPPO-grupo se, e somente se, $(n,q) \in \{(2,2),(2,4),(2,8),(3,2)\}$ ou $(n,q) = (2,3)$ e $G \cong \mathrm{SL}(2,3)$.*

Demonstração. Inicialmente, sabemos que $\mathrm{GL}(2,2) = \mathrm{SL}(2,2) \cong S_3$ tem subgrupo derivado cíclico de ordem 3. Logo G é CPPO-grupo neste caso. No caso em que $(n,q) = (2,3)$, temos que $\mathrm{SL}(2,3)' \cong Q_8$ e $\mathrm{SL}(2,3)$ é um CPPO-grupo. Mas $\mathrm{GL}(2,3)' = \mathrm{SL}(2,3)$ e $\mathrm{SL}(2,3)$ não é um EPPO-grupo. Segue que $\mathrm{GL}(2,3)$ não é um CPPO-grupo.

Podemos assumir $n \geqslant 3$ ou $n = 2$ e $q \geqslant 4$. Neste caso, como $\mathrm{GL}(n,q)' = \mathrm{SL}(n,q)$, pelo Teorema 3.9 as seguintes afirmações são equivalentes:

(a) $\mathrm{GL}(n,q)$ é um CPPO-grupo;

(b) $\mathrm{SL}(n,q)$ é um EPPO-grupo;

(c) $\mathrm{SL}(n,q)$ é um CPPO-grupo.

Observamos que para $(n,q) \in \{(2,5),(2,7),(2,9),(2,17),(3,4)\}$ temos que o subgrupo $Z(\mathrm{SL}(n,q))$ é cíclico de ordem prima e, por isto, $\mathrm{SL}(n,q)$ não é um EPPO-grupo. Para o caso $(n,q) = (3,2)$, temos que $\mathrm{GL}(3,2) = \mathrm{SL}(3,2) = \mathrm{PSL}(3,2) \cong \mathrm{PSL}(2,7)$ é um CPPO-grupo. Para $(n,q) \in \{(2,4),(2,8)\}$ temos que $Z(\mathrm{SL}(n,q)) = 1$ e $\mathrm{SL}(n,q) = \mathrm{PSL}(n,q)$ é um EPPO-grupo. □

O seguinte resultado é uma consequência imediata do Teorema 3.6 e das considerações sobre automorfismos externos de grupos simples que constam no Teorema 3.2 e na Seção 4.2.4 de [25].

Lema 3.11. *Seja G um CPPO-grupo finito simples e não abeliano. Então vale uma das seguintes afirmações:*

1. *$Out(G)$ é um grupo cíclico (de ordem no máximo 5);*
2. *$Out(G) \cong V_4$ e $G \cong A_6$;*
3. *$Out(G) \cong D_6 \times C_2$ e $G \cong \mathrm{PSL}(3,4)$.*

O isomorfismo $Out(\mathrm{PSL}(3,4)) \cong D_6 \times C_2$ nos mostra que existem exatamente dois subgrupos quase-simples não isomorfos G de $Aut(\mathrm{PSL}(3,4))$ tais que $G/\mathrm{PSL}(3,4) \cong S_3$. No que segue mostraremos que tais grupos possuem comutadores com ordens divisíveis por dois primos. Antes, precisamos descrever o grupo de automorfismos dos grupos projetivos lineares. As considerações a seguir seguem as descrições que podem ser encontradas em [16] e [25]. Ainda, abaixo consideramos $n > 2$ ou $n = 2$ e $q > 4$.

Tomemos $F = F_q$ um corpo com $q = p^m$ elementos, com p primo e $m \geqslant 1$. A correspondência $\varphi : F \longrightarrow F$ dada por $a \mapsto a^p$ é um automorfismo de corpo de F de ordem m, chamado o automorfismo de Frobenius de F. Dado $n \geqslant 2$, o automorfismo φ de F induz um automorfismo de $\mathrm{GL}(n,F)$, também de ordem m, que consiste de elevar cada entrada de uma matriz à p-ésima potência. Denotaremos também, por abuso de notação, este automorfismo por φ.

Seja $\beta : \mathrm{GL}(n,F) \longrightarrow \mathrm{GL}(n,F)$ dada por $A^\beta = (A^T)^{-1}$, onde A^T denota a transposta da matriz A. Então β é um automorfismo de $\mathrm{GL}(n,F)$ de ordem 2.

Seja $G = \mathrm{PSL}(n,q)$ e identifiquemos G com seu grupo de automorfismos internos $Inn(G) \leq Aut(G)$.

Temos a seguinte sequência de subgrupos normais

$$\mathrm{SL}(n,q) \leq \mathrm{GL}(n,q) \leq \Gamma\mathrm{L}(n,q) \coloneqq \mathrm{GL}(n,q)\langle\varphi\rangle \leq \Gamma\mathrm{L}(n,q)\langle\beta\rangle.$$

Tomando quocientes módulo o centro de $\mathrm{GL}(n,q)$ temos

$$G = \mathrm{PSL}(n,q) \leq \mathrm{PGL}(n,q) \leq \mathrm{P\Gamma L}(n,q) \leq \mathrm{P\Gamma L}(n,q)\langle\beta\rangle = Aut(G).$$

Adicionalmente, $\mathrm{PGL}(n,q)/\mathrm{PSL}(n,q)$ é um grupo cíclico de ordem $d = (n, q-1)$. Usando isto podemos concluir a classificação dos CPPO-grupos finitos da forma $\mathrm{GL}(n,q)$, $\mathrm{SL}(n,q)$ e $\mathrm{PGL}(n,q)$ através do Teorema 3.6, da Proposição 3.10 e do seguinte resultado cuja prova é óbvia e será omitida.

Proposição 3.12. *Um grupo da forma* $\mathrm{PGL}(n,q)$ *é um CPPO-grupo se, e somente se,* $\mathrm{PSL}(n,q)$ *o for.*

O seguinte resultado foi provado por A. Lucchini, F. Menegazzo e M. Morigi em [16].

Teorema 3.13 ([16], Teorema 1.12)**.** *Com as considerações anteriores, o grupo* $G = \mathrm{PSL}(n,q)$ *possui um complemento em* $Aut(G)$ *se, e somente se,* $((q-1)/d, d, m) = 1$.

Para a prova da Proposição 3.14 a seguir iremos fixar as notações e utilizar as considerações enumeradas a abaixo.

1. Tomamos $F = \{0, 1, a, a^2\}$ um corpo com 4 elementos. Então F tem característica 2 e todo elemento de F satisfaz a equação $2x = 0$. Adicionalmente, observamos que $1 + a = a^2$, $1 + a^2 = a$ e $a + a^2 = 1$.

2. Definimos $Q = \mathrm{SL}(3, F)$ o grupo especial linear de grau 3 sobre F;

3. Tomamos φ o automorfismo de Frobenius de Q. Então φ tem ordem 2;

4. Tomamos δ o automorfismo de Q induzido pela conjugação pela matriz

$$B_\delta = \begin{bmatrix} a & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \in \mathrm{GL}(3, F).$$

   Veja que

$$\begin{aligned} A^\delta &= \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}^\delta = \begin{bmatrix} a^2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix} \begin{bmatrix} a & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \\ &= \begin{bmatrix} a^2 a_{11} & a^2 a_{12} & a^2 a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix} \begin{bmatrix} a & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} a_{11} & a^2 a_{12} & a^2 a_{13} \\ a a_{21} & a_{22} & a_{23} \\ a a_{31} & a_{32} & a_{33} \end{bmatrix}. \end{aligned}$$

   Analogamente temos que

$$A^{\delta^2} = \begin{bmatrix} a_{11} & a a_{12} & a a_{13} \\ a^2 a_{21} & a_{22} & a_{23} \\ a^2 a_{31} & a_{32} & a_{33} \end{bmatrix}.$$

   Note que vale $|\delta| = |B_\delta| = 3$;

5. Ainda, tomamos β o automorfismo de Q que leva toda matriz $A \in Q$ em A^{-T}. Então $|\beta| = 2$.

6. Sendo $A = (A_{ij}) \in Q$, veja que

$$A^{\delta\varphi} = \begin{bmatrix} a_{11} & a^2 a_{12} & a^2 a_{13} \\ a a_{21} & a_{22} & a_{23} \\ a a_{31} & a_{32} & a_{33} \end{bmatrix}^\varphi = \begin{bmatrix} a_{11}^2 & a a_{12}^2 & a a_{13}^2 \\ a^2 a_{21}^2 & a_{22}^2 & a_{23}^2 \\ a^2 a_{31}^2 & a_{32}^2 & a_{33}^2 \end{bmatrix} = A^{\varphi\delta^2}.$$

Também temos que

$$\begin{aligned} A^{\beta\delta} &= \begin{bmatrix} a_{11} & a_{21} & a_{31} \\ a_{12} & a_{22} & a_{32} \\ a_{13} & a_{23} & a_{33} \end{bmatrix}^{-\delta} = \begin{bmatrix} a_{11} & a^2a_{21} & a^2a_{31} \\ aa_{12} & a_{22} & a_{32} \\ aa_{13} & a_{23} & a_{33} \end{bmatrix}^{-1} \\ &= \begin{bmatrix} a_{11} & aa_{12} & aa_{13} \\ a^2a_{21} & a_{22} & a_{23} \\ a^2a_{31} & a_{32} & a_{33} \end{bmatrix}^{-T} = A^{\delta^2\beta}. \end{aligned}$$

Temos pois que $\delta^{\varphi} = \delta^{\beta} = \delta^2$.

7. Denotamos por $\overline{\varphi}, \overline{\delta}, \overline{\beta}$ os automorfismos induzidos por φ, δ e β, respectivamente, sobre $\overline{Q} = Q/Z(Q) \cong \mathrm{PSL}(3,4)$.

8. Sendo $I : \overline{Q} \longrightarrow Aut(\overline{Q})$ a imersão canônica, definimos

$$G_1 = I(\overline{Q})\langle \overline{\delta}, \overline{\varphi} \rangle \leq Aut(\overline{Q}),$$

ainda,

$$G_2 = I(\overline{Q})\langle \overline{\delta}, \overline{\beta} \rangle \leq Aut(\overline{Q}).$$

Assim sendo, G_1 e G_2 são os dois subgrupos quase-simples de $Aut(\overline{Q})$ cujas imagens em $Out(\overline{Q})$ são isomorfas a S_3.

Com estas notações e considerações em mente provamos o seguinte resultado.

Proposição 3.14. *Seja G um grupo finito. Admita que G contém um subgrupo normal H, com $H \cong \mathrm{PSL}(3,4)$ e $C_G(H) = 1$. Então G é um CPPO-grupo se, e somente se, G/H for abeliano.*

Demonstração. Primeiramente, note que se G/H é abeliano, então $G' \leq H$. Sendo H um EPPO-grupo, temos que G é um CPPO-grupo.

Reciprocamente, admita que G/H não seja abeliano. Basta-nos mostrar que, neste caso, G não é um CPPO-grupo. Lembremos que $Out(H) \cong D_6 \times C_2$. Portanto, atráves da imersão canônica $G \hookrightarrow Aut(H)$ vemos que G é isomorfo a um dos grupos G_1, G_2 ou $Aut(H)$. Como subgrupos de CPPO-grupos são CPPO-grupos é suficiente mostrar que ambos G_1 e G_2 não são CPPO-grupos.

Mostraremos primeiramente que G_1 não é um CPPO-grupo.

Considere a matriz

$$A_1 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & a \\ 0 & 0 & 1 \end{bmatrix} \in Q \setminus Z(Q).$$

Temos que $A_1^2 = 1$ e também

$$A_1^{\varphi} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & a^2 \\ 0 & 0 & 1 \end{bmatrix}.$$

Segue que

$$[A_1, \varphi] = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & a \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & a^2 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & a+a^2 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix},$$

isto é, $[A_1, \varphi]$ tem ordem 2. Uma vez que $[A_1, \varphi] \in C_Q(\delta)$, em G_1 o comutador

$$[I(\overline{A_1})\overline{\delta}, \overline{\varphi}] = (I(\overline{A_1})^{-1} I(\overline{A_1})^{\overline{\varphi}})^{\overline{\delta}} [\overline{\delta}, \overline{\varphi}] = I(\overline{[A_1, \varphi]})^{\overline{\delta}} \overline{\delta} = I(\overline{[A_1, \varphi]})\overline{\delta}$$

tem ordem 6. Logo G_1 não é um CPPO-grupo.

Agora resta-nos mostrar que G_2 não é um CPPO-grupo. Para isto fazer, tomemos

$$A_2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & a & 1 \\ 0 & 0 & a^2 \end{bmatrix} \in Q \setminus Z(Q).$$

Note que

$$(A_2)^T = \begin{bmatrix} 1 & 0 & 0 \\ 0 & a & 0 \\ 0 & 1 & a^2 \end{bmatrix},$$

logo

$$(A_2)^{\beta} = ((A_2)^T)^{-1} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & a^2 & 0 \\ 0 & 1 & a \end{bmatrix}.$$

Uma vez que

$$A_2^{-1} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & a^2 & 1 \\ 0 & 0 & a \end{bmatrix},$$

obtemos que

$$[A_2,\beta] = \begin{bmatrix} 1 & 0 & 0 \\ 0 & a^2 & 1 \\ 0 & 0 & a \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & a^2 & 0 \\ 0 & 1 & a \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & a^2 & a \\ 0 & a & a^2 \end{bmatrix}.$$

Veja que

$$[A_2,\beta]^2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & a^2 & a \\ 0 & a & a^2 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & a^2 & a \\ 0 & a & a^2 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix},$$

isto é, $[A_2,\beta]$ tem ordem 2. Uma vez que $[A_2,\beta] \in C_Q(\delta)$, concluímos que em G_2 o comutador

$$[I(\overline{A_2})\overline{\delta},\overline{\beta}] = I(\overline{[A_2,\beta]})\overline{\delta}$$

tem ordem 6. Logo G_2 não é um CPPO-grupo. □

Lema 3.15. *Seja G um CPPO-grupo finito não trivial. Então $R(G) = 1$ se, e somente se, G é quase-simples. Em particular, se $R(G) = 1$, então $G' = K(G)$ e ou $G/K(G)$ é cíclico ou $G/K(G)$ é isomorfo ao grupo de Klein.*

Demonstração. Se $R(G) = 1$ segue da Proposição 3.3 e do Lema 3.2 que G é quase-simples. Reciprocamente, assuma que G seja quase-simples. Então G contém um subgrupo normal simples H de modo que $C_G(H) = 1$. Certamente H é não abeliano e por isto $H \cap R(G) = 1$. Mas então $[R(G),H] = 1$ e $R(G) \leq C_G(H) = 1$, isto é, $R(G) = 1$.

Assuma que $R(G) = 1$. Seja $H = K(G)$. Pela Proposição 3.3 temos que H é um grupo simples não abeliano. Identificando H com seu grupo de automorfismos internos, podemos observar G como um subgrupo de $Aut(H)$ através da imersão canônica $G \hookrightarrow Aut(H)$. Logo, nos é suficiente analisar as possibilidades listadas no Lema 3.11. Se H não for isomorfo a $\mathrm{PSL}(3,4)$, o Lema 3.11 permite-nos concluir que G/H é abeliano e ou é cíclico ou isomorfo ao grupo de Klein. Em qualquer caso, $H = G'$. No caso em que $H \cong \mathrm{PSL}(3,4)$ a Proposição 3.14 mostra-nos que G/H é um grupo abeliano, logo $H = G'$. Ainda, como $Out(H) \cong D_6 \times C_2$, segue que G/H é ou cíclico ou isomorfo ao grupo de Klein. □

Nas provas que se seguem iremos utilizar frequentemente a seguinte consequência do resultado acima.

Corolário 3.16. *Seja G um CPPO-grupo finito perfeito e não trivial. Se $R(G) = 1$, então G é simples.*

Demonstração. Seja G um grupo nas condições do enunciado. Pela Proposição 3.3, temos que $K(G)$ é um grupo simples não abeliano. Adicionalmente, o Lema 3.15 mostra que

$G' = K(G)$. Uma vez que G é perfeito, temos que $G = G' = K(G)$ é um grupo simples não abeliano. □

Generalizando sua prova da conjectura de Ore, Liebeck *et al* provaram em [15] que em um grupo finito perfeito G tal que $G/Z(G)$ é simples não abeliano todos os elementos são comutadores, apresentando uma pequena lista de exceções. Para nossos interesses, é suficiente a seguinte aplicação direta do Teorema 1 de [15].

Proposição 3.17. *Seja G um grupo finito perfeito tal que $G/Z(G)$ é um CPPO-grupo finito simples e não abeliano. Então vale exatamente uma das seguintes afirmações:*

1. *Todo elemento de G é um comutador;*
2. *$G/Z(G)$ é isomorfo a A_6 e vale uma das seguintes afirmações:*
   (a) *$Z(G) \cong C_3$ e os elementos não comutadores de G não centrais têm ordem 12;*
   (b) *$Z(G) \cong C_6$ e os elementos não comutadores de G não centrais têm ordem 15 ou 24.*
3. *$G/Z(G) \cong \mathrm{PSL}(3,4)$, $Z(G) \neq 1$, $\pi(Z(G)) \subseteq \{2,3\}$ e os elementos não centrais não comutadores de G têm ordens algum múltiplo de 6.*

Lema 3.18. *Seja G um EPPO-grupo finito com $Z(G) \neq 1$. Então G é um p-grupo para algum primo p.*

Demonstração. Basta observar que para um elemento $g \in Z(G)$ vale $G = C_G(g)$ e aplicar a Proposição 2.2. □

Proposição 3.19. *Seja G um CPPO-grupo finito perfeito tal que $G/Z(G)$ é um grupo simples não abeliano. Então G é simples.*

Demonstração. Observe que basta-nos analisar as possibilidades expostas na Proposição 3.17.

Inicialmente, se todo elemento de G for um comutador, então G é um EPPO-grupo. Mas G não é solúvel, logo segue do Lema 3.18 que $Z(G) = 1$. Por isto, G é simples.

Assuma portanto que G possui elementos não comutadores. Então ou $G/Z(G) \cong A_6$ ou $G/Z(G) \cong \mathrm{PSL}(3,4)$. Mas em qualquer um dos casos citados nos itens 2 e 3 da Proposição 3.17 podemos tomar um elemento central $z \in G$ de ordem prima diferente de 5 e $g \in G$ de ordem 5 tal que zg é um comutador. Logo G não é um CPPO-grupo. □

3.3 Prova do Teorema C

Iremos concluir este trabalho estabelecendo o seguinte resultado.

Teorema C. *Seja G um CPPO-grupo finito não solúvel. Então $R(G') = [G', R(G)] \leq O_2(G)$ e $G'/R(G')$ é isomorfo a um dos seguintes grupos* $\mathrm{PSL}(2,q)$, $q \in \{4,7,8,9,17\}$, $\mathrm{PSL}(3,4)$, $Sz(8)$, $Sz(32)$.

Para a prova do Teorema C necessitamos ainda de 2 lemas técnicos que provaremos a seguir.

Teorema 3.20 (Frobenius)**.** *Seja G um grupo finito e seja p um número primo. Então G possui um p-complemento normal se, e somente se, vale uma das seguintes:*

(a) $N_G(H)/C_G(H)$ é um p-grupo para todo p-subgrupo não trivial H de G;

(b) $N_G(H)$ possui um p-complemento para todo p-subgrupo não trivial H de G.

Lema 3.21. *Seja G um grupo contendo um subgrupo normal N tal que G/N é um EPPO-grupo simples não-abeliano. Seja $q \in \pi(G) \setminus \pi(N)$. Então existem um q-subgrupo abeliano elementar Q de G e um elemento $g \in G$, cuja ordem é potência de um primo distinto de q, tais que $Q = [Q,g]$.*

Demonstração. Pelo Teorema 3.20 existe um q-subgrupo H de G tal que $N_G(H)/C_G(H)$ não é um q-grupo. Seja $p \in \pi(N_G(H)/C_G(H)) \setminus \{q\}$ e tomemos um p-elemento $g \in N_G(H) \setminus C_G(H)$. Então $[H,g] \neq 1$ e, em particular, $g \notin N$. De fato, em caso contrário teríamos $[H,g] \leq H \cap N = 1$, o que contradiz a escolha de g. Tome agora $x \in Z(H)$ de ordem q. Devemos ter $x^g \neq x$ pois G/N é um EPPO-grupo. Definindo agora $Q = \langle x, x^g, \ldots, x^{g^{|g|-1}} \rangle$, temos que Q é abeliano elementar e normalizado por g. Logo, trocando Q por $[Q,g]$, se necessário, temos que $Q = [Q,g]$. □

É conhecido que o único grupo simétrico que possui automorfismo externo é o grupo S_6 e que, a menos de composição com um automorfismo interno, este automorfismo externo é único. O primeiro a descobrir este fato foi O. Hölder em [9].

Um automorfismo externo de S_6 é chamado de automorfismo excepcional. Além da prova dada por Hölder, existem diversas provas da existência de automorfismos excepcionais de S_6. Por exemplo, em [10], G. Janusz e J. Rotman tomam um subgrupo K de S_6, de ordem 120 e transitivo em $\{1,2,3,4,5,6\}$, e fazendo S_6 agir sobre o conjunto dos conjugados de K em S_6 constroem um automorfismo de S_6 cuja imagem de (12) não é uma transposição, logo se tratando de um automorfismo excepcional. Ainda neste mesmo artigo, Janusz e Rotman dão uma construção explícita de um automorfismo $\phi : S_6 \longrightarrow S_6$ assumindo os seguintes valores

1. $(12)^{\phi} = (12)(36)(45)$;
2. $(13)^{\phi} = (16)(24)(35)$;
3. $(14)^{\phi} = (13)(25)(46)$;
4. $(15)^{\phi} = (15)(26)(34)$;
5. $(16)^{\phi} = (14)(23)(56)$.

E para este automorfismo um cálculo direto mostra que $(123456)^{\phi} = (13)(456)$. Dado isto, quaisquer que sejam $a,b,c,d,e \in \{1,2,3,4,5,6\}$ dois a dois distintos existe um automorfismo externo de S_6 levando (123456) em $(ab)(cde)$. Isto ocorre pois elementos de grupos simétricos são conjugados se, e somente se, têm mesma estrutura de ciclos (veja [18, Teorema 3.6]).

Para provar a Proposição 3.23 a seguir, precisamos encontrar um comutador com propriedades específicas no grupo de automorfismos de $A_6 \cong \mathrm{PSL}(2,9)$, faremos isto no resultado abaixo. Porém, sabendo que $Aut(A_6) \cong Aut(S_6)$, para simplificar os cálculos trabalharemos no grupo $Aut(S_6)$.

Lema 3.22. *Seja $G = Aut(S_6)$ e seja $I : S_6 \longrightarrow G$ a imersão canônica. Então existem $\tau \in A_6$, $\sigma \in S_6 \setminus A_6$ e um automorfismo externo $\psi \in Aut(S_6)$ tal que $[I_\sigma, \psi I_\tau]$ tem ordem 3.*

Demonstração. Considere $\sigma = (123456)$ e $\tau = (456)$. Seja $\psi \in Aut(S_6)$ um automorfismo externo tal que $\sigma^{\psi} = (142)(56)$. Então

$$[I_\sigma, \psi I_\tau] = [I_\sigma, I_\tau][I_\sigma, \psi]^{I_\tau} = I_{[\sigma,\tau]}(I_{\sigma^{-1}\sigma^{\psi}})^{I_\tau} = I_{[\sigma,\tau]}I_{\tau^{-1}\sigma^{-1}\sigma^{\psi}\tau} = I_{\sigma^{-1}\tau^{-1}\sigma^{\psi}\tau},$$

de modo que o comutador $[I_\sigma, \psi I_\tau]$ tem a mesma ordem que $\sigma^{-1}\tau^{-1}\sigma^{\psi}\tau$. Como,

$$\sigma^{-1}\tau^{-1}\sigma^{\psi}\tau = (165432)(465)(142)(56)(456) = (143)(256),$$

segue que $|[I_\sigma, \psi I_\tau]| = |\sigma^{-1}\tau^{-1}\sigma^{\psi}\tau| = 3$, como desejado. □

Proposição 3.23. *Seja G um CPPO-grupo finito não solúvel. Então G' é perfeito.*

Demonstração. Assuma que o resultado seja falso e considere um contraexemplo G de ordem mínima. Certamente G não é um grupo perfeito, então G' é um subgrupo próprio de G. Também G' é não solúvel e a minimalidade de G mostra que $H = G''$ é um grupo perfeito, claramente não trivial. Minimalidade ainda resulta em $R(H) = 1$. Segue do Corolário 3.16 que H é um grupo simples não abeliano.

Para qualquer subgrupo normal M de G não contendo H vale $[M,H] \leq M \cap H = 1$. Em particular, $R(G) \leq C_G(H)$.

Afirmamos que $R(G) = Z(G)$. De fato, se não for este o caso, tomamos elementos $a \in G$ e $b \in R(G)$ de modo que o comutador $[b,a]$ é não trivial. Sendo G um CPPO-grupo, $[b,a]$ tem ordem uma potência de algum número primo r.

Afirmação: Se $g \in H$ é tal que ag normaliza um r'-subgrupo K de H, então ag centraliza K.

De fato, qualquer que seja $h \in K$, o comutador

$$[bh, ag] = [b,a][h,ag]$$

tem ordem uma potência de r, pois $R(G) \leq C_G(H)$ e G é um CPPO-grupo. Mas $[h,ag] \in K$ e portanto $[h,ag] = 1$. A escolha arbitrária de $h \in K$ permite-nos concluir que $[ag,K] = 1$, como afirmado.

Seja, agora, $q \in \pi(H) \setminus \{r\}$ e K um q-subgrupo não trivial de H. Tomemos um q-subgrupo de Sylow Q de H contendo K. Pelo Argumento de Frattini, existe um elemento $g \in H$ tal que $ag \in N_G(Q)$. Pelo argumento acima, ag centraliza Q. Mas $K \leq Q$ e então ag centraliza K. Dado agora $x \in N_H(K)$, temos que $ag, agx \in N_G(K)$. O argumento acima mostra-nos que agx centraliza K. Mas como ag centraliza K, concluímos que x centraliza K. A escolha arbitrária de $x \in N_H(K)$ mostra-nos que $N_H(K) = C_H(K)$. O Teorema 3.20 nos permite concluir que H possui um q-complemento normal, um absurdo pois H é simples. Isto prova que $R(G) = Z(G)$.

Considere agora M um subgrupo normal minimal de G contido em $R(G)$. Pela minimalidade de G temos que $G'M = HM$. Mas se $M \not\leq G'$, obteríamos do Lema de Dedekind que $G' = G' \cap G'M = G' \cap HM = H(G' \cap M) = H$, uma contradição. Então $M \leq G'$. Também temos $M \cap H = 1$, então $M = O_p(G')$ para algum primo p. Isto significa que G possui um único subgrupo normal minimal solúvel e, por isto, $R(G)$ é um p-grupo. Mais do que isto, como $M \leq Z(G)$ temos que

$$G'/H = MH/H \leq Z(G/H),$$

isto é, G/H é nilpotente de classe 2.

Para concluir esta prova, iremos analisar as possibilidades para o quociente $\overline{G}/\overline{H}$, onde $\overline{G} = G/R(G)$. Inicialmente, como $R(\overline{G}) = 1$, segue da Proposição 3.3 e do Lema 3.15 que $\overline{H} = K(\overline{G}) = \overline{G}'$ e que $\overline{G}/\overline{H}$ é ou cíclico ou isomorfo ao grupo de Klein.

Assuma que $\overline{G}/\overline{H}$ seja um grupo cíclico. Neste caso, podemos tomar um elemento $g \in G$ para o qual $G = \langle g \rangle Z(G)H$. Temos portanto que $G/H = \langle g \rangle Z(G)H/H$ é um grupo abeliano. Mas isto significa que $G' \leq H$, uma contradição.

Então $\overline{G}/\overline{H}$ é não cíclico. Portanto ou $H \cong A_6$ ou $H \cong \mathrm{PSL}(3,4)$ e, em ambos os casos temos $\overline{G}/\overline{H} \cong V_4$, uma consequência do Lema 3.15.

Considere elementos $a, b \in G$ para os quais possamos escrever $G = \langle a,b \rangle HZ(G)$. Observe que $[a,b] \notin H$, pois G/H é não abeliano. Por outro lado, G/H é nilpotente e seu p-subgrupo $R(G)H/H$ é tal que

$$\frac{G/H}{R(G)H/H} \cong \overline{G}/\overline{H} \cong V_4.$$

Segue que $p = 2$. Em particular, $[a, by]$ tem ordem potência de 2, para todo $y \in H$.

Se H for isomorfo a A_6, pelo Lema 3.22 podemos tomar $a, b \in G$ de tal modo que exista $h \in H$ satisfazendo $|[\overline{a}, \overline{bh}]| = 3$. Isto contradiz a conclusão do parágrafo acima.

Portanto, H é isomorfo a $\mathrm{PSL}(3,4)$. Podemos então assumir que $\overline{G} = \overline{H} \rtimes \langle \overline{a}, \overline{b} \rangle$ com $\langle \overline{a}, \overline{b} \rangle \cong V_4$ (veja Teorema 3.13). Pelo Teorema de Baer-Suzuki (Teorema 1.23), existe um elemento $\overline{g} \in \overline{G}$ tal que $\langle \overline{a}, \overline{a}^{\overline{g}} \rangle$ não é um grupo nilpotente. Em particular, existe $1 \neq \overline{y} \in \langle \overline{a}, \overline{a}^{\overline{g}} \rangle$ de ordem ímpar. Mas sendo que $\overline{G}/\overline{H}$ é isomorfo ao grupo de Klein, podemos assumir $y \in H$. Ainda, $\langle \overline{a}, \overline{a}^{\overline{g}} \rangle$ é um grupo diedral, então $\overline{y}^{\overline{a}} = \overline{y}^{-1}$ e assim $1 \neq [\overline{y}, \overline{a}]$ tem ordem ímpar. Por outro lado, $1 \neq [a,b] \in R(G)$ e a igualdade $[a, by] = [a,y][a,b]$ mostra que $[a,y]$ é um 2-elemento, uma contradição. Esta contradição conclui a prova. □

Provaremos agora o Teorema C. Para a comodidade do leitor iremos enunciá-lo mais uma vez.

Teorema C. *Seja G um CPPO-grupo finito não solúvel. Então $R(G') = [G', R(G)] \leq O_2(G)$ e $G'/R(G')$ é isomorfo a um dos seguintes grupos* $\mathrm{PSL}(2,q)$*, $q \in \{4,7,8,9,17\}$,* $\mathrm{PSL}(3,4)$*, $Sz(8)$, $Sz(32)$.*

Demonstração. Primeiramente, pela Proposição 3.23 temos que G' é perfeito. Assim, $G'/R(G')$ é um grupo perfeito não trivial com $R(G'/R(G')) = 1$. O Corolário 3.16 mostra que $G'/R(G')$ é um grupo simples não abeliano. O Corolário 3.8 agora mostra que $G'/R(G')$ é isomorfo a um dos grupos da lista $\mathrm{PSL}(2,q)$, com $q \in \{4,7,8,9,17\}$, $\mathrm{PSL}(3,4)$, $Sz(8)$ ou $Sz(32)$. Também temos $Z(G'/[G', R(G)]) = R(G')/[G', R(G)]$, portanto obtemos da Proposição 3.19 que $R(G') = [G', R(G)]$.

Resta-nos provar que $R(G')$ é um 2-grupo. Assuma que o resultado seja falso e tome um contraexemplo G de ordem mínima.

Inicialmente, a minimalidade de G e a Proposição 3.23 mostram que G é perfeito. Em particular, $G/R(G)$ é um grupo simples não abeliano.

Seja M um subgrupo normal minimal solúvel de G. Então M é um p-grupo abeliano elementar para algum número primo p. Pela minimalidade de G temos que $R(G)/M$ é um 2-grupo. Em particular, $p \neq 2$ e $M = O_p(R(G))$. Isto mostra também que G possui um único subgrupo solúvel normal minimal. Então, $F(G)$ é um p-grupo e, assim, $M = F(G)$.

Assuma primeiramente $M = R(G)$. Usamos o Lema 3.21 para tomar um 2-subgrupo abeliano elementar Q de G e um elemento $a \in G$ de modo que $Q = [Q,a]$ e tal que a ordem do elemento a é potência de um primo ímpar. Observe que como $[G,Q] \trianglelefteq G$ e G/M é um grupo simples não abeliano, temos $G = [G,Q]M$. Agora, $G/[G,Q]$ é um grupo solúvel perfeito, logo trivial e assim $G = [G,Q]$. Ora, se Q centraliza M, então $G = [G,Q] \leq C_G(M)$, isto é, $M \leq Z(G)$ e pelo Lema 3.19 concluímos que $M = 1$, uma contradição. Então Q não centraliza M. Como Q é não cíclico, pois G/M é um EPPO-grupo, segue que $(\langle a \rangle, Q, M)$ é uma torre nos termos do Lema 2.26 e G contém um comutador cuja ordem não é potência de primo, uma contradição. Concluímos assim que M é um subgrupo próprio de R e, disto, que R/M é um 2-grupo não trivial.

Observe que como $O_2(R) = 1$ não podemos ter $M \leq Z(R)$. Consequentemente, pela minimalidade de M, obtemos $M = [R,M] = [G,M]$. Agora, como G é perfeito e $M \not\leq Z(G)$, concluímos que

$$C_G(M) = M.$$

Considere um primo $q \in \pi(G) \setminus \{2,p\}$. Pelo Lema 3.21 podemos tomar um q-subgrupo abeliano elementar Q de G e um elemento $a \in G$ tal que $Q = [Q,a]$ e cuja ordem é potência de primo. Seja $L = \langle a \rangle QR$. Como M coincide com seu centralizador, a sequência $(\langle a \rangle, Q, M)$ é uma torre de L e pelo Teorema A obtemos $h(L) = 3$. Observe que como $Q = [Q,a]$ temos $Q \leq \gamma_\infty(L) \leq F_2(L)$. Adicionalmente, temos $M \leq F(L)$, de modo que $F(L)$ é um p-grupo. Agora, $R(G)F(L)/F(L)$ é um 2-grupo e assim $R(G) \leq F_2(L)$. Seja S um 2-subgrupo de Sylow de R. Sendo $F_2(L)/F(L)$ um grupo nilpotente, temos que $[Q,S] \leq F(L)$ e, portanto, $[Q,S]$ é um p-grupo. Desde que $[Q,S] \leq [Q,R] \leq R$, concluímos que $[Q,S] \leq M$, isto é, Q centraliza S módulo M. Mas $G = [G,Q]$ e então G centraliza S módulo M. Obtemos assim que

$$R/M = Z(G/M).$$

A Proposição 3.19 agora permite concluir que $R/M = 1$, isto é, $R = M$. Mas isto é uma contradição. A prova está completa. □

Capítulo 4

Considerações Finais

Para concluir este trabalho, faremos alguns comentários sobre os principais resultados obtidos e sobre possíveis questões a serem abordadas em investigações futuras.

Seja G um CPPO-grupo finito solúvel. Pelo Teorema A e pelo Teorema B, sabemos que $h(G) \leqslant 3$ e $|\pi(G')| \leqslant 3$. Como comentamos anteriormente, a cota $h(G) \leqslant 3$ é a melhor possível, pois $h(S_4) = 3$. Entretanto, não sabemos se a cota $|\pi(G')| \leqslant 3$ é a melhor possível. Portanto, é interessante responder o questionamento abaixo.

Questão 1. Se G é um CPPO-grupo finito solúvel, então é verdade que $|\pi(G')| \leqslant 2$?

Seja agora G um CPPO-grupo finito não solúvel. Embora o Teorema A nos garanta que $h(R(G)) \leqslant 3$, sabemos em verdade que vale $h(R(G)) \leqslant 2$. De fato, pelo Teorema C temos que $R(G)' \leq R(G') \leq O_2(G)$ é um 2-grupo e, por isto, $1 \leq R(G)' \leq R(G)$ é uma série de Fitting de $R(G)$. Veja também que um p-subgrupo de Sylow de $R(G)$ é abeliano, para todo primo ímpar p. Por sua vez, o quociente $G/R(G)$ tem estrutura conhecida. De fato, claramente $R(G/R(G)) = 1$ e pelo Lema 3.15 vemos que $G/R(G)$ é quase-simples e

$$K(G/R(G)) = G'R(G)/R(G) \cong G'/R(G').$$

Pelo Lema 3.11 e pela Proposição 3.14 obtemos que $[G/R(G) : G'R(G)/R(G)] \leqslant 6$, isto é, $[G : G'R(G)] \leqslant 6$ e $G/G'R(G)$ é cíclico ou isomorfo ao grupo de Klein.

Após obtermos os principais resultados deste trabalho, ficou aparente a similaridade entre subgrupos derivados de CPPO-grupos finitos e EPPO-grupos. Então, a seguinte questão surgiu naturalmente.

Questão 2. É verdade que se G é um CPPO-grupo finito, então G' é um EPPO-grupo?

Na literatura existem diversos resultados sobre algumas classes de EPPO-grupos e neste trabalho foram citados como exemplo resultados sobre EPPO-grupos localmente finitos e sobre EPPO-grupos profinitos. Assim sendo, sugerimos os seguintes problemas:

Problema 1. Obter resultados estruturais sobre CPPO-grupos localmente finitos.

Problema 2. Obter resultados estruturais sobre CPPO-grupos profinitos.

Seja F um grupo livre, livremente gerado por um conjunto X. Dizemos que um elemento $w = w(x_1, \ldots, x_n) \in F$ é uma palavra. Dado um grupo G e elementos $g_1, \ldots, g_n \in G$, podemos observar w como sendo uma função de variáveis $x_1, \ldots, x_n$ e calcular o elemento $w(g_1, \ldots, g_n)$ de G. Assim sendo, o subgrupo verbal de G associado à palavra w pode ser definido como sendo o subgrupo $w(G) = \langle w(g_1, \ldots, g_n);\ g_1, \ldots, g_n \in G \rangle$.

Exemplo 4.1. A palavra comutador $w = x^{-1}y^{-1}xy$ é tal que para todo grupo G vale $w(G) = G'$.

Observe que os CPPO-grupos são precisamente os grupos nos quais todos os valores da palavra comutador têm ordens potência de primo. Com isto em mente, é razoável fazer o seguinte questionamento.

Questão 3. Para quais palavras w pode-se limitar a altura de Fitting dos grupos finitos solúveis tais que todos os w-valores têm ordens potência de primo?

Casos especiais de palavras são os comutadores simples $w_k = [x_1, \ldots, x_k]$, $k \geqslant 2$. Como caso particular do problema acima, temos o seguinte questionamento.

Questão 4. Assuma que G é um grupo finito solúvel no qual todos os w_k-valores têm ordens potência de primo. Então $h(G)$ é limitada?

Obs.: O Teorema A responde afirmativamente a Questão 4 no caso $k = 2$.

Agradecemos imensamente às contribuições dos professores Dr. Mohsen Amiri (UFAM), Dr. Igor (UnB) e Dr. Martino Garonzi (UnB) para formulação de alguns dos problemas supracitados.

Bibliografia

[1] Bannuscher, W. and Tiedt, G. (1994). On a theorem of Deaconescu. *Rostok. Math. Kolloq.*, 47:23–26.

[2] Brandl, R. (1981). Finite groups all of whose elements are of prime power order. *Boll. Un. Mat. Ital. A (5)*, 18:491–493.

[3] Casolo, C., Jabara, E., and Spiga, P. (2014). On the fitting height of factorised soluble groups. *J. Group Theory*, 17(5):911–924.

[4] Deaconescu, M. (1989). Classification of finite groups with all elements of prime order. *Proc. Amer. Math. Soc.*, 106:625–629.

[5] Delgado, A. L. and Wu, Y.-F. (2002). On locally finite groups in which every element has prime power order. *Illinois J. Math.*, 46:885–891.

[6] Gorenstein, D. (1980). *Finite Groups*. Chelsea Publishing Company, New York, 2 edition.

[7] Heineken, H. (2006). On groups all of whose elements have prime power order. *Math. Proc. R. Ir. Acad.*, 106A:191–198.

[8] Higman, G. (1957). Finite Groups in Which Every Element Has Prime Power Order. *J. Lond. Math. Soc.*, s1-32:335–342.

[9] Hölder, O. (1895). Bildung zusammengesetzter gruppen. *Math. Ann.*, 46:321–422.

[10] Janusz, G. and Rotman, J. (1982). Outer automorphisms of S_6. *Amer. Math. Monthly*, 89:407–410.

[11] Kurosh, A. G. (1969). *Theory of Groups, Volume 2*. Chelsea Publishing Series. American Mathematical Society, 2 edition.

[12] Kurzweil, H. and Stellmacher, B. (2004). *The Theory of Finite Groups: An Introduction*. Universitext. Springer-Verlag.

[13] Lewis, M. L. (2023). Groups having all elements off a normal subgroup with prime power order. *Vietnam J. Math.*, 51:577–587.

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

[15] Liebeck, M. W., O'Brien, E. A., Shalev, A., and Tiep, P. H. (2011). Commutators in finite quasisimple groups. *Bull. Lond. Math. Soc.*, 43:1079–1092.

[16] Lucchini, A., Menegazzo, F., and Morigi, M. (2003). On the existence of a complement for a finite simple group in its automorphism group. *Illinois J. Math.*, 47:395 – 418.

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

[18] Rose, H. E. (2009). *A Course on Finite Groups*. Universitext. Springer, London.

[19] Shumyatsky, P. (1999). On groups with commutators of bounded order. *Proc. Amer. Math. Soc.*, 127:2583–2586.

[20] Shumyatsky, P. (2020). Profinite groups in which many elements have prime power order. *J. Algebra*, 562:188–199.

[21] Suzuki, M. (1961). Finite groups with nilpotent centralizers. *Trans. Amer. Math. Soc.*, 99:425–470.

[22] Suzuki, M. (1962). On a class of doubly transitive groups. *Ann of Math.*, 75:105–145.

[23] Thompson, J. G. (1959). Finite groups with fixed-point-free automorphisms of prime order. *Proc. Natl. Acad. Sci. USA*, 45:578–581.

[24] Turull, A. (1984). Fitting height of groups and of fixed points. *J. Algebra*, 86(2):555–566.

[25] Wilson, R. A. (2009). *The Finite Simple Groups*. Graduate Texts in Mathematics. Springer.

[26] Yang, W. and Zhang, Z. (2002). Locally soluble infinite groups in which every element has prime power order. *Southeast Asian Bull. Math.*, 26:857–864.