Universidade de Brasília
Departamento de Matemática
Programa de Pós-Graduação em Matemática

DISSERTAÇÃO

Grupos Central-por-Finito: Coberturas de Grupos e um Problema de Paul Erdős

Aluno: Rebeca Chuffi Saccochi
Orientadora: Cristina Acciarri

Brasília, dezembro de 2015

Rebeca Chuffi Saccochi[1]

Grupos Central-por-Finito: Coberturas de Grupos e um Problema de Paul Erdős

Dissertação apresentada ao Programa de Pós-Graduação em Matemática do Departamento de Matemática da Universidade de Brasília, em cumprimento às exigências para obtenção do Título de Mestre em Matemática

Orientadora: Profa. Cristina Acciarri

[1]O aluno foi bolsista de mestrado da CAPES/CNPq

Agradecimentos

Gostaria de agradecer aos meus pais, Vinícius Antunes Saccochi e Caroline Nakad Chuffi, e à minha irmã, Lara Chuffi Saccochi, pelo amor e paciência durante todos esses anos, mesmo nos momentos difíceis.

À minha orientadora, Cristina Acciarri, pela paciência, extrema dedicação ao trabalho que fizemos e conselhos valiosos tanto em termos acadêmica como para vida.

Aos professores e trabalhadores do Departamento de Matemática. Em particular, ao Professor José Antônio de Freitas, pela paciência ao ministrar a primeira matéria de Álgebra que eu fiz na graduação. À Professora Aline Pinto, pelas explicações excepcionais, pelo quadro impecável e por ser um exemplo de pessoa e de profissional. Ao Professor Celius Magalhães, por me ter me ajudado a superar meus medos e por ter acrescentado muito à minha formação acadêmica. À Professora Cátia Regina Gonçalves, pela sua maneira bem humorada de levar a vida que é uma inspiração para mim.

À Jéssyca Cristine Souza, pelo apoio incondicional em toda essa jornada, desde o primeiro semestre da graduação, sem ela com certeza eu não alcançaria metade do que foi conquistado. Muito obrigada por ser paciente, me acompanhar desde sempre e sempre me achar no cantinho da tristeza depois das provas.

À Angélica Felix, por ter me acompanhado desde a graduação, por ser essa amiga super atenciosa e mais importante, ser uma pessoa sincera e me fazer ter certeza de que todas as minhas sapatilhas são estranhas. Obrigada por tudo, amiga. Ao Bruno Xavier, pelas conversas descontraídas, pela ajuda em Geometria Diferencial e por me carregar no LoL.

Ao Leandro Chiarini, uma pessoa que me divertiu por anos. Nunca esquecerei da integral de "$ln(x)cos(x)$". Além disso, um amigo que me ajudou bastante, não só em termos de Matemática, mas me protegendo de pessoas que encaram meu sapato. Ao Michell Dias, pelos momentos divertidos de estudo na sala do mestrado e pelo companheirismo em todo esse período de mestrado (inclusive nos momentos de comer torta do natural no meio da tarde).

Ao Victor Barbosa Jatobá, por ter me ajudado ao longo desses quatro anos e três meses e por ter me influenciado a seguir esse caminho acadêmico. E também por ter me abandonado e fugido pra Chicago e me obrigado a me esforçar ainda mais para que tudo desse certo. Obrigada pelo apoio desde o começo (e até o fim, já era).

AGRADECIMENTOS

Aos meus treze gatos, Janine, Márcia, Fanha, Carinhosa, Mundo, Doce, Lili, Pietro, Irina, Tigor, Mandioca, Bumba e Macaxeira, por terem me acalmado em momentos de estresse e estarem sempre dispostos a me acompanhar.

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

Sumário

RESUMO

Um grupo G é dito central-por-finito se o índice do centro $[G : Z(G)]$ é finito. É possível caracterizar a classe dos grupos central-por-finito de várias maneiras. Uma dessas, devida a R. Baer [**19**], assegura que um grupo é central-por-finito se, e somente se ele admite uma cobertura finita por subgrupos abelianos. A partir de um problema de teoria dos grafos proposto por Paul Erdős, B. H. Neumann [**18**, 4.4] caracterizou os grupos central-por-finito de outra maneira, assegurando que um grupo é central-por-finito se, e somente se ele é um PE-grupo, isto é, um grupo cujo grafo não-comutativo $\Gamma(G)$ não possui subgrafos completos infinitos.

Essas duas caracterizações levam a considerar, de maneira natural, três indicadores numéricos relacionados a um grupo central por finito. Primeiro, $[G : Z(G)]$, o índice do centro, segundo, $a(G)$, o número mínimo de subgrupos abelianos necessários para cobrir o grupo G de forma irredundante, e terceiro, $\omega(G)$, o tamanho do maior subgrafo completo de $\Gamma(G)$, isto é, o tamanho do maior clique do grafo $\Gamma(G)$. Um problema interessante então é relacionar essas três quantidades, encontrando cotas de uma em função de outra e também determinar condições sob as quais valem as igualdades. Em geral, dado G um grupo central-por-finito, sempre temos que $\omega(G) \leq a(G) \leq [G : Z(G)] \leq c^{\omega(G)}$, onde c é uma constante. Além disso, quando G é finito, é natural relacionar os indicadores $[G : Z(G)]$, $a(G)$ e $\omega(G)$ não só entre eles, mas também com a ordem de G.

Portanto, neste trabalho vamos estudar as duas caracterizações de grupos central-por-finito mencionadas anteriormente, relacionar os três indicadores numéricos $\omega(G)$, $a(G)$ e $[G : Z(G)]$ e apresentar vários exemplos, entre eles a família de grupos extraespeciais de ordem p^{2n+1}.

Palavras-chave: Grupos Central-por-finito, PE-grupos, Coberturas de Grupos, Grafo não-comutativo.

Abstract

A group G is said to be central-by-finite if the index of the center $[G : Z(G)]$ is finite. It is possible to characterize the class of central-by-finite groups in many ways. One of them, due to R. Baer [**19**], guarantees that a group G is central-by-finite if and only if G can be covered by finitely many abelian subgroups. Motivated by a question on graph theory proposed by Paul Erdős, B. H. Neumann [**18**, 4.4] has characterized central-by-finite groups in a different way, ensuring that a group G is central-by-finite if and only if G is a PE-group, that is, a group whose non-commuting graph $\Gamma(G)$ contains no infinite complete subgraph.

Both characterizations lead us to consider, in a natural manner, three numerical indicators related to a central-by-finite group. First, $[G : Z(G)]$, the index of the center, second, $a(G)$, the minimum number of abelian subgroups necessary to cover the group G in an irredundant way, and finally, $\omega(G)$, the size of the biggest complete subgraph of $\Gamma(G)$, that is, the size of the biggest clique of $\Gamma(G)$. It is interesting, then, to relate those three quantities, finding bounds of one in function of the other and also determining conditions under which equalities hold. In general, for a central-by-finite group G we have that $\omega(G) \leq a(G) \leq [G : Z(G)] \leq c^{\omega(G)}$, where c is a constant. Besides that, when G is finite, it is natural to relate the indicators $[G : Z(G)]$, $a(G)$ e $\omega(G)$ not only with each other, but also with the order of G.

Therefore, in this essay we are going to study the two characterizations mentioned above, relate the three numerical indicators $\omega(G)$, $a(G)$ and $[G : Z(G)]$, and present many examples, among them, the class of extraspecial p-groups of order p^{2n+1}.

Keywords: Central-By-Finite Groups, PE-groups, Covering of Groups, Non-Commuting Graph.

Introdução

Seja G um grupo arbitrário, denotamos por $Z(G)$ o centro de G. Uma forma de medir quão "longe" um grupo é de ser abeliano é dada achando o índice $[G : Z(G)]$ de $Z(G)$ em G, já que G é abeliano se, e somente se $[G : Z(G)] = 1$. Dizemos que G é um grupo central-por-finito se o índice do centro $[G : Z(G)]$ é finito. Um resultado bem conhecido devido a R. Baer [**24**] caracteriza os grupos central-por-finito como grupos que admitem uma cobertura finita por subgrupos abelianos, isto é, grupos que podem ser vistos como a união de um número finito de subgrupos abelianos. Uma das implicações desse resultado é óbvia, pois se G é central-por-finito, podemos escolher um transversal $T = \{t_1, \ldots, t_n\}$ para $Z(G)$ sobre G e considerando os subgrupos $A_i = \langle Z(G), t_i\rangle$, temos que G pode ser visto como a união de n subgrupos abelianos A_i. A outra implicação do teorema de Baer é menos óbvia e segue de um resultado de B. H. Neumann [**19**], que trata de coberturas finitas de um G por classes laterais de subgrupos e garante que dada qualquer cobertura de um grupo G por um número finito de classes laterais de subgrupos H_i, sempre é possível retirar as classes laterais dos respectivos subgrupos de índice infinito sem perder a propriedade de cobertura de G. Essa observação aplicada ao nosso caso, garante que dada uma cobertura finita de G por subgrupos abelianos, sempre podemos excluir da mesma subgrupos de índice infinito, sem, por isso, perder a propriedade de cobertura de G. Sabendo disso, é simples achar um subgrupo central de índice finito em G.

Em vista dessa caracterização, dado G um grupo central-por-finito, é natural considerar o conceito de cobertura irredundante de G por subgrupos abelianos e definir o número $a(G)$ como o tamanho da menor cobertura irredundante de G por abelianos. Em particular, surge a questão: dado G um grupo central-por-finito, que relação existe entre o índice do centro $n = [G : Z(G)]$ e $a(G)$? De fato, B. H. Neumann em [**19**] observa que se o índice do centro de G é n, então $a(G) \leq n$ e que a igualdade vale se, e somente se $n = 1$. É possível também encontrar uma cota superior para n dependendo apenas de $a(G)$, porém a prova é mais técnica. De fato é possível estudar um problema mais geral, ou seja, considerar uma cobertura finita de G por classes laterais de subgrupos. Um caso particular dessas coberturas é justamente uma cobertura dada por subgrupos e quando nos reduzimos a esse caso, adicionando algumas condições sobre as interseções dos subgrupos da cobertura acha-se uma cota do tipo $n \leq c^{2^{a(G)}}$, onde c é uma constante.

Outra forma de olhar quando um grupo é "distante" de ser abeliano é considerando a relação de comutatividade entre pares de elementos em G. De fato, G será abeliano se, e somente se para todo par x e y de elementos de G, temos que x e y comutam. Portanto, se um grupo é abeliano e queremos achar um conjunto (não unitário) de elementos distintos que não comutam dois a dois, não achamos tal conjunto. Agora, considerando um grupo não-abeliano, sempre temos subconjuntos de elementos distintos que não comutam dois a dois e o maior tamanho desse subconjunto em G (quando for possível definir) dará informações sobre o quão "longe" de ser abeliano é o grupo. Notamos que existe uma maneira muito intuitiva de representar esses conceitos, associando a G um grafo.

Dado G um grupo, há várias maneiras de associar a G um grafo. Chamamos de grafo não-comutativo de G, denotado por $\Gamma(G)$, o grafo não-direcionado cujo conjunto de vértices é o conjunto de elementos de G e dois vértices x e y são ligados por uma aresta se, e somente se $[x, y] \neq 1$, isto é, se e somente se x e y não comutam como elementos de G. Em geral, dado Γ um grafo e V seu conjunto de vértices, um subconjunto X de V é dito um clique de Γ se o subgrafo induzido por X é completo, em outras palavras, se todos vértices de X estão conectados dois a dois por uma aresta. Considerando o grafo não-comutativo $\Gamma(G)$, um clique dele corresponde a um subconjunto de G cujos elementos não comutam dois a dois. Paul Erdős, em 1975, propôs o seguinte problema:

Seja G um grupo tal que $\Gamma(G)$ não contém nenhum subgrafo infinito completo; existe uma cota superior finita para a cardinalidade de um subgrafo completo de $\Gamma(G)$?

Chamaremos os grupos cujo grafo $\Gamma(G)$ não tem cliques infinitos de grupos de Paul Erdős, ou somente PE-grupos. B. H. Neumann [**18**] respondeu a essa questão afirmativamente, isto é, para G um PE-grupo, existe cota superior finita para a cardinalidade de um clique de $\Gamma(G)$. O interessante é que B. H. Neumann não somente mostra a existência de uma cota, mas de fato também prova que a classe dos PE-grupos coincide exatamente com a classe dos grupos central-por-finito. Lembramos que um grupo cujas classes de conjugação são todas finitas é chamado um FC-grupo. A ideia principal de Neumann foi mostrar que tanto PE-grupos quanto grupos central-por-finito são FC-grupos e logo ver que se G é um FC-grupo mas não é central-por-finito, então ele não pode ser um PE-grupo. Dessa forma, vemos que se G é um PE-grupo, então G é central-por-finito. A recíproca vem de uma observação mais elementar: se G é central-por-finito e seu centro tem índice n, então dados quaisquer $n + 1$ elementos de G, pelos menos dois deles estão na mesma classe lateral de $Z(G)$ e portanto comutam. Em vista da caracterização provada por Neumann é natural definir para um PE-grupo a quantidade $\omega(G)$, a cardinalidade do maior clique de $\Gamma(G)$. Em particular, segue que se $n > 1$ é o índice do centro, então $\omega(G) \leq n - 1$.

Agora, dado G um grupo central-por-finito, como ele é um PE-grupo, uma questão interessante é perguntar se é possível obter uma cota para $n = [G : Z(G)]$ em função de $\omega(G)$.

Em [**22**], L. Pyber mostrou que se G é um grupo tal que $\omega(G)$ é finito (de fato, ele é um PE-grupo), então existe uma constante c tal que $n \leq c^{\omega(G)}$. A ideia principal dessa demonstração foi reduzir o problema ao estudo de p-grupos de classe de nilpotência 2. De fato, Pyber encontra um subgrupo C tal que $C' \leqslant Z(C)$, de classe no máximo 2 em G e logo, usando a cadeia de subgrupos $Z(G) \leqslant Z(C) \leqslant C \leqslant G$ acha a cota desejada para o índice de $Z(G)$.

Das duas caracterizações citadas acima, segue que sempre temos três indicadores numéricos relacionados a um grupo G central-por-finito, n, o índice do centro, $a(G)$, o tamanho da menor cobertura irredundante finita de G por subgrupos abelianos e $\omega(G)$, a cardinalidade do maior clique de $\Gamma(G)$. Da mesma forma como já foi observada a relação entre n e $\omega(G)$ e entre n e $a(G)$, é também natural relacionar $\omega(G)$ com $a(G)$. Em [**3**], E. A. Bertram observa que como dois elementos de um clique de $\Gamma(G)$ não comutam, eles nunca podem pertencer a um mesmo subgrupo abeliano em uma cobertura finita de G. Assim, $\omega(G) \leq a(G)$. Considerando essa cota superior, é interessante nos perguntarmos quando temos a igualdade. Uma condição suficiente para que $\omega(G) = a(G)$ é pedir que todos os centralizadores dos elementos não centrais de G sejam abelianos. Com esse resultado é fácil verificar, por exemplo, que grupos não abelianos de ordem pq com p e q primos, $p < q$ e $q \equiv 1(\mathrm{mod} p)$ sãos tais que $\omega(G) = a(G)$, assim como os grupos extraespeciais de ordem p^3, para $p \geq 2$. Por outro lado, em [**3**] Bertram apresenta uma elegante prova devida a I. M. Isaacs da existência de uma função monótona f tal que $a(G) \leq f(\omega(G))$, o que nos dá uma cota superior para $a(G)$ em função de $\omega(G)$ do tipo $a(G) \leq (\omega(G)!)^2$. Resumindo, se G é um grupo central-por-finito, em geral temos que $\omega(G) \leq a(G) \leq [G : Z(G)] \leq c^{\omega(G)}$, para alguma constante c.

Notamos como as várias caracterizações dos grupos central-por-finito nos levam a relacionar entre si a quantidade $\omega(G)$, associada mais às características do grafo $\Gamma(G)$, e os indicadores $a(G)$ e $[G : Z(G)]$, mais explicitamente associados aos aspectos puramente estruturais do grupo G. De qualquer forma as estreitas relações entre essas quantidades são naturais, já que todas elas nos dão informações sobre as relações de comutatividade entre os elementos de G e, em algum sentido, todos medem quanto um grupo não-abeliano G está "longe" de ser abeliano. Como foi mencionado, um grupo G central-por-finito é sempre um FC-grupo e portanto faz sentido definir $k(G)$ como a maior cardinalidade de uma classe de conjugação em G. Veremos também que $k(G)$ tem uma relação estreita com os demais indicadores e tem um papel importante na obtenção de algumas das cotas.

Agora restringindo nossa atenção a um grupo finito G, surge naturalmente a questão de relacionar os três indicadores $\omega(G)$, $a(G)$ e $[G : Z(G)]$ não somente entre eles, mas também com a cardinalidade de G. Além da óbvia relação entre $|G|$ e o índice do centro de G, queremos destacar que em [**16**], D. R. Mason provou que para um grupo de ordem finita existe um inteiro $k \leq |G|/2 + 1$ e subgrupos abelianos $A_1, \ldots, A_k$ que formam uma cobertura irredundante de G. Assim, em particular temos que $a(G) \leq [|G|/2] + 1$. Ao que diz respeito a relação entre $\omega(G)$ e a cardinalidade de G, em [**3**] Bertram mostra, usando também um argumento de Teoria de Grafos, que se G é um grupo finito contendo um subgrupo próprio

M tal que para qualquer elemento não trivial x de M temos $C_G(x) \leqslant M$, então $\omega(G) \geq [|G|^{1/3}]$, onde $[r]$ é o maior inteiro menor ou igual a r. Em particular, desse resultado segue que se G é um grupo finito não-abeliano, p é um primo que divide a ordem de G e existe x em G tal que $C_G(x)$ tem ordem p, então $\omega(G) \geq [|G|^{1/3}]$.

Analisaremos os 2-grupos extraespeciais de ordem 2^{2a+1}. Para esses grupos, um resultado devido a I. M. Isaacs diz que $a(G) \geq 2^a + 1$ e $\omega(G) = 2a + 1$. Além disso, veremos que p-grupos extraespeciais de tamanho 2^{2a+1} e $a > 2$ nunca satisfazem $\omega(G) = a(G)$.

Em conclusão, essa dissertação tem como objetivo caracterizar e analisar grupos central-por-finito, relacionando os três indicadores numéricos $\omega(G)$, $a(G)$ e $[G : Z(G)]$ apresentados acima. O trabalho está dividido em cinco capítulos e um apêndice. No Capítulo 1, iremos lembrar alguns resultados e definições básicas de Teoria de Grupos que serão utilizados ao longo da dissertação. No Capítulo 2, vamos apresentar algumas definições de Teoria de Grafos, bem como algumas observações e resultados sobre grafos não-comutativos e uma versão infinita do teorema de Ramsey. No Capítulo 3, apresentaremos os resultados de Baer e Neumann caracterizando das duas maneiras já citadas grupos central-por-finito. No Capítulo 4 analisaremos as relações entre os indicadores quantitativos, $\omega(G)$, $a(G)$ e $[G : Z(G)]$, associados a um grupo central-por-finito. No Capítulo 5 vamos considerar a família dos grupos extraespeciais e analisar os indicadores $\omega(G)$, $a(G)$ e $[G : Z(G)]$ neste caso específico. Finalmente, no Apêndice vamos definir uma função para o programa GAP utilizada para construir o grafo não-comutativo de um grupo finito G e também iremos apresentar alguns detalhes técnicos de algumas demonstrações "analíticas" utilizadas nessa dissertação.

Capítulo 1

Preliminares

O capítulo a seguir tem como objetivo apresentar definições e resultados a respeito de Teoria de Grupos que serão utilizados ao longo deste trabalho. Assumiremos os Teoremas de Isomorfismo e o Teorema de Lagrange. Utilizamos como referências principais os livros de I. M. Isaacs, [**8**] e de D. Robinson [**23**].

Dado um grupo G, denotamos um subgrupo H de G por $H \leqslant G$. Um subgrupo próprio M de G é dito *maximal* se sempre que M está contido em H, para H um subgrupo, ou $M = H$ ou $G = H$. Definimos então o *subgrupo de Frattini*, denotado por $\Phi(G)$, como a interseção de todos os subgrupos maximais de G. Se G não tem subgrupos maximais, então definimos $\Phi(G) = G$.

Dado H um subgrupo de G, podemos definir uma relação de equivalência nos elementos de G da seguinte maneira:

$$x \sim y \Leftrightarrow xy^{-1} \in H.$$

Assim, as classes de equivalência dessa relação são chamadas de *classes laterais* de H em G. Se escolhermos um único elemento de cada classe lateral distinta, teremos um subconjunto T de G chamado *transversal* de H em G. Podemos definir as classes laterais à direita ou a esquerda, isto é, $\{Ha \mid a \in G\}$ ou $\{aH \mid a \in G\}$. O número de classes laterais à direita é mesmo que o número de classes laterais à esquerda e é chamado de *índice* de H em G. Denotaremos por $[G : H]$ o número de classes laterais. Um subgrupo N de G é dito *normal* se $gN = Ng$, para todo G em g e é denotado por $N \trianglelefteq G$. Definimos *centro de G* por $Z(G) = \{x \in G \mid xg = gx, \forall g \in G\}$ e temos que $Z(G)$ é um subgrupo normal de G. Se $K \leqslant H \leqslant G$, então

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

Vamos lembrar alguns resultados sobre índices de subgrupos.

Proposição 1.0.1. *Seja* $H, K \leqslant G$. *Então* $[G : H \cap K] \leq [G : H][G : K]$.

Demonstração. Denotaremos o conjunto de classes laterais à esquerda de um subgrupo $D \leqslant G$ por $\{aD\}$. Note que $H, K \leqslant G$, então $H \cap K$ também é um subgrupo de G. Considere a função $\varphi : \{a(H \cap K)\} \to \{aH\} \times \{aK\}$ tal que $\varphi(a(H \cap K)) = (aH, aK)$. Vamos mostrar que φ está bem definida. De fato, dados $a(H \cap K)$ e $b(H \cap K)$ em $\{a(H \cap K)\}$ temos que ab^{-1} está em $H \cap K$, isto é, ab^{-1} está em H e ab^{-1} está em H. Assim, por definição, $aH = bH$ e $aK = bK$, logo $\varphi(a(H \cap K)) = (aH, aK) = (bH, bK) = \varphi(b(H \cap K))$. Portanto φ está bem definida. Agora basta mostrar que φ é injetiva. Se $\varphi(a(H \cap K)) = \varphi(b(H \cap K))$, temos que $(aH, aK) = (bH, bK)$, e assim $aH = bH$ e $aK = bK$. Logo, ab^{-1} está em $H \cap K$, então $a(H \cap K) = b(H \cap K)$, e portanto φ é injetiva. Assim, temos o resultado. □

Da mesma forma temos que se $A_1, \ldots A_n$ são subgrupos de G,

$$[G : \textstyle\bigcap_{i=1}^{n} A_i] \leq [G : A_1] \cdots [G : A_n]. \tag{1.0.1}$$

Proposição 1.0.2. *Sejam G um grupo e H e K subgrupos de G. Se H e K têm índice finito em G e* $[G : H \cap K] = [G : H][G : K]$, *então* $G = HK$.

Demonstração. Primeiro temos que

$$[G : H \cap K] = [G : H][H : H \cap K] = [G : H][HK : K].$$

Logo, se $[G : H \cap K] = [G : H][G : K]$, então $[G : K] = [HK : K]$. Mas também temos que $[G : K] = [G : HK][HK : K] = [G : HK][G : K]$, logo $[G : HK] = 1$, isto é, $G = HK$. □

Dado X subconjunto de G, dizemos que G é *gerado* por X se sempre que g pertence a G, podemos escrever $g = c_1 \cdots c_n$ tais que c_i está em X ou c_i^{-1} está em X. Nesse caso, denotamos $G = \langle X \rangle$. Se X é finito, dizemos que G é *finitamente gerado*.

Proposição 1.0.3. *Seja H um subgrupo próprio de um grupo G tal que o índice* $[G : H]$ *é finito e seja p o menor divisor de* $[G : H]$. *Então existem um inteiro positivo* $1 \leq m \leq log_p[G : H]$ *e elementos* $x_1, \cdots, x_m$ *em G tais que* $G = \langle x_1, \cdots, x_m, H \rangle$.

Demonstração. Definimos $H_0 = H$ e para $j \geq 1$, definimos $H_j = \langle x_j, H_{j-1} \rangle$ para x_j algum elemento escolhido em $G \setminus H_{j-1}$ enquanto $H_{j-1} < G$. Como $[G : H]$ é finito, temos que existe um $m \geq 1$ tal que $H_m = G$. Dessa maneira, construímos a série de subgrupos $H = H_0 < H_1 < \cdots < H_m = G$. Agora temos que $[H_j : H_{j-1}]$ divide o índice de $[G : H]$ e como o menor primo que divide $[G : H]$ é p, temos que $[H_j : H_{j-1}] \geq p$. Assim,

$$[G : H] = [H_m : H_{m-1}] \cdots [H_1 : H_0] \geq p^m.$$

Logo, temos que $m \leq log_p[G : H]$.

Para completar a nossa demonstração, notamos que $G = H_m = \langle x_m, H_{m-1} \rangle = \cdots = \langle x_1, \cdots, x_m, H \rangle$, como queríamos. □

Agora, o menor primo p que divide a ordem de $[G : H]$ satisfaz $2^m \leq p^m$, então a Proposição 1.0.3 para $p = 2$ vale para qualquer subgrupo próprio de índice finito de G.

A *ordem* de um grupo é definida como a cardinalidade desse grupo. Seja g um elemento de G. A ordem de g, denotada por $o(g)$ é definida como $o(g) = n$, se n é o menor número inteiro não negativo tal que $x^n = 1$, e $o(g) = \infty$ caso contrário. Definimos o *expoente* de um grupo, denotado por $exp(G)$, o menor inteiro positivo m tal que $x^m = 1$ para todo x em G, quando esse inteiro existe. Caso contrário definimos $exp(G) = \infty$. A demonstração do próximo resultado pode ser encontrada em [**23**, 1.6.17]

Proposição 1.0.4 (Teorema de Cauchy). *Se p é um primo que divide a ordem de um grupo finito G, então G contém um elemento de ordem p.*

Agora vamos definir e apresentar algumas propriedades de comutadores. Dados x e y em G, o *comutador de x e y*, denotado por $[x, y]$, é definido por $[x, y] = x^{-1}y^{-1}xy$. Dizemos que x é igual o *conjugado* de y por u quando $x = u^{-1}yu$ e denotaremos $u^{-1}yu = y^u$. Temos também que $(g^{-1})^u = u^{-1}g^{-1}u$ e $g^u u^{-1}g^{-1}u = 1$ então,

$$(g^{-1})^u = (g^u)^{-1}. \tag{1.0.2}$$

Temos que x e y comutam se, e somente se, $[x, y] = 1$. Temos também que se x comuta com y, $xy = yx$, então $yx^{-1} = x^{-1}y$, portanto x^{-1} comuta com y.

Proposição 1.0.5. *Seja G um grupo e x, y e z elementos quaisquer de G, temos que:*

i) $[x, y] = [y, x]^{-1}$;
ii) $[xy, z] = [x, z]^y[y, z]$;
iii) $[x, yz] = [x, z][x, y]^z$.

As igualdades acimas são simples de verificar. A seguir vamos definir o conceito de ação de um grupo G em um conjunto não vazio X para apresentar a Equação das Classes.

Definição 1.0.6. Seja G um grupo e X um conjunto. Dizemos que G *age em* X se existe uma função $G \times X \to X$ definida por $(g, x) \mapsto x^g$, onde x^g é um elemento de X definido unicamente, e se além disso as seguintes igualdades valem:

(i) $x^1 = x$, para x em X;
(ii) $x^{gh} = (x^g)^h$, para x em X e g, h em G.

Dada uma ação de G em um conjunto X, é possível definir o *estabilizador* de um elemento em X, um subgrupo de G definido por

$$\mathrm{Stab}_G(x) = \{g \in G \mid x^g = x\}.$$

Podemos também definir subconjuntos de X, chamados *órbitas* de um elemento x em X, que formam uma partição de X, da seguinte maneira,

$$\mathrm{Orb}_G(x) = \{x^g \mid g \in G\}.$$

Por exemplo, podemos considerar a ação de G em G por conjugação, isto é, se x e g estão em G, definimos $x^g = x^{-1}gx$. Neste caso, $\mathrm{Stab}_G(x) = C_G(x)$ e $\mathrm{Orb}_G(x) = Cl(x)$, a classe de conjugação de x. A partir dessas definições, podemos apresentar o seguinte resultado que pode ser encontrado em [**8**, 4.10 Corollary]:

Teorema 1.0.7 (Equação das Classes). *Seja G um grupo e $Cl(x)$ a classe de conjugação de x. Então, para x em G temos que*

$$[G : C_G(x)] = |Cl(x)|.$$

Seja p um primo. Dizemos que G é um *p-grupo* se a ordem de G é p^b, para b um inteiro não negativo. Seja G um grupo qualquer, se H é um subgrupo de G e ao mesmo tempo é um p-grupo, então dizemos que H é um p-subgrupo de G. Agora se $|G| = p^\alpha m$ e p não divide m, dizemos que P é um *p-subgrupo de Sylow* se P é um subgrupo de G de ordem p^α. A seguir lembramos um dos resultados mais importantes sobre subgrupos de Sylow de um grupo finito. Os detalhes da demonstração podem ser encontrados em [**23**, 1.6.16]

Teorema 1.0.8 (Teorema de Sylow). *Seja G um grupo finito e p um número primo. Se $|G| = p^\alpha m$ tal que p não divide m, então:*

(i) Todo p-subgrupo de G está contido em algum p-subgrupo de Sylow. Em particular, p-subgrupos de Sylow sempre existem;

(ii) Se n_p é o número de p-subgrupos de Sylow em G, então $n_p \equiv 1 (\mathrm{mod}\, p)$;

(iii) Todos os p-subgrupos de Sylow são conjugados em G.

Capítulo 2

Grafos

O objetivo deste capítulo é explanar algumas noções básicas sobre Teoria de Grafos. Como principal referência deste capítulo usaremos o livro *Graph theory with applications* [**4**] de J. A. Bondy e U. S. R. Murty. Apresentaremos também resultados relacionados ao grafo não-comutativo de um grupo, bem como uma versão do Teorema de Ramsey.

2.1 Definições e resultados básicos

Intuitivamente, um grafo é pensado como um diagrama que contém um conjunto de pontos e um conjunto de linhas que ligam alguns desses pontos. Apresentaremos a definição formal de grafo abaixo, porém podemos visualizá-lo como um diagrama formado por pontos e linhas, como descrito acima, de forma que a parte relevante será definir quando dois pontos são ligados.

Definição 2.1.1. Um *grafo não direcionado* Γ é um trio ordenado $\{V(\Gamma), E(\Gamma), \psi_\Gamma\}$ que consiste de um conjunto não vazio $V(\Gamma)$, cujos elementos são chamados de vértices, um conjunto $E(\Gamma)$ disjunto de $V(\Gamma)$, cujos elementos são chamados de arestas e uma função ψ_Γ, chamada função de incidência, que associa cada aresta de Γ, isto é, cada elemento de $E(\Gamma)$, a um par não ordenado de vértices (não necessariamente distintos) de Γ. Se e é uma aresta e u e v é o par de vértices tal que $\psi_\Gamma(e) = (u, v)$ então dizemos que e liga u e v ou, de forma equivalente, que u e v são as extremidades de e.

Note que, mesmo utilizando o símbolo (u, v) para representar uma aresta ligando u e v, este par não é ordenado. Todos os grafos aqui considerados serão grafos não direcionados, por isso nos referiremos a eles simplesmente como grafos.

Definição 2.1.2. Um grafo Γ' é dito subgrafo de um grafo Γ, denotado por $\Gamma' \subseteq \Gamma$, se $V(\Gamma') \subseteq V(\Gamma), E(\Gamma') \subseteq E(\Gamma)$ e $\psi_{\Gamma'}$ é a restrição de ψ_Γ a $E(\Gamma')$. Dizemos que dois subgrafos são disjuntos se eles não tem vértices em comum.

Exemplo 2.1.3. Considere $V(\Gamma) = \{v_1, v_2, v_3, v_4, v_5\}$ e $E(\Gamma) = \{e_1, e_2, e_3, e_4, e_5, e_6, e_7, e_8\}$ com a seguinte função de incidência:

$$\psi_\Gamma(e_1) = (v_1, v_2),\ \psi_\Gamma(e_2) = (v_2, v_3),\ \psi_\Gamma(e_3) = (v_3, v_3),\ \psi_\Gamma(e_4) = (v_3, v_4),$$

$$\psi_\Gamma(e_5) = (v_2, v_4),\ \psi_\Gamma(e_6) = (v_4, v_5),\ \psi_\Gamma(e_7) = (v_2, v_5),\ \psi_\Gamma(e_8) = (v_2, v_5).$$

Como mencionamos anteriormente, podemos representar as arestas e_i por linhas e os vértices v_i por pontos. Tais pontos (vértices) são ligados por uma linha (aresta) de acordo com a função de incidência ψ_Γ. Por exemplo, $\psi_\Gamma(e_1) = (v_1, v_2)$ significa que temos dois pontos (vértices), v_1 e v_2, que devem ser ligados pela linha (aresta) e_1. Podemos então representar esse grafo da seguinte maneira:

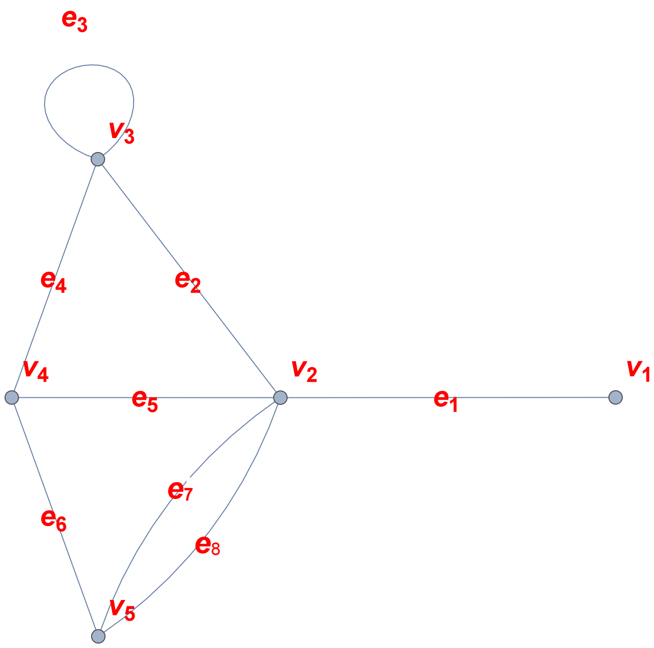

FIGURA 2.1.1. Exemplo de grafo Γ

DEFINIÇÃO 2.1.4. As extremidades de uma aresta são ditas *incidentes* à aresta e a aresta é dita *incidente* às suas extremidades. Dois vértices incidentes à mesma aresta são chamados *adjacentes* bem como duas arestas incidentes ao mesmo vértice. Uma aresta com extremidades iguais é chamada de *laço* e com extremidades distintas é chamada de *link*.

Para ilustrar a definição acima, voltemos a Figura 2.1.1. Os vértices v_3 e v_2 são incidentes à aresta e_2 (portanto v_3 e v_2 são adjacentes) e a aresta e_2 por sua vez, é incidente aos vértices v_3 e v_2. As arestas e_1, e_2, e_5, e_7 e e_8 são adjacentes duas a duas, pois são incidentes ao mesmo vértice comum v_2. Como a aresta e_3 tem extremidades iguais a v_3, e_3 é um laço e e_2, por sua vez, é um exemplo de link.

Existem várias maneiras de associar um grafo a um grupo. Neste trabalho utilizaremos o *grafo não-comutativo* associado a um grupo G, que pode ser definido como segue:

DEFINIÇÃO 2.1.5. Dado um grupo G, definimos o *grafo não-comutativo* de G, denotado por $\Gamma(G)$, como o grafo cujo conjunto de vértices é formado pelos elementos de $G \setminus Z(G)$, isto é, $V(\Gamma(G)) = G \setminus Z(G)$, e cuja relação entre as arestas é: dados g e h em $V(\Gamma(G))$, eles estão conectados por uma aresta de $\Gamma(G)$ se, e somente se $[g, h] \neq 1$ isto é, se g e h não comutam como elementos de G.

Podemos definir esse grafo utilizando como conjunto de vértices todos os elementos de G, isto é, incluindo também os elementos do centro, como é feito no artigo de B. H. Neumann [**18**]. Desta forma, elementos de $Z(G)$, como comutam com todos os elementos de G, não estarão ligados com nenhum vértice por uma aresta, portanto tais vértices serão representados por pontos soltos no grafo $\Gamma(G)$.

Utilizando os programas **GAP 4.7.5** [**7**] para calcular as arestas e **Wolfram Mathematica 10.0** [**17**] para plotar o grafo não-comutativo, como pode ser visto no Apêndice 6, podemos construir grafos não-comutativos de alguns grupos finitos de ordens não muito grandes. Por exemplo, considere o grupo diedral de ordem 6:

$$D_6 = \langle \rho, \tau \mid \tau^2 = \rho^3 = 1,\ \rho^\tau = \rho^{-1} \rangle.$$

Seu grafo não-comutativo pode ser representado pelo grafo abaixo, com 5 vértices, pois $Z(D_6) = \{1\}$. Observamos, por exemplo, que ρ e ρ^2 não são ligados por uma aresta pois $[\rho, \rho^2] = 1$ enquanto ρ e $\rho\tau$ estão, pois $[\rho, \rho\tau] = \rho \neq 1$.

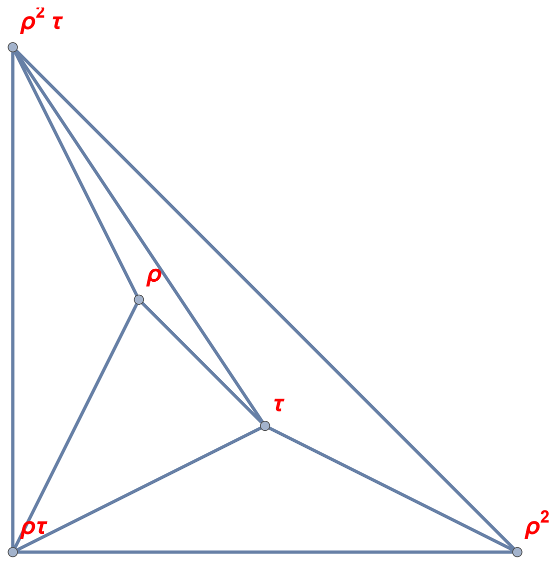

FIGURA 2.1.2. Grafo não-comutativo de D_6

DEFINIÇÃO 2.1.6. Um grafo é chamado *planar* se admite uma representação no plano na qual linhas (arestas) diferentes apenas se intersectam nos extremos, no caso das arestas serem incidentes a um vértice em comum, e não se intersectam, no caso de não serem incidentes a nenhum vértice em comum.

Dado um grafo planar, deve existir uma representação tal que as arestas não se intersectam fora das extremidades. Como há várias maneiras de representar um grafo, pode haver uma em que as arestas se intersectam fora das extremidades, mesmo o grafo sendo planar. Vamos mostrar um exemplo em que isso acontece. Considere o grupo diedral de ordem 8:

$$D_8 = \langle \rho, \tau \mid \tau^2 = \rho^4 = 1,\ \rho^\tau = \rho^{-1} \rangle$$

Podemos representar o grafo não-comutativo de D_8 como na Figura 2.1.3, um grafo com 6 vértices, pois $Z(D_8) = \{1, \rho^2\}$. Observamos que os elementos que não são ligados por uma aresta, como $\rho^2\tau$ e τ, comutam como elementos de D_8. Nessa representação, há arestas que se intersectam fora de suas extremidades, mas não necessariamente excluímos a opção desse grafo ser planar.

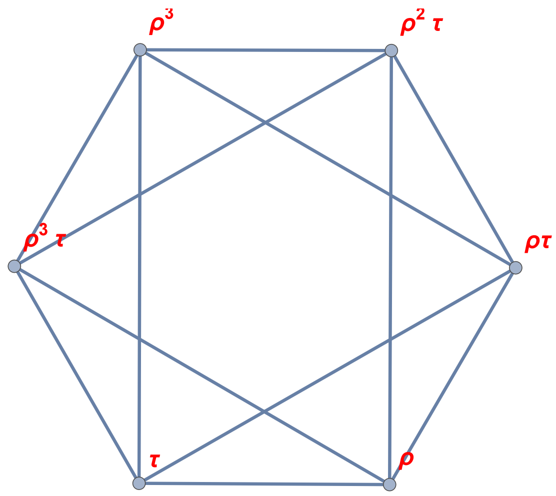

FIGURA 2.1.3. Grafo não-comutativo de D_8

A seguir, temos uma outra forma de representar o mesmo grafo:

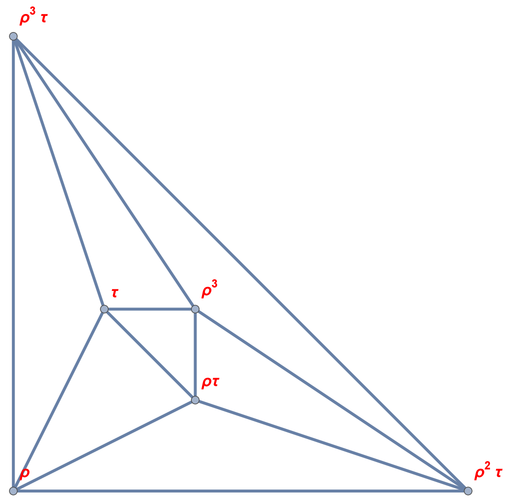

FIGURA 2.1.4. Grafo não-comutativo de D_8 - Planar

Na Figura 2.1.4, as arestas não se intersectam fora das suas extremidades, portanto podemos perceber que o grafo $\Gamma(D_8)$ é planar. Notamos que é possível caracterizar os grafos não comutativos planares e voltaremos a esse argumento mais tarde.

Definição 2.1.7. Um grafo Γ é dito *finito* se seu conjunto de vértices $V(\Gamma)$ e seu conjunto de arestas $E(\Gamma)$ são finitos e é dito *infinito* caso contrário. Um grafo Γ é dito *simples* se ele não tem nenhum laço e se dadas duas arestas distintas $e_i \neq e_j$, temos que $\psi_\Gamma(e_i) \neq \psi_\Gamma(e_j)$, ou seja, arestas distintas não têm as duas extremidades iguais.

Nesta seção, iremos considerar apenas grafos finitos a menos que se diga o contrário. De fato, fazemos esta restrição para trabalhar um pouco mais com a relação entre o número de vértices e o número de arestas de um grafo, bem como a relação de incidência entre vértices e arestas. Desta forma, para facilitar a notação, denotaremos por $v(\Gamma)$ o *número de vértices* e por $\varepsilon(\Gamma)$ o *número de arestas* de um grafo.

Uma observação importante sobre *grafos não-comutativos* é a seguinte. Note que, dado G um grupo, seu grafo não-comutativo sempre é um grafo simples, visto que $[x, x] = 1$ para todo x em G, portanto não há laços, e há apenas uma forma de ligar um vértice a outro por uma aresta pela forma pela qual o grafo é definido.

Dois grafos Γ_1 e Γ_2 são *iguais* ($\Gamma_1 = \Gamma_2$), se $V(\Gamma_1) = V(\Gamma_2)$, $E(\Gamma_1) = 1(\Gamma_2)$ e $\psi_{\Gamma_1} = \psi_{\Gamma_2}$. Portanto, dois grafos iguais podem ser representados pelo mesmo diagrama com os mesmos conjuntos de vértices e arestas (inclusive nomeados da mesma maneira) e com a mesma função de incidência. Por outro lado, é possível que dois grafos não sejam iguais, mas tenham a mesma estrutura a menos do nome dos vértices e arestas. Nesse caso, os dois grafos não são iguais, mas são chamados de *isomorfos*.

Definição 2.1.8. Dois grafos Γ_1 e Γ_2 são ditos *isomorfos*, denotado por $\Gamma_1 \cong \Gamma_2$, se existem bijeções $\theta : V(\Gamma_1) \longrightarrow V(\Gamma_2)$ e $\phi : E(\Gamma_1) \longrightarrow E(\Gamma_2)$ tais que $\psi_{\Gamma_1}(e) = (u, v)$ se, e somente se $\psi_{\Gamma_2}(\phi(e)) = (\theta(u), \theta(v))$. O par (θ, ϕ) é chamado de isomorfismo entre Γ_1 e Γ_2.

Temos que a relação de isomorfismo entre grafos é uma relação de equivalência. De fato, dado Γ um grafo, podemos definir θ e ϕ como a função identidade e assim Γ é isomorfo a Γ e portanto temos reflexividade. A relação é simétrica, pois sempre que Γ_1 e Γ_2 são isomorfos, se tomarmos as funções inversas das bijeções θ e ϕ, que também serão bijeções, teremos que Γ_2 e Γ_1 são isomorfos. Agora, se Γ_1 e Γ_2 são isomorfos com bijeções θ_1 e ϕ_1 e se Γ_2 e Γ_3 são isomorfos com bijeções θ_2 e ϕ_2, para ver que Γ_1 e Γ_3 são isomorfos, basta tomar como as novas duas bijeções a composta de θ_1 e θ_2 e a composta de ϕ_1 e ϕ_2.

Definição 2.1.9. Um grafo simples é dito *completo* se, dado qualquer par de vértices, há sempre uma aresta ligando um ao outro.

Para introduzir um conceito relacionado com grafos completos, precisamos da definição de um subgrafo induzido por um subconjunto de vértices.

Definição 2.1.10. Dado Γ um grafo. Denotamos $V(\Gamma) = V$ e seja V' um subconjunto de V não vazio. Definimos $\Gamma[V']$, o *subgrafo induzido por* V', como o subgrafo de Γ cujo conjunto de vértices é V' e cujo conjunto de arestas é formado pelas arestas de Γ que têm ambas extremidades em V'.

Definição 2.1.11. Dado Γ um grafo simples, um subconjunto S de $V(\Gamma)$ é dito um *clique* de Γ se $\Gamma[S]$ é completo. Definimos o tamanho do clique S como a cardinalidade do subconjunto S. Portanto, podemos definir $\omega(\Gamma)$ como o tamanho do maior clique de Γ.

Definição 2.1.12. Dado Γ um grafo, um subconjunto I de $V(\Gamma)$ é dito um conjunto *independente* de vértices de Γ se, dados quaisquer v_i e v_j em I, temos que v_i e v_j não são adjacentes, isto é, não estão conectados por uma aresta.

Definição 2.1.13. Seja Γ um grafo. O complementar de Γ é um grafo Γ' com o mesmo conjunto de vértices de Γ, isto é, $V(\Gamma) = V(\Gamma')$, e tal que x e y estão conectados por uma aresta em Γ' se, e somente se x e y não estão conectados por uma aresta em Γ. Em particular, um clique em Γ corresponde a um conjunto independente em Γ' e vice versa.

Dado G um grupo, é possível definir o grafo *comutativo* associado a G, que é exatamente o grafo complementar a $\Gamma(G)$. Assim, cliques no grafo não-comutativo de G equivalem a conjuntos independentes no grafo comutativo de G.

Utilizaremos um exemplo para esclarecer algumas das definições dadas acima. Novamente, considere o grafo não-comutativo de D_8 mostrado na Figura 2.1.3, considere $V(\Gamma(D_8)) = V$, $\Gamma(D_8) = \Gamma$, $V' = \{\tau, \rho^3\tau, \rho^3\}$ e $V'' = \{\rho^2\tau, \rho\tau, \rho\}$

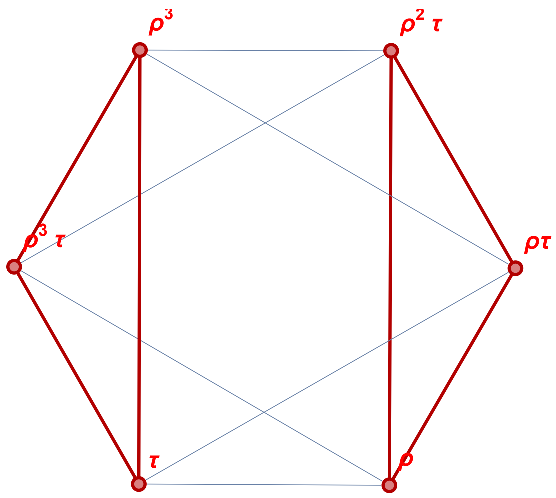

Figura 2.1.5. Grafo não-comutativo de D_8, destacando subgrafos induzidos por V' eV''

Como mostrado na Figura 2.1.5, o subgrafo em vermelho à direita é o subgrafo induzido por V', $\Gamma[V']$ e qualquer uma de suas arestas tem ambas extremidades em V'. Notamos também que este subgrafo, em particular, é um subgrafo completo pois, primeiro, $\Gamma[V']$ é um subgrafo de um grafo simples, portanto também é simples, e segundo, $\{\rho^3, \tau\}, \{\tau, \rho^3\tau\}$ e $\{\rho^3\tau, \rho^3\}$ são arestas de $\Gamma[V']$, assim qualquer par de vértices em V' está ligado por uma aresta. Da mesma maneira podemos construir o subgrafo $\Gamma[V'']$, que é representado pelo subgrafo em vermelho à esquerda na Figura 2.1.5. Como $V' \cap V'' = \emptyset$, temos que $\Gamma[V']$ e $\Gamma[V'']$ são subgrafos disjuntos de Γ. Temos ainda que $\Gamma[V']$ e $\Gamma[V'']$ são isomorfos. Seja

$$\psi(e_1) = (\rho^3, \rho^3\tau),\ \psi(e_2) = (\tau, \rho^3\tau),\ \psi(e_3) = (\tau, \rho^3)$$

$$\psi(e_4) = (\rho, \rho^2\tau),\ \psi(e_5) = (\rho\tau, \rho^2\tau),\ \psi(e_6) = (\rho\tau, \rho).$$

Defina então (θ, ϕ) da seguinte forma

$$\theta(\rho^3) = \rho^2\tau,\ \theta(\rho^3\tau) = \rho\tau,\ \theta(\tau) = \rho$$

$$\phi(e_1) = e_5,\ \phi(e_2) = e_6,\ \phi(e_3) = e_4.$$

Assim, temos o isomorfismo entro os dois subgrafos $\Gamma[V']$ e $\Gamma[V'']$. Por exemplo, $\psi(e_1) = (\rho^3, \rho^3\tau)$ e $\psi(\phi(e_1)) = \psi(e_5) = (\rho\tau, \rho^2\tau) = (\theta(\rho^3\tau), \theta(\rho^3))$.

Também temos que dados quatro vértices distintos de Γ, pelo menos dois deles comutam, isto é, pelo menos dois deles não estão ligados por uma aresta. Podemos ver isso notando que $[\tau, \rho^2\tau] = [\rho, \rho^3] = [\rho\tau, \rho^3\tau] = 1$, ou seja, dados quatro elementos de $G \setminus Z(G)$, no caso extremo em que três elementos desta lista não comutarem, o quarto comutará com pelo menos um dos outros três pela identidade anterior. Portanto, o tamanho máximo de um clique em Γ é 3, então $\omega(\Gamma) = 3$.

Definição 2.1.14. Seja Γ um grafo e $v \in V(\Gamma)$.

i) Definimos o *grau de um vértice v*, denotado por $d_\Gamma(v)$, como o número de arestas de Γ que são incidentes a v. Note que quando há um laço, tal aresta conta como duas incidências para a contagem de $d_\Gamma(v)$.
ii) Um grafo Γ é dito *k-regular* se $d_\Gamma(v) = k$, para todo v em $V(\Gamma)$. Um grafo é dito *regular* se é k-regular para algum k inteiro não negativo.

Notamos, por exemplo, na Figura 2.1.1, que $d_\Gamma(v_3) = 4$. Denotaremos por $\delta(\Gamma)$ o grau mínimo entre os graus dos vértices de Γ e por $\Delta(\Gamma)$ o grau máximo entre os graus dos vértices de Γ.

No grafo não-comutativo de D_8 da Figura 2.1.6, destacamos as arestas incidentes à ρ em vermelho. Dessa maneira, temos que

$$d_{\Gamma(D_8)}(\rho) = 4.$$

Observamos também que qualquer vértice v de $\Gamma(D_8)$ é tal que $d_{\Gamma(D_8)}(v) = 4$, portanto $\Gamma(D_8)$ é um grafo 4-regular.

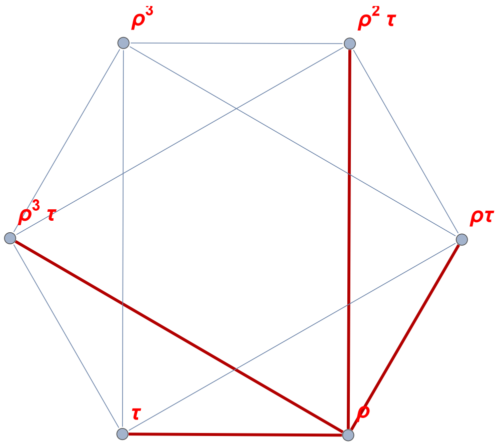

FIGURA 2.1.6. Grafo não-comutativo de D_8

DEFINIÇÃO 2.1.15. Dado Γ um grafo, definimos $M = (m_{ij})$, a matriz de incidência associada a Γ, como:

$$m_{ij} = \begin{cases} 0, & \text{se } v_i \text{ não é extremidade de } e_j; \\ 1, & \text{se } v_i \text{ é extremidade de } e_j, \text{ mas } e_j \text{ não é um laço;} \\ 2, & \text{se } v_i \text{ é extremidade de } e_j \text{ e } e_j \text{ é um laço.} \end{cases}$$

com v_i em $V(\Gamma)$, e_j em $E(\Gamma)$, $1 \le i \le v(\Gamma)$ e $1 \le j \le \epsilon(\Gamma)$.

O próximo resultado tem como objetivo relacionar o número de arestas $\epsilon(\Gamma)$ de um grafo Γ com os graus de cada vértice.

TEOREMA 2.1.16. *Seja Γ um grafo. Denote $V(\Gamma) = V$ e $d_\Gamma(v) = d(v)$ para todo v em V. Temos que*

$$\sum_{v \in V} d(v) = 2\epsilon(\Gamma). \tag{2.1.1}$$

DEMONSTRAÇÃO. Seja $M = (m_{ij})$ a matriz de incidência de Γ. Temos que, fixando v_i, a soma das entradas da linha i é precisamente $d(v_i)$, pois cada uma dessas entradas indica a incidência de v_i com cada uma das arestas de Γ. Portanto, $\sum_{v \in V} d(v)$ é exatamente a soma de todas as entradas de M. Por outro lado, se fixarmos uma aresta, ela tem sempre duas extremidades (distintas ou não), ou seja, cada aresta é contada duas vezes, uma como incidência da primeira extremidade e outra como incidência da segunda. Portanto somando todas as entradas de M, somamos todos os números de incidência, e o resultado é igual a duas vezes o número de arestas. Portanto $\sum_{v \in V} d(v) = 2\epsilon(\Gamma)$. □

COROLÁRIO 2.1.17. *Dado Γ um grafo, o número de vértices de grau ímpar é par.*

Demonstração. Sejam V_1 e V_2 os subconjuntos de vértices de grau ímpar e par de Γ, respectivamente. Como $V_1 \cup V_2 = V$, temos

$$\sum_{v \in V} d(v) = \sum_{v \in V_1} d(v) + \sum_{v \in V_2} d(v) \tag{2.1.2}$$

Note que $\sum_{v \in V} d(v)$ é um número par, pela identidade em (2.1.1). Temos que $\sum_{v \in V_2} d(v)$ também é par, pois é a soma dos graus do vértices de grau par, portanto a soma de número pares. Portanto, por (2.1.2), $\sum_{v \in V_2} d(v)$ também é um número par. Por outro lado, $\sum_{v \in V_2} d(v)$ é a soma de números ímpares pela definição de V_2. Para a soma de números ímpares ser par, a quantidade de termos na somatória deve ser par, portanto a cardinalidade de V_2 é par. $\square$

Agora apresentaremos um conceito que divide os vértices de um grafo em classes de equivalência e que, por consequência, divide o grafo em componentes. As informações sobre essas componentes são suficientes para dizer se, dados dois vértices de um grafo, é possível fazer um caminho alternando arestas e vértices, que parte do primeiro vértice e chega ao segundo.

Definição 2.1.18. Uma sequência $w = v_0e_1...e_kv_k$ finita e não vazia de termos que alternam entre vértices e arestas (e tal que v_{i-1} e v_i são extremidades de e_i para $1 \leq i \leq k$) é chamada de *caminho* em Γ se as arestas $\{e_1, ..., e_k\}$ e os vértices $\{v_0, ..., v_k\}$ são distintos. Chamaremos de (v_0, v_k)-caminho o caminho $w = v_0e_1...e_kv_k$ definido acima. O comprimento de um caminho é definido pela quantidade de arestas em w, isto é, k. Se $w = v_0e_1...e_kv_k$ é um caminho e v_k, v_0 são ligados por uma aresta e_{k+1}, então $w = v_0e_1...e_kv_ke_{k+1}v_0$ é chamado *ciclo*.

Definição 2.1.19. Seja Γ um grafo. Dois vértices u e v são ditos *conectados* se existe um caminho que liga u e v, chamado de (u, v)-caminho. Se u e v estão conectados, o tamanho do menor (u, v)-caminho é chamado de *distância entre u e v*, e é denotado por $d(u, v)$. Denotaremos por $diam(\Gamma) = \max_{u,v \in V(\Gamma)} d(u, v)$ o *diâmetro* de um grafo.

Notamos que a propriedade de ser conectado é uma relação de equivalência nos vértices de um grafo. Portanto, existe uma partição de V em conjuntos não vazios $V_1, ..., V_n$ tal que dois vértices são conectados se, e somente se, eles pertencem ao mesmo conjunto V_i.

Definição 2.1.20. Os subgrafos $\Gamma[V_1], \dots, \Gamma[V_n]$ induzidos por $V_1, \dots, V_n$ são chamados de *componentes* de Γ. Se Γ tem exatamente uma componente, Γ é dito *conectado*.

Na Figura 2.1.7, representamos um grafo Γ cujo conjunto de vértices V pode ser dividido em dois conjuntos, $V_1 = \{v_3, v_4, v_5, v_6\}$ e $V_2 = \{v_1, v_2\}$, pois todos os vértices de V_1 são conectados por uma aresta dois a dois, bem como os vértices de V_2. Portanto, as componentes de Γ são os grafos induzidos por V_1 e V_2, destacados em azul e vermelho, respectivamente.

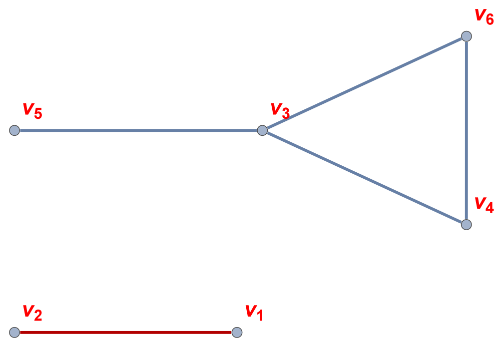

FIGURA 2.1.7. Γ, grafo com duas componentes

2.2 UMA VERSÃO DO TEOREMA INFINITO DE RAMSEY

Mostraremos nesta seção uma versão do Teorema Infinito de Ramsey [**5**], resultado que será utilizado no próximo capítulo.

TEOREMA 2.2.1. *Seja Γ um grafo simples infinito. Então Γ possui ou um clique infinito, ou um conjunto independente infinito.*

DEMONSTRAÇÃO. Primeiro, assumindo *Axioma da Escolha*, [**9**, Theorem 0.20], vamos mostrar que *qualquer conjunto infinito X tem um subconjunto infinito enumerável*. De fato, basta definir uma função $f : \mathbb{N} \to X$ que seja injetiva, pois dessa forma $f(\mathbb{N})$ é uma cópia de $\mathbb{N}$ em X, isto é, um subconjunto infinito enumerável. Como X é infinito, portanto não vazio, podemos escolher x_X elemento em X e definir $f(1) = x_X$. Suponha agora que $\{f(1), \ldots, f(n)\}$ já estejam definidos. Definimos então $A_n = X \setminus \{f(1), \ldots, f(n)\}$, que é um conjunto não vazio pois X é infinito e escolhemos x_{A_n} em A_n. Daí, definimos $f(n+1) = x_{A_n}$. Definindo a função f indutivamente desta forma, temos que ela é injetiva, pois dados m e n inteiro positivos diferentes, digamos, $m < n$ temos que $f(m)$ está em $\{f(1), \ldots, f(n-1)\}$ e $f(n)$ não está em $\{f(1), \ldots, f(n-1)\}$, logo $f(n)$ e $f(m)$ são diferentes, como queríamos.

Portanto, como Γ é um grafo infinito, temos que $V(\Gamma)$ é infinito, então existe um subconjunto infinito enumerável de vértices V' em $V(\Gamma)$. Assim, se provarmos o resultado para um grafo infinito enumerável, temos o resultado para qualquer grafo infinito, pois valerá para o subgrafo infinito enumerável induzido por V' e portanto valerá para Γ.

Assim, sem perda de generalidade vamos supor que $V(\Gamma) = \{v_1, \ldots\}$ é um conjunto infinito enumerável. A ideia da prova é construir indutivamente uma sequência de triplas $(x_i, Y_i, \varepsilon_i)$ que satisfaz as seguinte propriedades:

(i) os x_i são vértices distintos;
(ii) os Y_i são subconjuntos infinitos decrescentes de vértices, isto é, $Y_0 \supseteq Y_1 \supseteq \cdots \supseteq Y_i$;
(iii) os vértices x_i pertencem a Y_j se, e somente se $j < i$ e x_i é adjacente a todos vértice de Y_i (nesse caso definimos $\varepsilon_i = 1$) ou x_i não é adjacente a nenhum vértice de Y_i (nesse caso definimos $\varepsilon_i = 0$).

Começamos a construir a sequência com $Y_0 = V(\Gamma)$. Escolhendo $x_1 \in Y_0$ e considerando que Y_0 é infinito, há duas possibilidades:

(1) Se x_1 é adjacente a um número finito de vértices de Y_0 , então existem infinitos vértices de Y_0 que não são adjacentes a x_1;
(2) Caso contrário, x_1 é adjacente a um número infinito de vértices de Y_0.

Se tivermos no caso (1), se x_1 não é adjacente a ele mesmo, definimos Y_1 como o conjunto infinito de vértices de Y_0 que não são adjacentes a x_1 tirando o elemento x_1. Caso contrário, definimos Y_1 como o conjunto infinito de vértices de Y_0 que não são adjacentes a x_1. Se tivermos no caso (2), se x_1 for adjacente a ele mesmo, consideramos Y_1 como o conjunto infinito de vértices de Y_0 que são adjacentes a x_1 tirando o elemento x_1. Caso contrário, definimos Y_1 como o conjunto infinito de vértices de Y_0 que são adjacentes a x_1. Se estivermos no caso (1), definimos $\varepsilon_1 = 0$ e se estivermos no caso (2), definimos $\varepsilon_1 = 1$.

Definimos Y_i recursivamente a partir de Y_{i-1} da seguinte forma: escolhendo x_i em Y_{i-1}, já temos que $x_i \neq x_{i-1}$, pois como feito para $i = 1$, a escolha de Y_{i-1} é feita de forma que x_{i-1} não pertence a Y_{i-1}. Se existem infinitos vértices em Y_{i-1} que não são adjacentes a x_i, escolhemos Y_i como esse conjunto infinito de vértices, tirando x_i, caso ele esteja incluído. Se existem infinitos vértices que Y_{i-1} que são adjacentes a x_i, escolhemos Y_i como esse conjunto infinito de vértices, tirando x_i, caso ele esteja incluído. Assim, as condições (i) e (ii) para formar as triplas $(x_i, Y_i, \varepsilon_i)$ que gostaríamos são naturalmente satisfeitas. Para ver a condição (iii), temos que como $x_i \in Y_{i-1}$ por construção, se $j < i$ temos $j \leq i-1$ e portanto Y_{i-1} está contido em Y_j por (ii) e assim x_i está contido em Y_j. Por outro lado, suponha que x_i está em Y_j. Temos por construção que x_i está em Y_{i-1} e x_i não está em Y_i. Então, se tivéssemos $i \leq j$, teríamos que Y_j estaria contido em Y_i, um absurdo pois x_i está em Y_j, mas não está em Y_i. Portanto, $j < i$. Temos também por definição que, dependendo do ε_i, x_i é adjacente a todos os elementos de Y_{i-1} ou não é adjacente a nenhum. Assim, temos a sequência que queríamos no início.

Agora, notamos que a sequência $(\varepsilon_i)_{i\in\mathbb{N}}$ é uma sequência infinita na qual $\varepsilon_i = 0$ ou $\varepsilon_i = 1$, para todo i, além de ser uma sequência limitada. Segue que essa sequência possui subsequência $(\varepsilon_{i_r})_{r\in\mathbb{N}}$ convergente. Para tanto, tal subsequência, neste caso, deve ser constante com todos os termos iguais a 0 ou a 1.

Se temos uma subsequência $(\varepsilon_{i_r})_{r\in\mathbb{N}}$ constante tal que os termos são todos iguais a zero, temos a correspondente sequência infinita $(x_{i_r}, Y_{i_r}, \varepsilon_{i_r})_{r\in\mathbb{N}}$. Tomamos então a sequência infinita de vértices distintos (x_{i_r}), dados x_{i_k}, x_{i_l} termos de (x_{i_r}), temos que x_{i_k} e x_{i_l} não são adjacentes. De fato, suponha sem perda de generalidade que $i_k < i_l$. Então Y_{i_l} está contido em Y_{i_k} e como $\varepsilon_{i_k} = \varepsilon_{i_l} = 0$ temos por definição que x_{i_k} não é adjacente a nenhum elemento de Y_{i_k-1}. Então, como Y_{i_l} está contido em Y_{i_k}, que por sua vez está contido em Y_{i_k-1}, temos que x_{i_k} e x_{i_l} não podem ser adjacentes. Portanto, como todos os elementos da sequência $(x_{i_r})_{r\in\mathbb{N}}$ são distintos vértices, $\{x_{i_1}, x_{i_2}, \ldots\}$ é um conjunto infinito independente de vértices.

Da mesma forma, se temos uma subsequência $(\varepsilon_{i_r})_{r\in\mathbb{N}}$ constante tal que os termos são todos iguais a um, temos que x_{i_k} é adjacente a todos os vértices de Y_{i_k-1} e como x_{i_2} está em Y_{i_j} e Y_{i_j} está contido em Y_{i_k-1}, temos que x_{i_k} e x_{i_j} são adjacentes e isso vale para todos os termos da sequência, portanto $\{x_{i_1}, x_{i_2}, \ldots\}$ é um clique infinito de Γ.

□

2.3 Propriedades do grafo não-comutativo

Apresentaremos alguns resultados gerais sobre grafos não-comutativos associados à um grupos G que podem ser encontrados no artigo *Non-commuting graph of a group*, [**1**] de A. Abdollahi, S Akbari e H. R. Maimani.

Proposição 2.3.1. *Seja G um grupo não abeliano e $\Gamma(G)$ seu grafo não-comutativo. Então $diam(\Gamma(G)) = 2$. Em particular, $\Gamma(G)$ é um grafo conexo.*

Demonstração. Por simplicidade, denotaremos $V(\Gamma)$ apenas por V. Sejam x e y dois vértices distintos de V. Se x e y são adjacentes, então temos que existe uma aresta e os ligando, ou seja $w = xey$ é o menor caminho ligando x e y, assim $d(x, y) = 1$. Agora suponha que x e y não são adjacentes, isto é, $[x, y] = 1$. Como sem perda de generalidade podemos supor que $V = G \setminus Z(G)$, temos que x e y não estão em $Z(G)$, assim existem x' e y' em V tais que x não comuta com x' e y não comuta com y', isto é, existem arestas ligando x e x' e ligando y e y'. Agora, se x e y' são adjacentes ou se x' e y são adjacentes, denotando por e_{uv} uma aresta que liga u e v, temos o caminho $w = xe_{xy'}y'e_{y'y}y$ de tamanho 2 ligando x e y. Se x' e y são adjacentes, temos o caminho $w = xe_{xx'}x'e_{x'y}y$ de tamanho 2 ligando x e y. Como x e y não são adjacentes e que $d(x, y) > 1$, então $d(x, y) = 2$. Caso contrário, isto é, se x e y' não são adjacentes e se x' e y não são adjacentes, tomamos $z = x'y'$. Para o primeiro caso temos que,

$$[z, x] = [x'y', x] = [x', x]^{y'}[y', x] = [x', x]^{y'},$$

pois y' e x comutam. Mas se tivéssemos $[x', x]^{y'} = 1$, teríamos que $[x, x'] = 1^{y'^{-1}} = 1$, um absurdo, pois x e x' não comutam. Então $[x', x]^{y'} = [z, x] \neq 1$, ou seja, existe uma aresta e_{zx} ligando x e z. Analogamente, temos que $[z, y] \neq 1$ e assim existe uma aresta e_{yz} ligando x e z. Assim, temos um caminho $w = ye_{yz}ze_{zx}x$ de tamanho 2 ligando y e x, portanto, $d(x, y) = 2$. Logo temos que $diam(\Gamma(G)) \leq 2$. Suponha por absurdo que $diam(\Gamma(G)) = 1$. Então, dado qualquer a em $V = G\setminus Z(G)$, temos que a^{-1} está em V e $[a, a^{-1}] = 1$. Assim, se a e a^{-1} fossem distintos, como eles não são adjacentes, teríamos que $d(a, a^{-1}) = 2$, pela primeira parte da demonstração, e teríamos um absurdo, pois $diam(\Gamma(G)) = 1$. Assim, a única possibilidade é que $a = a^{-1}$.

Agora, dados a em $G \setminus Z(G)$, b em $Z(G)$ e g qualquer elemento de G, temos que

$$[ab, g] = [a, g]^b[b, g] = [a, g]^b.$$

Então, para todo g em G, se $[ab, g] = 1$ teríamos que $[a, g] = 1$, um absurdo, pois a não está no centro de G. Então, ab está em $G \setminus Z(G)$. Portanto, temos que $ab = (ab)^{-1}$ e assim $(ab)^2 = 1$. Temos, de forma análoga, que $a^2 = 1$. Então, como $b \in Z(G)$, temos

$$1 = (ab)^2 = abab = a^2b^2 = b^2.$$

Daí, temos que para todo elemento g em G, $g^2 = 1$, ou seja, G é abeliano, que é um absurdo, portanto $diam(\Gamma(G)) = 2$, como queríamos. Em particular, $\Gamma(G)$ é um grafo conectado pois dados x e y em V, temos que $d(x, y) = 1$ ou $d(x, y) = 2$, então sempre existe um (x, y)-caminho ligando x e y.

□

Como já foi observado é possível caracterizar os grafos não-comutativos que são planares. Mais precisamente temos o seguinte resultado:

Seja G um grupo não abeliano. $\Gamma(G)$ é planar se, e somente se G é isomorfo a D_8, S_3, ou Q_8.

A demonstração desse resultado será apresentada no próximo capítulo, já que uma das ferramentas "chave" usadas para a prova é o Teorema 3.1.10.

Capítulo 3

Grupos central-por-finito

Dizemos que um grupo G é *central-por-finito* se o índice $[G : Z(G)]$ é finito. Estamos interessados na classe de grupos central-por-finito pois é uma classe de grupos já muito estudada e com muitos resultados e propriedades interessantes. Temos, por exemplo, o bem conhecido Lema de Schur, que diz que se um grupo G é central-por-finito, então seu subgrupo derivado G' é finito. Também é interessante observar que o conjunto dos automorfismos internos $Inn(G)$ é finito se, e somente se G é central-por-finito, entre outras características.

O objetivo deste capítulo é apresentar duas caracterizações de um grupo G central-por-finito, uma relacionada ao grafo não-comutativo $\Gamma(G)$ e a outra relacionada com uma cobertura finita de G por subgrupos abelianos.

3.1 PE-grupos

Paul Erdös formulou o seguinte problema que foi respondido afirmativamente por B. H. Neumann em *A problem of Paul Erdös on groups* [**18**]:

Seja G um grupo tal que $\Gamma(G)$ não tem subgrafos completos infinitos. Neste caso, existe uma cota superior finita para a cardinalidade de um subgrafo completo de $\Gamma(G)$?

Chamamos então, grupos de Paul Erdös, ou PE-grupos, os grupos que satisfazem a hipótese do problema acima.

Definição 3.1.1. Dado G um grupo e seja $\Gamma(G)$ seu grafo não-comutativo. Dizemos que G é um *PE-grupo* se em $\Gamma(G)$ não existem subgrafos completos infinitos.

Observe que se G é um PE-grupo, então dado qualquer conjunto infinito de elementos de G, visto como subconjunto de vértices de $\Gamma(G)$, tal conjunto não pode induzir um subgrafo completo. Então pelo menos dois vértices desse conjunto infinito não estão ligados por uma aresta. Em termos da estrutura do grupo, temos então que se G é um PE-grupo, dado qualquer conjunto infinito de elementos de G, pelo menos dois deles não estão ligados por uma aresta em $\Gamma(G)$ e portanto, por definição, esses dois elementos comutam.

Nosso objetivo nesta seção é mostrar que G é um PE-grupo se, e somente se G é central-por-finito e desta forma teremos nossa primeira caracterização de grupos central-por-finito.

Dizemos que um grupo G é um *FC-grupo* se todas as classes de conjugação em G são finitas, isto é, $|Cl(x)|$ é finito para todo x em G. A seguir mostraremos que ambos, PE-grupos e grupos central-por-finito, são FC-grupos, e este é o primeiro passo para mostrar a caracterização mencionada acima.

Lema 3.1.2. *Seja G um grupo. Se G é central-por-finito, então G é um FC-grupo.*

Demonstração. Por hipótese temos que o índice $[G : Z(G)]$ é finito. Lembramos que $Z(G) = \bigcap_{x\in G} C_G(x) \leqslant C_G(x)$ para todo x em G. Assim, $[G : C_G(x)] \leq [G : Z(G)] < \infty$. Agora, pela Equação das Classes (Teorema 1.0.7), temos $[G : C_G(x)] = |Cl(x)|$ para todo x em G. Portanto, pela observação anterior, todas as classes de conjugação em G são finitas e assim G é um FC-grupo, como queríamos. □

Lema 3.1.3. *Se G é um PE-grupo, então G é um FC-grupo.*

Demonstração. Vamos mostrar o resultado por absurdo. Supondo que G não é um FC-grupo, vamos mostrar que G não pode ser um PE-grupo. Como G não é um FC-grupo, temos que existe um g em G tal que $|Cl(g)|$ é infinito. Defina então T_g como o conjunto de elementos de G tais que elementos distintos de T_g dão origem a conjugados distintos do elemento g.

Como $|Cl(g)|$ é infinito, temos que existem infinitos conjugados de g, isto é, existem infinitos elementos distintos g^s, com s em G. Portanto, T_g é um conjunto infinito. Seja $\Gamma(G)$ o grafo não-comutativo de G. Considere o subgrafo induzido por T_g, $\Gamma(G)[T_g]$, que denotaremos por $\Gamma[T_g]$. Como $\Gamma[T_g]$ é infinito, pelo Teorema de Ramsey (Teorema 2.2.1), $\Gamma[T_g]$ tem um clique infinito ou um conjunto independente infinito. Se $\Gamma[T_g]$ tem um clique infinito, então $\Gamma[T_g]$ tem um subgrafo infinito completo e portanto $\Gamma(G)$ também o tem. Assim, G não é um PE-grupo, que é um absurdo.

Agora se $\Gamma[T_g]$ tem um conjunto independente infinito, digamos $U \subset V(\Gamma[T_g]) = T_g$, temos que, para todo u e v em U, $[u, v] = 1$ pois, por definição de conjunto independente, não há arestas ligando u e v. Portanto todos os elementos de U comutam como elementos de G. Considere o conjunto

$$gU = \{gu \,|\, u \in U\}.$$

Notamos que $gu = gv$ se, e somente se $u = v$, assim como U é um conjunto infinito, gU é também um conjunto infinito. Se u e v são elementos distintos em U,

$$\begin{aligned}[gu, gv] &= (gu)^{-1}(gv)^{-1}(gu)(gv) = u^{-1}g^{-1}v^{-1}ugv \\ &= u^{-1}g^{-1}uv^{-1}gv = (g^{-1})^u g^v \\ &= (g^u)^{-1}g^v.\end{aligned}$$

Como, em particular, u e v estão em T_g, temos que g^u e g^v são dois elementos distintos e então $[gu, gv] = (g^u)^{-1}g^v \neq 1$. Por essa observação, dados quaisquer elementos distintos de gU eles não podem comutar. Portanto $\Gamma[gU]$ é um subgrafo completo infinito de $\Gamma(G)$ e portanto G não é um PE-grupo, uma contradição. □

Agora vamos caracterizar os FC-grupos em termos do índice de alguns subgrupos específicos.

Lema 3.1.4. *G é um FC-grupo se, e somente se o índice $[G : C_G(S)]$ é finito para todo subconjunto finito S de G.*

Demonstração. Lembramos que, pela Equação das Classes, temos que $[G : C_G(x)] = |Cl(x)|$, para todo x em G. Segue que G é um FC-grupo se, e somente se $[G : C_G(x)]$ é finito para todo x em G. Lembramos também que se S é um subconjunto finito de G e se para todo s em S o centralizador $C_G(s)$ tem índice finito em G, pelo Lema 1.0.1, $C_G(S) = \bigcap_{s\in S} C_G(s)$ também tem índice finito em G. Portanto se G é um FC-grupo, temos que $[G : \bigcap_{s\in S} C_G(s)]$ é finito, ou seja, $[G : C_G(S)]$ é finito, para qualquer conjunto finito S. Por outro lado, se $[G : C_G(S)]$ é finito para todo conjunto finito S de G, consideramos $S = \{g\}$, para $g \in G$. Assim teremos que $C_G(S) = C_G(g)$ sempre tem índice finito em G, como queríamos. □

Já sabemos que todo grupo central-por-finito é um FC-grupo. Considere H um grupo finito não-abeliano. Definimos

$$G = \{(x_i)_{i\in\mathbb{N}} \mid x_i \in H \text{ e } x_i \neq 1 \text{ apenas para um número finito de índices}\},$$

o produto direto de infinitas cópias de H, um subgrupo próprio do grupo $H \times \cdots \times H \times \cdots$ sem restrições nas entradas (x_i).

Como H é finito, para todo g elemento de G, temos que $Cl(g)$ é finita. Por outro lado, como $Z(G)$ é isomorfo ao produto direto infinito de cópias de $Z(H)$, logo $G/Z(G)$ é isomorfo ao produto direto de infinitas cópias de $H/Z(H)$. Como H não é abeliano, temos que $H/Z(H)$ é não trivial e portanto $G/Z(G)$ é um grupo infinito. Logo, temos que G não é central-por-finito. Logo nem todos os FC-grupos são central-por-finito. Agora vamos ver algumas condições suficientes para que um FC-grupo seja central-por-finito.

Lema 3.1.5. *Se G é um FC-grupo finitamente gerado, então G é central-por-finito.*

Demonstração. Primeiro observamos que se $G = \langle S\rangle$, então o centro de G é igual a $C_G(S)$. De fato, como $Z(G) = \bigcap_{x\in G} C_G(x)$, temos que $Z(G) \subseteq C_G(S)$. Por outro lado, dado x em $C_G(S)$ e g em G temos que como $G = \langle S\rangle$, $g = c_1c_2 \dots c_n$ tal que c_i ou c_i^{-1} estão em S, para todo i. Assim, como x está em $C_G(S)$, x comuta com todos os elementos de S e portanto também com os inversos dos elementos de S. Dessa forma, x comuta com todos os c_i e assim comuta com g para todo g em G. Portanto $C_G(S)$ está contido em $Z(G)$. Por hipótese G é um FC-grupo e é finitamente gerado, isto é, $G = \langle S\rangle$, com S um subconjunto finito. Do Lema 3.1.4 segue que $[G : C_G(S)] < \infty$. Mas pela observação feita antes, $[G : C_G(S)] = [G : Z(G)] < \infty$, ou seja, G é central-por-finito. □

Lema 3.1.6. *G é um grupo central-por-finito se, e somente se G é um FC-grupo e contém um subgrupo abeliano A tal que o índice $[G : A]$ é finito.*

Demonstração. Assuma que A é um subgrupo abeliano de G tal que $[G : A]$ é finito. Seja Q um conjunto de geradores do subgrupo abeliano A e R um transversal de A em G. Temos então que como $|R| = [G : A]$, por hipótese, R será finito. Note que $G = \bigcup_{r\in R} Ar$ e portanto, qualquer elemento de G pode ser escrito como ar, com r em R e a em A. Como A é gerado pelos elementos de Q temos que $S = Q \cup R$ é um conjunto de geradores para G. Pela demonstração do Lema 3.1.5, como G é gerado por S, temos que, $Z(G) = C_G(S) = C_G(Q \cup R)$. Também temos que,

$$C_G(Q \cup R) = \bigcap_{x\in Q\cup R} C_G(x) = \left(\bigcap_{x\in Q} C_G(x)\right) \bigcap \left(\bigcap_{y\in R} C_G(y)\right) = C_G(Q) \cap C_G(R).$$

Portanto,

$$Z(G) = C_G(Q) \cap C_G(R).$$

Agora, como Q é um conjunto de geradores de A e A é abeliano, os elementos de A comutam e em particular $A \subseteq C_G(Q)$. Assim, $[G : C_G(Q)] \leq [G : A] < \infty$, ou seja, $C_G(Q)$ tem índice finito em G. Agora como R é finito e G é um FC-grupo, pelo Lema 3.1.4, $C_G(R)$ tem índice finito. Assim, como vimos no Lema 1.0.1,

$$[G : Z(G)] = [G : C_G(Q) \cap C_G(R)] \leq [G : C_G(Q)][G : C_G(R)].$$

Temos que como $[G : C_G(Q)], [G : C_G(R)]$ ambos são finitos, $[G : Z(G)]$ também é finito e portanto G é central-por-finito.

Reciprocamente, se G é central-por-finito, temos que $[G : Z(G)] < \infty$ e $Z(G)$ é abeliano. Também, pelo Lema 3.1.2, qualquer grupo central-por-finito é um FC-grupo. □

Podemos formular o lema anterior na sua forma negativa e tal resultado será útil para mostrar que se G é um FC-grupo, mas não é central-por-finito, então G não é um PE-grupo.

Corolário 3.1.7. *Se G é FC-grupo, mas não é central-por-finito, e tem um subgrupo A com índice finito, então A não é abeliano.*

Demonstração. Suponha por absurdo que o subgrupo A de G com índice finito seja abeliano. Então, pelo Lema 3.1.6, temos que G é central-por-finito, uma contradição. □

Já vimos que tanto PE-grupos, como grupos central-por-finito são FC-grupos. Agora queremos mostrar que se G é um FC-grupo, mas não é central-por-finito, então G não pode ser um PE-grupo. Para tanto precisaremos primeiro do seguinte lema que é bastante técnico e utiliza ferramentas de teoria de grafos e algumas propriedades de comutadores (Veja Proposição 1.0.5).

LEMA 3.1.8. *Seja G um FC-grupo que não é central-por-finito e assuma que G contenha duas sequências finitas de elementos,*

$$(a_1, \ldots, a_n), \quad (b_1, \ldots, b_n)$$

com as seguintes propriedades:

(i) Se $i \neq j$, *então* $[a_i, a_j] \neq 1$;
(ii) Se $i \neq j$, *então* $[a_i, b_j] = 1$;
(iii) Para todo i, $[a_i, b_i] \neq 1$;
(iv) Para todo i, j, $[b_i, b_j] = 1$.

Então G contém outros dois elementos a_{n+1}, b_{n+1} *tais que as quatro propriedades (i),(ii),(iii) e (iv) continuam válidas para as sequências*

$$(a_1, \ldots, a_{n+1}), \quad (b_1, \ldots, b_{n+1})$$

de comprimento $n + 1$.

Seja $\Gamma(G) = \Gamma$ o grafo não-comutativo de G. Antes de começarmos a demonstração, vamos analisar o subgrafo induzido pelos vértices $V_n = \{a_1, \ldots, a_n, b_1, \ldots, b_n\}$. Observe que em $\Gamma[V_n]$ temos um subgrafo completo induzido pelos vértices $\{a_1, \ldots, a_n\}$, pois se $i \neq j$ temos pela propriedade (i) que $[a_i, a_j] \neq 1$, portanto para todo $i \neq j$ temos que a_i, a_j são adjacentes e assim o subgrafo induzido por $\{a_1, \ldots, a_n\}$ é completo. Temos também que, pela propriedade (iii), para todo i $[a_i, b_i] \neq 1$ e assim a_i e b_i são sempre adjacentes. Pela propriedade (ii), se $i \neq j$, então $[a_i, b_j] = 1$, ou seja, a_i e b_j não são adjacentes sempre que $i \neq j$. Por último, pela propriedade (iv) temos que nenhum b_i é adjacente a outro b_j, para $1 \leq i, j \leq n$. Para ilustrar nossa situação, vamos representar o grafo $\Gamma[V_n]$ nos casos $n = 2, 3, 4$.

FIGURA 3.1.1. Grafo induzido por $V_2 = \{a_1, a_2, b_1, b_2\}$.

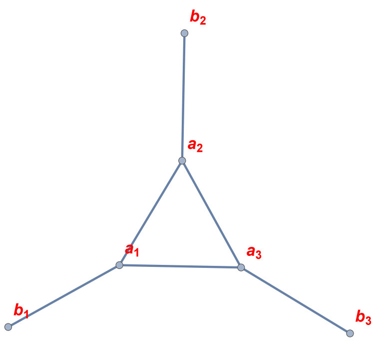

FIGURA 3.1.2. Grafo induzido por $V_3 = \{a_1, a_2, a_3, b_1, b_2, b_3\}$.

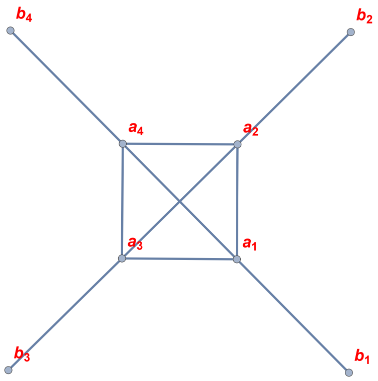

FIGURA 3.1.3. Grafo induzido por $V_4 = \{a_1, a_2, a_3, a_4, b_1, b_2, b_3, b_4\}$.

DEMONSTRAÇÃO DO LEMA 3.1.8. Sejam $S_n = \{a_1, \ldots, a_n, b_1, \ldots, b_n\}$ e $A_n = C_G(S_n)$. Como S é finito e por hipótese G é um FC-grupo, pelo Lema 3.1.4, $A_n = C_G(S_n)$ tem índice finito em G. Pelo Corolário 3.1.7, temos que A_n não é abeliano. Como A_n não é abeliano, em particular, temos que A_n não é trivial, e que existem dois elementos a, b em A_n tais que $[a, b] \neq 1$. Definimos:

$$a_{n+1} = ab_1b_2 \cdots b_n \quad \text{e} \quad b_{n+1} = b.$$

Para ilustrar a construção desta sequência, partindo do caso $n = 2$,

FIGURA 3.1.4

Como vimos, sejam $S_2 = \{a_1, a_2, b_1, b_2\}$ e $A_2 = C_G(S_2)$, como A_2 não é abeliano, escolhemos a e b em A_2 que não comutam. Assim, construímos:

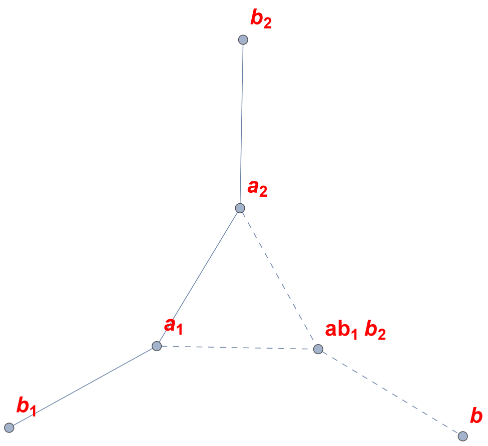

FIGURA 3.1.5

A partir da construção de a_3 e b_3, tomando A e B elementos de A_3 que não comutam, construímos:

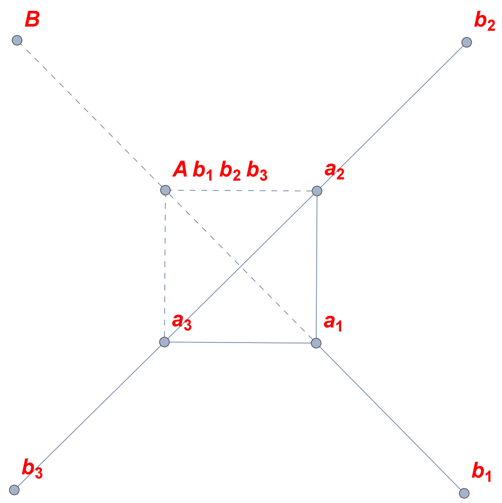

FIGURA 3.1.6

A seguir utilizaremos várias vezes propriedades dos comutadores vistas na Proposição 1.0.5. Observamos que b_{n+1} e a_{n+1} não estão em S, ou seja, de fato estamos acrescentando elementos distintos às sequências $(a_1, \dots, a_n)$ e $(b_1, \dots, b_n)$. Primeiro notamos que pela propriedade (iii), $[a_i, b_i] \neq 1$ para $1 \leq i \leq n$. Agora se tivéssemos $b_{n+1} = a_i$ para algum $1 \leq i \leq n$, teríamos que $[b_{n+1}, b_i] = [a_i, b_i] \neq 1$. Por outro lado, b_{n+1} está em $C_G(S_n)$, então b_{n+1} comuta com b_i, para todo $1 \leq i \leq n$, e assim temos um absurdo. Se tivéssemos $b_{n+1} = b_i$ para $1 \leq i \leq n$, seguiria que $[b_{n+1}, a_i] = [b_i, a_i] \neq 1$, mas novamente $b_{n+1} \in C_G(S_n)$ e assim b_{n+1} comuta com a_i, para todo $1 \leq i \leq n$, um absurdo. Agora se tivéssemos $a_{n+1} = a_i$ para $1 \leq i \leq n$, teríamos que $[a_{n+1}, b_i] = [a_i, b_i] \neq 1$ e por outro lado $[a_{n+1}, b_i] = [ab_1b_2 \cdots b_n, b_i] = [b_1b_2 \cdots b_n, b_i] = 1$ pois pela propriedade (iv) quaisquer b_i, b_j comutam e $a \in C_G(S_n)$, então a comuta com b_i, para $1 \leq i \leq n$. Finalmente, se tivéssemos $a_{n+1} = b_i$ para algum $1 \leq i \leq n$, teríamos que $a = b_n{}^{-1} \cdot b_1{}^{-1}$ sem o termo $b_i{}^{-1}$ e teríamos $[a, a_j] \neq 1$, para $i \neq j$, um absurdo por a está em $C_G(S_n)$. Agora vamos verificar que as quatro propriedades valem para as novas sequências $(a_1, \dots, a_{n+1})$ e $(b_1, \dots, b_{n+1})$:

(i') Para $1 \leq i \leq n$, temos que $[a_i, a_{n+1}] = [a_i, ab_1b_2 \dots b_n]$. Como a está em $C_G(S_n)$, temos que a comuta com a_i, b_j para $1 \leq i, j \leq n$. Fixando i, temos que b_j comuta com a_i sempre que $j \neq i$ e $1 \leq j \leq n$, e também temos que b_i e b_j comutam sempre que $1 \leq j, i \leq n$ pela propriedade (iv) . Portanto,

$$[a_i, a_{n+1}] = [a_i, ab_1b_2 \dots b_n] = [a_i, b_1b_2 \dots b_n]$$
$$= [a_i, b_i] \neq 1.$$

(ii') Para $1 \leq i \leq n$, temos que $[a_{n+1}, b_i] = [ab_1b_2 \dots b_n, b_i] = 1$, pois a comuta com b_j para $1 \leq j \leq n$ e b_i comuta com b_j para $1 \leq i, j \leq n$. Agora $[a_i, b_{n+1}] = [a_i, b] = 1$, pois

$b \in C_G(S_n)$.

(iii') Sabemos que $[a_i, b_i] \neq 1$ para $1 \leq i \leq n$. Agora como b e a comutam com b_i para $1 \leq i \leq n$ e como $[a, b] \neq 1$, segue que

$$\begin{aligned}[b_{n+1}, a_{n+1}] &= [b, ab_1b_2 \ldots b_n] \\ &= [b, a] \neq 1.\end{aligned}$$

(iv') Já temos que $[b_i, b_j] = 1$ para $1 \leq i, j \leq n$. Agora $[b_i, b_{n+1}] = [b_i, b] = 1$, pois $b \in C_G(S_n)$.

□

Como observamos anteriormente, vamos usar o Lema 3.1.8 para demonstrar o seguinte corolário:

Corolário 3.1.9. *Se G é um FC-grupo, mas não é central-por-finito, então G não é um PE-grupo.*

Demonstração. Se G fosse abeliano, teríamos que $Z(G) = G$ e portanto $[G : Z(G)] = 1$, ou seja, G seria central-por-finito, um absurdo. Portanto, G não é abeliano e assim, existem a_1, b_1 tais que $[a_1, b_1] \neq 1$. Note que $\{a_1\}$ e $\{b_1\}$ satisfazem trivialmente as quatro propriedades do Lema 3.1.8. Portanto, repetindo indutivamente o argumento do Lema 3.1.8, é possível construir a partir de $\{a_1\}$ e $\{b_1\}$ duas sequências infinitas $\{a_1, \ldots, a_n, \ldots\}$ e $\{b_1, \ldots, b_n, \ldots\}$ que satisfazem as propriedades do Lema 3.1.8. Em particular, a sequência infinita $\{a_1, \ldots, a_n, \ldots\}$ é constituída de elementos distintos que não comutam dois a dois, como já observamos, ou seja, $\{a_1, \ldots, a_n, \ldots\}$ induz um subgrafo completo infinito em $\Gamma(G)$. Portanto, G não é um PE-grupo. □

Finalmente, vamos mostrar a nossa primeira caracterização de um grupo central-por-finito.

Teorema 3.1.10. *G é um PE-grupo se, e somente se G é central-por-finito.*

Demonstração. Suponha por absurdo que G é um PE-grupo, mas não é central-por-finito. Pelo Lema 3.1.3, temos que todo PE-grupo é um FC-grupo, então G é um FC-grupo. Agora pelo Corolário 3.1.9, teríamos que G não é um PE-grupo, uma contradição.

Reciprocamente, suponha que G é central-por-finito. Como o índice de $Z(G)$ em G é finito, $[G : Z(G)] = n$, dados quaisquer $n + 1$ elementos $\{a_1, \ldots, a_{n+1}\}$ em G, como temos exatamente n classes laterais de $Z(G)$ sobre G, existem a_i, a_j, com $i \neq j$ tais que eles estão na mesma classe lateral módulo $Z(G)$, isto é, $a_i = a_j z$, para algum $z \in Z(G)$. Assim,

$$a_i a_j = a_j z a_j = a_j a_j z = a_j a_i,$$

ou seja, a_i e a_j comutam. Segue que em $\Gamma(G)$ não há cliques com mais de n elementos e portanto não pode haver cliques infinitos em Γ. Então G é um PE-grupo. □

Como dissemos no capítulo anterior, como consequência do Teorema 3.1.10, podemos caracterizar os grafos não-comutativos planares:

Proposição 3.1.11. *Seja G um grupo não abeliano.* $\Gamma(G)$ *é planar se, e somente se G é isomorfo a D_8, S_3, ou Q_8.*

Demonstração. D_8 e Q_8 têm grafos isomorfos e já vimos que $\Gamma(D_8)$ é planar. Agora, S_3 é isomorfo ao grupo D_6, e $\Gamma(D_6)$ é planar.

Reciprocamente, suponha que $\Gamma(G)$ é planar. Vamos denotar $\Gamma(G)$ por Γ simplicidade. Se $\omega(\Gamma) \geq 5$, então existe um clique X de cardinalidade maior ou igual a 5. Tomando Y subconjunto de X tal que $|Y| = 5$, temos que Y também induz um grafo completo de Γ. Como Γ é planar, teríamos que $\Gamma(Y)$ também é planar, um absurdo, pois por [**4**, Theorem 9.1] qualquer grafo completo de tamanho 5 não pode ser planar. Portanto, temos que $\omega(\Gamma) < 5$. Pelo Teorema 3.1.10, temos que $[G : Z(G)]$ é finito. Vamos mostrar que $|Z(G)| \leq 5$. Suponha por absurdo que $|Z(G)| > 5$ e considere um subconjunto finito Z de $Z(G)$ tal que $|Z| > 5$. Como G não é abeliano, existem x e y em G tais que $[x, y] \neq 1$. Definindo $T = Zx \cup Zy$, temos que $\Gamma(T)$ é planar e finito. Como Γ é simples, temos que $\Gamma(T)$ também é simples. O resultado [**4**, Corolary 9.5.3] diz que se Γ é um grafo finito, simples e planar, então o grau mínimo dos vértices de Γ é menor ou igual a 5. Então, aplicando no nosso caso temos que existe v um vértice em T tal que $d_\Gamma(v) \leq 5$. Mas por definição de T, quaisquer dois elementos de T não comutam, isto é, quaisquer dois elementos de T estão ligados por uma aresta. Como T têm cardinalidade maior que 6, pois x não está em Zy e Zy tem cardinalidade maior que 5, temos que $d_\Gamma(w) > 5$ para todo w em T, um absurdo. Portanto, temos que $|Z(G)| \leq 5$. Assim, como $Z(G)$ e $[G : Z(G)]$ são finito, temos que G também é finito. Novamente por [**4**, Corolary 9.5.3], temos que existe x em $G \setminus Z(G) = V(\Gamma)$ tal que $d_\Gamma(x) \leq 5$. Mas temos que $d_\Gamma(x) = |G \setminus C_G(x)| \leq 5$, portanto $|C_G(x)| \leq |G|/2$ e assim

$$\frac{|G|}{2} = |G| - \frac{|G|}{2} \leq |G| - |C_G(x)| = d_\Gamma(x).$$

Portanto $|G| \leq 10$. Se a ordem de G é 10, temos que G é abeliano ou G é isomorfo a D_{10}, cujo grafo $\Gamma(D_{10})$ podemos verificar no programa Mathematica, com o comando `PlanarGraphQ`, que não é planar. Agora se a cardinalidade de G é menor que 10, a única possibilidade de G não ser abeliano é G ter ordem 6 ou 8. Se G é não abeliano de ordem 6, então G é isomorfo a S_3 e se G é não abeliano de ordem 8, G é isomorfo a Q_8 ou D_8, como queríamos. □

3.2 Grupos cobertos por subgrupos abelianos

Um grupo G admite uma *cobertura finita por subgrupos abelianos* se pudermos escrever $G = \bigcup_{i=1}^{n} A_i$ tal que os A_i são subgrupos abelianos. Esta seção tem como objetivo mostrar uma caracterização de grupos central-por-finito devida a R. Baer que assegura que G é central-por-finito se, e somente se G admite uma cobertura finita por subgrupos abelianos.

O primeiro passo para mostrar o resultado principal desta seção é analisar grupos que têm uma cobertura finita por classes laterais, isto é,

$$G = \bigcup_{i=1}^{n} C_i g_i, \tag{3.2.1}$$

onde $C_i g_i$ são classes laterais a direita de subgrupos C_i de G. Se G pode ser escrito como essa união, queremos mostrar que as classes laterais de subgrupos com índice infinito podem ser omitidas em (3.2.1) sem perder a propriedade de cobertura de G. Esse resultado é fundamental para a demonstração da segunda caracterização dos grupos central-por-finito.

Notamos que em (3.2.1) não há perda de generalidade ao considerar as n classes laterais como classes laterais a direita, pois dados C subgrupo de G e xC uma classe lateral a esquerda, temos que $xC = xCxx^{-1} = C^{x^{-1}}x$, que é uma classe lateral a direita do subgrupo $C^{x^{-1}}$. Antes de demonstrar o resultado devido a R. Baer, vamos apresentar alguns lemas preliminares provados por B. H. Neumann em [**19**, §4].

Lema 3.2.1. *Seja G um grupo que é a união finita de n classes laterais de subgrupos $C_1, \ldots, C_n$ não necessariamente distintos de G , isto é,*

$$G = \bigcup_{i=1}^{n} C_i g_i.$$

Então pelo menos um dos subgrupos C_i tem índice finito em G.

Demonstração. Observamos que o lema é óbvio para grupos finitos. Vamos usar indução sobre o número de subgrupos entre $C_1, \ldots, C_n$ que são distintos. Se todos os C_i são iguais, digamos $C_i = C$ para todo i, então $G = \bigcup_{i=1}^{n} Cg_i$ e portanto $[G : C] \leq n$, ou seja, C tem índice finito em G. Assumimos que o resultado vale quando existem $r - 1$ ou menos subgrupos distintos entre os subgrupos $C_1, \ldots C_n$. Supomos que existem $r > 1$ subgrupos distintos entre os $C_1, \ldots, C_n$. Consideramos um desses subgrupos, digamos C_n, e assumimos que os subgrupos C_i em $G = \bigcup_{i=1}^{n} C_i g_i$ estão arranjados de forma que $C_1, \ldots, C_m$ são diferentes de C_n e $C_{m+1} = C_{m+2} \cdots = C_n$. Podemos fazer isso pois na união a ordem dos termos não importa. Agora temos dois casos, ou $G = \bigcup_{i=m+1}^{n} C_n g_i$ e pelo que vimos anteriormente, temos que C_n tem índice finito, ou existe h em G tal que h não pertence a $\bigcup_{i=m+1}^{n} C_n g_i$. Nesse último caso, como as classes laterais são iguais ou disjuntas, temos que

$$C_n h \cap \left(\bigcup_{i=m+1}^{n} C_n g_i\right) = \emptyset. \tag{3.2.2}$$

Como C_nh está contido em G, por (3.2.2) temos que C_nh está contido em $\bigcup_{i=1}^m C_ig_i$, ou seja, C_ng está contido em $\bigcup_{i=1}^m C_ig_ih^{-1}g$. Portanto, toda classe lateral a direita de C_n está contida em uma união finita de classes laterais a direita dos outros $r-1$ subgrupos C_i. Assim, $G = \bigcup_{i=1}^m C_ig_ih^{-1}g$ e por hipótese de indução, pelo menos um subgrupo C_i tem índice finito em G, como queríamos. □

Já sabemos que quando temos uma cobertura finita por classes laterais, pelo menos um dos subgrupos da cobertura tem índice finito. A seguir provaremos que se existe apenas um subgrupo de índice finito na cobertura, as classes laterais dos outros subgrupos podem ser omitidas da mesma.

Lema 3.2.2. *Seja G um grupo que é a união finita de n classes laterais de subgrupos $C_1, \ldots, C_n$ não necessariamente distintos de G , isto é, $G = \bigcup_{i=1}^n C_ig_i$. Se $C_1, \ldots, C_m$ têm índice infinito e $C_{m+1} = C_{m+2} \cdots = C_n$, então*

$$G = \bigcup_{i=1}^n C_ig_i = \bigcup_{i=m+1}^n C_ng_i,$$

ou seja, se apenas um subgrupo C_n tem índice finito, então as classes laterais dos subgrupos de índice infinito podem ser omitidas da cobertura.

Demonstração. Vamos supor por absurdo que não temos $G = \bigcup_{i=m+1}^n C_ng_i$, isto é, existe h em G tal que h não pertence a $\bigcup_{i=m+1}^n C_ng_i$. Nesse caso, temos que C_nh está contido em $\bigcup_{i=1}^m C_ig_i$ e portanto, como vimos na demonstração do lema anterior, temos que $G = \bigcup_{i=1}^m C_ig_ih^{-1}g$, onde g é qualquer elemento de G. Assim, pelo Lema 3.2.1, temos que existe um subgrupo C_i, para algum $1 \leq i \leq m$, tal que C_i tem índice finito, um absurdo, pois como C_i é diferente de C_n, para todos $1 \leq i \leq m$ temos por hipótese que C_i tem índice infinito. □

No próximo lema, vamos eliminar a hipótese de que exista apenas um subgrupo de índice finito. Mostraremos que mesmo assim as classes laterais dos subgrupos de índice infinitos podem ser omitidas da cobertura.

Lema 3.2.3. *Seja G um grupo que é a união finita de n classes laterais de subgrupos $C_1, \ldots, C_n$ não necessariamente distintos de G , isto é, $G = \bigcup_{i=1}^n C_ig_i$. Se $C_1, \ldots, C_m$ têm índices infinitos, então*

$$G = \bigcup_{i=m+1}^n C_ig_i,$$

ou seja, as classes laterais dos subgrupos de índice infinito podem ser omitidas da cobertura de G.

Demonstração. Pelo Lema 3.2.1, temos que pelo menos um dos subgrupos $C_{m+1}, \ldots, C_n$ tem índice finito. Não há perda de generalidade em supor que, de fato, todos os subgrupos $C_{m+1}, \ldots, C_n$ têm índice finito, pois caso exista C_i de índice infinito, para algum $m+1 \leq i \leq n$, podemos colocá-lo na lista dos subgrupos de índice infinito que queremos mostrar serem supérfluos para a cobertura de G. Definimos

$$D = \bigcap_{i=m+1}^{n} C_i.$$

Como D é a interseção de um número finito de subgrupos de índice finito, pelo Lema 1.0.1, temos que D também tem índice finito em G. Agora, como D está contido em C_i, para todo $m+1 \leq i \leq n$, então cada subgrupo C_i pode ser escrito como união finita de classes laterais de D, já que $[G : D] = [G : C_i][C_i : D]$ e $[G : D]$ e $[G : C_i]$ são ambos finitos. Então, como G pode ser escrito como união de classes laterais dos subgrupos $C_1, \ldots, C_n$ e cada C_i pode ser escrito como união finita de classes laterais de D, para $m+1 \leq i \leq n$, segue que G pode ser escrito como união de um número finito de classes de $C_1, \ldots, C_m$ e de D, isto é,

$$G = \left(\bigcup_{i=1}^{m} C_i g_i\right) \bigcup \left(\bigcup_{j=1}^{k} D y_j\right), \tag{3.2.3}$$

com $\bigcup_{j=1}^{k} D y_j = \bigcup_{i=m+1}^{n} C_i g_i$. Portanto, pelo Lema 3.2.2, como apenas D tem índice finito, as classes laterais de $C_1, \ldots, C_m$ podem ser omitidas da cobertura de G, isto é, $G = \bigcup_{j=1}^{k} D y_j = \bigcup_{i=m+1}^{n} C_i g_i$, como queríamos. □

Agora que já temos as ferramentas necessárias, devido a B. H. Neumann em [**19**, §4], vamos demonstrar a segunda caracterização de um grupo central-por-finito, que pode ser encontrada no livro de D. Robinson [**24**, Theorem 4.16].

Teorema 3.2.4. *Seja G um grupo. G é central-por-finito se, e somente se G admite uma cobertura finita por subgrupos abelianos.*

Demonstração. Suponha G é central-por-finito, isto é, $[G : Z(G)] = n$ para algum n inteiro positivo. Escolhemos um transversal $\{g_1, \cdots g_n\}$ para $Z(G) = Z$ em G. Assim, para qualquer g em G, temos que $g = g_i z$ para algum z em Z, portanto g está em $\langle g_i, Z\rangle$, que é um subgrupo abeliano pois os geradores comutam. Assim,

$$G = \bigcup_{i=1}^{n} \langle g_i, Z\rangle,$$

com $\langle g_i, Z\rangle$ todos subgrupos abelianos de G. Então G admite uma cobertura finita por subgrupos abelianos.

Reciprocamente, suponha que

$$G = \bigcup_{i=1}^{n} A_i,$$

onde os A_i são subgrupos abelianos. Pelo Lema 3.2.3, podemos supor sem perda de generalidade que todos os A_i têm índice finito. Seja $D = \bigcap_{i=1}^{n} A_i$, como já observamos, pelo Lema 1.0.1, D tem índice finito. Se g é um elemento de G, então g está em A_i para algum $1 \leq i \leq n$. Também temos que D está contido em A_i para todo $1 \leq i \leq n$ e como A_i é abeliano, os elementos de D comutam com todos os elementos de A_i, portanto os elementos de D comutam com todos os elementos de G. Segue que D é central e assim, como $[G : Z(G)] \leq [G : D] < \infty$, G é um grupo central-por-finito, como queríamos. □

Agora, demonstraremos mais dois resultados que dão uma cota superior para o índice de um dos subgrupos da cobertura.

Definição 3.2.5. Sejam G um grupo e C um subgrupo de G. Definimos a *"densidade"* de C, denotada por $\delta(C)$, como o inverso do seu índice em G, se o índice é finito, isto é,

$$\delta(C) = \frac{1}{[G : C]}$$

e $\delta(C) = 0$, se $[G : C]$ é infinito.

Lema 3.2.6. *Seja G um grupo que é a união finita de n classes laterais de subgrupos $C_1, \ldots, C_n$ não necessariamente distintos de G , isto é, $G = \bigcup_{i=1}^n C_i g_i$. Então*

$$\sum_{i=1}^{n} \delta(C_i) \geq 1.$$

Demonstração. Como pelo Lema 3.2.3, podemos omitir as classes laterais de subgrupos de índice infinito da cobertura de G e $\delta(C_i) = 0$ para subgrupos de índice infinito, podemos supor sem perda de generalidade que $C_1, \ldots, C_n$ têm todos índice finito. Denotaremos novamente D como a interseção dos subgrupos C_i, para $1 \leq i \leq n$. Agora, $C_i g_i$ é a união de $[C_i : D]$ classes laterais de D. Assim, $G = \bigcup_{i=1}^n C_i g_i$ é a união de $\sum_{i=1}^n [C_i : D]$ classes laterais de D. Como D também é um subgrupo de G, temos que G é a união de no mínimo $[G : D]$ classes laterais de D, ou seja,

$$[G : D] \leq \sum_{i=1}^{n} [C_i : D].$$

Assim, como $[G : D] = [G : C_i][C_i : D]$, temos que $[C_i : D] = [G : D]\delta(C_i)$. Portanto

$$\sum_{i=1}^{n} [C_i : D] = \sum_{i=1}^{n} [G : D]\delta(C_i) = [G : D] \sum_{i=1}^{n} \delta(C_i).$$

Logo,

$$\sum_{i=1}^{n} \delta(C_i) = \frac{\displaystyle\sum_{i=1}^{n} [C_i : D]}{[G : D]} \geq 1$$

□

Lema 3.2.7. *Seja G um grupo que é a união finita de n classes laterais de subgrupos $C_1, \ldots, C_n$ não necessariamente distintos de G , isto é, $G = \bigcup_{i=1}^n C_i g_i$. Então o índice de pelo menos um desses subgrupos em G não excede n.*

DEMONSTRAÇÃO. Notamos que o lema é óbvio para grupos finitos e sua demonstração não precisa do conceito de densidade de um subgrupo. De fato, suponha que $[G : C_i] > n$ para todo i. Daí, como $|C_i g_i| = |C_i|$ e $G = \bigcup_{i=1}^n C_i g_i$, temos que

$$[G : C_i] = \frac{|G|}{|C_i|} \leq \frac{\sum_{i=1}^n |C_i|}{|C_i|}.$$

Portanto, para todo i, temos que $n|C_i| < \sum_{i=1}^n |C_i|$. Assim, $n|C_1| + \cdots + n|C_n| < n \sum_{i=1}^n |C_i|$, um absurdo, então existe C_i tal que $[G : C_i] \leq n$.

No caso geral, pelo Lema 3.2.6, temos que $\sum_{i=1}^n \delta(C_i) \geq 1$. Supondo sem perda de generalidade que os subgrupos de índice finito são os m primeiros subgrupos C_i, segue que $\sum_{i=1}^m 1/[G : C_i] \geq 1$. Se $[G : C_i] > n$ para todo $i \leq m$, teríamos que

$$\frac{1}{[G : C_i]} < \frac{1}{n}.$$

Então,

$$\sum_{i=1}^m \frac{1}{[G : C_i]} < \sum_{i=1}^m \frac{1}{n} = \frac{m}{n} \leq 1,$$

um absurdo. Então existe C_i tal que $[G : C_i] \leq n$. $\square$

Capítulo 4

Análise Quantitativa

Como vimos no capítulo anterior, dado G um grupo, dizer que G é central-por-finito é equivalente a dizer que G é um PE-grupo ou que G pode ser coberto por um número finito de subgrupos abelianos, isto é, $G = \bigcup_{i=1}^{n} A_i$. Note que, se $G = \bigcup_{i=1}^{n} A_i$, a cobertura $A = \{A_1, \ldots, A_n\}$ é dita *irredundante* se qualquer subconjunto próprio de A não forma uma cobertura de G, ou equivalentemente, se nenhum subgrupo A_i pode ser retirado de A de forma que os subgrupos restantes ainda formem uma cobertura de G. Dessa forma, dado G um grupo central-por-finito, podemos definir o número $a(G)$ como a menor cardinalidade de uma cobertura irredundante, isto é, como o menor número de subgrupos abelianos necessários para cobrir G de forma que esta cobertura seja irredundante. Note que, pela demonstração do Teorema 3.1.10 temos que se G é central-por-finito com $[G : Z(G)] = n$, dados quaisquer $n + 1$ elementos de G, pelo menos dois desses $n + 1$ elementos estarão na mesma classe lateral de $Z(G)$ e portanto pelo menos dois elementos comutarão. Isso implica que o tamanho máximo de um subgrafo completo em $\Gamma(G)$, isto é, o tamanho máximo de um clique é n. Usando a notação do Capítulo 2, temos que $\omega(\Gamma(G)) \leq n$. No nosso caso, sempre estaremos considerando o grafo não comutativo $\Gamma(G)$ associado ao grupo G, então neste capítulo denotaremos $\omega(\Gamma(G))$ simplesmente por $\omega(G)$.

O objetivo deste capítulo é relacionar esses três indicadores quantitativos associados a um grupo central-por-finito G, isto é, relacionar n, o índice de $Z(G)$, $\omega(G)$, o tamanho do maior clique em $\Gamma(G)$, e $a(G)$ o tamanho da menor cobertura irredundante por subgrupos abelianos. No final também faremos algumas considerações sobre a relação entre $\omega(G)$ e a cardinalidade de G em um grupo finito.

4.1 Relacionando $[G : Z(G)]$ e $\omega(G)$

Dado G um grupo tal que $[G : Z(G)] = n$, já observamos que $\omega(G) \leq n$. Em geral, essa estimativa pode ser melhorada quando $n > 1$ para

$$\omega(G) \leq n - 1.$$

De fato, seja $X = \{x_1, \ldots, x_n\}$ qualquer subconjunto de G de tamanho n. Se pelo menos dois desses elementos, x_i e x_j, estão na mesma classe lateral de $Z(G)$, então x_i e x_j comutam e assim X não é um clique. Se todos os n elementos de X estão em classes laterais distintas de $Z(G)$, temos que entre esses n elementos existe um, digamos x_i, que está na classe lateral $Z(G)$, isto é, o elemento x_i é um elemento central de G. Desta forma, temos que x_i comuta com todos os outros $n-1$ elementos e portanto X não é um clique. Portanto, o tamanho de um clique em $\Gamma(G)$ deve ser sempre menor ou igual a $n-1$, isto é, $\omega(G) \leq n-1$, como queríamos.

Agora vamos dar um exemplo de um grupo G tal que $[G : Z(G)] = n$ e $\omega(G) = n-1$. De fato, consideramos D_8, o grupo diedral de ordem 8. No Capítulo 2, já havíamos determinado seu grafo não-comutativo (Ver Figura 2.1.3) e notado que $\omega(D_8) = 3$. Como $Z(D_8) = \{1, \rho^2\}$, temos que $[G : Z(D_8)] = n = 4$. Assim, $\omega(D_8) = n-1$. Notamos também que nem sempre $\omega(G)$ alcança o valor $n-1$. Como exemplo, consideramos D_6, o grupo diedral de ordem 6. Pelo grafo não-comutativo de D_6 (Ver Figura 2.1.2) temos que $\{\tau, \rho\tau, \rho^2\tau, \rho^2\}$ é um clique e que não há cliques de tamanho maior que quatro, logo $\omega(D_6) = 4$. Por outro lado, como $Z(D_6) = \{1\}$, temos que $[G : Z(D_6)] = n = 6$. Assim, $\omega(D_6) < n-1$.

Uma pergunta interessante sobre $\omega(G)$ é saber se para todo inteiro positivo m existe um grupo G tal que $\omega(G) = m$. Se G é um grupo abeliano, então $\omega(G) = 1$. Paul Erdős mostrou que não podemos atingir $\omega(G) = 2$. De fato, sejam G um grupo e a e b elementos de G tais que a e b não comutam. Então ambos a e b também não comutam com o elemento ab em G, ou seja, $\omega(G) > 2$. Agora seja m um inteiro positivo maior que 2, B. H. Neumann [**18**] observou que se G é o grupo diedral de ordem $4(m-1)$, então $\omega(G) = m$. Consideramos $G = D_{2n}$, com $n = 2(m-1)$, isto é

$$D_{2n} = \langle \rho, \tau \mid \tau^2 = \rho^n = 1, \rho^\tau = \rho^{-1} \rangle.$$

Notamos que para $0 \leq i, j \leq n-1$ e $i \neq j$, temos

$$[\rho, \tau\rho^i] = \rho^{n-2}$$
$$[\tau, \tau\rho^i] = \rho^{2i}$$
$$[\tau\rho^i, \tau\rho^j] = \rho^{2(i-j)}.$$

Vamos considerar $H = \{\rho, \tau, \tau\rho, \ldots, \tau\rho^{n-1}\}$ e retirar os elementos que comutam, para formar o nosso clique. Como $n > 2$ temos que ρ e $\tau\rho^i$ não comutam para nenhum i. Agora, $\rho^{2i} = 1$ para $i \neq 0$ somente quando $i = n/2$, ou seja, vamos retirar da lista H o elemento $\tau\rho^{n/2}$. Agora supondo que i e j são diferentes de $n/2$, vamos analisar quando $\tau\rho^i$ e $\tau\rho^j$ comutam. Temos que $\rho^{2(i-j)} = 1$ somente quando $i - j = n/2$, isto é, $i - (n/2) = j$. Para $i = n-1$, temos que $j = (n/2) - 1$ e analogamente, para $i = (n/2) - k$, temos que $j = (n/2) - k$, para $1 \leq k \leq (n/2) - 1$. Vamos então retirar da lista H os elementos $\tau\rho^{(n/2)-k}$, para $1 \leq k \leq (n/2) - 1$. Ao retirar esses elementos de H, ficamos com um clique K de tamanho $(n+1) - 1 - [(n/2) - 1] = (n/2) + 1$. No nosso caso, $n = 2(m-1)$, então $\omega(G) \geq m$. Se existisse um clique de tamanho maior que m, teríamos que adicionar a K algum elemento do tipo ρ^i, com $1 < i < n$, mas ρ^i comutaria com ρ. É possível ver também que qualquer outro clique de $\Gamma(D_{2n})$ tem tamanho menor ou igual a m. Assim, o tamanho do maior clique de D_{2n} com $n = 2(m-1)$ é exatamente m, como queríamos.

Dado G um grupo central-por-finito, sabemos que não existem em $\Gamma(G)$ subgrafos infinitos completos. Uma pergunta natural a se fazer neste ponto é: dado que $\Gamma(G)$ não possui subgrafos completos maiores que $\omega(G)$, se é possível determinar uma cota superior para n, o índice de $Z(G)$, em termos de $\omega(G)$. L. Pyber, em seu trabalho *The number of pairwise non-commuting elements and the index of the centre in a finite group*,[**22**], mostrou que se G é um grupo tal que $\omega(G) = m$, então

$$[G : Z(G)] \leq c^m, \tag{4.1.1}$$

onde c é uma constante. Primeiro, observamos que é possível considerar apenas grupos finitos pelo seguinte resultado cuja demonstração pode ser encontrada em [**13**, §2]:

Teorema 4.1.1. *Dado G um grupo com $\omega(G)$ finito, existe H um grupo finito tal que $H/Z(H)$ e $G/Z(G)$ são isomorfos e $\omega(G) = \omega(H)$.*

Vamos denotar por $k(G)$ o tamanho máximo de uma classe de conjugação de G. O próximo lema será o primeiro passo para conseguirmos uma cota para $[G : Z(G)]$ em função de m.

Lema 4.1.2. *Seja G um grupo finito tal que $\omega(G) = m$. Então, $k(G) \leq 4m^2$.*

Demonstração. Suponha que as disjuntas classes de conjugação de G estejam indexadas de forma crescente em relação a sua ordem, isto é,

$$1 \leq |Cl(g_1)| \leq |Cl(g_2)| \leq \cdots .$$

Seja r o menor inteiro tal que

$$|Cl(g_1)| + \cdots + |Cl(g_r)| > \frac{|G|}{2}.$$

Primeiro vamos mostrar que $|Cl(g_r)| \leq 2m$. De fato, considere o conjunto

$$X = G \setminus \left(\bigcup_{j=1}^{r-1} Cl(g_j) \right).$$

Pela escolha de r temos que $|Cl(g_1)| + \cdots + |Cl(g_{r-1})| \leq \frac{|G|}{2}$ e assim, como as classes de conjugação são disjuntas, temos que

$$|X| \geq \frac{|G|}{2}.$$

Como X é um subconjunto de G, temos que existe um subconjunto $X' = \{x_1, \ldots, x_l\}$ de X com $l \leq m$ e tal que X' é um clique de cardinalidade maximal de X. Assim, dado x elemento de $X \setminus X'$ temos que x comuta com algum x_i, caso contrário teríamos um absurdo pelo fato de

X' ser o clique de cardinalidade maximal. Portanto, X está contido em $C_G(x_1) \cup \ldots \cup C_G(x_l)$ e assim existe j, com $1 \leq j \leq l$, tal que

$$|C_G(x_j)| \geq \frac{1}{m}|X| \geq \frac{|G|}{2m}.$$

Como x_j está em X, por definição temos que $Cl(x_j) = Cl(g_i)$ para algum $i \geq r$. Logo, pela forma como as classes de conjugação foram ordenadas, temos que

$$|Cl(g_r)| \leq |Cl(x_j)| = [G : C_G(x_j)] \leq 2m.$$

Agora para $Y = Cl(g_1) \cup \ldots \cup Cl(g_r)$ temos que $|Y| > \frac{1}{2}|G|$, logo $|Y| + |Y| > |G|$. Mas dado g um elemento em G, temos que o conjunto gY tem a mesma cardinalidade de Y, logo $|gY| + |Y| > |G|$. Assim, existe um elemento y que está em $gY \cap Y$, isto é, $y = gy_1$, com y_1 em Y. Logo, g está em YY e portanto $G = YY$. Então, dado g um elemento de G, temos que g pertence a $Cl(g_i)Cl(g_j)$ para $1 \leq i, j \leq r$ e temos que $Cl(g)$ está em $Cl(g_i)Cl(g_j)$. Mas $|Cl(g_i)Cl(g_j)| \leq |Cl(g_r)|^2 \leq (2m)^2$, logo $|Cl(g)| \leq 4m^2$ para todo g em G, e portanto $k(G) \leq 4m^2$, como queríamos. □

Proposição 4.1.3. *Se* $\{a_1, \ldots, a_s\}$ *é um clique de* $\Gamma(G)$*, então*

$$\omega\left(\bigcap_{i=1}^{s} C_G(a_i)\right) \leq \omega(G) - s + 1.$$

Em particular, se pegarmos $s = \omega(G)$*, temos que* $\bigcap_{i=1}^{s} C_G(a_i)$ *é um subgrupo abeliano.*

Demonstração. Seja $\{b_1, \ldots, b_l\}$ um clique do grafo não-comutativo de $\bigcap_{i=1}^{s} C_G(a_i)$. Como cada b_i, para $1 \leq i \leq l$, comuta com a_j, para todo $1 \leq j \leq s$, temos que o conjunto $\{b_1, \ldots, b_{l-1}, b_l a_1, \ldots, b_l a_s\}$ é um clique de $\Gamma(G)$ de tamanho $l+s-1$ e portanto $l+s-1 \leq \omega(G)$ e assim $l \leq \omega(G) - s + 1$. Podemos considerar o clique $\{b_1, \ldots, b_l\}$ de maior cardinalidade de $\bigcap_{i=1}^{s} C_G(a_i)$, isto é, $l = \omega\left(\bigcap_{i=1}^{s} C_G(a_i)\right)$ e assim temos o resultado. Em particular, se $s = \omega(G)$, temos que $\omega\left(\bigcap_{i=1}^{s} C_G(a_i)\right) \leq 1$, isto é, $\bigcap_{i=1}^{s} C_G(a_i)$ é abeliano.

□

Por definição temos que $Z(G)$ está contido em $A = \bigcap_{i=1}^{s} C_G(a_i)$. Queremos mostrar que $Z(G) = A$ e para tanto vamos mostrar que $A \leqslant Z(G)$, resultado que pode ser encontrado em [**26**, Theorem 5.1].

Suponha por absurdo que existe um elemento a que está em A, mas não está em $Z(G)$. Então existe um elemento b em G tal que $[a, b] \neq 1$. Para cada $1 \leq i \leq s$ defina $y_i = a_i$, se $[a_i, b] \neq 1$ e $y_i = aa_i$ se $[a_i, b] = 1$. Assim, $\{y_1, \ldots, y_s, b\}$ é um clique de tamanho $s + 1$, um absurdo. Portanto, temos que $Z(G) = A$. Assim, quando $s = \omega(G)$ e pelo Lema 4.1.2, temos que

$$[G : Z(G)] = [G : A] \leq \prod_{i=1}^{s} [G : C_G(a_i)] \leq (4s^2)^s = 2^{2s(1+logs)},$$

onde *logs* é na base 2.

De fato, L.Pyber conseguiu uma estimativa ainda melhor para o índice do centro em função de $m = \omega(G)$. Ele prova o seguinte:

$$[G : Z(G)] \leq 2^{2^{25}m} 2^{3(2+2\log m)^5}.$$

Os detalhes da demonstração de tal resultado podem ser achados em [**22**, Theorem 6.1.]. Não apresentaremos a demonstração aqui, porém daremos uma ideia dos passos que foram seguidos para obter essa cota.

Como já foi observado, é possível, sem perda de generalidade, considerar G um grupo finito. A ideia principal de Pyber é encontrar em G um subgrupo nilpotente C de classe no máximo 2, isto é, $C' \leqslant Z(C)$, e utilizar uma cadeia de subgrupos $Z(G) \leqslant Z(C) \leqslant C \leqslant G$ para reduzir o problema inicial de estimativa do índice de $Z(G)$ em G. Em [**22**], mostra-se que tal subgrupo nilpotente C de classe no máximo 2 é exatamente o subgrupo $C_G(G')$, onde G' denota o subgrupo derivado de G.

Primeiro, aplicando o Lema 4.1.2 e um resultado importante de P. M. Neumann e M. R. Vaughan-Lee [**21**] que diz que

$$|G'| \leq k^{\frac{1}{2}(3+5logk)}, \quad \text{onde } k = k(G)$$

é possível mostrar que existe uma cota superior para $|G'|$ que depende apenas de $\omega(G) = m$. Logo, pela Proposição 1.0.3 existem $\{g_1, \ldots, g_t\}$ geradores de G' com t que depende também de $\omega(G) = m$. Assim, é mostrado que existe uma cota superior para $[G : C]$ que depende apenas de m. Além disso, com um argumento semelhante, mostra-se que também é possível dar uma cota superior para o índice $[Z(C) : Z(G)]$ um função de m. Uma vez que temos cotas para os índices $[G : C]$ e $[Z(C) : Z(G)]$ dependendo de $\omega(G) = m$, para alcançarmos o objetivo final faltaria apenas majorar o índice de $Z(C)$ em C.

Utilizando os Lemas 4.1.2 e 4.1.3, o autor mostra que é possível, para um p-grupo nilpotente P de classe 2, dar uma cota superior do índice de $Z(P)$ em P apenas em função de $\omega(P)$. Agora, como C é nilpotente finito de classe no máximo 2, por [**23**, 5.2.4], temos que C é o produto direto dos seus subgrupos de Sylow, que em particular são p-grupos. Mas sabendo que $\omega(A \times B) \geq \omega(A)\omega(B)$ para quaisquer grupos A e B, como é mostrado na seção 3 de [**22**], temos que é possível achar uma cota superior para o índice de $Z(C)$ em C que depende apenas de $\omega(G) = m$. Assim, temos que

$$[G : Z(G)] = [G : C][C : Z(C)][Z(C) : Z(G)]$$

e usando as cotas achadas antes se chega a cota desejada para o índice de $Z(G)$ em função de m.

4.2 Relacionando $[G : Z(G)]$ e $a(G)$

Como vimos no Teorema 3.2.4, todo grupo central-por-finito pode ser coberto por um número finito de subgrupos abelianos. Portanto, é natural buscar uma relação entre n e

$a(G)$. A primeira questão a ser perguntada é dado G um grupo central-por-finito tal que $[G : Z(G)] = n$, se podemos limitar o valor de $a(G)$ em termos de n.

Notemos que dado $T = \{t_1, \ldots, t_n\}$ um transversal de $Z(G)$ em G, podemos definir os subgrupos $A_i = \langle Z(G), t_i\rangle$. Temos que cada A_i é abeliano, pois seus geradores comutam e também, dado g um elemento de G, g está em alguma classe lateral de $Z(G)$ em G, ou seja, $g = zt_i$, para z um elemento central e t_i um elemento no transversal T. Dessa forma, temos que g está sempre em $\langle Z(G), t_i\rangle$ para algum $1 \leq i \leq n$, logo $G = \bigcup_{i=1}^{n} A_i$. Assim, temos que $G = \bigcup_{i=1}^{n} A_i$ é uma cobertura irredundante de tamanho n por subgrupos abelianos. Como $a(G)$ é o tamanho da menor cobertura irredundante por subgrupos abelianos, temos que

$$a(G) \leq n.$$

Observamos que a igualdade vale apenas quando $n = 1$. De fato, se $n = 1$, então temos $G = Z(G)$, logo G é a sua própria cobertura por abelianos de tamanho 1 e portanto $a(G) = 1$. Por outro lado, se $n > 1$, seja $T = \{1, t_2, \ldots, t_n\}$ um transversal de $Z(G)$ em G. Temos, com a notação que utilizamos anteriormente, que $G = \bigcup_{i=1}^{n} A_i$. Mas como $n > 1$, temos que $G = \bigcup_{i=1}^{n} A_i = \bigcup_{i=2}^{n} A_i$, pois $A_1 = Z(G)$ que já está contido em A_i, para $2 \leq i \leq n$. Assim, $a(G) < n$.

Uma vez que temos um grupo G que pode ser coberto por um número finito de subgrupos abelianos, já sabemos que ele é central-por-finito e portanto $[G : Z(G)]$ é finito. A questão é determinar se é possível limitar o índice do centro, n, em termos de $a(G)$. No artigo *Groups covered by finitely many subsets* [**20**], B.H.Neumann encontrou algumas cotas possíveis. De fato, ele considerou um problema ainda mais geral, analisando grupos que não são cobertos por um número finito de classes laterais de subgrupos. A seguir daremos detalhes do estudo feito por B. H. Neumann em [**20**] e veremos as consequências dele para o problema de achar uma cota de $[G : Z(G)] = n$ em função de $a(G)$.

4.2.1 Grupos cobertos por classes laterais

Vamos começar a examinar a situação geral de um grupo G coberto por um número finito de classes laterais de subgrupos. Sejam $C_i = A_i g_i$, com $1 \leq i \leq m$, classes laterais de $A_1, \ldots, A_m$ subgrupos de G não necessariamente distintos. Como mencionamos no Capítulo 3, não há perda de generalidade em considerar classes laterais à direita. Assumiremos que

$$G = \bigcup_{i=1}^{m} C_i$$

de tal forma que essa seja uma cobertura irredundante de G. Podemos assumir também, pelo Lema 3.2.2, que todos os C_i sejam classes laterais de subgrupos A_i de índice finito, pois todas as classes C_i com A_i subgrupos de índice infinito podem ser omitidas da cobertura de G. Vamos mostrar que existe uma cota para esses índices $[G : A_i]$ dependendo apenas de m.

Se $G = \bigcup_{i=1}^{m} C_i$ é uma cobertura irredundante de G por classes laterais, denotaremos:

$$D_1 = A_1,\ D_2 = A_1 \cap A_2,\ \ldots,\ D_m = \bigcap_{i=1}^{m} A_i. \tag{4.2.1}$$

O lema a seguir nos dará a primeira cota superior para o índice $[G : D_m]$. A estimativa desse índice é relevante pois, no caso que nos interessa, $G = \bigcup_{i=1}^{m} A_i$, onde $A_1, \ldots, A_n$ são subgrupos abelianos, temos que $\bigcap_{i=1}^{m} A_i \leqslant Z(G)$ e assim $[G : Z(G)] \leq [G : \bigcap_{i=1}^{m} A_i] = [G : D_m]$. Assim, conseguir uma cota superior para o índice de D_m implica conseguir uma cota superior para o índice do centro de G.

Lema 4.2.1. *Sejam $A_1, \ldots, A_m$ subgrupos de G não necessariamente distintos e $C_i = A_i g_i$ classes laterais desses subgrupos. Se $G = \bigcup_{i=1}^{m} C_i$ é uma cobertura irredundante de G por classes laterais, então*

$$[G : A_i] \leq \prod_{j=1}^{m} j^{2^{j-2}} \quad e \quad [G : D_m] \leq \prod_{j=1}^{m} j^{2^{j-1}}$$

Demonstração. Se $m = 1$ temos que $G = C_1$, então $[G : D_1] = 1$ e não há nada a demonstrar. Assim, vamos supor que $m > 1$. Denotaremos o índice dos subgrupos A_i por $\alpha_i = [G : A_i]$ e denotaremos também $\delta_k = [G : D_k]$ onde os D_k são definidos em (4.2.1). Como já observamos, podemos supor que todos os A_i têm índice finito, ou equivalentemente, α_i é finito para todo i. Pelo Lema 1.0.1, temos que

$$\delta_k \leq \prod_{i=1}^{k} \alpha_i, \quad k = 1, \ldots, m \tag{4.2.2}$$

e como α_i é finito para todo i, temos que os δ_k são finitos para todo $1 \leq k \leq m$. Também notamos que se acharmos uma cota superior para todos os α_i, por (4.2.2) temos uma cota para δ_m. Por outro lado, se temos uma cota superior para $\delta_m = [G : D_m]$, como $D_m \leqslant A_i$, para todo $1 \leq i \leq m$, temos que $\alpha_i = [G : A_i] \leq [G : D_m] = \delta_m$ também será limitado superiormente.

Agora observamos que se B é um subgrupo de G contendo D_m com $[G : B] = \beta$, como $[G : D_m] = [G : B][B : D_m]$ temos que $[B : D_m] = \frac{\delta_m}{\beta}$, isto é, B é a união de $\frac{\delta_m}{\beta}$ classes laterais distintas de D_m. Notamos também que o mesmo vale para qualquer classe lateral Bg de B, visto que, se $B = \bigcup_{i=1}^{l} D_m h_i$, então $Bg = \bigcup_{i=1}^{l} D_m h_i g$. Consideramos a união $\bigcup_{i=1}^{k} C_i$, com $1 \leq k < m$. Como estamos considerando uma cobertura irredundante, temos que $\bigcup_{i=1}^{k} C_i$ não é igual a todo G. Como $C_i = A_i g_i$ e como cada $D_k \leqslant A_i$ sempre que $1 \leq i \leq k$, temos que cada A_i é a união de classes laterais de D_k, para $1 \leq i \leq k$. Logo, temos que $\bigcup_{i=1}^{k} C_i$ é a união de classes laterais de D_k. Mas como $\bigcup_{i=1}^{k} C_i$ não é todo G, temos que existe pelo menos uma classe lateral $D_k g$ que não está em $\bigcup_{i=1}^{k} C_i$. Segue que a classe $D_k g$ tem que ser coberta pelos

C_i restantes, isto é,

$$D_k g \subseteq \bigcup_{i=k+1}^{m} C_i. \tag{4.2.3}$$

Agora como D_k e A_i são subgrupos de G que contém D_m para todo $1 \leq k, i \leq m$, vimos que $D_k g$ é a união de $\frac{\delta_m}{\delta_k}$ classes de D_m e C_i é a união de $\frac{\delta_m}{\alpha_i}$ classes de D_m. Assim, por (4.2.3), como ambos os lados são uniões de classes laterais de D_m e as classes laterais são disjuntas ou iguais temos que

$$\frac{\delta_m}{\delta_k} \leq \sum_{i=k+1}^{m} \frac{\delta_m}{\alpha_i}. \tag{4.2.4}$$

Por (4.2.2), temos que $\frac{1}{\delta_k} \geq \prod_{i=1}^{k} \frac{1}{\alpha_i}$. De (4.2.4) segue que $\prod_{i=1}^{k} \frac{1}{\alpha_i} \leq \frac{1}{\delta_k} \leq \sum_{i=k+1}^{m} \frac{1}{\alpha_i}$, e assim temos

$$\prod_{i=1}^{k} \frac{1}{\alpha_i} \leq \sum_{i=k+1}^{m} \frac{1}{\alpha_i}, \tag{4.2.5}$$

para $1 \leq k < m - 1$. Observe que também podemos considerar o que corresponde formalmente ao caso $k = 0$ em (4.2.5), isto é,

$$1 \leq \sum_{i=1}^{m} \frac{1}{\alpha_i}. \tag{4.2.6}$$

Observe que a desigualdade (4.2.6) já havia sido demonstrada no capítulo anterior, no Lema 3.2.6. Aqui vamos mostrá-la de outra maneira. De fato, sabendo que C_i é a união de $\frac{\delta_m}{\alpha_i}$ classes laterais de D_m e G é a união de δ_m classes laterais de D_m, logo, como $G = \bigcup_{i=1}^{m} C_i$ e ambos os lados podem ser visto como união de classes laterais de D_m, temos que

$$\delta_m \leq \sum_{i=1}^{m} \frac{\delta_m}{\alpha_i}. \tag{4.2.7}$$

Notamos que a desigualdade (4.2.7) leva em consideração que a mesma classe lateral de D_m pode ocorrer em mais de um C_i. Lembramos que $\delta_m \geq 1$, pois é o índice de um subgrupo e que δ_m também é finito . Dividindo os dois lados de (4.2.7) por δ_m temos a desigualdade (4.2.6). Agora, condensando (4.2.6) e (4.2.5), temos:

$$\prod_{i=1}^{j-1} \frac{1}{\alpha_i} \leq \sum_{i=j}^{m} \frac{1}{\alpha_i} \quad j = 1, \ldots, m \tag{4.2.8}$$

se substituirmos k por $j - 1$. A seguir utilizaremos (4.2.8) para achar as cotas superiores desejadas. Suponha sem perda de generalidade que os C_i estão numerados de acordo com a ordem crescente dos índices. Notamos que caso isso não ocorra, basta renomeá-los. Desta maneira, temos que:

$$\alpha_1 \leq \alpha_2 \leq \cdots \leq \alpha_m.$$

Logo,

$$\frac{1}{\alpha_1} \geq \frac{1}{\alpha_2} \geq \cdots \geq \frac{1}{\alpha_m}. \tag{4.2.9}$$

Notemos que $\frac{1}{\alpha_i} \leq \frac{1}{\alpha_j}$ sempre que $j \leq i \leq m$ por (4.2.9). Logo,

$$\sum_{i=j}^{m} \frac{1}{\alpha_i} \leq \frac{m-j+1}{\alpha_j}.$$

Portanto, por (4.2.8) temos que

$$\prod_{i=1}^{j-1} \frac{1}{\alpha_i} \leq \frac{m-j+1}{\alpha_j},$$

ou, equivalentemente

$$\alpha_j \leq (m-j+1) \prod_{i=1}^{j-1} \alpha_i.$$

Assim, temos cotas superiores para cada α_j dependendo de m e de α_i para $1 \leq i < j$. De forma concreta temos que,

$$\begin{aligned}
&\alpha_1 \leq m \\
&\alpha_2 \leq (m-1)\alpha_1 \leq (m-1)m \\
&\alpha_3 \leq (m-2)\alpha_1\alpha_2 \leq (m-2)(m-1)m^2 \\
&\alpha_4 \leq (m-3)\alpha_1\alpha_2\alpha_3 \leq (m-3)(m-2)(m-1)^2 m^4 \\
&\quad \vdots \\
&\alpha_m \leq 1 \cdot 2 \cdot 3^2 \cdot \cdots \cdot m^{2^{m-2}}
\end{aligned}$$

Notamos que a cota $\alpha_1 \leq m$ já havia sido observada no capítulo anterior, no Lema 3.2.7. Lembramos que $\alpha_1 \leq \alpha_2 \leq \ldots \leq \alpha_m$, então $\alpha_i \leq \alpha_m \leq 1 \cdot 2 \cdot 3^2 \cdot \cdots \cdot m^{2^{m-2}}$, para todo $1 \leq i \leq m$. Logo, $\alpha_i \leq \prod_{j=1}^{m} j^{2^{j-2}}$, para todo $1 \leq i \leq m$ e dessa forma temos a primeira parte do lema. Agora, por (4.2.2) sabemos que $\delta_m \leq \alpha_1 \cdots \alpha_m$. Assim, temos que

$$\delta_m \leq \alpha_1 \cdots \alpha_m \leq m^{\left(1+\sum_{k=0}^{m-2} 2^k\right)}.(m-1)^{\left(1+\sum_{k=0}^{m-3} 2^k\right)}.(m-2)^{\left(1+\sum_{k=0}^{m-4} 2^k\right)} \cdot \cdots \cdot 2^2 \cdot 1.$$

Logo, pela soma de uma progressão geométrica temos

$$[G : D_m] = \delta_m \leq 1 \cdot 2^2 \cdot \dots \cdot m^{2^{m-1}} = \prod_{j=1}^{m} j^{2^{j-1}}$$

o que demonstra a segunda parte do lema. □

O próximo teorema é um resultado técnico que vale em geral para números reais. Como sua demonstração é muito extensa, ela será omitida neste capítulo, mas pode ser encontrada no Apêndice 6. Como corolário deste teorema, teremos as novas cotas superiores para o índice de D_m.

Teorema 4.2.2. *Sejam $\alpha_1, \dots, \alpha_m$ m números reais positivos tais que*

$$1 \leq \alpha_1 \leq \alpha_2 \leq \cdots \leq \alpha_m \quad e \quad \prod_{i=1}^{j-1} \frac{1}{\alpha_i} \leq \sum_{i=j}^{m} \frac{1}{\alpha_i},$$

para $1 \leq j \leq m$, então

$$\alpha_m \leq y_m \quad e \quad \prod_{i=1}^{m} \alpha_i \leq {y_m}^2$$

onde $y_1 = 1$ e $y_{i+1} = {y_i}^2 + y_i$, quando $i \geq 1$.

Corolário 4.2.3. *Sejam $A_1, \dots, A_m$ subgrupos de G não necessariamente distintos e $C_i = A_i g_i$ classes laterais desses subgrupos. Se $G = \bigcup_{i=1}^{m} C_i$ é uma cobertura irredundante de G por classes laterais, então*

$$\Delta_m = [G : \bigcap_{i=1}^{m} A_i] \leq {y_m}^2$$

onde $y_1 = 1$ e $y_{i+1} = {y_i}^2 + y_i$, para $i \geq 1$.

Demonstração. No Teorema 4.2.2, basta tomar $\alpha_i = [G : A_i]$ para $1 \leq i \leq m$. Temos então por (4.2.8) que os α_i satisfazem as hipóteses. Mas $[G : \bigcap_{i=1}^{m} A_i] \leq \prod_{i=1}^{m} \alpha_i \leq {y_m}^2$ e assim temos que o resultado vale. □

Através do Lema 4.2.1, mostramos a existência de cotas superiores para cada α_i e para o índice de D_m. Como já mencionamos, no caso particular em que G é coberto por m subgrupos abelianos, temos que a existência de uma cota superior para $[G : D_m]$ implica na existência de uma cota superior para o índice de $Z(G)$, que é o que queremos.

Se G é coberto por subgrupos abelianos e $m = a(G)$, temos $[G : Z(G)] \leq [G : \bigcap_{i=1}^{m} A_i]$. Assim, do Corolário 4.2.3, segue que

$$n = [G : Z(G)] \leq [G : \bigcap_{i=1}^{m} A_i] \leq {y_{a(G)}}^2.$$

De fato, é possível melhorar as cotas obtidas pelo Corolário 4.2.3 se trabalharmos um pouco mais na desigualdade (4.2.8). Note que, pelo Lema 4.2.1, em nossa primeira estimativa, tínhamos que se $a(G) = 4$, então $\alpha_4 \leq 4608$. Já pelo Teorema 4.2.2, temos que $\alpha_4 \leq 42$. Dessa forma, como o índice do centro é menor ou igual ao produto dos α_i temos que a estimativa para $[G : Z(G)] = n$ em função de $a(G)$ foi significantemente melhorada.

Agora vamos fazer uma análise da interseção de classes laterais. Sejam A e A' subgrupos com índice finito em G tais que o índice de $A \cap A'$ é exatamente o produto do índice de A em G pelo índice de A' em G. Sejam $[G : A] = \alpha$, $[G : A'] = \alpha'$ e $[G : D] = \delta$, com $D = A \cap A'$. Suponhamos, que $\delta = \alpha\alpha'$. Pela Proposição 1.0.2 , temos que $G = AA'$. Portanto, se $C = Ag$ e $C' = A'g'$ são duas classes laterais de A e A' respectivamente, temos que existem a em A e a' em A' tais que

$$gg'^{-1} = aa'.$$

Assim, temos que $a^{-1}g = a'g'$ está em $C \cap C'$. Portanto,

$$Da^{-1}g = Da'g' \subseteq C \cap C'.$$

Logo, como já vimos na demonstração do Lema 4.2.1, temos que C é a união de $\frac{\delta}{\alpha} = \alpha'$ classes laterais de D e C' é a união de $\frac{\delta}{\alpha'} = \alpha$ classes laterais de D. Então, como pelo menos uma classe lateral de D está em ambas as coberturas temos que $C \cup C'$ é a união de no máximo

$$\frac{\delta}{\alpha'} + \frac{\delta}{\alpha} - 1 = \alpha' + \alpha\left(1 - \frac{1}{\alpha}\right)$$

classes laterais de D.

Agora suponha que $C \cup C'$ é a união de exatamente $\frac{\delta}{\alpha'} + \frac{\delta}{\alpha}$ classes laterais de D. Nesse caso temos que C e C' são disjuntas e que $\delta < \alpha\alpha'$, pois se tivéssemos a igualdade, cairíamos no caso anterior. Mas, em geral $\delta = [G : D] = [G : A'][A' : D]$, então δ é sempre múltiplo de α'. Assim,

$$\delta \leq (\alpha - 1)\alpha' = \alpha\alpha'\left(1 - \frac{1}{\alpha}\right). \tag{4.2.10}$$

Portanto, se C e C' não têm interseção, temos que (4.2.10) vale. É possível mostrar que o mesmo vale para subgrupos de A, ou seja, se B é um subgrupo de A, $[G : B] = \beta$ e $[G : A' \cap B] = \delta'$, então sempre que C e C' são disjuntos temos que

$$\delta' \leq \beta\alpha'\left(1 - \frac{1}{\alpha}\right).$$

Vamos agora aplicar a observação acima na situação em que $G = \cup_{i=a}^{m} C_i$ é uma cobertura irredundante de G. Fixamos uma classe lateral, digamos, C_1. Assim, dividimos os C_i restantes de acordo com seu índice, da seguinte maneira: para $2 \leq i \leq m$, se C_i tem interseção vazia com C_1, então $i \in I$ e se C_i tem interseção não vazia com C_1, então $i \in J$. Assim, por (4.2.2) e aplicando (4.2.10) temos que para $1 \leq k \leq m$

$$\delta_k \leq \prod_{i=1}^{k} \alpha_i \leq \alpha_1 \cdot \prod_{i \leq k, i \in I} \alpha_i \left(1 - \frac{1}{\alpha_1}\right) \cdot \prod_{j \leq k, j \in J} \alpha_j. \tag{4.2.11}$$

Também temos que (4.2.4) pode ser melhorada da seguinte forma,

$$\frac{\delta_m}{\delta_k} \leq \sum_{i > k, i \in I} \frac{\delta_m}{\alpha_i} + \sum_{j > k, j \in J} \frac{\delta_m}{\alpha_j} \left(1 - \frac{1}{\alpha_1}\right). \tag{4.2.12}$$

Para combinar (4.2.12)e (4.2.11), para i em I e j em J, sejam

$$\beta_i = \alpha_i \left(1 - \frac{1}{\alpha_1}\right) \quad \text{e} \quad \beta_j = \alpha_j.$$

Assim, análogo ao que obtivemos em (4.2.5), temos que

$$\frac{1}{\alpha_1} \prod_{l=2}^{k} \frac{1}{\beta_l} \leq \left(1 - \frac{1}{\alpha_1}\right) \sum_{l=k+1}^{m} \frac{1}{\beta_l}, \quad k = 1, \ldots, m-1. \tag{4.2.13}$$

Temos também o análogo a (4.2.6), que vem da desigualdade similar a (4.2.7), ou seja,

$$\delta_m \leq \frac{\delta_m}{\alpha_1} \sum_{i \in I} \frac{\delta_m}{\alpha_i} + \left(1 - \frac{1}{\alpha_1}\right) \sum_{j \in J} \frac{\delta_m}{\alpha_j},$$

e isso nos dá

$$1 \leq \frac{1}{\alpha_1} + \left(1 - \frac{1}{\alpha_1}\right) \sum_{i=2}^{m} \frac{1}{\beta_i},$$

isto é

$$\sum_{i=2}^{m} \frac{1}{\beta_i} \geq 1. \tag{4.2.14}$$

Agora, seguindo o raciocínio de antes, numeramos as classes de forma que $\alpha_1 \leq \alpha_i$, para $i > 1$ e de forma que

$$\beta_2 \leq \beta_3 \leq \cdots \leq \beta_m.$$

Note que se 2 pertence a I, temos que $\beta_2 = \alpha_2 \left(1 - \frac{1}{\alpha_1}\right) \geq \alpha_1 \left(1 - \frac{1}{\alpha_1}\right) = \alpha_1 - 1$ e se 2 pertence a J, então temos que $\beta_2 = \alpha_2 \geq \alpha_1 > \alpha_1 - 1$. Portanto, sempre temos que $\beta_2 \geq \alpha_1 - 1$. Para $i = 2, \ldots, m$, utilizamos a notação

$$z_i = \frac{1}{\beta_i} \quad \text{e} \quad \theta = \frac{1}{\alpha_1 - 1}.$$

Assim as desigualdades (4.2.13) e (4.2.14) podem ser reescritas de forma que corresponde às relações (6.2.1) e (6.2.2) (Veja demonstração do Teorema 4.2.2 no Apêndice 6), ou seja,

$$1 \geq \theta \geq z_2 \geq z_3 \geq \cdots \geq z_m \geq 0 \tag{4.2.15}$$

$$\sum_{i=2}^{m} z_i \geq 1 \tag{4.2.16}$$

$$\sum_{i=k}^{m} z_i \geq \theta \prod_{i=2}^{k-1} z_i \tag{4.2.17}$$

para $k = 2, \ldots, m$. Repetindo um processo análogo ao feito para demonstrar o Teorema 4.2.2, agora nas condições anteriores e usando o fato que α_1 é inteiro, podemos melhorar as cotas do Corolário 4.2.3 para

$$\begin{aligned}
&\Delta_3 \leq 6,\\
&\Delta_4 \leq 36,\\
&\Delta_5 \leq 320,\\
&\Delta_m \leq 3{v_{m-1}}^2, \quad \text{para } m \geq 6,
\end{aligned}$$

onde $v_4 = 10$, $v_5 = 110$ e $v_{i+1} = {v_i}^2 + v_i$, ou $v_m = [{c_1}^{2^{m-1}}]$ com $c_1 = 1,3419$ aproximadamente. Então, temos que $\Delta_m \leq {c_1}^{2^m}$, isto é, aplicando a situação anterior no nosso problema para $m = a(G)$, temos que

$$[G : Z(G)] \leq {c_1}^{2^{a(G)}},$$

onde c_1 é uma constante.

Usando o fato que todos α_i são inteiro, é possível melhorar ainda mais as cotas para $m \geq 6$. Nesse caso, obtemos:

$$\Delta_m \leq 4{w_{m-1}}^2, \quad m \geq 6,$$

onde $w_4 = 8$, $w_5 = 72$ e $w_{i+1} = {w_i}^2 + w_i$, ou $w_m = [{c_2}^{2^{m-1}}]$ com $c_2 = 1,3070$ aproximadamente. Então, temos que $\Delta_m \leq {c_2}^{2^m}$, isto é, aplicando a situação anterior no nosso problema para $m = a(G)$, temos que

$$[G : Z(G)] \leq {c_2}^{2^{a(G)}},$$

onde c_2 é uma constante. Note que neste caso, c_2 é uma constante menor que c_1 que tínhamos obtido anteriormente.

Finalmente, considerando a nossa situação principal, onde as classes $C_i = A_i$ são subgrupos de G, podemos melhorar mais ainda nossas cotas se adicionarmos a condição de que todos os subgrupos A_i tem interseção não vazia dois a dois, isto é, o conjunto I definido anteriormente é vazio e $\beta_j = \alpha_j$ para todo j. Neste caso, temos que $\beta_2 = \alpha_2 \geq \alpha_1 = \theta/(\theta+1)$, então a condição (4.2.15) se torna

$$1 \geq \frac{\theta}{\theta+1} \geq z_2 \geq z_3 \geq \cdots \geq z_m \geq 0 \tag{4.2.18}$$

Nesse caso, com um argumento semelhante ao feito para demonstrar o Teorema 4.2.2, porém mais trabalhoso, temos o seguinte resultado:

Teorema 4.2.4. *Se $\Delta'_m = [G : \cap_{i=1}^m A_i]$ e G pode ser coberto de forma irredundante por m subgrupos $A_1, \ldots, A_m$, então*

$$\begin{aligned} \Delta'_3 &\leq 4, \\ \Delta'_4 &\leq 27, \\ \Delta'_5 &\leq 256, \\ \Delta'_m &\leq 4{y_{m-1}}^2, \quad m \geq 6. \end{aligned}$$

onde $y_1 = 1$, $y_{i+1} = {y_i}^2 + y_i$.

Notamos então que se um grupo G pode ser coberto por 3 subgrupos abelianos, então o índice $[G : Z(G)] \leq 4$ e, de fato, ele pode atingir o valor 4. Seja Q_8 o grupo dos quatérnios de ordem 8. Temos que $Q_8 = \langle i \rangle \cup \langle j \rangle \cup \langle k \rangle$ é uma cobertura irredundante de Q_8 e $Z(Q_8) = \{1, -1\}$, então $[Q_8 : Z(Q_8)] = 4$.

4.3 Relacionando $\omega(G)$ e $a(G)$

Nesta seção, dado G um grupo central-por-finito, queremos relacionar o tamanho do maior clique de $\Gamma(G)$ com o tamanho da menor cobertura irredundante de G por subgrupos abelianos. Uma das referências principais desta seção é o artigo *Some applications of graph theory to finite groups*[**3**], de E. A. Bertram. Vamos ver que, em geral, $\omega(G) \leq a(G)$, apresentar alguns casos em que $\omega(G) = a(G)$ e obteremos cotas de $a(G)$ em função de $\omega(G)$.

Primeiro, sejam $G = \bigcup_{i=1}^{a(G)} A_i$ uma cobertura irredundante de G de tamanho mínimo por subgrupos abelianos e $X \subset V(\Gamma(G))$ um clique de maior cardinalidade de $\Gamma(G)$, isto é, um clique de tamanho $\omega(G)$. Então, se tivéssemos $\omega(G) > a(G)$, pelo Princípio da Casa dos Pombos, teríamos dois elementos de X no mesmo subgrupo abeliano A_j, para algum $1 \leq j \leq a(G)$. Assim, como A_j é abeliano, teríamos que esses dois elementos do clique X comutam, um absurdo. Portanto,

$$\omega(G) \leq a(G). \tag{4.3.1}$$

A seguir, vamos apresentar alguns exemplos de grupos tais que $\omega(G) = a(G)$. Vamos ver também alguns resultados relacionados ao problema de achar condições sobre G para que $\omega(G)$ seja igual a $a(G)$.

Seja $n > 2$ um número ímpar e considere o grupo diedral D_{2n} de ordem $2n$

$$D_{2n} = \langle \rho, \tau \mid \tau^2 = \rho^n = 1, \rho^\tau = \rho^{-1} \rangle.$$

Note que para $0 \leq i, j \leq n-1$ e $i \neq j$, temos

$$[\rho, \tau\rho^i] = \rho^{n-2}$$
$$[\tau, \tau\rho^i] = \rho^{2i}$$
$$[\tau\rho^i, \tau\rho^j] = \rho^{2(i-j)}.$$

Agora se $i \neq 0$, temos que $\rho^{2i} = 1$ apenas quando $i = n/2$ e como n é ímpar, i não é inteiro neste caso. Da mesma forma, $\rho^{2(i-j)} \neq 1$, para $0 \leq i, j \leq n-1$ e $i \neq j$. Também temos que $\rho^{n-2} \neq 1$, pois $n > 2$ e n é o menor inteiro positivo tal que $\rho^n = 1$. Assim, temos que os elementos de $X = \{\rho, \tau, \tau\rho, \tau\rho^2, \ldots, \tau\rho^{n-1}\}$ não comutam dois a dois. Logo, X é um clique de $\Gamma(D_{2n})$ de tamanho $n+1$, portanto $\omega(D_{2n}) \geq n+1$.

No trabalho *On coverings of a finite group by abelian subgroups* [**16**], D. R. Mason demonstrou que se G é um grupo finito, então existe um inteiro $k \leq |G|/2 + 1$ e subgrupos abelianos $A_1, \ldots, A_k$ tais que $G = \bigcup_{i=1}^{k} A_i$. Em particular,

$$a(G) \leq |G|/2 + 1. \tag{4.3.2}$$

Então, pela desigualdade (4.3.2) no caso de D_{2n}, temos que $\omega(D_{2n}) \leq a(D_{2n}) \leq \frac{|D_{2n}|}{2} + 1$. Portanto, $\omega(D_{2n}) = a(D_{2n}) = n+1$, para $n > 2$ um número ímpar.

A próxima proposição nos dará uma condição suficiente para que um grupo central-por-finito G satisfaça $\omega(G) = a(G)$.

Proposição 4.3.1. *Seja G um grupo central-por-finito não abeliano. Se para todo x elemento não central de G tivermos que $C_G(x)$ é abeliano, então $\omega(G) = a(G)$.*

Demonstração. Sejam $X = \{g_1, \ldots, g_m\}$ um clique de maior cardinalidade de $\Gamma(G)$, isto é, $m = \omega(G)$ e x um elemento de G. Se x não comuta com g_i para todo $1 \leq i \leq m$, temos que $\{x, g_1, \ldots, g_m\}$ é um clique de tamanho $m+1$, um absurdo, pois o tamanho máximo de qualquer clique é m. Assim, existe g_i em X tal que x comuta com g_i e portanto x está em $C_G(g_i)$. Segue então que $G = \bigcup_{i=1}^{m} C_G(g_i)$. Agora, temos que g_i não é um elemento central e g_j não está em $C_G(g_i)$ para $i \neq j$. Por hipótese, todos os $C_G(g_i)$ são abelianos e portanto $G = \bigcup_{i=1}^{m} C_G(g_i)$ é uma cobertura irredundante finita, por subgrupos abelianos, de tamanho $m = \omega(G)$. Assim, $a(G) \leq \omega(G)$. Como, por (4.3.1) temos em geral que $\omega(G) \leq a(G)$, concluímos que $\omega(G) = a(G)$, como queríamos. □

Pela Proposição 4.3.1, temos imediatamente que, por exemplo, grupos não abelianos de ordem pq, com p e q primos distintos, $p < q$ e $q \equiv 1 (\mathrm{mod}\, p)$, são tais que $\omega(G) = a(G)$.

De fato, temos que qualquer subgrupo próprio de G tem ordem p,q ou 1. Assim, se x é um elemento não central de G, $C_G(x)$ é um subgrupo próprio de G. Assim, $C_G(x)$ tem ordem p,q ou 1, então $C_G(x)$ é cíclico e portanto abeliano. Logo, pela Proposição 4.3.1, concluímos que $\omega(G) = a(G)$.

Notamos que a condição de todos os centralizadores de elementos não centrais serem abelianos não é necessária para termos $\omega(G) = a(G)$. De fato, considere S_4 o grupo simétrico de grau 4. Lembramos que S_4 não é abeliano. Dado, por exemplo, o elemento $x = (12)(34)$ em S_4, temos que $C_{S_4}(x) = \langle (12), (13)(24), (34)\rangle$. Agora temos, por exemplo, que $(34)(13)(24) = (1324)$ e $(13)(24)(34) = (1423)$, então os elementos (34) e $(13)(24)$ de $C_{S_4}(x)$ não comutam, portanto $C_{S_4}(x)$ não é abeliano. Vamos mostrar que mesmo assim $\omega(S_4) = a(S_4)$. Observamos que S_4 pode ser coberto pelos seguintes dez subgrupos abelianos:

$$A_1 = \langle (1234)\rangle,\ A_2 = \langle (1324)\rangle,\ A_3 = \langle (1243)\rangle,\ A_4 = \langle (123)\rangle,\ A_5 = \langle (124)\rangle,\ A_6 = \langle (134)\rangle,$$

$$A_7 = \langle (234)\rangle,\ A_8 = \{(12), (34), (12)(34), 1\},\ A_9 = \{(13), (24), (13)(24), 1\},$$

$$A_{10} = \{(14), (23), (14)(23), 1\}.$$

Notamos que os subgrupos A_i para $1 \leq i \leq 10$ possuem interseção trivial dois a dois, então a cobertura de S_4 formada por eles é irredundante. Assim, temos que $a(S_4) \leq 10$ e como $\omega(S_4) \leq a(S_4)$ temos que $\omega(S_4) \leq 10$. Também é possível ver que o conjunto $X = \{(1234), (1324), (1243), (123), (124), (134), (234), (12), (13), (14)\}$ é um clique de $\Gamma(S_4)$ de tamanho 10. Assim, $\omega(S_4) \geq 10$. Logo $a(S_4) = \omega(S_4) = 10$.

A seguir estaremos interessados em achar cotas superiores para $a(G)$ em termos de $\omega(G)$. O próximo resultado pode ser encontrado em [**3**], porém é um resultado devido a I.M. Isaacs e comunicado a E.A. Bertram por meio de correspondência privada.

Teorema 4.3.2. *Defina a função f indutivamente da seguinte forma: $f(1) = 1$ e $f(n) = n + \binom{n}{2} f(n-1)$. Se G é um grupo tal que $\omega(G)$ é finito, então $a(G) \leq f(\omega(G))$; em particular, $a(G)$ é finito.*

Demonstração. Denotaremos $\omega(G)$ apenas por ω. Sejam x e y elementos de G que não comutam e $\{c_1, \ldots, c_\omega\}$ elementos de $C_G(x) \cap C_G(y)$. Note que se x fosse igual a $c_i y$ então y e x comutariam, um absurdo. Então, o conjunto $\{x, c_1 y, \ldots, c_\omega y\}$ tem tamanho $\omega + 1$ e portanto pelo menos dois elementos dele comutam. Como x não comuta com y e cada c_i comuta com x e y, para todo $1 \leq i \leq \omega$, temos que x não comuta com $c_i y$, para todo $1 \leq i \leq \omega$. Assim, existem $c_i y$ e $c_j y$, com $1 \leq i, j \leq \omega$ e $i \neq j$, tais que $c_i y$ e $c_j y$ comutam. Como cada c_i comuta com y, temos

$$1 = [c_i y, c_j y] = [c_i, c_j],$$

logo c_i e c_j comutam. Mostramos que dados quaisquer ω elementos de $C_G(x) \cap C_G(y)$, pelo menos dois deles comutam, ou seja, $\omega(C_G(x) \cap C_G(y)) < \omega(G)$ sempre que x e y não comutam.

Agora, seja $X = \{x_1, \dots, x_\omega\}$ um conjunto de elementos que não comutam dois a dois e para $k \neq j$ chamamos

$$B_{jk} = C_G(x_j) \cap C_G(x_k).$$

Como x_k e x_j não comutam, estamos na situação anterior e portanto $\omega(B_{jk}) < \omega(G)$. Vamos usar indução sobre ω para mostrar o resultado. Primeiro note que se $\omega(G) = 1$, temos que G é abeliano, então $\omega(G) = 1 = a(G) = f(1) = f(\omega(G))$, então o resultado é óbvio. Agora, suponha que $\omega(G) > 1$. Por indução, como $\omega(B_{jk}) < \omega(G)$ temos que o resultado vale para B_{jk}, isto é, $a(B_{jk}) \leq f(\omega(B_{jk}))$. Mas como $\omega(B_{jk}) < \omega(G)$, temos que $\omega(B_{jk}) \leq \omega(G) - 1$ pois ambos são números inteiros positivos. Assim, como por definição f é uma função monótona, temos

$$a(B_{jk}) \leq f(\omega(B_{jk})) \leq f(\omega - 1), \tag{4.3.3}$$

ou seja, B_{jk} pode ser coberto por no máximo $f(\omega - 1)$ subgrupos abelianos. Agora, seja $A_j = C_G(x_j) \setminus \bigcup_{k \neq j} B_{jk}$. Dado qualquer elemento g em G, temos que g comuta com algum x_j, para $1 \leq j \leq \omega$, pois caso contrário $X \cup \{g\}$ seria um clique de tamanho $\omega + 1$, um absurdo. Logo, $G = \bigcup_{j=1}^{\omega} C_G(x_j)$ e temos que

$$G = \bigcup_{j=1}^{\omega} \left(\langle A_j \rangle \cup \left(\cup_{k \neq j} B_{jk} \right) \right).$$

Assim, como $a(B_{jk}) \leq f(\omega - 1)$, se provarmos que cada $\langle A_j \rangle$ é abeliano, teremos que a menor cobertura minimal por subgrupos abelianos de G tem no máximo $\omega + \binom{\omega}{2} f(\omega - 1) = f(\omega)$ subgrupos abelianos, como queríamos.

Vamos provar agora que cada $\langle A_j \rangle$ é abeliano. Sejam u e v elementos quaisquer do conjunto A_j. Se u comutasse com x_i para algum $i \neq j$ e $1 \leq i \leq \omega$, teríamos que u está em $B_{ji} = C_G(x_i) \cap C_G(x_j)$, um absurdo pois $A_j = C_G(x_j) \setminus \bigcup_{k \neq j} B_{jk}$. Assim, $L = \{x_1, \dots, x_{j-1}, u, x_{j+1}, \dots, x_\omega\}$ é um clique de tamanho ω. Então, v comuta com algum elemento de L. Pelo mesmo argumento que fizemos para u, temos que v não pode comutar com nenhum x_i para $i \neq j$, então v comuta com u e portanto $\langle A_j \rangle$ é abeliano para todo $1 \leq j \leq \omega$, como queríamos. □

Notamos que, em geral, por definição da função f temos que $f(n) \leq (n!)^2$. Vamos mostrar por indução sobre n. Se $n = 1$, temos que $f(1) = 1 = 1!^2$. Vamos mostrar que o resultado vale para $n > 1$. Temos que $f(n) = n + \binom{n}{2} f(n-1) \leq n + \binom{n}{2}(n-1)!^2$. Mas como $\binom{n}{2} = n(n-1)/2$, temos que

$$\begin{aligned} f(n) \leq n + \frac{n!(n-1)(n-1)!}{2} &= n + \frac{n![n! - (n-1)!]}{2} = n + \frac{n!^2 - n!(n-1)!}{2} \\ &= \frac{n!^2(-n!(n-1)! + 2n)}{2}. \end{aligned}$$

Mas como para $n > 1$ temos que $n!(n-1)! \geq 2n$, temos que

$$f(n) \leq \frac{n!^2(-n!(n-1)! + 2n)}{2} \leq \frac{n!^2}{2} < n!^2.$$

Então, pelo Teorema 4.3.2 e pela observação anterior, temos que em geral

$$a(G) \leq f(\omega(G)) < (\omega(G)!)^2. \tag{4.3.4}$$

Resumindo as informações encontradas nas seções anteriores, temos que

$$\omega(G) \leq a(G) \leq [G : Z(G)] \leq c^{\omega(G)},$$

para c uma constante. Notemos que usando o resultado obtido por Pyber para o índice $[G : Z(G)]$ é possível melhorar a cota de $a(G)$ obtida no Teorema 4.3.2. A igualdade entre as três quantidades vale somente quando $\omega(G) = [G : Z(G)]$, o que já vimos ser pouco interessante pois só é possível quando $[G : Z(G)] = 1$.

4.4 Relacionando ω e $|G|$ em um grupo finito

Nesta seção vamos considerar G um grupo finito. A relação que existe entre a cardinalidade de G e o índice $[G : Z(G)]$ é clara pelo Teorema de Lagrange. Por outro lado, pelo resultado de D. R. Mason [**16**], sabemos que $a(G) \leq |G|/2 + 1$. Agora queremos relacionar o tamanho do maior clique de $\Gamma(G)$, isto é, ω, com a ordem do grupo G. Claramente usando o resultado de D. R. Mason e a relação entre $a(G)$ e $\omega(G)$ temos que $\omega(G) \leq |G|/2 + 1$. A próxima proposição dá algumas informações mais detalhadas sobre uma cota inferior para $\omega(G)$ em função da cardinalidade do grupo, impondo certas condições sobre o grupo G.

Proposição 4.4.1. *Seja G um grupo finito não abeliano e p qualquer número primo que divide a ordem de G. Se existe um elemento x em G tal que $|C_G(x)| = p$, então temos que $\omega(G) \geq [| G |^{1/3}]$, onde $[y]$ é o maior inteiro menor ou igual a y.*

Demonstração. Seja x o elemento de G tal que $|C_G(x)| = p$ e $P = \langle x \rangle$ o subgrupo cíclico de ordem p gerado por x. Notamos que $C_G(P) = P$. Seja S um p-subgrupo de Sylow de G com P contido em S. Então, como $Z(S)$ é não trivial e está contido em P, temos que $Z(S) = P$ e portanto, como $C_G(P) = P$, temos que $S = P$. Portanto P é um p-Sylow de G, ou seja, p^2 não divide a ordem de G. Também temos pelo "Teorema N/C" [**23**, 1.6.13] que $N_G(P)/C_G(P)$ é isomorfo a um subgrupo de $Aut(P)$, que por sua vez é isomorfo a C_{p-1}, pois p é primo. Portanto temos que $|G| = pme$, onde $m = [G : N_G(P)]$ e $e = [N_G(P) : P]$, com e um divisor de $p - 1$. Temos também que m é o número de conjugados P^x de P. Agora, dados $\{x_1, \ldots, x_m\}$ quaisquer m elementos distintos e não triviais, um em cada conjugado de P, temos que eles não comutam dois a dois. De fato, como $C_G(P^x) = C_G(P)^x = P^x$, dois elementos só comutam se estiverem no mesmo conjugado de P. Assim, $\{x_1, \ldots, x_m\}$ é um clique de $\Gamma(G)$, ou seja,

$$\omega(G) \geq m.$$

Suponha por absurdo que $\omega(G)^3 < |G|$. Então $m^3 \leq \omega(G)^3 < |G|$, ou seja $m^3 < |G|$. Como $|G| = pme$, temos que $m^2 < pe$. Mas como e é um divisor de $p-1$, em particular $e < p$ e assim $m^2 < p^2$. Como p e m são inteiros positivos, temos que $m < p$. Temos também por Teoria de Sylow que $m = [G : N_G(P)] \equiv 1(\mathrm{mod} p)$ e como $m < p$, temos que $m = 1$ e portanto P é um subgrupo normal em G. Mas $p < pme = pe < p^2$, logo $p < |G| < p^2$ e como o grupo G/P tem a mesma cardinalidade do seu subgrupo $N_G(P)/P$, temos que $G/P = N_G(P)/P$. Como $N_G(P)/P$ é isomorfo a um subgrupo de C_{p-1}, em particular G/P é cíclico.

Agora seja $q < p$ um primo que divide e e Q um subgrupo de G de ordem q (existe pela Proposição 1.0.4). Vamos mostrar que x não normaliza Q. Suponha por absurdo que $Q^x = Q$. Assim, para todo y em Q, os elementos $(x^{-1}y^{-1}x)y = x^{-1}(y^{-1}xy)$ estão em $Q \cap P$, pois P é normal. Mas como P e Q são cíclicos de ordem prima, com primos distintos, logo $Q \cap P = 1$. Então y está em $C_G(x) = C_G(P) = P$. Escolhendo y não trivial em Q, temos um absurdo pois $Q \cap P = 1$. Isso mostra que p não divide $|N_G(Q)|$, pois caso contrário, como o único subgrupo de ordem p é P, teríamos que $P \subseteq N_G(Q)$, e x normalizaria Q, o que já vimos ser um absurdo. Como p divide a ordem de G e p não divide $|N_G(Q)|$, temos que p divide $[G : N_G(Q)]$, isto é, Q tem pelo menos p conjugados em G, digamos $Q_1, \ldots, Q_p$, com $Q_i = \langle x_i \rangle$. Se x_i e x_j são distintos e comutam, então $H = \langle x_i, x_j \rangle$ é abeliano. Mas como x_j não pertence a $\langle x_i \rangle$, pois os conjugados se interceptam trivialmente, temos que H é o produto direto de $\langle x_i \rangle$ e $\langle x_j \rangle$, portanto H tem ordem q^2 e não é cíclico. Pela ordem temos que $H \cap P = 1$, então H é isomorfo a HP/P, que é subgrupo de G/P. Sendo G/P cíclico, H também seria cíclico, uma contradição. Se os x_i não comutam dois a dois, para $1 \leq i \leq p$, temos que $\omega(G) \geq p > m$. Logo, $\omega(G)^3 > m^3 > |G|$, um absurdo. Portanto, $\omega(G)^3 < |G|$ não pode acontecer e o resultado segue.

□

Notamos que a demonstração anterior é devida a I. M. Isaacs. A Proposição 4.4.1 também pode ser obtida como corolário do seguinte teorema mais geral:

Teorema 4.4.2. *Seja G um grupo finito que contém um subgrupo próprio M tal que para todo x em $M - \{1\}$, temos que $C_G(x) \subseteq M$. Então $\omega(G) \geq [|G|^{1/3}]$, onde $[r]$ é o maior inteiro menor ou igual a r.*

Os detalhes da demonstração do Teorema 4.4.2 podem ser encontrados em [**3**]. Aqui só queríamos destacar que uma das ferramentas na demonstração é o seguinte resultado de Teoria de Grafos devido a V. K. Wei [**15**]:

Teorema 4.4.3. *Sejam Γ um grafo finito e simples, e $d(v)$ o grau de um vértice v em Γ. Então,*

$$\omega(\Gamma) \geq \sum_{v \in V(\Gamma)} \frac{1}{(d(v)+1)},$$

e a igualdade é válida se, e somente se Γ é a união de subgrafos induzidos por cliques disjuntos de cardinalidade maximal.

Como exemplo do resultado na Proposição 4.4.1, considere G um grupo não abeliano de ordem pq, com $p < q$ com p e q primos. Temos que G tem um elemento de ordem p, isto é, existe x tal que $N = \langle x \rangle$ tem ordem p. Então, como N está contido em $C_G(x)$, temos que $C_G(x)$ tem ordem p ou pq. Se $C_G(x)$ tem ordem pq, então temos que x está no centro de G e portanto N é um subgrupo normal de G, um absurdo, pois como $p < q$, temos que existe um subgrupo M de ordem q que é normal, pelo Teorema de Sylow. Então, se N também for normal, como $G = MN$ e $N \cap M$ é trivial, temos que G é o produto direto de dois subgrupos abelianos, portanto G também seria abeliano. Assim, temos que a ordem de $C_G(x)$ é necessariamente p e pela Proposição 4.4.1, temos que $\omega(G) \geq [(pq)^{1/3}]$.

Considere o grupo de ordem $3 \cdot 7 = 21$ dado por $G = C_7 \rtimes C_3 = \langle f_2, f_1 \rangle$. Já vimos, como consequência da Proposição 4.3.1, que $a(G) = \omega(G)$. O grafo não comutativo de G está representado na Figura 4.4.1 abaixo.

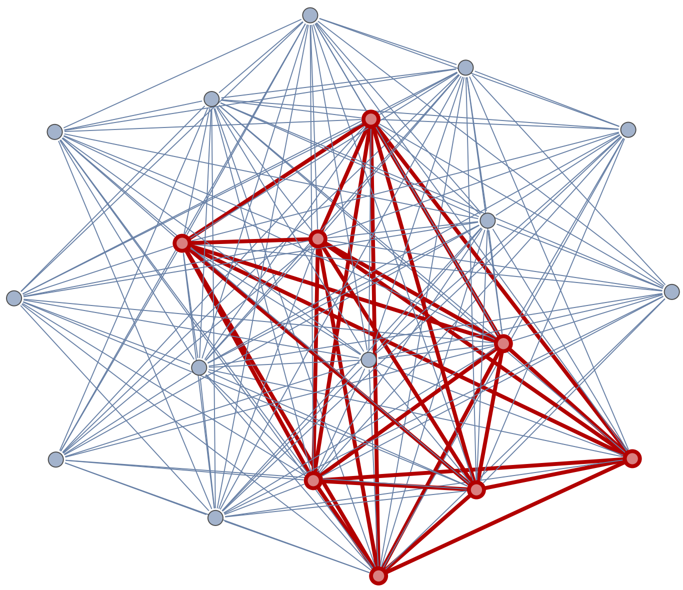

FIGURA 4.4.1. Grafo não-comutativo de $G = C_7 \rtimes C_3$

O subgrafo ressaltado em vermelho é o subgrafo induzido pelo clique de tamanho maximal

$$X = \{f_1, f_2, f_1 f_2, f_1^2 f_2, f_1 f_2^2, f_1 f_2^4, f_1^2 f_2^4, f_1^2 f_2^2\},$$

encontrado através do comando `FindClique[g]` no programa Mathematica, isto é, $\omega(G) = 8$. Denotando por $X = \{x_1, \ldots, x_8\}$ os elementos do clique, temos pela demonstração da Proposição 4.3.1, que $G = \bigcup_{i=1}^{8} C_G(x_i)$ e essa é uma cobertura irredundante por subgrupos abelianos. Pela Proposição 4.4.1 e pelo resultado de Mason (4.3.2), como $[(3 \cdot 7)^{1/3}] = 2$, temos que $2 \leq \omega(G) = a(G) \leq 11$. De fato, analisando o grafo não-comutativo de G, temos que $\omega(G) = a(G) = 8$.

Capítulo 5

Grupos extraespeciais

Neste capítulo vamos definir a classe dos p-grupos extraespeciais de ordem p^{2a+1}, caracterizar esse grupos como produto central de subgrupos de ordem p^3, analisar as relações entre $\omega(G)$, $a(G)$ e $[G : Z(G)]$ para essa família de grupos. Para as definições e resultados básicos sobre grupos extraespeciais teremos como referência o livro *Group Theory*, [**25**, Vol. I e II], de M. Suzuki.

5.1 Produto Central

Definição 5.1.1. Sejam G um grupo e H e K dois subgrupos de G. Dizemos que G é o *produto central* (interno) de H e K, denotado por $H * K$ (e às vezes também por $H \circ K$), se $[H, K] = 1$ e $G = HK$.

Vamos agora observar algumas consequências da definição de produto central.

Teorema 5.1.2. *Sejam G um grupo e H e K dois subgrupos de G. Se $G = H * K$ e $D = H \cap K$, então temos que:*

(i) H e K são subgrupos normais em G;

(ii) D está contido em $Z(H)$ e em $Z(K)$;

(iii) Existe um homomorfismo sobrejetor do produto direto $H \times K$ em G. Seja H_1 um grupo isomorfo a H via $t : H \to H_1$ e K_1 um grupo isomorfo a K via $k : K \to K_1$. Seja $G_1 = H_1 \times K_1$, então a função $f : D \to G_1$ definida como $f(x) = (t(x), k(x)^{-1})$ define um isomorfismo entre D e algum subgrupo de $Z(G_1)$. Se Z denota a imagem desse isomorfismo, então G_1/Z é isomorfo a G.

Demonstração.

(i) Como $[H, K] = 1$, temos que K está em $C_G(H)$, que por sua vez é sempre subgrupo de $N_G(H)$. Então, como H também é sempre subgrupo de $N_G(H)$, temos que K, H estão em $N_G(H)$. Como $G = HK$, e em particular K está em $N_G(K)$ temos que K é um subgrupo normal de G. Analogamente, temos que H é normal em G, como queríamos.

(ii) Como observamos em (i), temos que K está em $C_G(H)$, logo $D = H \cap K$ está contido em $H \cap C_G(H) = Z(H)$. De forma análoga, temos que D está contido em $Z(K)$.

(iii) Pelas propriedades de produto direto temos que $Z(G_1) = Z(H_1)\times Z(K_1)$. Vamos mostrar que f define um homomorfismo injetor entre. De fato, se x pertence a $\mathrm{Ker} f$, então $t(x) = 1$, mas como k é um isomorfismo, temos que $x = 1$, então f é uma função injetora. Agora vamos mostrar que $\mathrm{Im} f$ está contido em $Z(G_1)$. Sejam x em D e $(t(x), k(x)^{-1})$ em $\mathrm{Im} f$. Temos que $t(x)$ está em $Z(H_1)$, pois dado y elemento de H_1, temos que existe h em H tal que $y = t(h)$. Como D está em $Z(H)$, temos que x está em $Z(H)$. Logo

$$yt(x) = t(hx) = t(xh) = t(x)y,$$

e portanto $t(x)$ está em $Z(H_1)$. Analogamente, $k(x)^{-1} = k(x^{-1})$ está em $Z(K_1)$. Como $Z(G_1) = Z(H_1) \times Z(K_1)$, temos que $(t(x), k(x)^{-1})$ está em $Z(G_1)$.

Agora definimos $g : G_1 \to G$ da seguinte forma: dado (h_1, k_1) em G_1, existem únicos h e k tais que $(h_1, k_1) = (t(h), k(k))$. Então, $g((h_1, k_1)) = hk$ e g está bem definida. Também temos que g é um homomorfismo, pois $(hh')(kk') = (hk)(h'k')$, para h, h' em H e k, k' em K, pois $[H, K] = 1$. Note que g é sobrejetora, pois dados g um elemento em G, temos que $g = hk$. Assim, $g((t(h), k(k)) = g$.

Falta mostrar que $\mathrm{Ker} g = Z = \mathrm{Im} f$. De fato, seja $(t(h), k(k))$ um elemento de $\mathrm{Ker} g$, temos que $h = k^{-1}$, isto é, h está em D. Assim, $f(h) = (t(h), k(h^{-1})) = (t(h), k(k))$, então $\mathrm{Ker} g$ está contido em Z. Por outro lado, seja x em D e $(t(x), k(x^{-1}))$ um elemento de Z. Então, $f((t(x), k(x^{-1}))) = 1$, então $\mathrm{Ker} g = Z$. Portanto, pelo Teorema de Isomorfismo, temos que G_1/Z é isomorfo a G, como queríamos.

□

Podemos também construir o produto central *"externo"* de dois grupos quaisquer. Sejam H e K dois grupos, e suponha que D_1, um subgrupo de $Z(H)$, é isomorfo a D_2, um subgrupo de $Z(K)$. O resultado a seguir descreve o produto central de H com K.

Teorema 5.1.3. *Sejam H_1 e K_1 dois grupos, e D_1 um subgrupo de $Z(H_1)$. Suponha adicionalmente que um isomorfismo φ entre D_1 e um subgrupo de $Z(K_1)$ é dado. O subconjunto Z do produto direto $H_1 \times K_1$ consistindo dos elementos da forma $(x, \varphi(x^{-1}))$, onde x está em D_1, é um subgrupo de $Z(H_1 \times K_1)$. O grupo $(H_1 \times K_1)/Z$ é o produto central de $H = H_1Z/Z$ e $K = K_1Z/Z$. Temos que H é isomorfo a H_1 e K é isomorfo a K_1, e o subgrupo D_1Z/Z de H é identificado com o subgrupo $\varphi(D_1)Z/Z$ de K via o isomorfismo $\overline{\varphi}$ induzido por φ.*

Notamos que em geral a estrutura do produto central não depende apenas da estrutura dos fatores H e K, mas também do isomorfismo φ (Veja [**25**, Vol. I, Chapter 4, Central Products, Exercise 5]). O produto central de mais de grupos pode ser definido de maneira similar. Suponha que $H_1, \ldots, H_n$ são subgrupos de um grupo G tais que H_i e H_j comutam elemento a elemento para $i \neq j$ e $G = H_1 \cdots H_n$. Nesse caso, dizemos que G é o produto central "interno" de $H_1, \ldots, H_n$. Em particular, o seguinte resultado vale.

TEOREMA 5.1.4. *Seja G o produto central de $H_1, \ldots, H_n$. Então, a função definida por*

$$(h_1, \ldots, h_n) \mapsto h_1 \cdots h_n$$

é um homomorfismo sobrejetor do produto direto $H_1 \times \cdots \times H_n$ em G. O kernel desse homomorfismo é um subgrupo do centro do produto direto.

5.2 p-grupos Extraespeciais

DEFINIÇÃO 5.2.1. Seja $\phi(G)$ o subgrupo de Frattini de G. Um p-grupo finito G é dito p-grupo extraespecial se

$$\phi(G) = Z(G) = G' \quad \text{e} \quad |Z(G)| = p.$$

Por exemplo, temos que os grupos Q_8, grupos dos quatérnios de ordem 8 e D_8, grupo diedral de ordem 8 são 2-grupos extraespeciais. Primeiro, sabemos que $Z(Q_8) = \{1, -1\}$, $Q_8' = \langle [i, j] \rangle = \{1, -1\}$ e como os subgrupos maximais de Q_8 são $\{1, -1, i, -i\}, \{1, -1, j, -j\}$ e $\{1, -1, k, -k\}$, temos que $\phi(Q_8) = \{1, -1\}$. Também temos que $|Z(Q_8)| = 2$, então Q_8 é um 2-grupo extrespecial. Para D_8, temos que $Z(D_8) = \{1, \rho^2\}$, $D_8' = \langle [\rho, \tau] \rangle = \{1, \rho^2\}$ e por último, $\langle \rho \rangle$, $\langle \rho^2, \tau \rangle$ e $\langle \rho^3\tau, \rho\tau \rangle$ são os subgrupos maximais de D_8 e a interseção deles é $\{1, \rho^2\}$. Também temos que $|Z(D_8)| = 2$, então D_8 também é um 2-grupo extraespecial.

Definimos agora os p-grupos $M(p^3)$ e $E(p^3)$ de ordem p^3, para $p \geq 3$, da seguinte forma:

$$M(p^3) = \langle x, y \mid x^{p^2} = y^p = 1, x^y = x^{1+p} \rangle,$$
$$E(p^3) = \langle x, y \mid x^p = y^p = [x, y]^p = 1, [x, y] \in Z(E(p^3)) \rangle$$

Notamos que o grupo $E(p^3)$ tem expoente p e o grupo $M(p^3)$ tem expoente p^2. O próximo teorema caracteriza os grupos não-abelianos de ordem p^3.

TEOREMA 5.2.2. *Um p-grupo G não-abeliano de ordem p^3 é isomorfo a um dos seguintes grupos:*

(i) Se $p = 2$, então G é isomorfo a D_8 ou Q_8.
(ii) Se $p > 2$, então G é isomorfo a $M(p^3)$ ou $E(p^3)$.

Os detalhes do resultado anterior podem ser encontrados em [**25**, Theorem 4.13]. O teorema a seguir pode ser encontrado em [**25**, Theorem 4.18, Vol.II] e caracteriza p-grupos extraespeciais como produto central de cópias dos grupos $M(p^3)$ e $E(p^3)$, ou de D_8 e Q_8 da seguinte maneira:

TEOREMA 5.2.3. *Um p-grupo extraespecial é o produto central de grupos de ordem p^3. Mais precisamente, temos que se G é um p-grupo extraespecial, então $|G| = p^{2a+1}$ para algum inteiro positivo a e um dos seguintes casos acontece:*

(i) Se $exp(G) = p$, então $p > 2$ e G é o produto central de a cópias de grupos isomorfos a $E(p^3)$;

(ii) *Se $exp(G) = p^2$ e $p > 2$ então G é o produto central de $M(p^3)$ e $(a-1)$ cópias de grupos isomorfos a $E(p^3)$;*

(iii) *Se $p = 2$, ou G é produto central de a cópias de D_8 ou G é produto central de Q_8 e $(a-1)$ cópias de D_8.*

Em cada caso, a estrutura do produto central é unicamente determinada pela estrutura dos fatores.

Agora vamos mostrar um resultado básico para p-grupos extraespeciais de ordem p^{2a+1}.

Lema 5.2.4. *Seja G um grupo extraespecial de ordem p^{2a+1}. Então para x em $G \setminus Z(G)$, temos que $Cl(x)$ tem tamanho p e $C_G(x)$ é um subgrupo maximal de G.*

Demonstração. Temos que dado x^y um elemento de $Cl(x)$, podemos escrever

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

portanto $Cl(x)$ está contido no conjunto $G'x$. Assim, como $|G'x| = p$ e a cardinalidade de $Cl(x)$ divide a ordem de G, temos que $Cl(x)$ tem cardinalidade 1 ou p. Mas como x está em $G \setminus Z(G)$, temos que $|Cl(x)| > 1$ e portanto $|Cl(x)| = p$. Pela equação das classes (Teorema 1.0.7), temos que $[G : C_G(x)] = |Cl(x)| = p$. Então $C_G(x) = p^{2a}$, então $C_G(x)$ é um subgrupo maximal de G.

□

Uma consequência da demonstração do Lema 5.2.4 é que se G é um p-grupo extraespecial de ordem p^{2a+1}, então $\Gamma(G)$ é um grafo regular. De fato, temos que $d_{\Gamma(G)}(x) = |G \setminus C_G(x)| = p^{2a+1} - p^{2a} = p^{2a}(p-1)$, isto é, $d_{\Gamma(G)}(x)$ é o mesmo para todo x em $V(\Gamma(G))$.

A seguir vamos analisar os indicadores $\omega(G)$ e $a(G)$ para p-grupos extraespeciais. Como vimos na Proposição 4.3.1 uma condição suficiente para que $\omega(G) = a(G)$ é que todos os centralizadores dos elementos não centrais sejam abelianos. De fato p-grupos extraespeciais de ordem p^3 satisfazem essa condição, como mostrado na seguinte proposição.

Proposição 5.2.5. *Se G é um p-grupo extraespecial de ordem p^3, então $\omega(G) = a(G)$.*

Demonstração. Vamos mostrar que todos os elementos não centrais de G têm centralizadores abelianos. De fato, seja x um elemento de $G \setminus Z(G)$. Pelo Lema 5.2.4, temos que $Cl(x)$ tem tamanho p e portanto $C_G(x)$ tem cardinalidade p^2, já que $a = 1$. Como p é primo e todo grupo de ordem p^2 é abeliano, temos que $C_G(x)$ é abeliano. Portanto, aplicando a Proposição 4.3.1 temos que $\omega(G) = a(G)$, como queríamos. □

Para um p-grupo extraespecial de ordem p^{2a+1}, com $a > 1$ não é possível usar a Proposição 4.3.1 da forma que fizemos para grupos de ordem p^3, pois nenhum centralizador de elementos não centrais é abeliano. De fato, por [**2**, Theorem 4.7, Proof(d)], nenhum subgrupo abeliano tem índice menor que p^a em um p-grupo extraespecial, então pelo Lema

5.2.4 como o índice de $C_G(x)$ é p, para x um elemento não central, e como $a > 1$, temos que $C_G(x)$ não é abeliano.

Notamos que a Proposição 5.2.5 acima, em particular, vale para D_8 e Q_8, quando consideramos para $p = 2$. Para esses dois grupos existe uma maneira direta de verificar que $\omega(G) = a(G)$ sem utilizar a Proposição 5.2.5. Já mencionamos algumas vezes que $\omega(D_8) = 3$. Temos que o grafos não comutativos de D_8 e de Q_8 são isomorfos e portanto $\omega(Q_8) = 3$. Vamos explicitar uma cobertura irredundante para D_8 e Q_8 de tamanho 3. Sejam $A_1 = \langle\rho\rangle$, $A_2 = \langle\rho^2, \tau\rangle$, $A_3 = \langle\rho\tau\rho^3\tau\rangle$. Então, $D_8 = A_1 \cup A_2 \cup A_3$ e essa cobertura é irredundante, logo $a(G) \leq 3$. Mas como $\omega(G) \leq a(G)$, temos que $a(G) \geq 3$ e portanto $a(G) = 3 = \omega(G)$. Para Q_8, consideramos os subgrupos $B_1 = \langle i\rangle$, $B_2 = \langle j\rangle$, $B_3 = \langle k\rangle$. Assim, $Q_8 = B_1 \cup B_2 \cup B_3$ e pelo mesmo argumento que fizemos para D_8, temos $a(G) = 3 = \omega(G)$.

Considerando 2-grupos extraespeciais de ordem 2^{2a+1} em geral, um resultado devido a I. M. Issacs garante que $a(G) \geq 2^a + 1$, $\omega(G) = 2a + 1$ e $[G : Z(G)] = 2^{2a}$. Primeiro vamos demonstrar um lema que será útil na prova do resultado mencionado antes.

Lema 5.2.6. *Sejam G um p-grupo extraespecial e x e y elementos de G, tais que* $[x, y] \neq 1$. *O subgrupo $\langle x, y\rangle$ gerado por x e y é um p-grupo extraespecial de ordem p^3.*

Demonstração. Seja $E = \langle x, y\rangle$. Como $[x, y]$ é não trivial e pertence a $G' \cap E$, temos que $G' \cap E = G'$, pois G' tem ordem p. Assim, G' está contido em E. Temos, pelo Teorema da Base de Burnside [**23**, 5.2.5], que $G/\Phi(G)$ é um espaço vetorial sobre um corpo de ordem p. Como $\Phi(G) = G' = Z(G)$, temos que a imagem de E no espaço vetorial $G/\Phi(G)$ é um grupo abeliano. Assim, temos que $x\Phi(G)$ e $y\Phi(G)$ geram um subspaço de dimensão 2, logo E tem ordem p^3. Como já vimos, $E/Z(G)$ é abeliano elementar do tipo (p, p) e $Z(G)$ é um subgrupo de ordem p. Então, como E não é um grupo abeliano, temos por [**25**, 4.16(c), Vol. II] que E é extraespecial de ordem p^3. □

Teorema 5.2.7. *Seja G um* 2*-grupo extraespecial de ordem* 2^{2a+1}. *Então*

(i) $[G : Z(G)] = 2^{2a}$*;*

(ii) $\omega(G) = 2a + 1$*;*

(iii) $a(G) \geq 2^a + 1$.

Demonstração. (i) É claro pois $Z(G)$ tem ordem 2.

(ii) Para a prova deste item seguimos as observações de E. Yalçin em [**27**]. Suponha que G seja o produto central de $H_1, \ldots, H_a$ grupos onde H_i é isomorfo a Q_8 e D_8. Suponha que H_i são gerados por a_i e b_i para cada $1 \leq i \leq a$. Sabemos que existe uma cópia isomorfa a H_i no produto central de $H_1, \ldots, H_a$, então vamos usar a mesma notação a_i e b_i para a imagem isomorfa desses elementos no produto central.

Seja $X_1 = \{a_1, b_1\, a_1 b_1\}$, definimos indutivamente $X_n = \{a_n, b_n\} \cup a_n b_n X_{n-1}$ para $n \geq 2$ um conjunto de cardinalidade $2n + 1$. Notamos primeiro que $\langle a_i, b_i\rangle$ e $\langle a_j, b_j\rangle$ comutam elemento a elemento para $i \neq j$ por definição de produto central. Temos que X_1 é um conjunto de elementos que não comutam dois a dois, pois são os geradores de uma cópia de D_8 ou Q_8. Vamos mostrar que X_n é um clique de $\Gamma(G)$ por indução. Temos que X_1 é um clique de $\Gamma(G)$ se $|G| = 2^3$. Suponha que X_{n-1} também seja um clique para $n > 1$. Como $X_n = \{a_n, b_n\} \cup a_nb_nX_{n-1}$, vamos ver que seus elementos não comutam dois a dois. De fato, nenhum dos elementos de X_{n-1} comutam dois a dois e todos os elementos de X_{n-1} comutam com a_n e b_n, portanto, para x e y elementos distintos de X_{n-1} temos que

$$[a_nb_nx, a_nb_ny] = [x, y] \neq 1$$
$$[a_n, a_nb_ny] = [a_n, b_n] \neq 1$$
$$[b_n, a_nb_ny] = [b_n, a_n] \neq 1,$$

isto é, X_n é um clique de $\Gamma(G)$. Assim, X_a é um clique de $\Gamma(G)$ de cardinalidade $2a + 1$.

Agora vamos mostrar por indução que não há clique com cardinalidade maior que $2a + 1$. Para $a = 1$, temos que G tem ordem 2^3, assim G é isomorfo a D_8 ou Q_8, e portanto um clique tem tamanho no máximo 3. Agora se $a > 1$, $X = \{x, y, \ldots\}$ um clique de $\Gamma(G)$. Temos pelo Lema 5.2.6, que $\langle x, y\rangle$ é um 2-grupo extraespecial de ordem 2^3. Pelo resultado [**25**, 4.17, Vol.II], temos que $G = \langle x, y\rangle * C_G(\langle x, y\rangle)$ e pela demonstração do Teorema 5.2.3 em [**25**, 4.16], temos também que $C_G(\langle x, y\rangle)$ é um 2-grupo extraespecial. Então, concluímos que $C_G(\langle x, y\rangle)$ tem ordem 2^{2a-1} e portanto $[G : C_G(\langle x, y\rangle)] = 4$. Como os elementos de $X \setminus \{x, y\}$ não comutam com x e y, temos que eles pertencem a classe lateral $xyC_G(\langle x, y\rangle)$. Agora seja z_1 e z_2 elementos de $X \setminus \{x, y\}$, então $z_1 = xyw_1$ e $z_2 = xyw_2$ com w_1 e w_2 em $C_G(\langle x, y\rangle)$. Como z_1 e z_2 não comutam entre si , temos que w_1 e w_2 também não comutam. Assim, do conjunto $X \setminus \{x, y\}$ obtemos um clique de $C_G(\langle x, y\rangle)$ de tamanho $|X| - 2$. Por hipótese de indução, temos que $|X| - 2 \leq 2a - 1$, então temos que $|X| \leq 2a + 1$, como queríamos.

(iii) Suponha que $G = \bigcup_{i=1}^{s} A_i$ é uma cobertura irredundante de tamanho minimal por subgrupos abelianos, isto é, $s = a(G)$. Se $Z(G)$ não está contido em algum A_i, podemos substituí-lo pelo subgrupo abeliano $\langle A_i, t\rangle$, onde $Z(G) = \langle t\rangle$. Desta forma, definimos $B_i = A_i$, se $Z(G)$ está em A_i, e $B_i = \langle A_i, t\rangle$, se $Z(G)$ não está em A_i. Temos que $G = \bigcup_{i=1}^{s} B_i$ é uma cobertura irredundante por subgrupos abelianos de tamanho $s = a(G)$, pela minimalidade de $a(G)$. Portanto temos que $Z(G)$ está contido em B_i para todo i. Por [**2**, Theorem 4.7, Proof(d)], nenhum subgrupo abeliano tem índice menor que 2^a, temos que os B_i tem ordem no máximo 2^{a+1}. Como $Z(G)$ tem ordem 2, temos que cada A_i é a união de no máximo $2^a - 1$ classes não triviais de $Z(G)$. Assim, como $G = \bigcup_{i=1}^{s} B_i$ temos que G pode ser coberto por no máximo $s(2^a - 1)$ classes não triviais de $Z(G)$. Por outro lado, como $[G : Z(G)] = 2^{2a}$, temos que o número de classes não triviais de $Z(G)$ em G é $2^{2a} - 1$, isto é, $s(2^a - 1) \geq 2^{2a} - 1$, ou seja, $s \geq 2^a + 1$, como queríamos. Como $s = a(G)$, temos o nosso resultado.

$\square$

Como consequência do Teorema 5.2.7, se G é um 2-grupo extraespecial de ordem 2^{2a+1} e $a > 2$, então $\omega(G)$ é estritamente menor que $a(G)$, pois para $a > 2$ temos que $2a + 1 < 2^a + 1$. Para $a = 1$, vimos que $\omega(G) = a(G)$. Os únicos 2-grupos extraespeciais que faltam ser analisados são os com $a = 2$, isto é, de ordem 2^5. De fato, para ambas as classes de isomorfismo descritas no Teorema 5.2.3, temos pelo Teorema 5.2.7 que $\omega(G) = 5$. Agora, utilizando o programa GAP achamos uma cobertura de abelianos de G de tamanho 5, isto é, $\omega(G) = 5 = a(G)$. Para isso, de todos os subgrupos de G, filtramos os subgrupos abelianos de ordem maximal, isto é, de ordem $2^{2+1} = 8$. Assim, através da lista obtida, analisamos as interseções desses subgrupos e escolhemos os de menor interseção. Após alguns testes obtivemos uma cobertura de tamanho 5 de subgrupos de tamanho 8.

Em geral, para p-grupos extraespeciais não é imediato encontrar o valor de $\omega(G)$. No artigo *On non-commuting sets in an extraspecial p-group*, [**6**], A. Y. M. Chin encontrou valores exatos de $\omega(G)$ para p-grupos extraespeciais de ordem p^3 com $p \neq 2$, e encontrou cotas inferiores e superiores para $\omega(G)$ quando G é um p-grupo extraespecial de ordem p^{2a+1} com $p \neq 2$ e $a > 1$. Quando não temos o valor de $a(G)$, a melhor cota que conseguimos até agora para $\omega(G)$ é $\omega(G) \leq [G : Z(G)]$. O resultado a seguir, apesar de não depender de $[G : Z(G)]$ é melhor do que nossa cota anterior, como vamos observar.

Teorema 5.2.8. *Seja G um p-grupo extraespecial de ordem p^{2a+1}, com p um primo ímpar. Então, $\omega(G) = p + 1$, para $a = 1$ e para $a \geq 2$ temos que*

$$ap + 1 \leq \omega(G) \leq \frac{p(p-1)^a - 2}{p - 2}.$$

A primeira consequência desse teorema é que se G é um p-grupo extraespecial de ordem p^3 com $p > 2$ temos que $\omega(G) = p + 1$. Utilizando os programas **GAP 4.7.5** [**7**] para calcular as arestas e **Wolfram Mathematica 10.0** [**17**] para plotar e achar um clique maximal em $\Gamma(G)$, podemos exibir o grafo não comutativo de um 3-grupo extraespecial de ordem 3^3 e expoente 3 gerado por f_1, f_1 e f_3. O programa **Wolfram Mathematica 10.0** [**17**], através do comando `"FindClique[g]"`, acha o clique maximal $X = \{f_1, f_1, f_1 f_2, {f_1}^2 f_2\}$. Na Figura 5.2.1 temos o clique de tamanho 4 destacado em vermelho.

Agora seja H um 3-grupo extraespecial de ordem 3^5, isto é, com $a = 2$. Para esse grupo, o Teorema 5.2.8 nos diz que

$$7 \leq \omega(G) \leq 10.$$

Não temos a informação de $a(G)$, então a cota uma forma de estimar $\omega(G)$ que já conhecemos é $\omega(H) \leq [H : Z(H)] = 3^4$, ou seja, o Teorema 5.2.8 melhora bastante essa cota inicial. Esse grafo pode ser calculado e plotado, porém a quantidade de vértices impossibilita uma aparência apresentável. Porém, para esse caso o comando `"FindClique[g]"` encontra $\omega(H) = 7$.

Pelo Teorema 5.2.8, temos uma cota superior e inferior para $\omega(G)$ para p-grupos extraespeciais de ordem p^{2a+1} e $p > 2$. Note que para $p > 2$, usando o mesmo argumento que fizemos no Teorema 5.2.7, é possível observar que $a(G) \geq p^a + 1$ para G um p-grupo extraespecial de ordem p^{2a+1}. Tendo isso em vista, apesar de termos a cota trivial $a(G) \leq [G : Z(G)]$, uma problema seria determinar cotas superiores melhores para $a(G)$. Agora, vimos que podemos determinar quando 2-grupos extraespeciais de ordem 2^{2a+1} satisfazem $\omega(G) = a(G)$. Outro problema interessante em aberto seria caracterizar p-grupos extraespeciais de ordem p^{2a+1} tais que $\omega(G) = a(G)$, $p > 2$ e $a > 1$.

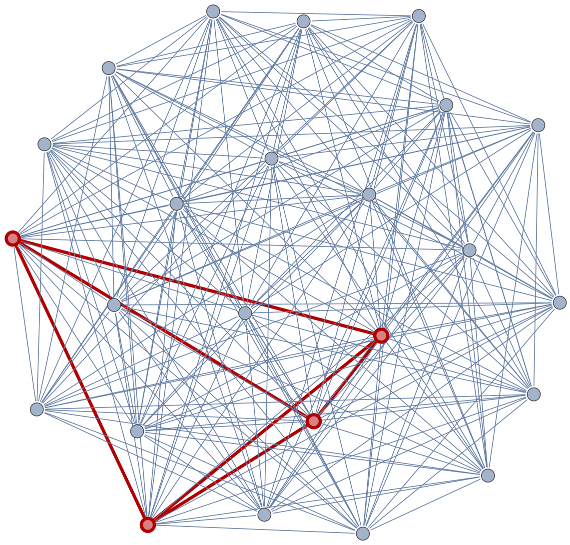

FIGURA 5.2.1. $\Gamma(G)$, G um 3-grupo extraespec. de ordem 3^3 e exp. 3

CAPÍTULO 6

APÊNDICE

6.1 CONSTRUÇÃO DE $\Gamma(G)$ NO GAP

A função $NC2$ foi construída para o programa **GAP 4.7.5**, [**7**], e tem como objetivo retornar a lista de arestas do grafo não-comutativo associado a um grupo G. A função $NC2$ é definida da seguinte forma:

```
NC2:= function (G)
local V, lati, y, v, temp, r;
V:= Difference( G, Centre(G));
lati:=[];

for v in V do
temp:=Difference(V,[v]);
r:=Filtered(temp, y-> v*y<>y*v);
for y in r do
if not([v,y] in lati) and not([y,v] in lati) then
Add(lati,[v,y]);
fi;
od;
od;

return(lati);

end;
```

Para exemplificar, seja G o grupo diedral de ordem 8. Para obter as grafo não-comutativo de D_8, procedemos da seguinte forma:

```
gap> Read("C:/Users/vinicius/Desktop/NC2.txt");
gap> G:=DihedralGroup(IsPermGroup,8);
Group([ (1,2,3,4), (2,4) ])

gap> NC2(G);
[ [ (2,4), (1,2)(3,4) ], [ (2,4), (1,2,3,4) ], [ (2,4), (1,4,3,2) ],
[ (2,4), (1,4)(2,3) ], [ (1,2)(3,4), (1,2,3,4) ], [ (1,2)(3,4), (1,3) ],
[ (1,2)(3,4), (1,4,3,2) ], [ (1,2,3,4), (1,3) ], [ (1,2,3,4), (1,4)(2,3) ],
[ (1,2)(3,4), (1,3) ], [ (1,2)(3,4), (1,4,3,2) ], [ (1,2,3,4), (1,3) ],
[ (1,2,3,4), (1,4)(2,3) ],  [ (1,3), (1,4,3,2) ], [ (1,3), (1,4)(2,3) ],
[ (1,4,3,2), (1,4)(2,3) ] ]
gap>
```

Dessa forma, se o grupo D_8 visto como subgrupo de permutações é gerado por (1234) e $(2,4)$, a lista acima nos dá os elementos que estão ligados por uma aresta, por exemplo, (24) e (12)(34) são ligados por uma aresta em $\Gamma(D_8)$.

6.2 Demonstração Teorema 4.2.2

Como vimos no Capítulo 4, temos o seguinte resultado que agora será demonstrado:

Teorema. Sejam $\alpha_1, \ldots, \alpha_m$ m números reais positivos tais que

$$1 \leq \alpha_1 \leq \alpha_2 \leq \cdots \leq \alpha_m \quad e \quad \prod_{i=1}^{j-1} \frac{1}{\alpha_i} \leq \sum_{i=j}^{m} \frac{1}{\alpha_i},$$

para $1 \leq j \leq m$, então

$$\alpha_m \leq y_m \quad e \quad \prod_{i=1}^{m} \alpha_i \leq {y_m}^2$$

onde $y_1 = 1$ e $y_{i+1} = {y_i}^2 + y_i$, quando $i \geq 1$.

Demonstração Teorema 4.2.2. Para $1 \leq i \leq m$ defina $x_i = \frac{1}{\alpha_i}$ e denote $x = (x_1, \ldots, x_m)$. Assim, temos, por hipótese, que os x_i satisfazem as seguintes relações:

$$1 \geq x_1 \geq \cdots \geq x_m \geq 0, \tag{6.2.1}$$

$$\varphi_j(x) = \sum_{i=j}^{m} x_i - \prod_{i=1}^{j-1} x_i \geq 0, \quad \text{para } 1 \leq j \leq m. \tag{6.2.2}$$

Em geral, ao longo desta demonstração, se os números reais $x_1, \ldots, x_m$ satisfazem (6.2.1) e (6.2.2) chamaremos $x = (x_1, \ldots, x_m)$ de vetor solução. Dito isso, queremos achar os vetores solução que minimizam ou x_m ou $\prod_{i=1}^m x_i$. Definimos então

$$\xi = \inf x_m, \quad e \quad \pi = \inf \prod_{i=1}^{m} x_i,$$

onde o ínfimo é tomado sobre todos os vetores solução. Denotaremos o conjunto de vetores solução por K. Dado $x = (x_1, \ldots, x_m)$ um vetor em K, se $x_m = \xi$ ou $\pi = \prod_{i=1}^m x_i$ dizemos que x é otimizado. Quando for necessário sermos mais específicos, dado $x = (x_1, \ldots, x_m)$ um vetor em K, se $x_m = \xi$ dizemos que x é ξ-otimizado e se $\pi = \prod_{i=1}^m x_i$ dizemos que x é π-otimizado.

Agora vamos mostrar que de fato existem vetores solução otimizados. Primeiro, note que o conjunto K de vetores solução é um conjunto compacto de $\mathbb{R}^n$. De fato, um vetor é solução se satisfaz as relações em (6.2.2) e (6.2.1). Vamos denotar por $L = \{(x_1, \ldots, x_m) \in \mathbb{R}^n \mid 1 \geq x_1 \geq \cdots \geq x_m \geq 0\}$. Agora, consideramos, para $1 \leq j \leq m$, as funções $\varphi_j : L \to \mathbb{R}$ e notamos que, por (6.2.2), o conjunto K de vetores solução é a interseção das imagens inversas de φ_j do intervalo $[0, +\infty)$, para $1 \leq j \leq m$, ou seja, $K = \bigcap_{j=1}^m \varphi_j{}^{-1}([0, +\infty))$. Notemos que cada função φ_j é contínua. Também temos que o complementar em $\mathbb{R}$ do conjunto $[0, +\infty)$ é o conjunto aberto $(-\infty, 0)$ de $\mathbb{R}$, portanto $[0, +\infty)$ é fechado. Como a imagem inversa por uma função contínua de um conjunto fechado é fechada e a interseção de fechados é sempre fechada, então $K = \bigcap_{j=1}^m \varphi_j{}^{-1}([0, +\infty))$ é fechado. Por outro lado, L é limitado e $K \subseteq L$ portanto K é limitado. Como em $\mathbb{R}^m$ um conjunto é compacto se, e somente se ele é fechado e limitado, temos que o conjunto de vetores solução K é compacto em $\mathbb{R}^m$, como queríamos. Agora, consideramos as funções $f : K \to \mathbb{R}$ e $g : K \to \mathbb{R}$ definidas por $f(x_1, \ldots, x_m) = x_m$ e $g(x_1, \ldots, x_m) = \prod_{i=1}^m x_i$. Temos que f e g são contínuas e K é compacto, então pelo Teorema de Weierstrass [**10**, Corolário 3, p.21] f e g assumem valor mínimo em K e portanto, existem vetores solução otimizados, como queríamos. A seguir, vamos determinar esses vetores otimizados.

Seja $x = (x_1, \ldots, x_m)$ um vetor solução. Se uma das coordenadas fosse igual a zero, digamos $x_j = 0$, por (6.2.1), teríamos que $x_{j+1} = x_{j+2} = \ldots = x_m = 0$ e assim $\sum_{i=j}^m x_i = 0$. Portanto $\varphi_j(x) = -\prod_{i=1}^{j-1} x_i \geq 0$ e como cada x_i é não negativo, teríamos que $\varphi_j = -\prod_{i=1}^{j-1} x_i = 0$. Portanto, existiria um x_i com $1 \leq i \leq j-1$ tal que $x_i = 0$. Pegando j mínimo, teríamos que $j = 1$ e portanto todas as coordenadas de x seriam nulas, e por (6.2.2) para $j = 1$ teríamos um absurdo. Portanto, as coordenadas de qualquer vetor solução $x = (x_1, \ldots, x_m)$ são todas positivas. Assim, como o ínfimo de f e g são atingidos em K, temos que, em particular, ξ e π são ambos positivos.

Agora, consideramos um vetor solução x tal que

$$\varphi_1(x) = \sum_{i=1}^{m} x_i - 1 > 0.$$

Vamos mostrar que, nesse caso, x não pode ser um vetor solução otimizado, em outras palavras, se x é um vetor otimizado, então $\varphi_1(x) = 0$. Definimos

$$x'_j = \frac{x_j}{\sum_{i=1}^m x_i} \qquad j = 1, \ldots, m.$$

Vamos verificar que $x' = (x'_1, \ldots, x'_m)$ também é um vetor solução. Primeiro, como $x_j \geq x_{j+1}$, para $1 \leq j \leq m-1$, e $\sum_{i=1}^m x_i > 1$, temos que

$$x'_j = \frac{x_j}{\sum_{i=1}^m x_i} \geq \frac{x_{j+1}}{\sum_{i=1}^m x_i} = x'_{j+1}.$$

Como $x_j > 0$, para todo $1 \leq j \leq m$, pois x é um vetor solução, temos que $x'_j > 0$. Também temos que $x_j \leq 1$ para todo $1 \leq j \leq m$ e portanto

$$x'_j = \frac{x_j}{\sum_{i=1}^m x_i} \leq \frac{1}{\sum_{i=1}^m x_i} < 1,$$

portanto as relações em (6.2.1) valem para o vetor x'.

Agora, vamos conferir também que as relações em (6.2.2) valem para o vetor $x' = (x'_1, \ldots, x'_m)$. Para $1 \leq j \leq m$, temos que

$$\begin{aligned}\varphi_j(x') &= \sum_{i=j}^m x'_i - \prod_{i=1}^{j-1} x'_i = \left(\sum_{i=j}^m \frac{x_i}{\sum_{k=1}^m x_k}\right) - \left(\prod_{i=1}^{j-1} \frac{x_i}{\sum_{k=1}^m x_k}\right) \\ &= \frac{\sum_{i=j}^m x_i}{\sum_{k=1}^m x_k} - \frac{\prod_{i=1}^{j-1} x_i}{(\sum_{k=1}^m x_k)^{j-1}}. \end{aligned} \tag{6.2.3}$$

Por (6.2), se $j = 1$ temos que $\varphi_1(x') = 0$. Se $1 < j \leq m$, temos que $(\sum_{k=1}^m x_k)^{j-2} \geq 1$ pois, por hipótese, $\varphi_1(x) > 0$. Logo, $(\sum_{k=1}^m x_k)^{j-2} \left(\sum_{i=j}^m x_i\right) \geq \left(\sum_{i=j}^m x_i\right)$. Assim,

$$\begin{aligned}\varphi_j(x') &= \frac{\sum_{i=j}^m x_i}{\sum_{k=1}^m x_k} - \frac{\prod_{i=1}^{j-1} x_i}{(\sum_{k=1}^m x_k)^{j-1}} \\ &= \frac{(\sum_{k=1}^m x_k)^{j-2}\left(\sum_{i=j}^m x_i\right) - \prod_{i=1}^{j-1} x_i}{(\sum_{k=1}^m x_k)^{j-1}} \geq \frac{\left(\sum_{i=j}^m x_i\right) - \prod_{i=1}^{j-1} x_i}{(\sum_{k=1}^m x_k)^{j-1}} = \frac{\varphi_j(x)}{(\sum_{k=1}^m x_k)^{j-1}} \geq 0,\end{aligned}$$

pois como x é um vetor solução. Resumindo, vimos que se x é um vetor solução tal que $\varphi_1(x) > 0$, temos que $x' = (x'_1, \ldots, x'_m)$ também é um vetor solução. Mais ainda, como $\sum_{i=1}^m x_i > 1$, temos que $x'_j = \frac{x_j}{\sum_{i=1}^m x_i} < x_j$ para $1 \leq j \leq m$ e em particular $x'_m < x_m$ e também $\prod_{i=1}^m x'_i < \prod_{i=1}^m x_i$. Assim, x não pode ser um vetor solução otimizado como queríamos provar. Logo, se x é qualquer vetor solução otimizado, temos que

$$\varphi_1(x) = 0.$$

Agora, como estamos procurando vetores solução otimizados, vamos considerar apenas vetores solução x tais que $\varphi_1 = 0$, isto é,

$$\sum_{i=1}^{m} x_i = 1. \tag{6.2.4}$$

Para um tal vetor x, escrevemos $\sum_{i=1}^{m} x_i = \sum_{i=1}^{j-1} x_i + \sum_{i=j}^{m} x_i$ e assim temos $\sum_{i=j}^{m} x_i = 1 - \sum_{i=1}^{j-1} x_i$. Portanto,

$$\varphi_j(x) = 1 - \sum_{i=1}^{j-1} x_i - \prod_{i=1}^{j-1} x_i \quad j = 2, \ldots, m. \tag{6.2.5}$$

Então, notamos que cada $\varphi_j(x)$, com $2 \leq j \leq m$, depende apenas das $j-1$ primeiras coordenadas do vetor x.

Agora, se $m = 1$, temos que por (6.2.4) existe um único vetor solução otimizado, isto é, $x = x_1 = 1$. Se $m = 2$, temos que $x_1 + x_2 = 1$ e logo $1 - x_1 = x_2$. Assim, por (6.2.5) temos que $\varphi_2(x) = (1 - x_1) - x_1 = x_2 - x_1 \geq 0$. Portanto, $x_2 \geq x_1$. Mas por hipótese, $x = (x_1, x_2)$ é um vetor solução, então por (6.2.1) temos que $x_1 \geq x_2$ e daí, $x_1 = x_2 = \frac{1}{2}$.

Agora suponhamos que $m > 2$. Seja x um vetor solução tal que $x_{j-1} = x_j$ para algum $1 < j \leq m$. Então, como $0 \leq x_i \leq 1$ para $1 \leq i \leq m$, temos que

$$\sum_{i=j}^{m} x_i \geq x_j = x_{j-1} \geq \prod_{i=1}^{j-1} x_i. \tag{6.2.6}$$

Notamos que a igualdade acima ocorre se $\sum_{i=j}^{m} x_i = x_j$ e $x_{j-1} = \prod_{i=1}^{j-1} x_i$. Mas como todas as coordenadas de um vetor solução são positivas, temos que $j = m$ pela primeira igualdade. Agora, por (6.2.4) para $m > 2$ temos que $x_i < 1$ para todas as coordenadas. Assim, $x_{j-1} = \prod_{i=1}^{j-1} x_i$ implica que $\prod_{i=1}^{j-2} x_i = 1$ um absurdo. Portanto, $j - 1 = 1$, ou seja, $j = 2 = m$. Mas como $m > 2$, então 6.2.6 não pode ser uma igualdade, portanto $\sum_{i=j}^{m} x_i > \prod_{i=1}^{j-1} x_i$ e assim $\varphi_j(x) > 0$ sempre que $x_{j-1} = x_j$, para $2 \leq j \leq m$.

Agora assuma que x é um vetor solução tal que

$$\varphi_1(x) = \varphi_2(x) = \cdots = \varphi_{s-1}(x) = 0 \quad e \quad \varphi_s(x) > 0. \tag{6.2.7}$$

Denotaremos por p o número de índices $i > s$ tais que $x_i = x_s$ e assim $p \geq 0$. Temos que se $s + p < m$, então $x_s = x_{s+1} = \ldots = x_{s+p} > x_{s+p+1}$. Agora se $s + p = m$, temos que $x_s = x_{s+1} = \ldots = x_{s+p} = x_m$. Como $\varphi_j(x) > 0$ sempre que $x_{j-1} = x_j$, temos que

$$\varphi_j(x) > 0 \quad j = s + 1, \ldots, s + p. \tag{6.2.8}$$

Vamos considerar agora o vetor $x' = (x'_1, \ldots, x'_m)$ definido da seguinte maneira:

$$x'_i = \begin{cases} x_i, \text{ se } i \neq \{s-1, s+p\} \\ x_{s-1} + \epsilon, \text{ se } i = s-1 \\ x_{s+p} - \epsilon, \text{ se } i = s+p \end{cases}$$

e vamos determinar $\epsilon > 0$ de forma que x' também seja um vetor solução. Primeiro note que para $1 \leq j \leq s-1$ temos que $x_i = x'_i$ sempre que $1 \leq j \leq s-1$. Daí, por (6.2.2), temos que $\prod_{i=1}^{j-1} x_i = \prod_{i=1}^{j-1} x'_i$ e $\sum_{i=j}^{m} x_i = \sum_{i=j}^{m} x'_i$, pois $x'_{s-1} + x'_{s+p} = x_{s-1} + x_{s+p}$. Então para $1 \leq i \leq j-1$ temos que $\varphi_j(x') = \varphi_j(x) = 0$, pois $\varphi_1(x) = \varphi_2(x) = \ldots = \varphi_{s-1}(x) = 0$.

Se $j > s+p$, temos que $x_i = x'_i$ para $j \leq i \leq m$. Assim,

$$\sum_{i=j}^{m} x_i = \sum_{i=j}^{m} x'_i.$$

Agora, observamos que

$$\begin{aligned}\prod_{i=1}^{j-1} x'_i = x_1 \cdots (x_{s-1} + \epsilon) \cdots (x_{s+p} - \epsilon) \cdots x_j &= \prod_{i=1}^{j-1} x_i \frac{(x_{s-1} + \epsilon)(x_{s+p} - \epsilon)}{x_{s-1} x_{s+p}} \\ &= \prod_{i=1}^{j-1} x_i \left(1 - \frac{\epsilon^2}{x_{s-1} x_{s+p}} + \frac{\epsilon}{x_{s-1}} - \frac{\epsilon}{x_{s+p}}\right).\end{aligned}$$

Logo,

$$\begin{aligned}\varphi_j(x') = \sum_{i=j}^{m} x'_i - \prod_{i=1}^{j-1} x'_i &= \sum_{i=j}^{m} x_i - \prod_{i=1}^{j-1} x_i \left(1 - \frac{\epsilon^2}{x_{s-1} x_{s+p}} + \frac{\epsilon}{x_{s-1}} - \frac{\epsilon}{x_{s+p}}\right) \\ &= \sum_{i=j}^{m} x_i - \prod_{i=1}^{j-1} x_i + \prod_{i=1}^{j-1} x_i \left(\frac{\epsilon^2}{x_{s-1} x_{s+p}} - \frac{\epsilon}{x_{s-1}} + \frac{\epsilon}{x_{s+p}}\right) \\ &= \varphi_j(x) + \prod_{i=1}^{j-1} x_i \left(\frac{\epsilon^2}{x_{s-1} x_{s+p}} - \frac{\epsilon}{x_{s-1}} + \frac{\epsilon}{x_{s+p}}\right).\end{aligned}$$

Agora, como $x_{s-1} \geq x_{s+p}$, temos que $\frac{\epsilon}{x_{s+p}} - \frac{\epsilon}{x_{s-1}} \geq 0$. Temos também que $\varphi_j(x) \geq 0$ então $\varphi_j(x') > 0$, quando $j > s+p$.

Por último, se $s \leq j \leq s+p$, temos por construção que $\varphi_s(x) > 0$ e por (6.2.8), temos que $\varphi_j(x) > 0$ para $s+1 \leq j \leq s+p$. Agora,

$$\begin{aligned}\prod_{i=1}^{j-1} x'_i = x'_1 \cdots x'_{j-1} = x_1 \cdots (x_{s-1} + \epsilon) \cdots x_{j-1} &= \prod_{i=1}^{j-1} x_i \frac{x_{s-1} - \epsilon}{x_{s-1}} \\ &= \prod_{i=1}^{j-1} x_i \left(1 - \frac{\epsilon}{x_{s-1}}\right).\end{aligned}$$

Também temos que

$$\sum_{i=j}^{m} x'_i = x'_j + \cdots + x'_{s+p} + \cdots + x'_m = x_j + \cdots + (x_{s+p} - \epsilon) + \cdots + x_m = \sum_{i=j}^{m} x_i - \epsilon.$$

Portanto,

$$\begin{aligned}\varphi_j(x') &= \sum_{i=j}^{m} x'_i - \prod_{i=1}^{j-1} x'_i = \sum_{i=j}^{m} x_i - \epsilon - \prod_{i=1}^{j-1} x_i + \prod_{i=1}^{j-1} x_i \left(\frac{\epsilon}{x_{s-1}}\right) \\ &= \varphi_j(x) + \epsilon\left(\frac{\prod_{i=1}^{j-1} x_i}{x_{s-1}} - 1\right) \\ &= \varphi_j(x) + \epsilon A_j,\end{aligned}$$

onde $A_j = \dfrac{\prod_{i=1}^{j-1} x_i}{x_{s-1}} - 1$.Temos que $m > 2$ por hipótese, $\varphi_1(x) = 0$ e já notamos que $x_i < 1$, para $1 \leq i \leq m$. Logo, temos que $A_j < 0$ para todo $s \leq j \leq s + p$. Fixando j podemos escolher ϵ tão pequeno quando se queira, neste caso, $\epsilon \leq \frac{\varphi_j(x)}{-A_j}$, pois, como vimos, $\varphi_j(x) > 0$ para $s \leq j \leq s+p$. Assim, escolhemos ϵ suficientemente pequeno para que seja $\epsilon \leq \frac{\varphi_j(x)}{-A_j}$ para todo $s \leq j \leq s+p$. Logo, para este ϵ temos que $\varphi_j(x') \geq 0$. Portanto, resumindo o argumento acima para $1 \leq j \leq m$, as relações (6.2.2) valem para o vetor x' definido anteriormente. A condição (6.2.1) também é válida para ϵ suficientemente pequeno, portanto x' é um vetor solução, como queríamos.

Agora note que $x'_m \leq x_m$. De fato, se $s + p = m$, então $x'_m = x'_{s+p} = x_{s+p} - \epsilon < x_{s+p} = x_m$. Se $s + p < m$, então $x'_m = x_m$. Pelo mesmo raciocínio feito antes, temos que

$$\prod_{i=1}^{m} x'_i = \prod_{i=1}^{m} x_i \left(1 + \frac{\epsilon}{x_{s-1}} - \frac{\epsilon}{x_{s+p}} - \frac{\epsilon^2}{x_{s+p}x_{s-1}}\right) < \prod_{i=1}^{m} x_i$$

pois $\frac{\epsilon}{x_{s-1}} - \frac{\epsilon}{x_{s+p}} \leq 0$ e $-\frac{\epsilon^2}{x_{s+p}x_{s-1}} < 0$. Portanto, isso mostra que um vetor solução x que satisfaz as condições em (6.2.7) não pode ser um vetor π-otimizado. Assim, temos que se $\hat{x} = (\hat{x}_1, \ldots, \hat{x}_m)$ é π-otimizado, temos que $\varphi_1(\hat{x}) = \cdots = \varphi_m(\hat{x}) = 0$. Não é difícil ver que o mesmo vale para vetores ξ-otimizados. De fato, vimos que para ϵ suficientemente pequena, os vetores x' que satisfazem

$$\begin{cases} \varphi_1(x') = \ldots = \varphi_{s-1}(x') = 0 \\ \varphi_s(x') < \varphi_s(x) \\ x'_m \leq x_m \end{cases}$$

existem e portanto denotaremos por S o conjunto não vazio desses vetores. Dado x' um vetor em S, pelo raciocínio anterior é possível achar x'' em S tal que $\varphi_s(x'') < \varphi_s(x')$ e $x''_m \leq x'_m \leq x_m$. Seguindo o mesmo raciocínio, temos que existe u vetor em S que minimiza a função $\varphi_s(y)$ e, como vimos, esta função pode ficar tão próxima de zero quanto se queira. Assim, seu mínimo é $\varphi_s(u) = 0$. Podemos trocar, então, s por $s + 1$ nas condições acima.

Assim, depois de um número finito de passos teremos um vetor u tal que $\varphi_1(u) = \cdots = \varphi_m(u) = 0$ e $u_m \leq x_m$, então $u_m = \xi$.

Agora, já sabemos que os vetores solução otimizados $z = (z_1, \ldots, z_m)$ que estamos procurando são vetores solução tais que $\varphi_1(z) = \cdots = \varphi_m(z) = 0$. Primeiro, para $j > 1$ temos por (6.2.5) que

$$\varphi_j(z) = 1 - \sum_{i=1}^{j-1} z_i - \prod_{j=1}^{j-1} z_i = 0.$$

Isolando z_{j-1} temos que

$$z_{j-1} = \frac{1 - \sum_{i=1}^{j-2} z_i}{1 + \prod_{i=1}^{j-2} z_i} = \frac{\prod_{i=1}^{j-2} z_i}{1 + \prod_{i=1}^{j-2} z_i},$$

pois $\varphi_{j-1}(z) = 1 - \sum_{i=1}^{j-2} z_i - \prod_{j=1}^{j-2} z_i = 0$. Como todas as coordenadas de um vetor solução são positivas, podemos escrever $z_i = 1/\alpha'_i$ para $1 \leq i \leq m$. Assim,

$$\alpha'_{j-1} = \frac{1}{z_i} = 1 + \frac{1}{\prod_{i=1}^{j-2} z_i} = 1 + \prod_{i=1}^{j-2} \alpha'_i \quad j = 2, \ldots, m \tag{6.2.9}$$

Daí, temos que $\alpha'_1 = \alpha'_{2-1} = 2$, $\alpha'_2 = 1 + \alpha'_1 = 3$, $\alpha'_3 = 7$, e assim por diante. De forma geral, definimos a sequência $\{y_i\}$ como $y_1 = 1$ e $y_{i+1} = {y_i}^2 + y_i$. Então, temos que $\alpha'_1 = y_1 + 1$, $\alpha'_2 = y_2 + 1$, $\alpha'_{m-1} = y_{m-1} + 1$. Para determinarmos α'_m, notamos que $\varphi_1(z) = 0$. Então, $\sum_{i=1}^{m-1} z_i + z_m = 1$, daí

$$z_m = 1 - \sum_{i=1}^{m-1} z_i = \prod_{i=1}^{m-1} z_i,$$

pois $\varphi_m(z) = 0$. Então,

$$\alpha'_m = \frac{1}{z_m} = \prod_{i=1}^{m-1} \alpha'_i = \alpha'_{m-1}(\alpha'_{m-1} - 1) = (y_{m-1} - 1)y_{m-1} = y_m,$$

pois $\alpha'_{j-1} = 1 + \prod_{i=1}^{j-2} \alpha'_i$, por (6.2.9) e dessa forma construímos os vetores que precisávamos. Notamos que

$$\prod_{i=1}^{m} \alpha'_i = \alpha'_m \prod_{i=1}^{m-1} \alpha'_i = {\alpha'_i}^2 = {y_m}^2$$

Como z é um vetor solução otimizado, temos que os α_i iniciais satisfazem as desigualdades pedidas e a demonstração está completa.

$\square$

Referências Bibliográficas

[1] A. Abdollahi S. Akbari e H. R. Maimani, *Non-commuting graph of a group*, J. Algebra **298** (2006), no. 2, 468–492.

[2] Y. Berkovich and Z. Janko, *Groups of Prime Power Order*, Walter de Gruyter **2** (2008).

[3] E. A. Bertram, *Some applications of graph theory to finite groups*, Discrete Math. **44** (1983), no. 1, 31–43.

[4] J. A. Bondy e U. S. R. Murty, *Graph theory with applications*, Macmillan London **290** (1976).

[5] P. J. Cameron, *Synchronization 8: The infinite* (2010).

[6] A. Y. M. Chin, *On non-commuting sets in an extraspecial p-group*, J. Group Theory **8** (2005), no. 2, 189–194.

[7] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.7.8* (2015).

[8] I. M. Isaacs, *Algebra: a graduate course*, Amer. Math. Soc. **100** (1994).

[9] J. L. Kelley, *General topology*, Springer Science & Business Media (1975).

[10] E. L. Lima, *Análise Real, Volume 1*, IMPA (2011).

[11] ______, *Análise Real, Volume 2*, IMPA (2011).

[12] J. E. Littlewood e G. Pólya e G. H. Hardy, *Inequalities*, *(Cambridge Mathematical Library)* (1988).

[13] I. D. Macdonald, *Some explicit bounds in groups*, Proc. Lond. Math. Soc. **3** (1969), no. 11, 23-56.

[14] R. Maehara, *The Jordan curve theorem via the Brouwer fixed point theorem*, JSTOR (1984), 641–643.

[15] D. R. Mason, *Coding for a multiple access channel, Ph.D dissertation*, Univ. of Hawaii (1980), 104-106.

[16] ______, *On coverings of a finite group by abelian subgroups*, Math. Proc. Cambridge Philos. Soc. **83** (1978), no. 02, 205–209.

[17] Inc. Wolfram Research, *Mathematica, Version 10.0*, Wolfram Research, Inc. (2014).

[18] B. H. Neumann, *A problem of Paul Erdös on groups*, J. Aust. Math. Soc. **21** (1976), no. 04, 467–472.

[19] ______, *Groups covered by permutable subsets*, Lond. Math. Soc. **s1-29** (1954), no. 2, 236-248.

[20] ______, *Groups covered by finitely many cosets*, Publ. Math. Debrecen **3** (1954), no. 3–4, 227–242.

[21] P. M. Neumann e M. R. Vaughan-Lee, *An essay on BFC groups*, Proc. Lond. Math. Soc. **3** (1977), no. 2, 213–237.

[22] L. Pyber, *The number of pairwise non-commuting elements and the index of the centre in a finite group*, J. Lond. Math. Soc. **2** (1987), no. 2, 287–295.

[23] D. Robinson, *A Course in the Theory of Groups*, Springer Science & Business Media **80** (2012).

[24] ______, *Finiteness conditions and generalized soluble groups, Parte 1*, Springer Science & Business Media **63**, 105-106.

[25] M. Suzuki, *Group theory*, Springer New York (1986).

[26] M. J. Tomkinson, *Groups covered by finitely many cosets or subgroups*, Comm. Algebra **15** (1987), no. 4, 845–859.

[27] E. Yalçin, *Set covering and Serre's theorem on the cohomology algebra of a p-group*, J. Algebra **245** (2001), no. 1, 50–67.