UNIVERSIDADE FEDERAL DO CEARÁ
CENTRO DE CIÊNCIAS
DEPARTAMENTO DE MATEMÁTICA
CURSO DE PÓS-GRADUAÇÃO EM MATEMÁTICA

MARCELO MENDES DE OLIVEIRA

APLICAÇÕES DA TEORIA DOS GRAFOS À TEORIA DOS GRUPOS

FORTALEZA
2008

MARCELO MENDES DE OLIVEIRA

APLICAÇÕES DA TEORIA DOS GRAFOS À TEORIA DOS GRUPOS

Dissertação submetida à Coordenação do Curso de Pós-Graduação em Matemática, da Universidade Federal do Ceará, como requisito parcial para obtenção do grau de Mestre em Matemática.
Área de concentração: Álgebra

Orientador: Prof. Dr. José Robério Rogério.

FORTALEZA
2008

Oliveira, Marcelo Mendes de
O48a Aplicações da teoria dos grafos à teoria dos grupos/
Marcelo Mendes de Oliveira. - Fortaleza: 2008.
77 f.

Orientador: Prof. Dr. José Robério Rogério.
Dissertação (mestrado) – Universidade Federal do
Ceará, Departamento de Matemática, 2008.

1 - Álgebra

CDD 512

Aos meus pais, Felipe e Jesus,
à minha esposa, Derlange,
e a meus filhos, Camila e Lucas,
os quais eu sacrifiquei com ausência
para realizar esta etapa.

AGRADECIMENTOS

Em primeiro lugar, agradeço a Deus por me ter dado o gosto pelo estudo, o dom de aprender Matemática com prazer desde a infância e a oportunidade de concluir meu mestrado em um país em que a maioria da população não tem acesso à educação de qualidade.

Em seguida, agradeço a meu pai, Felipe, e a minha mãe, Jesus, aos quais devo meus primeiros aprendizados e condições para me desenvolver como estudante, e a meus irmãos e irmãs Flora, Mauro, Alba, Marcos, Maurício, Rose, Márcia, Sílvio, Álvaro, Renato, Vera, Fernando e Eduardo, modelos de apreendedores de conhecimentos e de vitórias estudantis. O segredo de um bom desempenho acadêmico inicia-se na família.

À minha esposa, Derlange, por compreender e apoiar toda a minha ausência devido aos estudos, sobretudo no período inicial do mestrado. À minha filha, Camila, pelo brilho que põe em meu olhar todos os dias e desculpas por tantos "Não, não posso ir brincar agora.", umas das partes mais duras desse período. Ao meu filho, Lucas, por também alegrar ainda mais os meus dias.

A meus anjos, pessoas que, em seus pequenos gestos - quer tenham sido apenas em me escutar, quer tenham sido me cedendo um local melhor para estudar - tanto me ajudaram: Prof. Cleiton Albuquerque, Prof. Caminha, Prof. Caio, Prof. Abdênago, Profa. Andreane, e tantos outros que não citei.

A meus colegas de mestrado Sibério, Carlos Augusto, Davi, Samuel, Bruno pelos bons momentos de aula e estudo juntos. Ao Samuel, ao Carneiro e ao Bruno pelas dicas de programação. Ao Yuri e ao Carneiro pelos papers.

A meus alunos por falta de mais tempo e dedicação a eles em seus próprios desafios e pelo incentivo, em especial Régis Prado por colaborar com um pouco desta dissertação.

Às escolas Farias Brito e Ari de Sá Cavalcante, nas quais trabalho, por terem sido flexíveis com meus horários durante todo o período de meus estudos e pelo apoio e torcida de todos dessas instituições.

Por fim, agradeço a meu orientador José Robério Rogério pelo tema escolhido, atenção, revisão do texto e valiosas colaborações, aos professores Othon Dantas e Trajano Nóbrega que compuseram minha banca e também colaboraram para melhorar este texto com maestria, além dos professores das disciplinhas, em especial, Prof. Caminha, com o qual fiz boa parte delas.

"Buscai primeiro o Reino de Deus
e a sua justiça e todas as outras
coisas vos serão acrescentadas."
(Mateus 6:33)

RESUMO

O propósito desta dissertação é apresentar aplicações da Teoria dos Grafos à Teoria dos Grupos. De posse do grafo associado a um grupo finito, nós obtemos vários resultados interessantes sobre a estrutura do grupo analisando tal grafo à luz de técnicas-padrão da Teoria dos Grafos. Mais precisamente, os números cromático e de independência do grafo de um grupo finito nos permitem estimar a cardinalidade máxima de um subgrupo abeliano do mesmo, bem como o tamanho mínimo possível de um subconjunto do grupo formado por elementos que não comutam dois a dois; no caso de grupos finitos abelianos, nós também estudamos seus subconjuntos livres de somas.

Palavras-chave: Grupos. Grafos.

ABSTRACT

This report deals with applications of Graph Theory to Group Theory. Once we construct the graph associated to a finite group, we get several interesting results on the group structure by analysing its associated graph with the help of various standard graph-theoretic tools. More precisely, the chromatic and independence numbers of the graph of a finite group allows us to estimate the maximal cardinality of an abelian subgroup of it, as well as the minimal size of a subset of the group, all of whose elements don't commute in pairs; for finite abelian groups, we also study their free-sum subsets.

Keywords: Groups. Graphs.

NOTAÇÕES

$d(v)$	grau do vértice v em um grafo
Γ	grafo Γ
$\alpha(\Gamma)$	número de independência do grafo Γ
$a(G)$	número mínimo de subgrupos abelianos cobrindo o grupo G
$\|X\|$	cardinalidade do conjunto X
$C(x)$	centralizador do elemento x
G	grupo G
$Z(G)$	centro de G
$k(G)$	número de classes de conjugação de G
x^G	classe de conjugação de x em G
$C_G(x)$	centralizador do elemento x em G
$\lfloor x \rfloor$	parte inteira do número real x
$S + S$	conjunto dos elementos que são soma de elementos do conjunto S
$S - S$	conjunto dos elementos que são diferença de elementos do conjunto S
$\frac{1}{2}S$	conjunto dos elementos cujos dobros estão no conjunto S
$A \dot\cup B$	união disjunta dos conjuntos A e B
$-S$	conjunto dos elementos $-x$ tais que x está no conjunto S
$\|G : H\|$	índice do subgrupo H em relação a G
S_n	grupo das permutações de n letras
A_n	grupo das permutações pares de n letras
K_n	grafo completo de n vértices
$A \leq G$	A é subgrupo de G
$\langle X \rangle$	subgrupo gerado pelos elementos do conjunto X
(u, v)	aresta unindo os vértices u e v em um grafo ou máximo divisor comum dos números naturais u e v
$\exists$	existe
D_{2n}	grupo diedral de ordem $2n$
$a \equiv b \mod n$	a e b deixam o mesmo resto na divisão pelo inteiro n
$o(x)$	ordem de x em um grupo
$C_G(H)$	centralizador do subgrupo H em G
$H \trianglelefteq G$	H é subgrupo normal de G
$H \triangleleft G$	H é subgrupo normal próprio de G
HN	conjunto dos elementos hn com $h \in H$ e $n \in N$
$H \times N$	produto direto dos grupos H e N
$X - Y$	conjunto dos elementos de X que não estão em Y
H^x	conjunto dos elementos $x^{-1}hx$ com $h \in H$, $x \in G > H$
O_x	órbita de x em um grupo
$\mathbb{Z}_n$	conjunto das classes de equivalência de $\mathbb{Z}$ módulo n
$H + a$	classe lateral de H

Sumário

Notações **6**

Introdução **7**

1 DEFINIÇÕES E RESULTADOS BÁSICOS **12**
1.1 Grafos 12
1.2 Grupos e Grafos 15
1.3 Dois Resultados Básicos 16

2 SUBGRUPOS ABELIANOS, $\alpha(G)$ E $a(G)$ **19**
2.1 Uma Cota Superior para a Cardinalidade de um Subgrupo Abeliano 19
2.2 Cotas Inferiores para $\alpha(\Gamma)$ 27
2.3 Grupos com Cota Superior para $\alpha(G)$ 39
2.4 Mais Cotas Inferiores para $\alpha(G)$ 44
2.5 Uma Cota Superior para $a(G)$ 48

3 SUBCONJUNTOS LIVRES DE SOMAS **51**
3.1 Introdução 51
3.2 Subconjuntos Livres de Somas Localmente Maximais 54

A TEORIA DE RAMSEY **66**

B SOBRE A CARDINALIDADE DE $S+S$ E $S-S$ **69**

Referências Bibliográficas **71**

INTRODUÇÃO

Como relacionar Teoria dos Grafos e Teoria dos Grupos? Num primeiro momento, podemos pensar em uma correspondência entre os elementos do grupo com os vértices de um grafo. Mas como seria a regra para haver uma aresta unindo dois vértices desse grupo? Veremos neste texto boas maneiras (regras) de interligá-los.

Jerry Griggs e Tom Ramsey utilizaram Teoria dos Grafos e Princípio Extremo para provar o

Teorema 0.0.1 (Wei)**.** *Seja $d(v)$ o grau do vértice v no grafo Γ e $\alpha(\Gamma)$, o número de independência de Γ. Então*

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

com igualdade ocorrendo se, e somente se, Γ for uma união de cliques disjuntas.

Esse interessante resultado nos dá uma cota mínima para $\alpha(G)$, que é a quantidade máxima de elementos que um grupo suporta sem haver comutatividade entre dois desses elementos, a partir do número de independência de um grafo, utilizando apenas a Teoria dos Grafos. Ele foi demonstrado por V. K. Wei [10] em 1980.

Ainda como conseqüência desse teorema, obtemos uma cota inferior para a quantidade mínima de subgrupos abelianos necessários para a cobertura de um grupo.

Outro fato obtido a partir desse teorema é o

Lema 0.0.1. *Seja G um grupo finito não-abeliano com $k(G)$ classes de conjugação tal que*

$$\alpha(G) \leq |G|^r - 1, 0 < r < 1.$$

Então:

a) Para cada $x \in G, |C(x)| \geq |G|^{\frac{1-r}{2}}$.

b) Existe um elemento $g \in G - Z(G)$ *com* $|C(g)| > |G|^{1-r}$ *e* $|C(x) \cap C(g)| > |G|^{\frac{1-3r}{2}}$, *para cada* $x \in G$.

c) Finalmente, em todo grupo finito G, *pelo menos* $k(G) - \alpha(G)$ *das classes de conjugação distintas em* G *satisfazem* $\left|x^G\right| < |G|^{\frac{1}{2}}$.

que é utilizado para mostrar o

Teorema 0.0.2. *Seja* G *um grupo contendo um subgrupo próprio* M *tal que sempre que* $x \in M - \{1\}$, *tem-se* $C_G(x) \leq M$. *Então*

$$\alpha(G) \geq \left\lfloor |G|^{\frac{1}{3}} \right\rfloor.$$

Ainda com o número de independência de um grafo, obtemos o

Teorema 0.0.3. *Definamos uma função* $f(n)$ *indutivamente por* $f(1) = 1$ *e*

$$f(n) = n + \binom{n}{2} f(n-1).$$

Seja $a(G)$ *a quantidade mínima de subgrupos abelianos que cobrem o grupo* G. *Se* $\alpha(G) < \infty$, *então*

$$a(G) \leq f(\alpha(G)).$$

Em particular, $a(G) < \infty$.

que majora a quantidade mínima de subgrupos abelianos necessários para cobrir um grupo.

Ao final, temos os teoremas

Teorema 0.0.4. *Seja* G *um grupo abeliano e finito e* S, *um conjunto livre de somas (a soma de dois elementos de* S *não pode estar em* S*) localmente maximal em* G *(*R *livre de somas e* $S \subseteq R \subseteq G$ *implica* $R = S$*). Seja* c *uma constante positiva. Então:*

i) $G = S \cup (S + S) \cup (S - S) \cup \frac{1}{2}S$.

ii) Se $|G|$ *é ímpar, então* $|S| \geq \frac{1}{6}\left((24|G| - 15)^{\frac{1}{2}} - 3\right)$.

iii) Se $|G|$ *é par, então* $|S| \geq \frac{1}{6}\left((12|G| - 23)^{\frac{1}{2}} - 1\right)$.

iv) Se $|S+S| \leq c|S|$, *então*

$$|S| \geq \frac{|G|}{c^2+c+2}$$

para $|G|$ *ímpar e*

$$|S| \geq \frac{|G|}{2(c^2+c+1)}$$

para $|G|$ *par.*

que fornece uma cota inferior para a cardinalidade de um subconjunto livre de somas localmente maximal, e o

Teorema 0.0.5. *Seja* S *um conjunto livre de somas localmente maximal no grupo abeliano finito* G*. Então,*

$$|S-S| + |S \cup -S| - 3 \leq |G| \left(1 - |S-S|^{-1}\right),$$

com igualdade se, e somente se, $S-S$ *é um subgrupo de* G*,* $|G : S-S| = 3$ *e* S *é uma classe lateral de* $S-S$*.*

que relaciona a cardinalidade de um grupo com subconjuntos livres de somas localmente maximais.

O texto está exposto da seguinte forma.

O capítulo 1 traz definições e resultados básicos de grafos e de grupos a serem utilizados ao longo desta dissertação.

O capítulo 2 relaciona grupos e grafos a partir da seguinte associação:

$$xy = yx; x, y \in G \Leftrightarrow x \text{ é adjacente } y \text{ em } \Gamma_G,$$

sendo Γ_G o grafo associado a G. É bastante utilizado o conceito de número de independência $\alpha(\Gamma)$ de um grafo.

Já o capítulo 3 apresenta grupos aditivos abelianos associados a seus subconjuntos livres de somas, tornando dois vértices adjacentes se a diferença entre eles estiver em $S-S$ (S livre de somas), além de abordar a relação entre Teoria dos Grupos e Teoria de Ramsey, que

é melhor discutida no primeiro apêndice com definições, resultados e exemplos.

O segundo apêndice, que encerra este texto, detalha um fato utilizado no capítulo 3 sobre as cardinalidades de $S+S$ e $S-S$, que surgiu a partir de um questionamento de Paul Erdös.

Capítulo 1

DEFINIÇÕES E RESULTADOS BÁSICOS

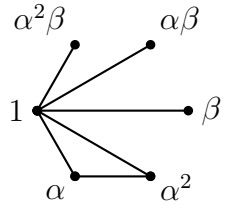
Este primeiro capítulo apresenta definições de grafos, grupos e algumas relacionando ambos, ilustrando-as se necessário. A partir dessas definições, já são percebidos alguns resultados interessantes. Também é neste capítulo que são demonstrados pequenos fatos utilizados durante o texto a seguir.

1.1 Grafos

Começamos definindo conceitos básicos da Teoria dos Grafos.

Um **grafo** é simplesmente um conjunto de pontos (**vértices**) unidos ou não por segmentos (**arestas**). Se existe aresta unindo dois vértices desse grafo, então dizemos que eles são **adjacentes**. Neste texto, a letra Γ sempre denotará um grafo.

Um grafo pode representar cidades (vértices) e rotas aéreas (arestas) entre essas cidades, mas também pode está associado a um grupo como no exemplo a seguir:



Exemplo de Grafo associado a S_3

em que cada aresta está desenhada entre dois vértices se, e somente se, os elementos correspondentes no grupo comutam.

Multigrafo é um grafo que possui **arestas múltiplas** (várias arestas conectando dois vértices) ou **loops** (arestas com extremidades coincidentes). Nesta dissertação, os grafos nunca são multigrafos.

O grau $d(x)$ de um vértice é o número de arestas incidentes nesse vértice x, ou, equivalentemente, o número de vértices adjacentes a x, por não termos multigrafos. Observe que $\sum_{x\in\Gamma} d(x)$ é o dobro da quantidade de arestas (as arestas são contadas duas vezes, uma para cada um de seus vértices) e, portanto, a quantidade de vértices com grau ímpar do grafo é um número par.

No exemplo anterior do grafo associado a S_3, $d(1) = 5, d(\alpha) = d(\alpha^2) = 2$, enquanto os demais têm grau 1.

Em um **grafo k-regular** cada vértice x tem grau $d(x) = k$. Nos exemplos a seguir, todos os vértices têm grau 2.

Um grafo é **regular** (simplesmente) quando todos os seus vértices têm o mesmo grau.

Dizemos que um grafo é **completo** quando qualquer par de vértices está unido por arestas. A notação usual para um grafo completo de n vértices é K_n e ele possui $\binom{n}{2}$ arestas.

Em um **subgrafo** H completo de Γ, o conjunto dos vértices é um subconjunto do conjunto dos vértices de Γ em que todo par está unido por uma aresta de Γ. Um subgrafo completo maximal de Γ é chamado de **clique** .

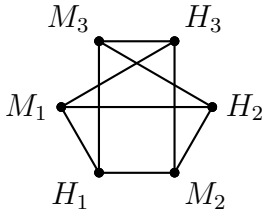
Exemplos de subgrafos 2-regulares de K_5

Seja Γ um **grafo não-direcionado** (suas arestas não possuem orientação), sem loops ou arestas múltiplas, cujos vértices são $x_1, x_2, ..., x_n$. Γ pode ser k-**colorido pelos vértices**, ou, simplesmente, k-**colorido**, sempre que for possível particionar o conjunto

$$\{x_1, x_2, ..., x_n\}$$

dos vértices em k subconjuntos sem que haja dois vértices em um mesmo subconjunto unidos por uma aresta de Γ, ou seja, sempre que pudermos colorir os vértices de Γ com k cores sem que haja aresta unindo vértices que tenham a mesma cor.

Por exemplo, em um conjunto de 6 pessoas dividido em 2 subconjuntos de 3 homens H_1, H_2, H_3 e 3 mulheres M_1, M_2, M_3, podemos construir o grafo em que os vértices são as pessoas e cujas arestas representam possíveis casais, realizando uma 2-coloração:

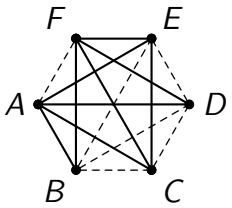


Exemplo de uma 2-coloração

Também é possível **colorir as arestas** desde que seus vértices possuam determinada relação. Um exemplo prático é o seguinte:

Em uma festa com s pessoas, em que $s \geq 6$, há três pessoas que se conhecem mutuamente ou três que não se conhecem duas a duas entre si, supondo recíproca a relação conhecer.

Podemos representar as pessoas na festa como vértices de um grafo. Em seguida, pintamos as arestas do grafo completo formado com duas cores, de acordo com o tipo de relacionamento (arestas) entre as pessoas (conhecidas ou desconhecidas) representadas pelos dois vértices extremos de cada aresta. Encerraremos esse exemplo no primeiro apêndice sobre Teoria de Ramsey.



Exemplo de uma coloração por arestas com 2 cores de um K_6

Um **conjunto independente** em um grafo Γ é uma coleção de vértices sem haver dois deles conexos por uma aresta de Γ. Pode ser entendido também como um subconjunto de vértices que induz um subgrafo consistindo apenas de **vértices isolados** (vértices com grau 0). Para um grafo finito Γ, seja $\alpha(\Gamma)$ (o **número de independência** de Γ) a maior cardinalidade de um conjunto independente de Γ.

1.2 Grupos e Grafos

Nesta seção, veremos alguns bons exemplos de associação entre grupos e grafos. O primeiro vem a seguir.

Sejam G um grupo finito e $x, y \in G$. Associaremos o grafo $\Gamma = \Gamma_G$ a G da seguinte forma: os vértices de Γ associados a x e a y são adjacentes se, e somente se, $xy = yx$. Se o grupo for abeliano, isto é, se quaisquer dois elementos comutam em relação à operação do grupo, então o grafo associado é completo. Essa será a correspondência (ou regra) utilizada em todo o capítulo 2.

Assim, para um grupo com essa regra para construção das arestas, $\alpha(G)$ (ou $\alpha(\Gamma)$) conta a quantidade máxima de elementos desse grupo em que dois quaisquer não comutam.

Já a relação entre um subgrupo abeliano e uma k-coloração, também com a regra acima, é a seguinte. Se um grafo pode ser k-colorido, ou seja, se é possível pintar seus vértices com k cores sem que haja dois vértices com a mesma cor unidos por uma aresta, então a cardinalidade de um subgrupo abeliano é no máximo k. De fato, se um subgrupo abeliano tivesse mais que k elementos, então dois deles estariam associados a vértices adjacentes (pois o subgrupo é abeliano) com a mesma cor, o que não pode ocorrer.

Definimos a **classe de conjugação** contendo x no grupo G como

$$x^G = \left\{y^{-1}xy; y \in G\right\}.$$

O **centralizador de x em G** é dado por

$$C(x) = \left\{y \in G; y^{-1}xy = x\right\} = \{y \in G; xy = xy\}.$$

Para o grafo Γ, ainda com a regra acima, o centralizador significa o conjunto dos vértices adjacentes a x, além do próprio vértice x. Assim, temos a seguinte relação:

$$|C(x)| = d(x) + 1, \forall x \in G.$$

O **centro** $Z(G)$ de G é dado por

$$Z(G) = \bigcap_{x \in G} C(x)$$

ou ainda

$$Z(G) = \{x \in G; xy = xy, \forall y \in G\}.$$

Relacionando com Γ, o centro representa o conjunto dos vértices com grau $n-1$, sendo n o número total de vértices de Γ. De fato, se no grupo o elemento comuta com todos os outros, então o vértice associado no grafo está adjacente a todos os outros. É um fato bastante conhecido que o centro de S_n, $n \geq 3$, é **trivial**, isto é, seu único elemento é a identidade. O primeiro exemplo deste capítulo ilustra esse resultado para $n = 3$.

No capítulo 3, os vértices do grafo associado ao grupo são adjacentes se, e somente se, a diferença entre esses elementos do grupo abeliano estiver em $S - S$, sendo S um **subconjunto livre de somas** (isto é, se $x, y \in S$, então $x + y \notin S$) do grupo. Tais representações são conhecidas como Grafos de Cayley.

No primeiro apêndice, definimos em um dos exemplos o grafo associado a $\mathbb{Z}_{13}$ unindo suas arestas se, e somente se, a diferença entre os elementos do grupo for um resíduo cúbico módulo 13.

1.3 Dois Resultados Básicos

Proposição 1.3.1. *Seja G um grupo com centro $Z(G)$. Se $x \in G$, então*

$$\left|x^G\right| = 1 \Leftrightarrow x \in Z(G).$$

Prova.

$$\left|x^G\right| = 1 \Leftrightarrow x^G = \{x\}$$

$$\Leftrightarrow y^{-1}xy = x, \forall y \in G$$

$$\Leftrightarrow xy = yx, \forall y \in G$$

$$\Leftrightarrow x \in Z(G).$$

□

Corolário 1.3.1. *Se G é um grupo, então*

$$\left|x^G\right| = 1, \forall x \in G,$$

se, e somente se, G é abeliano.

Prova.

$$\left|x^G\right| = 1, \forall x \in G$$

$$\Leftrightarrow x \in Z(G), \forall x \in G,$$

ou seja, G abeliano. □

Proposição 1.3.2. *Se G é um grupo e $x \in G$, então*

$$\left|x^G\right| |C(x)| = |G|.$$

Prova. Seja $C = C(x)$ e $\widetilde{G}$, o conjunto de todas as classes laterais à direita de C.

Defina

$$f : x^G \longrightarrow \widetilde{G}$$

por

$$f\left(y^{-1}xy\right) = Cy.$$

i) f está bem definida. De fato,

$$y^{-1}xy = z^{-1}xz$$

$$\Rightarrow zy^{-1}xyz^{-1} = x$$

$$\Rightarrow \left(yz^{-1}\right)^{-1} xyz^{-1} = x$$

$$\Rightarrow yz^{-1} \in C \Rightarrow Cy = Cz.$$

ii) f é uma função injetora pois

$$f\left(y^{-1}xy\right) = f\left(z^{-1}xz\right) \Rightarrow Cy = Cz$$

$$\Rightarrow yz^{-1} \in C$$

$$\Rightarrow \left(yz^{-1}\right)^{-1} xyz^{-1} = x$$

$$\Rightarrow zy^{-1}xyz^{-1} = x$$

$$\Rightarrow y^{-1}xy = z^{-1}xz.$$

iii) f é sobrejetora uma vez que

$$y \in G \Rightarrow Cy = f\left(y^{-1}xy\right).$$

Assim, f é uma função bijetora e

$$\left|x^G\right| = \left|\widetilde{G}\right| = \frac{|G|}{|C|}.$$

□

Capítulo 2

SUBGRUPOS ABELIANOS, $\alpha(G)$ E $a(G)$

Neste segundo capítulo, trataremos grupos multiplicativos. O primeiro resultado utiliza um simples lema de coloração da Teoria dos Grafos para obter uma cota superior para cardinalidade de subgrupos abelianos, do qual derivamos alguns exemplos. Em seguida, demonstramos o teorema de Wei, que relaciona o número de independência $\alpha(\Gamma)$ e os graus dos vértices de um grafo Γ e será bastante utilizado neste e no próximo capítulo. Aqui os grafos associados aos grupos são construídos unindo vértices com arestas se os elementos correspondentes no grupo comutarem. A função $a(G)$, que é o número mínimo de subgrupos abelianos que cobrem G, surge em vários momentos deste capítulo. Também apresentamos alguns corolários e interessantes exemplos a partir da teoria estudada.

2.1 Uma Cota Superior para a Cardinalidade de um Subgrupo Abeliano

Primeiramente, utilizaremos a Teoria dos Grafos para obter um majorante para a cardinalidade de um subgrupo abeliano no Teorema 2.1.1. Na demonstração, faremos uso do seguinte

Lema 2.1.1. *Seja Γ um grafo e $d(x)$, o grau do vértice x. Se, para algum inteiro $q > 1$,*

$$|\{x \in \Gamma | d(x) \geq q\}| \leq q,$$

então Γ pode ser q-colorido.

Prova. Se n é o número de vértices do grafo, então temos dois casos:

i) $n \leq q$. Basta pintar os vértices com cores diferentes.

ii) $n > q$. Façamos indução sobre n. Seja x um vértice de grau mínimo no grafo. Retire esse vértice e todas as arestas incidentes nele, induzindo o grafo $\Gamma - \{x\}$.

Se $d(x) \geq q$, então teríamos todos os $n > q$ vértices com grau maior que ou igual a q, o que contraria a hipótese. Assim, $d(x) < q$.

Daí, em $\Gamma - \{x\}$, $|\{x \in \Gamma | d(x) \geq q\}| \leq q$ ainda ocorre. Por hipótese de indução, é possível q-colorir $\Gamma - \{x\}$. Em seguida, pintamos x com uma cor não utilizada nos vértices adjacentes a x (tal cor existe pois $d(x) < q$) e a demonstração está completa.

□

Teorema 2.1.1. *Seja G um grupo finito com n elementos, com as classes de conjugação ordenadas de acordo com as cardinalidades:*

$$1 \leq \left|{x_1}^G\right| \leq \left|{x_2}^G\right| \leq ...$$

Seja m o menor inteiro i tal que

$$\left|{x_1}^G\right| + \left|{x_2}^G\right| + ... + \left|{x_i}^G\right| \geq |C(x_i)|.$$

Então, cada subgrupo abeliano $A \leq G$ tem ordem

$$|A| \leq \left|{x_1}^G\right| + \left|{x_2}^G\right| + ... + \left|{x_m}^G\right|.$$

Prova. Inicialmente, perceba que tal m existe pois

$$\left|{x_1}^G\right| + \left|{x_2}^G\right| + ... + \left|{x_k}^G\right| = |G| = n \geq |C(x_i)|, \forall i,$$

sendo k o número de classes de conjugação, pois $G = \dot{\bigcup_{1 \leq i \leq k}} x_i^G$.

O teorema é verdadeiro se G é abeliano. De fato, G abeliano dá $\left|{x_i}^G\right| = 1$ e $|C(x_i)| = n$, $\forall i$, e, portanto, $m = n$. Logo,

$$|A| \leq \left|{x_1}^G\right| + \left|{x_2}^G\right| + ... + \left|{x_n}^G\right| = n.$$

Vejamos agora o caso G não-abeliano. Seja $C(x_l)$ o centralizador, diferente de G, de maior cardinalidade. Então,

$$\left|{x_1}^G\right| = \left|{x_2}^G\right| = ... = \left|{x_{l-1}}^G\right| = 1$$

($Z(G)$ tem $l - 1$ elementos) para os elementos de $Z(G)$ e

$$|C(x_l)| \geq |C(x_{l+1})| \geq ...(*)$$

Seja $A < G$ um subgrupo abeliano de cardinalidade máxima de G. Assim, $Z(G) \leq A$ (caso contrário, existiria $x \in Z(G)$, $x \notin A$. Daí, o subgrupo gerado por A e x seria abeliano e conteria propriamente A, uma contradição pois A é abeliano com cardinalidade máxima). Então $Z(G) \leq A \cap C(x_l)$ (pois $Z(G) \leq C(x_l)$).

Vejamos agora que $|A| \leq |C(x_l)|$. De fato, se $A \subseteq C(x_l)$, então o resultado é imediato. Senão, suponha que exista um elemento $a \in A$ tal que $a \notin C(x_l)$. Como A é abeliano, $A \leq C(a)$ e $|A| \leq |C(a)|$. Agora, observe que $a \in x_i^G$ para algum $i \notin \{1, 2, ..., l-1\}$, pois se $a \in Z(G)$, então a estaria em $C(x_l)$ pelo parágrafo anterior, o que não pode ocorrer pois estamos tomando $a \notin C(x_l)$. Daí,

$$|C(a)| \leq |C(x_l)|$$

e

$$|A| \leq |C(x_l)|.$$

Em seguida, afirmamos que $m \geq l$. De fato, se $m < l$, então $x_1, x_2, ..., x_m$ estão todos em $Z(G)$. Logo,

$$\left|{x_1}^G\right| = \left|{x_2}^G\right| = ... = \left|{x_m}^G\right| = 1,$$

$$C(x_m) = n$$

e

$$\left|{x_1}^G\right| + \left|{x_2}^G\right| + ... + \left|{x_m}^G\right| \geq n \Rightarrow m \geq n.$$

Portanto, $n < l$, o que é absurdo.

Se $m = l$, então

$$|A| \leq |C(x_l)| = |C(x_m)| \leq \left|{x_1}^G\right| + \left|{x_2}^G\right| + ... + \left|{x_m}^G\right|$$

e o problema acaba por A ter cardinalidade máxima.

Assuma, então, $m \geq l+1$. Considere Γ associado a G, construindo uma aresta unindo os dois vértices associados a dois elementos do grupo sempre que estes comutarem. Γ_{G-Z} é o grafo obtido a partir de G deletando-se $Z = Z(G)$ (que se compõe dos elementos que estão em correspondência com os vértices conectados a todos os outros) e todas as

arestas incidentes em seus vértices.

Afirmação. Nas notações acima, Γ_{G-Z} pode ser $\sum_{i=l}^{m} \left|{x_i}^G\right|$-colorido.

Prova(Afirmação): A idéia será mostrar que em Γ_{G-Z} o número de vértices de grau $\geq q = \sum_{i=l}^{m} \left|{x_i}^G\right|$ é $\leq q$. O resultado virá em seguida pelo Lema 2.1.1.

Em G, cada vértice y tem grau $|C(y)| - 1$. Assim, cada vértice $y \in G - Z$ tem grau

$$|C(y)| - 1 - |Z|$$

em Γ_{G-Z}, pois todos os elementos do centro Z eram adjacentes a y (observe que o grafo considerado não possui loops).

Vamos contar $|\{y \in G - Z | d(y) \geq q\}|$. Temos

$$|C(y)| - 1 - |Z| \geq q = \sum_{i=l}^{m} \left|{x_i}^G\right|,$$

o que dá

$$|C(y)| - 1 \geq |Z| + \sum_{i=l}^{m} \left|{x_i}^G\right| = \sum_{i=1}^{m} \left|{x_i}^G\right| \geq |C(x_m)|,$$

pela definição de m. Então $|C(y)| > |C(x_m)|$ ou $\left|y^G\right| < \left|{x_m}^G\right|$, pois

$$\left|y^G\right| |C(y)| = \left|{x_m}^G\right| |C(x_m)| = |G|.$$

Portanto, $y \in \bigcup_{i=l}^{m-1} x_i^G$ (por (*) e $m > l$) e $\sum_{i=l}^{m-1} \left|x_i^G\right|$ é um limite superior para $|\{y \in G - Z | d(y) \geq q\}|$. Finalmente, observe que essas união e soma estão bem definidas pois $m \geq l + 1$. □

Desde que os elementos de Z estavam unidos a todos os outros, precisamos de mais $|Z|$ cores para trazermos de volta os elementos de Z e as arestas partindo deles. Assim, Γ pode ser $\left(|Z| + \sum_{i=l}^{m} \left|x_i^G\right|\right)$-colorido, ou seja, $\left(\sum_{i=1}^{m} \left|x_i^G\right|\right)$-colorido e, portanto,

$$|A| \leq \sum_{i=1}^{m} \left|x_i^G\right|,$$

pois, caso $|A| > \sum_{i=1}^{m} \left|x_i^G\right|$, A abeliano, teríamos dois vértices de A com a mesma cor, o que não pode ocorrer.

Como A foi escolhido com cardinalidade máxima, o teorema está provado.

□

Exemplo 2.1.1. *Seja $M = \{m_1, m_2, ..., m_{2k-1}\}$ um grupo abeliano de ordem ímpar $2k-1, k \geq 2$. Se x tem ordem 2 (isto é, $x^2 = 1$ e $x \neq 1$) e satisfaz*

$$xmx = m^{-1}(*),$$

$\forall m \in M$, então $\langle x, M\rangle$ (grupo gerado por x e M e chamado de Grupo Diedral Generalizado) tem $4k-2$ elementos e classes de conjugação com as seguintes cardinalidades:

$$1, \underbrace{2, 2, ..., 2}_{k-1}, 2k-1,$$

como veremos a seguir.

i) $1^G = \{1\}$.

ii) ${m_i}^G = \{m_i, {m_i}^{-1}\}$. *De fato,*

$$1m_i1 = m_i,$$

$$m_j m_i {m_j}^{-1} = m_i m_j {m_j}^{-1} = m_i,$$

pois M abeliano dá $m_i m_j = m_j m_i$. Além disso,

$$xm_i x^{-1} = xm_i x = {m_i}^{-1},$$

$$xm_j m_i (xm_j)^{-1} = xm_j m_i {m_j}^{-1} x$$

$$= xm_i m_j {m_j}^{-1} x = xm_i x = {m_i}^{-1}.$$

Como M é um grupo, o inverso de m_i está em $M - \{1\}$ e $m_i \neq m_i^{-1}$ pois $|M|$ é ímpar. Assim, os $2k-2$ elementos de $M - \{1\}$ formam $k-1$ classes de 2 elementos cada uma.

iii) $x^G = \{xm_1, xm_2, ..., xm_{2k-1}\}$ *pois*

$$1x1^{-1} = x,$$

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

$$m_i x {m_i}^{-1} = m_i x x m_i x = {m_i}^2 x = m_j x,$$

por (*) e M *ser um grupo. Observe que* $m_j x$ *não pode estar em* M*. De fato, obviamente, esse elemento não pode ser* 1 *nem* m_j*. Se* $m_j x = m_i$*, então* $x = {m_j}^{-1} m_i$ *e, portanto,* $x \in M$*, um absurdo pois* x *tem ordem* 2 *e* $|M| = 2k - 1$ *(contradiz o Teorema de Lagrange) .*

Além disso,

$$x m_j x (x m_j)^{-1} = x m_j x {m_j}^{-1} x^{-1}$$

$$= x m_j x x m_j x x = x m_j m_j = x m_k,$$

já que M *é um grupo.*

Somando parcialmente as cardinalidades das classes, obtemos $1, 3, 5, ...$ *O menor índice* m *para que se cumpra a condição do teorema 1 é* $m = k$ *e a igualdade da desigualdade proposta ocorre com* M *pois*

$$\sum_{i=1}^{m} \left|x_i^G\right| = 1 + \underbrace{2 + 2 + ... + 2}_{k-1} = 2k - 1 = |M|.$$

Observe que $C(m_i) = M, \forall i$ *e* $C(x) = \langle x \rangle$ *.*

■

Exemplo 2.1.2. *O grupo* S_3 *das permutações de* 3 *letras satisfaz a igualdade*

$$\sum_{i=1}^{m} \left|x_i^G\right| = |C(x_l)|,$$

sendo l definido como no Teorema 2.1.1, isto é, $C(x_l)$ é o centralizador de maior cardinalidade e diferente de G.

De fato, sendo

$$S_3 = \{1, \alpha, \alpha^2, \beta, \alpha\beta, \alpha^2\beta\},$$

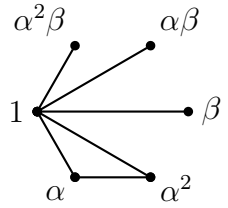
em que $\alpha^3 = 1, \beta^2 = 1, \beta\alpha = \alpha^2\beta$, temos cardinalidades das 3 classes de conjugação iguais a

$$1, 2, 3.$$

Portanto, as cardinalidades dos centralizadores são

$$6, 3, 2,$$

o que pode ser visualizado em



Grafo associado a S_3

Novamente, como no exemplo anterior, $m = 2$ e o centralizador diferente de S_3 de maior cardinalidade tem 3 elementos. Assim,

$$\sum_{i=1}^{m} \left|x_i^G\right| = 1 + 2 = 3 = |C(x_l)|\,.$$

■

Segundo Bertram [1], grupos solúveis com no máximo 7 classes de conjugação, exceto S_4, cumprem a igualdade encontrada no exemplo 2.1.2 e a maioria (não todos) é de Frobenius.

Além disso, ainda por Bertram [1], em S_4 e em cada grupo não-solúvel com no máximo 7 classes de conjugação, ocorre

$$\sum_{i=1}^{m} \left|x_i^G\right| > |C(x_l)|\,,$$

e em S_n com $n \geq 7$ tem-se

$$\sum_{i=1}^{m} \left|x_i^G\right| < |C(x_l)|\,.$$

Exemplo 2.1.3. *Considere o grupo $G = S_4$. A tabela a seguir nos dá as cardinalidades das classes de conjugação e dos centralizadores de G.*

i	x_i	$\left\|x_i^G\right\|$	$\|C(x_i)\|$
1	1	1	24
2	(1 2)(3 4)	3	8
3	(1 2)	6	4
4	(1 2 3 4)	6	4
5	(1 2 3)	8	3

Assim, $m = 3, l = 2$ e

$$\sum_{i=1}^{3} \left|x_i^G\right| = 1 + 3 + 6 > 8 = |C(x_l)|\,.$$

■

Exemplo 2.1.4. *Agora, vejamos $G = S_7$. Novamente, a seguir temos as cardinalidades das classes de conjugação e dos centralizadores de G.*

i	x_i	$\left\|x_i^G\right\|$	$\|C(x_i)\|$
1	1	1	5040
2	(1 2)	21	240
3	(1 2 3)	70	72
4	(1 2)(3 4)	105	48
5	(1 2)(3 4)(5 6)	105	48
6	(1 2 3 4)	210	24
7	(1 2)(3 4)(5 6 7)	210	24
8	(1 2 3)(4 5 6)	280	18
9	(1 2)(3 4 5)	420	12
10	(1 2 3)(4 5 6 7)	420	12
11	(1 2 3 4 5)	504	10
12	(1 2)(3 4 5 6 7)	504	10
13	(1 2)(3 4 5 6)	630	8
14	(1 2 3 4 5 6 7)	720	7
15	(1 2 3 4 5 6)	840	6

Logo, $m = 3, l = 2$ *e*

$$\sum_{i=1}^{3} \left|x_i^G\right| = 1 + 21 + 70 < 240 = |C(x_l)|\,.$$

Observe que o Teorema 2.1.1 garante que $C_{S_7}((1\ 2))$ *não é abeliano.*

■

2.2 Cotas Inferiores para $\alpha(\Gamma)$

Como vimos no capítulo 1, o número de independência de Γ, denotado por $\alpha(\Gamma)$, representa a maior cardinalidade de um conjunto independente de Γ (coleção de vértices sem haver dois deles conexos por uma aresta de Γ).

Os resultados desta seção encontram cotas inferiores para $\alpha(\Gamma)$ (Γ - grafo) e, portanto, para $\alpha(G)$ (G - grupo).

O seguinte teorema relaciona $\alpha(\Gamma)$ e os graus dos vértices de Γ. Esse resultado foi provado em 1980 por V. K. Wei [10] removendo um vértice v_0 de grau mínimo, todos os vértices adjacentes a v_0 e todas as arestas incidentes em qualquer um desses vértices. A demonstração apresentada aqui, de Jerry Griggs e Tom Ramsey, deleta um vértice de grau máximo.

Teorema 2.2.1 (Wei)**.** *Seja $d(v)$ o grau do vértice v no grafo Γ e $\alpha(\Gamma)$, o número de independência de Γ. Então*

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

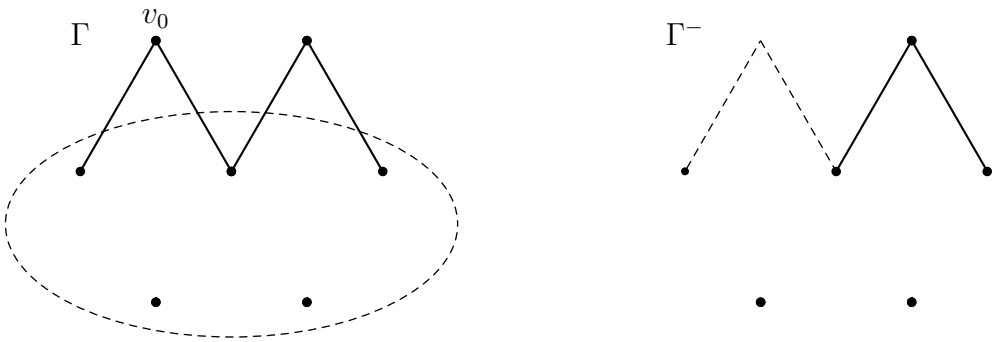
com igualdade ocorrendo se, e somente se, Γ for uma união de cliques disjuntas.

Prova. Claramente, a igualdade ocorre se Γ não tem arestas, caso em que $\alpha(\Gamma) = |\Gamma|$ e $d(v) = 0$, $\forall v \in \Gamma$, ou se Γ tem apenas 2 vértices, situação em que $\alpha(\Gamma) = 1$ e $d(v) = 1$, $\forall v \in \Gamma$. Se não tivermos essas configurações, vejamos o que acontece.

Seja v_0 um vértice de Γ de grau máximo, isto é,

$$d(v_0) \geq d(v), \forall v \in \Gamma.$$

Denote por Γ^- o grafo formado por todos os vértices de $\Gamma - \{v_0\}$ e todas as arestas de Γ não-incidentes em v_0, ou seja, o grafo induzido a partir de Γ removendo-se v_0 e todos as arestas incidentes nele.



Exemplo de Γ e Γ^- associado

Os vértices dentro da elipse em destaque nessa última figura (à esquerda) formam um conjunto independente.

Denotemos por $d^-(v)$ o grau de v em Γ^-. Para cada $v \in \Gamma^-$,

$$d^-(v) = d(v),$$

se (v, v_0) não é uma aresta de Γ, e

$$d^-(v) = d(v) - 1,$$

se (v, v_0) é uma aresta de Γ. Logo, $d^-(v) \leq d(v)$.

Segue que

$$\alpha(\Gamma) = \alpha\left(\Gamma^{-}\right) + 1,$$

se v_0 havia sido contado para $\alpha(\Gamma)$ e não existia outro subconjunto gerando $\alpha(\Gamma)$, ou

$$\alpha(\Gamma) = \alpha\left(\Gamma^{-}\right),$$

caso contrário. Assim, podemos analisar duas situações:

1^a. Se $\alpha(\Gamma) = \alpha(\Gamma^{-}) + 1$, então podemos mostrar que

$$\alpha(\Gamma) > \sum_{v\in\Gamma} \frac{1}{d(v)+1}.$$

De fato, suponha por indução sobre o número de vértices que $\alpha(\Gamma^{-}) \geq \sum_{v\in\Gamma^{-}} \frac{1}{d^{-}(v)+1}$. Daí,

$$\begin{aligned}\sum_{v\in\Gamma} \frac{1}{d(v)+1} &\leq \frac{1}{d(v_0)+1} + \sum_{v\in\Gamma^{-}} \frac{1}{d^{-}(v)+1} \\ &< 1 + \sum_{v\in\Gamma^{-}} \frac{1}{d^{-}(v)+1} \leq 1 + \alpha\left(\Gamma^{-}\right) \\ &= \alpha(\Gamma).\end{aligned}$$

2^a. Agora assuma $\alpha(\Gamma) = \alpha(\Gamma^{-})$. Pode ser provado que sempre vale

$$\sum_{v\in\Gamma^{-}} \frac{1}{d^{-}(v)+1} \geq \sum_{v\in\Gamma} \frac{1}{d(v)+1}$$

ou que, equivalentemente,

$$\sum_{v\in\Gamma^{-}} \left[\frac{1}{d^{-}(v)+1} - \frac{1}{d(v)+1}\right] \geq \frac{1}{d(v_0)+1},$$

usando que $\Gamma = \Gamma^{-} \cup \{v_0\}$. Então, vejamos.

A última desigualdade se torna

$$\sum_{\substack{v\in\Gamma^- \\ \exists(v,v_0)}} \left[\frac{1}{d^-(v)+1} - \frac{1}{d(v)+1}\right] + \sum_{\substack{v\in\Gamma^- \\ \nexists(v,v_0)}} \left[\frac{1}{d^-(v)+1} - \frac{1}{d(v)+1}\right] \geq \frac{1}{d(v_0)+1}$$

$$\Leftrightarrow \sum_{\substack{v\in\Gamma^- \\ \exists(v,v_0)}} \left[\frac{1}{d(v)} - \frac{1}{d(v)+1}\right] + \sum_{\substack{v\in\Gamma^- \\ \nexists(v,v_0)}} \left[\frac{1}{d(v)+1} - \frac{1}{d(v)+1}\right] \geq \frac{1}{d(v_0)+1},$$

pois para cada $v \in \Gamma^-$, $d^-(v) = d(v) - 1$, se (v, v_0) é uma aresta de Γ, e $d^-(v) = d(v)$, se (v, v_0) não é uma aresta de Γ. Assim, ficamos com

$$\sum_{\substack{v\in\Gamma^- \\ \exists(v,v_0)}} \frac{1}{d(v)(d(v)+1)} \geq \frac{1}{d(v_0)+1}(*),$$

o que é verdade pois o somatório do lado esquerdo possui $d(v_0)$ parcelas e cada uma delas é, no mínimo, $\frac{1}{d(v_0)(d(v_0)+1)}$ já que $d(v_0) \geq d(v)$, $\forall v \in \Gamma$, por hipótese.

Agora, assumimos $\alpha(\Gamma^-) \geq \sum_{v\in\Gamma^-} \frac{1}{d^-(v)+1}$ como hipótese de indução sobre a quantidade de vértices. Daí,

$$\alpha(\Gamma^-) \geq \sum_{v\in\Gamma^-} \frac{1}{d^-(v)+1}$$

$$\Rightarrow \alpha(\Gamma) \geq \sum_{v\in\Gamma^-} \frac{1}{d^-(v)+1} \geq \sum_{v\in\Gamma} \frac{1}{d(v)+1}.$$

Isso prova a primeira parte do teorema.

Em seguida, se Γ é a união de cliques disjuntas $\Gamma_1, \Gamma_2, ..., \Gamma_s$, então $\alpha(\Gamma) = s$ (formando o conjunto independente com um vértice de cada uma das cliques) e, em cada Γ_i, teremos

$$\sum_{v\in\Gamma_i} \frac{1}{d(v)+1} = \sum_{v\in\Gamma_i} \frac{1}{|\Gamma_i| - 1 + 1} = |\Gamma_i| \frac{1}{|\Gamma_i|} = 1.$$

Logo,

$$\sum_{v\in\Gamma} \frac{1}{d(v)+1} = \sum_{i=1}^{s} \sum_{v\in\Gamma_i} \frac{1}{d(v)+1} = \sum_{i=1}^{s} 1 = s = \alpha(\Gamma).$$

Neste momento, suponha que ocorra a igualdade $\alpha(\Gamma) = \sum_{v\in\Gamma} \frac{1}{d(v)+1}$. Como

$$\alpha(\Gamma) \geq \alpha(\Gamma^-) \geq \sum_{v\in\Gamma^-} \frac{1}{d^-(v)+1} \geq \sum_{v\in\Gamma} \frac{1}{d(v)+1},$$

devemos ter

$$\alpha(\Gamma) = \alpha(\Gamma^-) = \sum_{v\in\Gamma^-} \frac{1}{d^-(v)+1} = \sum_{v\in\Gamma} \frac{1}{d(v)+1} (**).$$

Por indução sobre o número de vértices, nós podemos assumir que Γ^- é uma união de cliques disjuntas, digamos $\Gamma_1, \Gamma_2, ..., \Gamma_r$, sendo $r = \alpha(\Gamma^-)$. Logo, $r = \alpha(\Gamma)$ (por (**)). Então v_0 deve ser adjacente a todo vértice em algum Γ_i, pois, caso contrário, existiria um conjunto independente em Γ de cardinalidade $r+1$ (v_0 e um vértice de cada Γ_i, $1 \leq i \leq r$).

Se v_0 é adjacente a todo vértice em alguma Γ_i e não tem outros vértices adjacentes, então Γ é uma união disjunta das cliques.

Senão, v_0 é adjacente a um vértice v^0 que não está em Γ_i e, então, $d(v_0) \geq |\Gamma_i| + 1$ e $d(v) = |\Gamma_i|$, para cada $v \in \Gamma_i$. Assim, como

$$\left\{v \in \Gamma^-; \exists(v, v_0)\right\} \supseteq \Gamma_i \cup \left\{v^0\right\},$$

teríamos

$$\begin{aligned}
&\sum_{\substack{v\in\Gamma^- \\ \exists(v,v_0)}} \frac{1}{d(v)\,(d(v)+1)} \\
&\geq |\Gamma_i| \frac{1}{|\Gamma_i|\,(|\Gamma_i|+1)} + \frac{1}{d(v^0)\,(d(v^0)+1)} \\
&> \frac{1}{|\Gamma_i|+1} > \frac{1}{|\Gamma_i|+1+1} \geq \frac{1}{d(v_0)+1},
\end{aligned}$$

pois $d(v_0) \geq |\Gamma_i| + 1$. Mas isso é absurdo uma vez que (*) e (**) nos dão

$$\sum_{\substack{v\in\Gamma^- \\ \exists(v,v_0)}} \frac{1}{d(v)\,(d(v)+1)} = \frac{1}{d(v_0)+1}.$$

Isso conclui essa demonstração.

□

Esse teorema nos dá o seguinte

Corolário 2.2.1. *Nas notações do Teorema 2.2.1,*

$$\alpha(\Gamma) \geq \frac{|V(\Gamma)|^2}{|V(\Gamma)| + 2\,|E(\Gamma)|},$$

com igualdade se, e somente se, Γ *for uma união disjunta de cliques de mesma cardinalidade, sendo* $E(\Gamma)$ *o conjunto das arestas e* $V(\Gamma)$*, o conjunto dos vértices de* Γ*.*

Prova. Por Cauchy-Schwartz,

$$\left(\sum_{v\in\Gamma} \frac{1}{d(v)+1}\right)\left(\sum_{v\in\Gamma} (d(v)+1)\right) \geq \left(\sum_{v\in\Gamma} 1\right)^2 = |V(\Gamma)|^2.$$

Daí,

$$\sum_{v\in\Gamma} \frac{1}{d(v)+1} \geq \frac{|V(\Gamma)|^2}{|V(\Gamma)| + 2\,|E(\Gamma)|},$$

pois

$$\sum_{v\in\Gamma} (d(v)+1) = \sum_{v\in\Gamma} d(v) + \sum_{v\in\Gamma} 1 = 2\,|E(\Gamma)| + |V(\Gamma)|.$$

Pelo Teorema 2.2.1, $\alpha(\Gamma) \geq \sum_{v\in\Gamma} \frac{1}{d(v)+1}$. Logo,

$$\alpha(\Gamma) \geq \frac{|V(\Gamma)|^2}{|V(\Gamma)| + 2\,|E(\Gamma)|}.$$

Para ocorrer a igualdade nessa última desigualdade, devemos ter $\frac{1}{\frac{d(v)+1}{d(v)+1}}$ constante, ou seja, $d(v)$ constante, pela condição de igualdade da desigualdade de Cauchy-Schwartz, e, pelo Teorema 2.2.1, Γ como uma união de cliques disjuntas.

□

Novamente, associe a G o grafo $\Gamma = \Gamma_G$ construindo uma aresta unindo os dois vértices associados a dois elementos do grupo sempre que estes comutarem. Assim, $\alpha(\Gamma)$ (ou $\alpha(G)$) denota a cardinalidade máxima dentre os subconjuntos de elementos de G que não comutam.

Definição 2.2.1. *$a(G)$ denota o número mínimo de subgrupos abelianos cuja união cobre G.*

Como no máximo um elemento de um mesmo subgrupo abeliano dos $a(G)$ que cobrem G pode ser contabilizado para $\alpha(G)$, então $\alpha(G) \leq a(G)$. Isso mostra que nossas cotas inferiores para $\alpha(G)$ também servem para $a(G)$.

Se $k(G)$ denota o número de classes de conjugação ${x_1}^G, {x_2}^G, ..., {x_{k(G)}}^G$ distintas de G e A é um subgrupo abeliano qualquer de G, então nós temos o seguinte

Corolário 2.2.2.

a) $|G| \leq \alpha(G) \cdot k(G)$;

b) $|A|^2 \leq k(G) \cdot |G|$;

c) $|A|^2 \leq \alpha(G) \cdot (k(G))^2$,

com igualdade ocorrendo em cada caso se, e somente se, G é abeliano e $A = G$ em b) e c).

Prova. Para o item a), veja que, para cada $x \in G$, o centralizador $C(x) = \{g \in G; gx = xg\}$ significa o conjunto dos vértices de Γ que estão conectados a x, além do próprio x. Logo, $d(x) = |C(x)| - 1$ (lembrando que Γ não possui loops). Assim,

$$2\,|E\,(\Gamma)| = \sum_{x \in G} d(x) = \sum_{x \in G} (|C(x)| - 1)$$

$$= \sum_{\substack{classes \\ distintas}} \left|x^G\right| |C(x)| - |G|$$

$$= k(G)\,|G| - |G|\,,$$

pois $|C(x)| \cdot \left|x^G\right| = |G| = |V(\Gamma)|\,, \forall x \in G$ e $k(G)$ é a quantidade de classes distintas. Portanto,

$$|V(\Gamma)| + 2\,|E(\Gamma)| = k(G) \cdot |V(\Gamma)|\,.$$

Pelo Corolário 2.2.1, segue que

$$\alpha(\Gamma) \geq \frac{|V(\Gamma)|}{k(G)}.$$

e a igualdade vale se, e somente se, Γ é uma união de cliques disjuntas de mesma cardinalidade. Mas sendo G um grupo, o vértice correspondente a 1 deve estar unido a todos os outros. Assim, o grafo associado a G deve ser completo e, portanto, G é abeliano,

completando a parte a).

Para provar o item seguinte, vamos assumir A subgrupo abeliano com cardinalidade máxima. Somando sobre as $k_G(A)$ G-classes distintas $a^G, a \in A$, e usando que $A = \dot{\bigcup_{a\in A}} \left(a^G \cap A\right)$, obtemos

$$\begin{aligned}
|A| &= \sum_{a\in A} \left|a^G \cap A\right| \\
&\leq \max_{a\in A} \left|a^G\right| \cdot k_G(A) \\
&= \left|a_0^G\right| \cdot k_G(A) \\
&\leq \frac{|G| \cdot k(G)}{|C(a_0)|} \\
&\leq \frac{|G| \cdot k(G)}{\min\limits_{a\in A} |C(a)|},
\end{aligned}$$

pois $k_G(A) \leq k(G)$ e $\left|a_0^G\right| |C(a_0)| = |G|$.

Além disso, como A é abeliano, $C(a)$ contém A. Assim, $\min |C(a)| \geq |A|$ e, portanto,

$$|A| \leq \frac{|G| \cdot k(G)}{|A|}$$

e

$$|A|^2 \leq |G| \cdot k(G).$$

Se G é abeliano ($k(G) = |G|$) e $A = G$ ($|A| = |G|$), então ocorre a igualdade.

Agora, assuma que tenhamos a igualdade. Se vale a igualdade, então

$$\begin{aligned}
|A| &= \frac{|G| \cdot k(G)}{\min\limits_{a\in A} |C(a)|} \\
&= \frac{|G| \cdot k(G)}{|A|}
\end{aligned}$$

e, assim, $|C(a)| = |A|, \forall a \in A$ e, então,

$$|a^G| = |b^G|, \forall a, b \in A.$$

Logo

$$|a^G| = 1, \forall a \in A,$$

pois $|1^G| = 1$, o que dá A abeliano.

Temos ainda

$$|G| = |a^G|\,|C(a)| = 1 \cdot |A| = |A|,$$

que dá $G = A$.

Finalmente, c) segue diretamente de a) e b).

□

Recordemos os grupos diedrais de ordem $2n$, n inteiro positivo. Eles são dados por

$$D_{2n} = \langle x, y; x^2 = y^n = 1, xyx = y^{-1} \rangle$$

$$= \{1, y, y^2, ..., y^{n-1}, x, xy, xy^2, ..., xy^{n-1}\}.$$

Exemplo 2.2.1. *Para os grupos diedrais $G = D_{2n}$,*

$$k(D_{2n}) = \begin{cases} \frac{n+3}{2} & se \quad n \equiv 1 \mod 2 \\ \frac{n}{2} + 3 & se \quad n \equiv 0 \mod 2 \end{cases}$$

De fato,

i) se n é ímpar, então temos as classes 1^G, $\{x, xy, xy^2, ..., xy^{n-1}\}$ e $(y^j)^G$, com $j = 1, 2, ..., \frac{n-1}{2}$, num total de

$$2 + \frac{n-1}{2} = \frac{n+3}{2}$$

classes. (A idéia de encontrar tais classes é semelhante à usada no exemplo 2.1.1)

ii) se n é par, então temos as classes 1^G, $\{x, xy^2, ..., xy^{n-2}\}$, $\{xy, xy^3, ..., xy^{n-1}\}$, $\left(y^{\frac{n}{2}}\right)^G$ e $(y^j)^G$, com $j = 1, 2, ..., \frac{n-2}{2}$, num total de

$$4 + \frac{n-2}{2} = \frac{n}{2} + 3$$

classes.

Em cada um dos casos acima, o subgrupo abeliano $A = \langle y; y^n = 1\rangle$ de ordem n cumpre

$$\lim_{n\to\infty} \frac{k \cdot |G|}{|A|^2} = 1,$$

pois $|G| = 2n = 2|A|$, nesse caso.

■

Vejamos agora exemplos de grupos em que ocorre $\alpha(G) = a(G)$.

Exemplo 2.2.2. *Com n ímpar, os grupos diedrais $G = D_{2n}$ mostram que*

$$\alpha(G) = a(G) = \frac{1}{2}|G| + 1.$$

De fato, Mason mostra em [7] que quando o centro do grupo é trivial (que é o caso de D_{2n}, n ímpar), então

$$a(G) \leq \frac{1}{2}|G| + 1.$$

Por outro lado,

$$\{x, y, xy, xy^2, ..., xy^{n-1}\}$$

mostra que $\alpha(G) = n + 1$. Assim, ocorre a igualdade.

■

Exemplo 2.2.3. *Se G é não-abeliano, $|G| = pq$, em que $p < q$ são primos e $q \equiv 1 \mod p$, então todos os seus subgrupos próprios, inclusive seus centralizadores, são abelianos por terem ordens primas. Daí, $\alpha(G) = a(G)$.*

Na verdade, todo grupo não-abeliano G, em que todos os centralizadores diferentes de G são abelianos, satisfaz $\alpha(G) = a(G)$. De fato, sendo

$$g_1, g_2, ..., g_{\alpha(G)}$$

a maior coleção de elementos de G sem comutatividade dois a dois, temos

$$G = \bigcup_{j=1}^{\alpha(G)} C(g_j),$$

pois cada $x \in G$ deve comutar com pelo menos um dos g_i.

Como cada centralizador $C(g_j)$ é abeliano, segue que

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

Mas $\alpha(G) \leq a(G)$ sempre. Logo, ocorre a igualdade.

■

Exemplo 2.2.4. *Se G é não-abeliano, $|G| = pq^2$, em que p e q são primos e $q < p < q^2$, então todos os seus centralizadores diferentes de G são abelianos.*

Para mostrar essa afirmação, seja $x \neq 1$ um elemento de G, $o(x)$, a ordem de x em G e $C(x)$, o centralizador de x em G. Considere também o subgrupo $N = \langle x \rangle$ gerado por x, cujo centralizador em G é $C_G(N) = C(x)$, pois N é cíclico. Denotemos $C_G(N) = C(x) = C$. Claramente, $N \trianglelefteq C$.

O teorema de Lagrange garante que $o(x)$ divide pq^2. Assim, analisaremos os seguintes casos:

i) $o(x) = pq$.

Nesse caso, $C = N$ pois C é um subgrupo próprio. Logo, C é cíclico e, portanto, abeliano.

ii) $o(x) = q^2$.

Análogo ao caso anterior.

iii) $o(x) = p$.

Se $C = N$, então novamente temos C abeliano. Senão, $|C| = pq$, pois $C \neq G$.

Seja H um q-subgrupo de Sylow de C. Daí, $|H| = q$. Além disso, $N \triangleleft C$ garante que $HN \leq C$. Como $|N| = p$ nesse caso, $|HN| = pq$ e, portanto, $C = HN$.

Como N centraliza H (pois H está contido em C), então N normaliza H. Além disso, é claro que H normaliza H. Segue que H é subgrupo normal de $HN = C$.

Por outro lado, $(|H|, |N|) = 1$. Assim, $C = H \times N$ e C é cíclico. Portanto, C é abeliano também nesse caso.

iv) $o(x) = q$.

Vamos supor $C \neq N$ (caso contrário, não temos mais nada a fazer).

Se $|C| = q^2$, então C é abeliano.

Senão, $|C| = pq$. Daí, podemos aplicar os teoremas de Sylow e mostrar que C possui um único p-subgrupo de Sylow. Sendo H esse subgrupo, segue que $H \triangleleft C$. Aqui também ocorre $(|H|, |N|) = 1$ e, como no caso anterior, C é abeliano novamente.

Daí, todo centralizador próprio de G é abeliano e, portanto, $\alpha(G) = a(G)$, pelo exemplo 2.2.3.

■

Exemplo 2.2.5. *No exemplo 2.2.3, vimos que se em um grupo G não-abeliano todos os centralizadores diferentes de G são abelianos, então $\alpha(G) = a(G)$. Mas essa condição não é necessária.*

Com efeito, no grupo não-abeliano S_4 (das simetrias dos símbolos $1, 2, 3, 4$) o centralizador de $(1\ 2)(3\ 4)$ não é abeliano (de fato, $(1\ 3)(2\ 4)$ e $(3\ 4)$ estão nesse centralizador e não comutam entre si).

Além disso, S_4 é coberto por 10 subgrupos abelianos:

$$\langle (1\ 2\ 3\ 4) \rangle, \langle (1\ 3\ 2\ 4) \rangle, \langle (1\ 2\ 4\ 3) \rangle,$$

$$\langle(1\ 2\ 3)\rangle, \langle(1\ 2\ 4)\rangle, \langle(1\ 3\ 4)\rangle, \langle(2\ 3\ 4)\rangle,$$

$$\{(1\ 2), (3\ 4), (1\ 2)(3\ 4), 1\},$$

$$\{(1\ 3), (2\ 4), (1\ 3)(2\ 4), 1\},$$

$$\{(1\ 4), (2\ 3), (1\ 4)(2\ 3), 1\},$$

que se intersectam dois a dois apenas em $\{1\}$*. Logo,* $a(S_4) \leq 10$*.*

Por outro lado, os 7 primeiros geradores da cobertura acima juntamente com $(1\ 2), (1\ 3)$ *e* $(1\ 4)$ *formam uma coleção de 10 permutações sem comutatividade duas a duas. Assim,* $\alpha(S_4) \geq 10$*.*

Portanto,

$$10 \leq \alpha(S_4) \leq a(S_4) \leq 10$$

o que dá

$$\alpha(S_4) = a(S_4) = 10.$$

■

2.3 Grupos com Cota Superior para $\alpha(G)$

Lema 2.3.1. *Seja* G *um grupo finito não-abeliano com* $k(G)$ *classes de conjugação distintas tal que*

$$\alpha(G) \leq |G|^r - 1, 0 < r < 1.$$

Então:

a) Para cada $x \in G, |C(x)| \geq |G|^{\frac{1-r}{2}}$*.*

b) Existe um elemento $g \in G - Z(G)$ *com* $|C(g)| > |G|^{1-r}$ *e* $|C(x) \cap C(g)| > |G|^{\frac{1-3r}{2}}$*, para cada* $x \in G$*.*

c) Finalmente, em todo grupo finito G, pelo menos $k(G)-\alpha(G)$ das classes de conjugação distintas em G satisfazem $\left|x^G\right| < |G|^{\frac{1}{2}}$.

Prova. a) Veja que

$$\frac{1}{|G|}\sum_{\substack{classes\\distintas}}\left|x^G\right|^2 = \sum_{\substack{classes\\distintas}}\frac{\left|x^G\right|^2}{|G|} = \sum_{\substack{classes\\distintas}}\frac{\left|x^G\right|}{|C(x)|} = \sum_{x\in G}\frac{1}{|C(x)|},$$

pois $|G| = |C(x)||x^G|, \forall x \in G$.

Do Teorema 2.2.1, temos

$$\alpha(G) \geq \sum_{x\in G}\frac{1}{d(x)+1} = \sum_{x\in G}\frac{1}{|C(x)|}.$$

Daí,

$$\frac{1}{|G|}\sum_{\substack{classes\\distintas}}\left|x^G\right|^2 \leq \alpha(G) \leq |G|^r - 1 < |G|^r$$

$$\Rightarrow \sum_{\substack{classes\\distintas}}\left|x^G\right|^2 < |G|^{r+1}$$

$$\Rightarrow \left|x^G\right|^2 < |G|^{r+1}, \forall x \in G,$$

já que $\left|x^G\right|^2 \leq \sum_{\substack{classes\\distintas}}\left|x^G\right|^2, \forall x \in G$. Logo, obtemos sucessivamente

$$|x^G| < |G|^{\frac{r+1}{2}}, \frac{|G|}{|C(x)|} < |G|^{\frac{r+1}{2}}$$

e

$$|C(x)| > |G|^{\frac{1-r}{2}}.$$

b) Novamente do Teorema 2.2.1,

$$\alpha(G) \geq \sum_{x \in G} \frac{1}{|C(x)|} = \sum_{x \in G - Z(G)} \frac{1}{|C(x)|} + \sum_{x \in Z(G)} \frac{1}{|C(x)|}$$

$$= \sum_{x \in G - Z(G)} \frac{1}{|C(x)|} + \frac{|Z(G)|}{|G|},$$

desde que os centralizadores dos elementos do centro $Z(G)$ são exatamente G.

Suponha que $|C(x)| \leq |G|^{1-r}, \forall x \in G - Z(G)$. Daí,

$$\alpha(G) - \frac{|Z(G)|}{|G|} \geq \sum_{x \in G - Z(G)} \frac{1}{|G|^{1-r}}$$

$$= \frac{|G| - |Z(G)|}{|G|^{1-r}} = |G|^r - \frac{|Z(G)|}{|G|^{1-r}}.$$

Da hipótese,

$$\alpha(G) - \frac{|Z(G)|}{|G|} \leq |G|^r - 1 - \frac{|Z(G)|}{|G|}.$$

Assim,

$$|G|^r - \frac{|Z(G)|}{|G|^{1-r}} \leq |G|^r - 1 - \frac{|Z(G)|}{|G|},$$

donde

$$1 \leq \frac{|Z(G)|}{|G|^{1-r}} - \frac{|Z(G)|}{|G|}$$

e

$$\frac{1}{|Z(G)|} \leq \frac{1}{|G|^{1-r}} - \frac{1}{|G|} < \frac{1}{|G|^{1-r}}.$$

Mas $|Z(G)| \leq |C(x)|, \forall x \in G$ e $|C(x)| \leq |G|^{1-r}$ para $x \in G - Z(G)$ por hipótese. Portanto,

$$|Z(G)| \leq |G|^{1-r},$$

contradizendo o parágrafo anterior. Logo, existe g em $G - Z(G)$ tal que $|C(g)| > |G|^{1-r}$.

Em seguida, de $|C(x) \cap C(g)| = \frac{|C(x)||C(g)|}{|C(x)C(g)|}$ e $|C(x)C(g)| \leq |G|$ (pois $C(x)C(g) \subseteq G$), obtemos

$$|C(x) \cap C(g)| \geq \frac{|C(x)|\,|C(g)|}{|G|}.$$

Segue que

$$|C(x) \cap C(g)| > \frac{|G|^{\frac{1-r}{2}} \cdot |G|^{1-r}}{|G|} = |G|^{\frac{1-3r}{2}},$$

pois $|C(x)| \geq |G|^{\frac{1-r}{2}}$ pelo item anterior.

c) Denote por $l(G)$ o número de classes de conjugação distintas de G satisfazendo $\left|x^G\right|^2 < |G|$. Segue que $k(G) - l(G)$ classes cumprem $\left|x^G\right|^2 \geq |G|$ ($k(G)$ é o total de classes de conjugação distintas). Daí,

$$\sum_{\substack{classes\\distintas}} \left|x^G\right|^2 \geq \sum_{\substack{classes\\distintas\\|x^G|^2 \geq |G|}} \left|x^G\right|^2 \geq |G|\left(k(G) - l(G)\right).$$

Na prova do item a), vimos que

$$\sum_{\substack{classes\\distintas}} \left|x^G\right|^2 \leq \alpha(G)|G|.$$

Assim, $\alpha(G) \geq k(G) - l(G)$ e, portanto,

$$l(G) \geq k(G) - \alpha(G).$$

□

Como observação a esse último Lema, suponha que

$$\left|x^G\right| \geq |G|^r,$$

para toda classe não-central de G. Assim, estamos negando o resultado obtido no item b) desse Lema e, portanto, a hipótese não ocorre, isto é,

$$\alpha(G) > |G|^r - 1$$

e

$$\alpha(G) \geq \lfloor |G|^r \rfloor .$$

Em particular, se $r = \frac{1}{2}$, então obtemos

$$\alpha(G) \geq \left\lfloor |G|^{\frac{1}{2}} \right\rfloor .$$

Além disso, ainda com $r = \frac{1}{2}$, $\left|x^G\right| < |G|^{\frac{1}{2}}$ se, e somente se, $x \in Z(G)$ (pois $\left|x^G\right| = 1$ se $x \in Z(G)$). Logo, $l(G) = |Z|$. Usando o desenvolvimento do item c), temos

$$|Z| = l(G) \geq k - \alpha(G),$$

ou seja,

$$\alpha(G) \geq k - |Z|.$$

Agora, vamos comparar $\left\lfloor |G|^{\frac{1}{2}} \right\rfloor$ e $k - |Z|$ para saber qual é o melhor limite inferior para $\alpha(G)$ no caso em que $r = \frac{1}{2}$.

Como $|x^G| \geq |G|^{\frac{1}{2}}$ para as $k - |Z|$ classes não-centrais, passando o somatório sobre essas classes, obtemos

$$|G| - |Z| \geq |G|^{\frac{1}{2}} (k - |Z|) .$$

Mas $|G| > |G| - |Z|$. Segue que

$$|G| > |G|^{\frac{1}{2}} (k - |Z|)$$

e

$$k - |Z| < |G|^{\frac{1}{2}},$$

ou seja, $\alpha(G) \geq k - |Z|$ não melhora o limite inferior dado por

$$\alpha(G) \geq \left\lfloor |G|^{\frac{1}{2}} \right\rfloor .$$

Outra observação é que nem sempre vale $k(G) - \alpha(G) \geq 0$. Nosso exemplo é o grupo A_4 das permutações pares de ordem 4. Por um lado, $G = A_4$ possui 4 classes de conjugação:

1^G, $(1\ 2)(3\ 4)^G$ (a união dessas duas classes forma o conhecido Grupo de Klein), $(1\ 2\ 3)^G$, $(2\ 3\ 4)^G$. Logo, $k(A_4) = 4$. Por outro, $\alpha(A_4) = 5$, tomando cada um dos elementos de $(1\ 2\ 3)^G$ além de $(1\ 2)(3\ 4)$.

2.4 Mais Cotas Inferiores para $\alpha(G)$

A partir do Lema 2.3.1, obtemos como conseqüência mais uma cota inferior para $\alpha(G)$, nos casos em que o grupo contém um subgrupo M fechado para os centralizadores (isto é, sempre que $x \in M - \{1\}$, tem-se $C_G(x) \leq M$) e em que existe um elemento de um grupo não-abeliano com centralizador de cardinalidade prima.

Teorema 2.4.1. *Seja G um grupo contendo um subgrupo próprio M tal que sempre que $x \in M - \{1\}$, tem-se $C_G(x) \leq M$. Então*

$$\alpha(G) \geq \left\lfloor |G|^{\frac{1}{3}} \right\rfloor.$$

Prova. Suponha

$$\alpha(G) < \left\lfloor |G|^{\frac{1}{3}} \right\rfloor \leq |G|^{\frac{1}{3}},$$

ou seja,

$$\alpha(G) \leq |G|^{\frac{1}{3}} - 1.$$

Essa é exatamente a hipótese do Lema 2.3.1 se $r = \frac{1}{3} \in (0, 1)$. Pelo item b) desse lema, $\exists g \in G - Z(G)$ com

$$|C(x) \cap C(g)| > |G|^{\frac{1-3r}{2}} = 1, \forall x \in G,$$

o que indica que $C(x) \cap C(g)$ possui elemento diferente de 1, uma contradição pois se

i) $g \in M - \{1\}$, então $C(g) \leq M$. Tome $x \notin M$ (pois M é subgrupo próprio).

   Se $y \in M - \{1\}$, então $C(y) \leq M$, ou seja, os elementos que comutam com y estão todos em M. Assim, $xy \neq yx$ e $y \notin C(x)$.

   Se $y \in G - M$, então $y \notin C(g)$ (desde que $C(g) \leq M$).

   Assim, $C(x) \cap C(g) = \emptyset$.

ii) $g \notin M$, tome $x \in M - \{1\}$ e, portanto, $C(x) \leq M$.

Se $y \in G - M$, então $y \notin C(x)$ (como no caso anterior).

Se $y \in M - \{1\}$, então $C(y) \leq M$, o que dá $y \notin C(g)$ (pois se $y \in C(g)$, então $g \in C(y)$, dando $g \in M$, que contraria a hipótese).

Novamente, $C(x) \cap C(g) = \emptyset$.

Segue que $\alpha(G) \geq \left\lfloor |G|^{\frac{1}{3}} \right\rfloor$.

□

Vamos a mais um

Corolário 2.4.1. *Seja p um primo qualquer dividindo a ordem de um grupo não-abeliano G. Se existe um elemento $x \in G$ tal que $|C(x)| = p$, então*

$$\alpha(G) \geq \left\lfloor |G|^{\frac{1}{3}} \right\rfloor.$$

Prova. Basta mostrar que $C(x)$ cumpre as condições de M do Teorema 2.4.1.

Como p é primo, $C(x)$ é abeliano e cíclico. Denotemos $C(x) = \{1, x, x^2, ..., x^{p-1}\}$, o que dá $o(x) = p$. Vamos mostrar que para $y \in C(x) - 1$, digamos $y = x^k, k \in \{1, 2, ..., p-1\}, C(y) = C(x)$.

Obviamente,

$$x\beta = \beta x, \forall \beta \in C(x).$$

Logo,

$$x^k\beta = \beta x^k, \forall \beta \in C(x).$$

Assim, $C(x) \subseteq C(y)$.

Seja $\beta \in C(y)$. Como $(k, p) = 1$, existem a e b inteiros tais que $ak + bp = 1$, dando

$$x^{ak+bp} = x,$$

que implica

$$x^{ak} \cdot x^{bp} = x$$

e, portanto,

$$x^{ak} = x.$$

Mas de $x^k\beta = \beta x^k$ resulta

$$x^{ak}\beta = \beta x^{ak},$$

ou seja,

$$x\beta = \beta x, \forall \beta \in C(x).$$

Logo, $C(y) \subseteq C(x)$.

Segue que $C(x) = C(y)$.

□

Exemplo 2.4.1. *Um grupo G é dito de Frobenius se existe $\{1\} \neq H < G$ tal que*

$$H^x \cap H = \{1\}, \forall x \in G, x \notin H.$$

Grupos de Frobenius são exemplos de grupos contendo subgrupo fechado para os centralizadores. Com efeito, seja $h \in H - \{1\}$ e $x \in C(h)$ (isto é, $xh = hx$). Se $x \notin H$, então

$$h^x = h \in H^x \cap H$$

e, portanto, $h = 1$, absurdo. Logo, $x \in H$ e, conseqüentemente, $C(h) \subset H$.

■

Exemplo 2.4.2. *Outro exemplo de grupo G contendo subgrupo fechado para os centralizadores é um grupo de permutação transitivo de p (p primo) símbolos ($G \leq S_p$) agindo transitivamente sobre $X = \{1, 2, ..., p\}$.*

Sejam

$$G_x = \{g \in G; g(x) = x\}, x \in X,$$

e

$$O_x = \{g(x); g \in G\}$$

a órbita de $x \in X$*. Logo,*

$$|O_x| = |G : G_x|\,.$$

Como a ação é transitiva, existe apenas uma órbita, cuja ordem é, portanto, p*.*

A idéia, a partir de agora, será mostrar que um p*-subgrupo de Sylow* $P \leq G$ *é fechado para os centralizadores. Como a maior potência de* p *dividindo* $p!$ *é* p*, segue que* $|P| = p$*. Daí,* P *é cíclico, isto é,* $\exists a \in G$ *com* $o(a) = p$ *tal que* $P = \langle a \rangle$*.*

Precisamos mostrar que $C(a) \subseteq P, \forall a \in P$*. Na verdade, podemos demonstrar que* $C(P) = P$*.*

Como $o(a) = p$*, temos que* a *é um* p*-ciclo. Daí,* $P \cap G_x = \{1\}$*.*

Além disso, $|G : P|$ *divide* $\frac{p!}{p} = (p-1)!$ *e* $|G : G_x| = p$*. Portanto,* $(|G : P|, |G : G_x|) = 1$*. Logo,* $G = PG_x$*.*

Afirmação. $C(P) \cap G_x = \{1\}$.

Prova. Dado $b \in C(P) \cap G_x$, então

$$ba(x) = ab(x) = a(x),$$

pois $b \in C(P), a \in P$ e $b(x) = x$, já que $b \in G_x$.

Assim,

$$ba^2(x) = aba(x) = a^2(x).$$

Por indução, temos

$$ba^r(x) = a^r(x), \forall r.$$

Logo, $b = 1$ e segue o resultado. □

Como $C(P) \subset G = PG_x$*, segue que* $C(P) = PG_x \cap C(P)$*. Pela regra de Dedekind,*

$$PG_x \cap C(P) = P\,(C(P) \cap G_x) = P,$$

pois $P \leq C(P)$*. Assim,* $C(P) = P$*.*

■

2.5 Uma Cota Superior para $a(G)$

Finalizando este capítulo, lembrando novamente que $a(G)$ representa a quantidade mínima de subgrupos abelianos que cobrem o grupo G, passemos ao seguinte

Teorema 2.5.1. *Definamos uma função $f(n)$ indutivamente por $f(1) = 1$ e*

$$f(n) = n + \binom{n}{2} f(n-1).$$

Se $\alpha(G) < \infty$, então

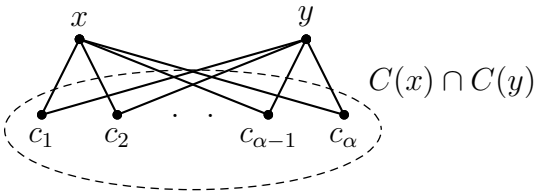
$$a(G) \leq f(\alpha(G)).$$

Em particular, $a(G) < \infty$.

Prova. Denote $\alpha(G) = \alpha$. Sejam $x, y \in G$ com $xy \neq yx$. Suponha que existam

$$c_1, c_2, ..., c_\alpha \in C(x) \cap C(y)$$

(ou seja, $xc_j = c_j x$ e $yc_j = c_j y, \forall j \in \{1, 2, ..., \alpha\}$) elementos não comutando dois a dois.



Então dois dos elementos $x, c_1 y, c_2 y, ..., c_\alpha y$ devem comutar, pois α é a quantidade máxima de elementos em G sem haver dois que comutem.

Suponha que x comute com algum $c_j y$. Então, como $c_j \in C(x)$,

$$xc_j y = c_j yx.$$

Portanto,

$$c_j xy = c_j yx$$

e

$$xy = yx.$$

absurdo.

Agora, suponha que existam $c_i y$ e $c_j y$ comutando, ou seja,

$$c_i y c_j y = c_j y c_i y.$$

Daí,

$$c_i c_j y^2 = c_j c_i y^2$$

e, portanto,

$$c_i c_j = c_j c_i,$$

novamente uma contradição. Assim,

$$\alpha\left(C(x) \cap C(y)\right) < \alpha(G),$$

sempre que $xy \neq yx$.

Agora, sejam $x_1, x_2, ..., x_\alpha$ elementos que não comutam dois a dois e defina

$$B_{jk} = C(x_j) \cap C(x_k),$$

para $j \neq k$, num total de $\binom{\alpha}{2}$ conjuntos. Como $x_j x_k \neq x_k x_j$, temos

$$\alpha(B_{jk}) < \alpha(G)$$

pelo parágrafo anterior e, portanto,

$$\alpha(B_{jk}) \leq \alpha - 1.$$

Por indução sobre α, segue que

$$a(B_{jk}) \leq f\left(\alpha(B_{jk})\right) \leq f(\alpha - 1)$$

(pois f é crescente). Assim, B_{jk} pode ser coberto por $f(\alpha - 1)$ subgrupos abelianos.

Seja agora $A_j = C(x_j) - \bigcup_{k \neq j} B_{jk}, 1 \leq j \leq \alpha$.

Afirmação. $\langle A_j \rangle$ é abeliano, $1 \leq j \leq \alpha$.

Prova(Afirmação): Sejam $u, v \in A_j$. Então,

$$x_1, ..., x_{j-1}, u, x_{j+1}, ..., x_\alpha (j \leq \alpha)$$

formam um conjunto C de α elementos que não comutam dois a dois, pois, pela definição de A_j, u não comuta com x_k, $k \in \{1, ..., j-1, j+1, ..., \alpha\}$.

Mas em

$$C \cup \{v\}$$

há $\alpha+1$ elementos e, portanto, dois deles comutam. Logo, v comuta com algum elemento de C. Como u e v estão em A_j, que não contém elementos que comutam com os demais de C pela definição de A_j, esses elementos comutam e $\langle A_j \rangle$ é abeliano. □

Portanto, $a(\langle A_j \rangle) = 1, \forall j$.

Como

$$G = \bigcup_{1 \leq j \leq \alpha} \langle A_j \rangle \cup \bigcup_{1 \leq j \leq \alpha} B_{jk},$$

segue que

$$a(G) \leq \alpha + \binom{\alpha}{2} f(\alpha - 1) = f(\alpha(G)).$$

□

Obtemos, assim, uma cota superior para $a(G)$.

Outra cota superior muito interessante para $a(G)$ foi utilizada no exemplo 2.2.2 e é devida a D.R. Mason [7]: quando o centro do grupo G é trivial, isto é, $Z = \{1\}$ e $|Z| = 1$, há no máximo $\frac{1}{2}|G| + 1$ subgrupos abelianos que cobrem G.

Capítulo 3

SUBCONJUNTOS LIVRES DE SOMAS

Neste capítulo, todos os grupos são aditivos abelianos. Começamos apresentando algumas definições para grupos aditivos, seguidas de resultados básicos e exemplos. Os resultados relacionarão os conjuntos $S+S$, $S-S$ e $\frac{1}{2}S$, sendo S um subconjunto livre de somas ou livre de somas localmente maximal do grupo G. Nesta parte a colaboração da Teoria dos Grafos virá da seguinte associação: dois vértices serão adjacentes se, e somente se, sua diferença pertence a $S-S$, sendo S um subconjunto livre de somas localmente maximal em um grupo G. Alguns fatos são complementados nos dois apêndices a seguir.

3.1 Introdução

Definição 3.1.1. *Seja G um grupo finito. Um subconjunto S de G é chamado* ***livre de somas*** *se sempre que $x, y \in S$, então $x+y \notin S$. Além disso, sejam*

$$S+S = \{x+y; x, y \in S\}$$

e

$$S-S = \{x-y; x, y \in S\}.$$

Exemplo 3.1.1. *$\emptyset$ é trivialmente livre de somas.*

■

Exemplo 3.1.2. *Sendo $\mathbb{Z}_6 = \{0,1,2,3,4,5\}$ e $S = \{1,3\} \subset \mathbb{Z}_6$, S é um subconjunto livre de somas de $\mathbb{Z}_6$.*

■

Exemplo 3.1.3. $\{1\}$ *é subgrupo não-vazio livre de somas em qualquer grupo.*

■

Lema 3.1.1. *S é livre de somas se, e somente se, $S \cap (S+S) = \emptyset = S \cap (S-S)$.*

Prova. $\Rightarrow$) Dado $x \in S+S$, $\exists a, b \in S$ tais que $x = a+b$. Daí, $x \notin S$ pois S é livre de somas. Logo,

$$S \cap (S+S) = \emptyset.$$

Dado $x \in S-S$, $\exists a, b \in S$ tais que $x = a-b$, que não pertence a S pois b e $(a-b)+b = a$ estão em S, que é livre de somas. Logo,

$$S \cap (S-S) = \emptyset.$$

$\Leftarrow$) Se $x, y \in S$, então $x+y \in S+S$. Como $S \cap (S+S) = \emptyset$, temos $x+y \notin S$. Logo, S é livre de somas.

□

Esse lema será bastante utilizado nas demonstrações seguintes.

Definição 3.1.2. *Define-se $\frac{1}{2}S = \{x \in G; 2x \in S\}$, sendo G um grupo.*

Lema 3.1.2. *Se S é livre de somas, então $\frac{1}{2}S$ é livre de somas.*

Prova. Suponha $x, y \in \frac{1}{2}S$. Então, $2x$ e $2y$ estão em S. Como S é livre de somas,

$$2x + 2y = 2(x+y) \notin S$$

e, portanto, $x+y \notin \frac{1}{2}S$. Assim, $\frac{1}{2}S$ é livre de somas também. □

Lema 3.1.3. *Seja G um grupo finito. Se $|G|$ é ímpar e $S \subseteq G$, então*

$$\left|\frac{1}{2}S\right| = |S|.$$

Prova. Defina $f : \frac{1}{2}S \to S$ dada por $f(x) = 2x$. Se mostrarmos que f é bijetora, segue o resultado.

Dado $x \in S$, então $\frac{x}{2} \in \frac{1}{2}S$ por definição. Logo, f é sobrejetora.

Suponha $f(x) = f(y)$. Daí, $2x = 2y$ e $2(x - y) = 0$. Logo, $o(x - y)|2$. Mas $|G|$ é ímpar, o que dá $o(x - y) = 1$, ou seja, $x - y = 0$ e $x = y$. Assim, f é injetora.

Portanto, f é bijetora. □

Lema 3.1.4. *Sejam $A, B \subseteq G$, sendo G um grupo. Então,*

$$G = A + B \quad ou \quad |G| \geq |A| + |B|.$$

Prova. Se $G \neq A + B$, então escolha $g \in G$ tal que $g \notin A + B$ (tal elemento existe pois $A + B \subseteq G$, já que G é um grupo). Defina o conjunto

$$B' = \{g - b; b \in B\}.$$

Assim,

$$|B'| = |B|,$$

além de $B' \subseteq G$.

Agora, suponha que $A \cap B' \neq \emptyset$. Então, existe $a \in A \cap B'$. Logo,

$$a = g - b \Leftrightarrow g = a + b,$$

o que contradiz a definição de g. Logo, $A \cap B' = \emptyset$ e, portanto,

$$|G| \geq |A| + |B'| = |A| + |B|,$$

pois $A \cup B' \subseteq G$ e $|A \cup B'| = |A| + |B'| - |A \cap B'|$. □

3.2 Subconjuntos Livres de Somas Localmente Maximais

Definição 3.2.1. *Seja G m grupo finito. Um subconjunto S de G* ***livre de somas*** *é chamado* ***localmente maximal*** *se, sempre que T é um subconjunto livre de somas de G e $S \subseteq T$, tivermos $S = T$ necessariamente.*

Exemplo 3.2.1. *Sendo $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ e $S = \{1, 3, 5\} \subset \mathbb{Z}$, S é um subconjunto livre de somas localmente maximal de $\mathbb{Z}_6$, pois $0 = 0+0$, $2 = 1+1$ e $4 = 1+3$ não podem ser inseridos (caso contrário, o subconjunto não seria livre de somas).*

■

Conjuntos livres de somas localmente maximal têm sido estudados devido à sua relação com os números de Ramsey

$$R(\underbrace{3, 3, ..., 3}_{k}),$$

que é o menor inteiro positivo n tal que em qualquer coloração das arestas com k cores do grafo completo K_n existe (pelo menos) um triângulo monocromático. Mais detalhes a respeito desse assunto podem ser vistos no Apêndice A.

Lema 3.2.1. *Seja G um grupo abeliano finito e S, um subconjunto de G livre de somas localmente maximal. Então*

$$|S| \leq \frac{1}{2}|G|.$$

Em particular, como todo $R \subset G$ livre de somas está contido em um subconjunto livre de somas localmente maximal, temos que $|R| \leq \frac{1}{2}|G|$ ocorre para qualquer $R \subset G$ livre de somas.

Prova. Pelo Lema 3.1.4,

$$G = S + S \text{ ou } |G| \geq 2|S|.$$

Como S é livre de somas , então $(S + S) \cap S = \emptyset$. Se $G = S + S$, então

$$G \cap S = \emptyset,$$

o que implicaria $S = \emptyset$ já que $S \subset G \neq \emptyset$. Mas isso é um absurdo pois S é livre de somas localmente maximal. Assim,

$$|G| \geq 2|S|.$$

□

Lema 3.2.2. *Seja G um grupo finito. Se $|G|$ é par e S é um subconjunto livre de somas de G, então*

$$\left|\frac{1}{2}S\right| \leq \frac{1}{2}|G|.$$

Prova. Pelo lema anterior, todo conjunto livre de somas em um grupo finito qualquer tem cardinalidade menor que ou igual a $\frac{1}{2}|G|$ e, pelo Lema 3.1.2, $\frac{1}{2}S$ é livre de somas.

Por outro lado,

$$\left|\frac{1}{2}S\right| = \frac{1}{2}|G|$$

ocorre quando

$$S = \{2 + 4i\}_0^{n-1} \subset \mathbb{Z}_{4n}.$$

Por fim, o exemplo $G = \mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ e $S = \{0, 1, 2, 3\}$ mostra que se S não for livre de somas, então o resultado não necessariamente é verdadeiro, pois $\frac{1}{2}S = \{0, 1, 3, 4\}$ dá $\left|\frac{1}{2}S\right| = 4 > 3 = \frac{1}{2}|G|$. □

Exemplo 3.2.2. *No exemplo dado na prova do Lema 3.2.2 para $\left|\frac{1}{2}S\right| = \frac{1}{2}|G|$,*

$$S = \{2, 6, 10, 14, ..., 4n - 2\} \subset \mathbb{Z}_{4n}$$

e

$$\frac{1}{2}S = \{1, 3, 5, ..., 2n - 1, 2n + 1, 2n + 3, ..., 4n - 1\}.$$

Portanto, $\left|\frac{1}{2}S\right| = 2|S|$.

Por outro lado, o conjunto livre de somas

$$S = \{(2, 0), (2, 2), (2, 3)\} \subset \mathbb{Z}_4 \oplus \mathbb{Z}_4$$

e não localmente maximal, pois $S \cup \{(2,1)\}$ é livre de somas, mostra que não necessariamente ocorre $\left|\frac{1}{2}S\right| \leq 2\,|S|$, uma vez que

$$\frac{1}{2}S = \{(1,0),(3,0),(1,2),(3,2),(1,1),(3,3),(3,1),(1,3)\}.$$

Seria verdade que S livre de somas localmente maximal implica $\left|\frac{1}{2}S\right| \leq 2\,|S|$?

■

Teorema 3.2.1. *Seja G um grupo e S, um conjunto livre de somas localmente maximal em G. Seja c uma constante positiva. Então:*

i) $G = S \cup (S+S) \cup (S-S) \cup \frac{1}{2}S$.

ii) Se $|G|$ é ímpar, então $|S| \geq \frac{1}{6}\left((24|G|-15)^{\frac{1}{2}} - 3\right)$.

iii) Se $|G|$ é par, então $|S| \geq \frac{1}{6}\left((12|G|-23)^{\frac{1}{2}} - 1\right)$.

iv) Se $|S+S| \leq c|S|$, então

$$|S| \geq \frac{|G|}{c^2+c+2}$$

para $|G|$ ímpar e

$$|S| \geq \frac{|G|}{2(c^2+c+1)}$$

para $|G|$ par.

Prova.

i) Suponha $x \in G - S \cup (S+S) \cup (S-S)$. Sendo $S = \{s_1, s_2, ..., s_n\}$, $S \cup \{x\} = \{x, s_1, s_2, ..., s_n\}$ não é livre de somas pois S foi tomado maximal. Por isso, temos 3 possibilidades

   1. $s_i + s_j = s_k$, que não pode por S ser livre de somas;
   2. $s_i + x = s_j$ e $x \in S - S$, absurdo pela escolha de x;
   3. $x + x = s_i$ e $2x \in S$, o que dá $x \in \frac{1}{2}S$,

e, portanto,

$$G = S \cup (S+S) \cup (S-S) \cup \frac{1}{2}S.$$

ii),iii) Inicialmente, observe que

$$|S+S| \leq \binom{|S|}{2} + |S|(*)$$

(a primeira parcela vem de elementos distintos de S e a segunda, de elementos iguais) e

$$|S-S| \leq 1 + 2\binom{|S|}{2}(**)$$

(a primeira parcela vem de elementos iguais, a segunda, de elementos distintos e o fator 2 pela escolha da ordem entre as parcelas na diferença).

Para ii, $\left|\frac{1}{2}S\right| = |S|$ (pelo Lema 3.1.3). Logo, de i), temos

$$|G| \leq |S| + |S+S| + |S-S| + \left|\frac{1}{2}S\right|$$

$$\leq |S| + \binom{|S|}{2} + |S| + 1 + 2\binom{|S|}{2} + |S|,$$

por (*), (**) e $\left|\frac{1}{2}S\right| = |S|$. Assim,

$$|G| \leq 3|S| + 1 + 3\frac{|S|\,(|S|-1)}{2} = \frac{3}{2}|S|^2 + \frac{3}{2}|S| + 1.$$

Resolvendo a inequação em $|S|$, obtemos

$$|S| \geq \frac{1}{6}\left((24|G|-15)^{\frac{1}{2}} - 3\right).$$

Para iii,

$$\left|\frac{1}{2}S\right| \leq \frac{1}{2}|G|.$$

(pelo Lema 3.2.2). Logo, por i),

$$|G| \leq |S| + |S+S| + |S-S| + \left|\frac{1}{2}S\right|$$

$$\leq |S| + \binom{|S|}{2} + |S| + 1 + 2\binom{|S|}{2} + \frac{1}{2}|G|,$$

por (*), (**) e $\left|\frac{1}{2}S\right| \leq \frac{1}{2}|G|$. Daí,

$$\frac{1}{2}|G| \leq 2|S| + 1 + 3\frac{|S|\,(|S|-1)}{2}$$

$$= \frac{3}{2}|S|^2 + \frac{1}{2}|S| + 1$$

$$\Rightarrow |G| \leq 3|S|^2 + |S| + 2.$$

Resolvendo a inequação em $|S|$, obtemos $|S| \geq \frac{1}{6}\left((12|G|-23)^{\frac{1}{2}} - 1\right)$.

iv) $|S+S| \leq c|S|$ implica $|S-S| \leq c^2|S|$ (***) (veja demonstração no Apêndice B).

Se $|G|$ é ímpar, temos $\left|\frac{1}{2}S\right| = |S|$(pelo Lema 3.1.3). Assim, por i),

$$|G| \leq |S| + |S+S| + |S-S| + \left|\frac{1}{2}S\right|$$

$$\leq |S| + c|S| + c^2|S| + |S|,$$

por (***) e $\left|\frac{1}{2}S\right| = |S|$. Assim,

$$|G| \leq |S|(c^2 + c + 2).$$

Agora se $|G|$ é par, temos $\left|\frac{1}{2}S\right| \leq \frac{1}{2}|G|$(pelo Lema 3.2.2) e, portanto, por i),

$$|G| \leq |S| + |S+S| + |S-S| + \left|\frac{1}{2}S\right|$$

$$\leq |S| + c|S| + c^2|S| + \frac{1}{2}|G|,$$

por (***) e $\left|\frac{1}{2}S\right| \leq \frac{1}{2}|G|$. Portanto,

$$|G| \leq |S|2(c^2 + c + 1).$$

□

Antes do próximo teorema, considere um grupo G de ordem divisível por 3 e H, um subgrupo de índice 3 em G. Então,

$$G = H \dot{\cup} (H + a) \dot{\cup} (H + 2a),$$

em que a e $2a$ não estão em H, mas $3a \in H$.

Sendo $S = H + a$, então $S + S = H + 2a$ e $S - S = H$. Daí,

$$G = S \dot{\cup} (S + S) \dot{\cup} (S - S)$$

e $S \cap (S + S) = \emptyset = S \cap (S - S)$. Logo, S é livre de somas. Para mostrar que S é livre de somas localmente maximal, temos a seguinte

Afirmação. Nas notações acima, se $x \in G - S$, então $T = S \cup \{x\}$ não é livre de somas e, portanto, S é livre de somas localmente maximal.

Prova(Afirmação): Como $x \notin S$, então temos dois casos:

i) $x \in S + S = H + 2a$. Neste caso, $x = h + 2a = (h + a) + a$. Isso significa que T não é livre de somas pois $h + a$ e a estão em $S = H + a$ e $S \subset T$.

ii) $x \in S - S = H$.

Aqui, basta tomar $a \in S = H + a$ e ver que $x + a$ também está em $S = H + a$. Novamente, T não é livre de somas.

□

Além disso,

$$S \cup -S = S \dot{\cup} (S + S).$$

Daí,

$$|S - S| + |S \cup -S| - 3 = |G| - \frac{|G|}{|S - S|},$$

pois $H = S - S$ implica $\frac{|G|}{|S-S|} = |G : H| = 3$.

Agora, vejamos o último resultado, que é uma relação entre a cardinalidade de um grupo e subconjuntos livres de somas localmente maximais.

Teorema 3.2.2. *Seja S um conjunto livre de somas localmente maximal no grupo finito G. Então,*

$$|S - S| + |S \cup -S| - 3 \leq |G| \left(1 - |S - S|^{-1}\right),$$

com igualdade se, e somente se, $S - S$ é um subgrupo de G, $|G : S - S| = 3$ e S é uma classe lateral de $S - S$.

Prova. O exemplo anterior a este teorema mostra que tomando $S = H + a$ (classe lateral de $H = S - S \leq G$) com $|G : H| = 3$ temos a igualdade.

Para a recíproca, seja S um subconjunto livre de somas localmente maximal em G.

Se $R = \{x_1, x_2, ..., x_r\}$ é um conjunto qualquer de elementos distintos de G com $x_i - x_j \notin S - S, 1 \leq i \neq j \leq r$, então

$$r \leq |G| - |S - S| - |S \cup -S| + 3.$$

De fato, considere o r-conjunto definido por $y_i = x_i - x_1, 1 \leq i \leq r$. Apenas $y_1 = 0$ está em $S - S$ pela definição de R.

Se houvesse y_i e y_j, $i, j \geq 2$, em S, então $y_i - y_j = x_i - x_j$ estaria em $S - S$, o que não pode ocorrer. Logo, no máximo um dos $y_i, i \geq 2$, pertence a S. Analogamente, no máximo um dos $y_i, i \geq 2$, pertence a $-S$.

Como S é livre de somas, $(S - S) \cap S = \emptyset = (S - S) \cap (-S)$ e, assim,

$$(S - S) \cap (S \cup -S) = \emptyset.$$

Portanto, em G, há três subconjuntos disjuntos de elementos:

i. $Y = \{0 = y_1, y_2, ..., y_r\}$;

ii. $(S - S) - \{0\}$;

iii. $S \cup -S$, descontando no máximo dois elementos já possivelmente contados em Y.

Assim,

$$|G| \geq r + (|S - S| - 1) + (|S \cup -S| - 2)\,.$$

Segue que

$$r \leq |G| - |S - S| - |S \cup -S| + 3.$$

Agora, ainda com S dado no grupo abeliano $G = \{g_1, g_2, ..., g_n\}$, associe a G o grafo Γ_S cujos vértices são $g_1, g_2, ..., g_n$ e com uma aresta entre g_i e g_j se, e somente se, $g_i - g_j \in S - S$. (Grafo de Cayley)

Para cada g_i em G há $|S - S| - 1$ elementos $g_j \neq g_i$ tais que

$$g_i - g_j \in (S - S) - \{0\}.$$

Ou seja, Γ_S é grafo regular pois cada vértice tem grau $|S - S| - 1$. Sendo E o conjunto de arestas de Γ_S, temos

$$|E| = \frac{1}{2} n\,(|S - S| - 1)\,.$$

Juntamente com o Corolário 2.2.1, obtemos

$$\alpha(G) \geq \frac{|G|^2}{|G| + 2|E|} = \frac{|G|}{|S - S|},$$

com igualdade se, e somente se, Γ_S for uma união de cliques disjuntas, cada uma com cardinalidade $|S - S|$ pois Γ_S é regular.

Um conjunto independente em Γ_S é um conjunto de elementos distintos $g_1, g_2, ..., g_r$ que satisfaz

$$g_i - g_j \notin S - S$$

para $i \neq j$. Logo,

$$\frac{|G|}{|S - S|} \leq \alpha(G) \leq |G| - |S - S| - |S \cup -S| + 3,$$

e a desigualdade foi provada.

Agora, para ocorrer a igualdade, devemos ter

1. $\alpha(G) = \frac{|G|}{|S-S|}$, o que ocorre se, e somente se, Γ_S é uma união de cliques disjuntas de cardinalidade $|S - S|$;

2. $\alpha(G) = |G| - |S - S| - |S \cup -S| + 3$.

Vejamos o que essas sentenças geram passo a passo:

- $S - S$ é um subgrupo de G.

  Pela definição de Γ_S, 0 está conectado a todos os elementos de $(S-S)-\{0\}$. Por 1, 0 não pode se conectar a nenhum outro elemento (pela cardinalidade de cada clique) e, também por 1, está formada a clique $S - S$ (Γ_S é, pela igualdade assumida, uma união de cliques disjuntas). Segue que $S - S$ é um subgrupo de G.

- S é uma classe lateral de $S - S$.

  Afirmação. S é uma clique em Γ_S.

  Prova(Afirmação): Note que cada par de elementos de S está conectado por arestas de Γ_S (veja definição de Γ_S).

  Suponha que exista $a \notin S$ e a conectado a cada elemento de S (observe que Γ_S é uma união de cliques disjuntas). Daí,

  $$(a - S) \cup (S - a) \subseteq S - S.(*)$$

  Então:

  i) $2a \notin S$.

  Suponha que $\exists s \in S$ tal que $2a = s$. Assim,

  $$a = s - a \in S - S,$$

  por (*). Além disso, $s \notin S - S$ já que $s \in S$ e $S \cap (S - S) = \emptyset$ por S ser livre de somas. Mas os elementos de $S - S$ só se conectam a elementos que também estejam em $S - S$ pois $S - S$ é uma clique. Logo, $2a \notin S$.

  ii) $a \notin S + S$.

  Suponha que $\exists s_i, s_j \in S$ tais que

  $$a = s_i + s_j.$$

Então, $s_i = a - s_j \in S - S$ por (*). Daí, $s_i \in S \cap (S - S)$, o que não pode ocorrer já que S é livre de somas (e, portanto, $S \cap (S - S) = \emptyset$). Assim, $a \notin S + S$.

iii) $a \notin S - S$.

Suponha que $\exists s_i, s_j \in S$ tais que

$$a = s_i - s_j \quad \text{ou} \quad a - s_i = -s_j.$$

Por (*),

$$-s_j \in S - S \quad \text{ou} \quad s_j \in S - S,$$

o que contradiz a hipótese de S ser livre de somas (S e $S - S$ têm interseção vazia). Assim, $a \notin S - S$.

□

Agora, vamos analisar o conjunto $S \cup \{a\}$. Sendo

$$S = \{s_1, s_2, ..., s_k\},$$

temos

$$S \cup \{a\} = \{a, s_1, s_2, ..., s_k\}.$$

Vimos que $2a \notin S$, $a \notin S + S$ e $a \notin S - S$. Portanto, $S \cup \{a\}$ é livre de somas, contradizendo a hipótese de que S é livre de somas localmente maximal. Logo, não existe $a \notin S$ com a conectado a todos os elementos de S, o que implica que S é uma clique em Γ_S e, conseqüentemente, $|S| = |S - S|$.

Vamos mostrar agora que S é uma classe lateral não-trivial de $S - S$.

Afirmação. Nas notações acima, $S = s + (S - S), \forall s \in S$.

Prova(Afirmação): Se $x \in S$, então

$$x = s + (x - s), \forall s \in S,$$

mostra que $x \in s + (S - S)$. Logo, $S \subseteq s + (S - S)$. Mas $|S| = |S - S|$ dá que S é uma classe lateral de $S - S$.

□

- $|G : S - S| = 3$.

  Analogamente, $-S$ também é uma classe lateral de $S - S$.

  Temos duas possibilidades: $S = -S$ ou $S \cap -S = \emptyset$.

  Suponha $S = -S$. Então $S \cup -S = S$. Por 1, 2 e $|S - S| = |S|$, temos

$$\frac{|G|}{|S - S|} = \alpha(G) = |G| - |S - S| - |S \cup -S| + 3$$

$$\Rightarrow \frac{|G|}{|S|} = |G| - 2|S| + 3$$

$$\Rightarrow |G|\,(|S| - 1) = |S|\,(2|S| - 3)\,.$$

  Mas $|S| - 1$ é primo com $|S|$ (pois são números inteiros consecutivos) e com $2|S| - 3$ (sendo $d = (|S| - 1, 2|S| - 3)$, então d divide $2 \cdot (|S| - 1) - (2|S| - 3) = 1$. Portanto, $d = 1$.).

  Assim, $|S| = 2 = |G|$ e $S = G$, o que não pode ocorrer pois S é livre de somas.

  Logo, $S \cap -S = \emptyset$ e, portanto, $|S \cup -S| = 2|S|$. Observe também que a cardinalidade de um subconjunto livre de somas localmente maximal é no mínimo 2. Daí,

$$\frac{|G|}{|S|} = |G| - 3|S| + 3$$

$$\Rightarrow |G| = |S||G| - 3|S|\,(|S| - 1)$$

$$\Rightarrow |G|\,(1 - |S|) = 3|S|\,(1 - |S|)$$

$$\Rightarrow |G| = 3|S|$$

ou

$$|G| = 3|S - S|,$$

dando que $S - S$ tem índice 3 em G.

□

Apêndice A

TEORIA DE RAMSEY

O filósofo inglês Frank P. Ramsey (1903-1930) provou por volta 1928, pouco antes de morrer próximo de completar 27 anos, em seu artigo *On a Problem of Formal Logic*, publicado em 1930, o teorema a seguir de existência dos chamados números de Ramsey.

Definição A.0.2. *$R = R(k_1, k_2, ..., k_n)$ é chamado **Número de Ramsey**. Ele denota a quantidade mínima R de vértices de um K_R grafo completo colorido por arestas com n cores para que haja uma k_1-clique monocromática da primeira cor, ou uma k_2-clique monocromática da segunda cor,..., ou uma k_n-clique com vértices pintados com a mesma n-ésima cor.*

Teorema A.0.3 (**Teorema de Ramsey**)**.** *Nas notações acima, existe $R(k_1, k_2, ..., k_n)$, sendo n inteiro positivo.*

Uma demonstração desse teorema pode ser encontrada em [9].

Um exemplo da teoria de Ramsey é apresentado mais classicamente da seguinte forma:

Exemplo A.0.3. *Em uma festa com s pessoas, em que $s \geq 6$, há três pessoas que se conhecem mutuamente ou três que não se conhecem duas a duas entre si, supondo recíproca a relação conhecer.*

■

Relacionado com esse, temos da teoria dos grupos o seguinte

Exemplo A.0.4. *Os elementos não-nulos de $\mathbb{Z}_5$ dos inteiros módulo 5 podem ser particionados em dois conjuntos livres de somas $S_1 = \{1, 4\}$ e $S_2 = \{2, 3\}$ para mostrar que*

$R(3,3) > 5$.

De fato, associemos S_1 a uma cor C_1 e S_2, a uma cor C_2 da seguinte forma: sendo $v_0, ..., v_4$ os vértices de K_5 associado a G, colorimos a aresta que une v_i a v_j com a cor C_k se $i - j \in S_k$. Como $S_k = -S_k$, essa coloração está bem definida. Desde que S_1 e S_2 são livres de somas, não há triângulos monocromáticos nessa pintura.

De fato, se v_i, v_j, v_l fossem vértices de um triângulo monocromático, então $v_i - v_j$, $v_j - v_l$, $v_l - v_i$ estariam em um mesmo subconjunto S_k, $k = 1$ ou $k = 2$, um absurdo pois $v_i - v_j + v_j - v_l = v_i - v_l$ e S_k é livre de somas.

Assim, $R(3,3,2) > 5$.

■

Voltando ao primeiro exemplo, vamos mostrar que o resultado ocorre com 6 pessoas (ou mais). Escolha uma pessoa P qualquer do grupo. Se representarmos a relação *conhecer* com arestas de cor 1 e a *não conhecer* com arestas de cor 2, de P partem 3 arestas às pessoas A, B, C de uma das cores, digamos cor 1 sem perda de generalidade. Então, há aresta da cor 1 unindo A, B, C ou as arestas unindo A, B, C são todas da cor 2. Em qualquer caso, o resultado está provado. Portanto, $R(3,3) = 6$.

Exemplo A.0.5. *Vamos estudar $R(3,5)$. Considere*

$$\mathbb{Z}_{13} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\},$$

e associe-o a um grafo em que cada elemento é um vértice.

Os resíduos cúbicos não-nulos de $\mathbb{Z}_{13}$ são

$$1, 5, 8, 12.$$

Se a diferença entre dois vértices é um resíduo cúbico, então colorimos a aresta correspondente de vermelho. Caso contrário, a pintamos de azul. Como $1 = -12 \mod 13$ e $5 = -8 \mod 13$, a pintura está bem definida.

Nesse grafo, não há subconjunto de três vértices conectados por segmentos vermelhos, nem subconjunto de cinco vértices unidos por linhas azuis. Logo,

$$R(3,5) > 13.$$

■

Exemplo A.0.6. *É fácil ver que*

$$R(2, m) = m, m = 2, 3, ...$$

Em particular, $R(2, 4) = 4$. *Além disso,* $R(3, 3) = 6$ *pelos exemplos A.0.3 e A.0.4.*

Também pode ser mostrado que se $R(k-1, m) = 2p$ *e* $R(k, m-1) = 2q$, *então*

$$R(k, m) < 2p + 2q = R(k-1, m) + R(k, m-1),$$

que é uma conseqüência da desigualdade

$$R(k, m) \leq R(k-1, m) + R(k, m-1)$$

(veja [6]). Segue que

$$R(3, 4) < 4 + 6,$$

o que dá $R(3, 4) \leq 9$.

Como $R(2, 5) = 5$ *e*

$$R(3, 5) \leq R(2, 5) + R(3, 4) \leq 5 + 9,$$

segue que $R(3, 5) = 14$ *e, portanto,* $R(3, 4) = 9$.

■

Esses foram mais alguns interessantes resultados unindo a Teoria dos Grafos, através dos estudos de Ramsey, à Teoria dos Grupos. Em [6] encontram-se mais exemplos.

Apêndice B

SOBRE A CARDINALIDADE DE $S+S$ E $S-S$

O objetivo deste segundo apêndice é demonstrar um resultado utilizado no item iv do Teorema 3.2.1 do capítulo 3.

Seja S um subconjunto de um grupo finito e aditivo G. Como definimos no capítulo 3,

$$S+S=\{s_i+s_j; s_i, s_j \in S\},$$

$$S-S=\{s_i-s_j; s_i, s_j \in S\}.$$

Em 1976, I.Z. Ruzsa respondeu em [8] de forma elementar à seguinte pergunta de P. Erdös:

Para toda constante positiva c, existe c' tal que para todo conjunto S,

$$|S+S| \leq c|S| \Rightarrow |S-S| \leq c'|S|?$$

no caso em que $c'=c^2$.

Em [5], G.A. Freiman trata os conjuntos satisfazendo $|S+S| \leq c|S|$ de forma profunda. Um dos teoremas desse livro responde rapidamente à pergunta de Erdös. Vejamos agora a solução de Ruzsa.

O resultado segue do

Teorema B.0.4. *Nas notações acima,* $|S||S-S| \leq |S+S|^2$.

De fato, se $|S+S| \leq c|S|$, então

$$|S+S|^2 \leq c^2|S|^2.$$

Pelo teorema acima, $|S||S-S| \leq c^2|S|^2$, o que dá

$$|S-S| \leq c^2|S|.$$

Esse teorema é conseqüência do

Teorema B.0.5. *Para* S, X, Y *conjuntos finitos, temos*

$$|S||X-Y| \leq |S-X||S-Y|.$$

fazendo $X = Y = -S$.

Passemos, então, à prova desse último resultado.

Prova. Se mostrarmos a existência de uma função injetora de $S \times (X-Y)$ em $(S-X) \times (S-Y)$, então teremos provado o teorema.

Definamos $f : S \times (X-Y) \to (S-X) \times (S-Y)$ por

$$f(s,d) = (s-x, s-y),$$

em que $d = x - y \in X - Y$, tomando x maximal. Vamos mostrar que f é injetora.

De fato, se

$$f(s,d) = f(s',d'),$$

em que $d' = x' - y' \in X - Y$, x' maximal, então

$$(s-x, s-y) = (s'-x', s'-y').$$

Daí,

$$\begin{cases} s-x = s'-x' \\ s-y = s'-y' \end{cases}$$

o que dá $x - y = x' - y'$, ou seja, $d = d'$. Como x e x' são maximais, $x = x'$ e, portanto, $s = s'$.

Logo, $(s, d) = (s', d')$ e f é injetora. □

Referências Bibliográficas

[1] BERTRAM, E. A. On large cyclic subgroups of finite groups. *Proc. Amer. Math. Soc.*, Honolulu, n.56, p.63-66, 1976.

[2] BERTRAM, E. A. Some applications of graph theory to finite groups. *Discrete Mathematics*, Honolulu, n. 44, p.31-43, 1983.

[3] BHATTACHARYA, P. B.; JAIN, S. K.; NAGPAUL, S. R. *Basic abstract algebra*. 2nd ed. New York: Cambridge University Press, 1995.

[4] DUMMIT, D. S.; FOOTE, R. M. *Abstract algebra*. 2nd ed. New York: John Wiley, 1999.

[5] FREIMAN, G. A. *Foundations of a Structural Theory of Set Addition*. Trad. B. Volkmann. Providence: American Mathematical Society, 1973.

[6] GREENWOOD, R. E.; GLEASON, A. M. Combinatorial relations and chromatic graphs. *Canad. J. Math.*, Ottawa, n.7, p.1-7, 1955.

[7] MASON, D. R. On coverings of finite groups by abelians subgroups. *Math. Proc. Cambridge Philos. Soc.*, Cambridge, n.83, p.205-209, 1978.

[8] RUZSA, I. Z. On the cardinality of $A + A$ e $A - A$. *Colloquia Mathematica Societatis János Bolyai*, Amsterdam, n.18, p.933-938, 1976.

[9] WALLIS, W. D.; STREET, A. P.; WALLIS, J. S. Combinatorics: room squares, sum-free sets, Hadamard matrices. *Lecture Notes in Math*, New York, n.292, p.21-264, 1972.

[10] WEI, V. K. *Coding for a multiple access channel*. Honolulu: Univ. of Hawaii, 1980. Tese (Ph.D in Electrical Engineering).

Índice Remissivo

k-coloração, 13, 15, 19
k_r-clique, 66
Órbita, 47

Ação transitiva, 46, 47
Arestas, 12
Arestas múltiplas, 13

Cayley, 16, 61
Centralizador, 15, 38, 44
Centralizador abeliano, 37, 38
Centro, 15, 22, 41
Centro trivial, 16
Classe de conjugação, 15, 25, 26, 40, 42
Clique, 13, 33, 62, 63
Coloração por arestas, 14
Conjunto independente, 15, 27, 28, 31, 61

Dedekind, regra, 47
Desigualdade de Cauchy-Schwartz, 32

Frobenius, 25, 46

Grafo, 12
Grafo k-colorido, 13
Grafo k-regular, 13
Grafo completo, 13, 15, 33
Grafo induzido, 20, 28
Grafo não-direcionado, 13
Grafo regular, 13, 61
Grau de um vértice, 13
Grupo A_4, 43
Grupo S_3, 24
Grupo S_4, 25, 26, 38
Grupo S_7, 26
Grupo abeliano, 15
Grupo de Klein, 44
Grupo de permutação transitivo, 46
Grupo diedral, 35, 36
Grupo diedral generalizado, 23
Grupo não-abeliano, 38, 39, 44
Grupo não-solúvel, 25
Grupo solúvel, 25

Loop, 13, 22

Multigrafo, 13

Número de classes de conjugação, 33
Número de independência, 15, 27
Número de Ramsey, 66

Ramsey, 14, 54, 66

Subconjunto livre de somas, 16, 51, 52, 54, 55, 63
Subconjunto livre de somas localmente maximal, 54, 56, 60, 63
Subgrafo, 13
Subgrupo abeliano, 15
Subgrupo cíclico, 47
Subgrupo fechado para os centralizadores, 44, 46
Subgrupo gerado, 21
Sylow, 38, 47

Teorema de Bezout, 45
Teorema de Lagrange, 24, 37

Vértices, 12

Vértices adjacentes, 12
Vértices isolados, 15