Aplicações da Teoria dos Grafos à Teoria dos Grupos

Marcelo Mendes

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

Começamos com algumas definições. 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.

O seguinte teorema relaciona $\alpha(\Gamma)$ e os graus dos vértices de Γ. Esse resultado foi provado em 1980 por V. K. Wei em sua dissertação de Ph.D. 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 o vértice de grau máximo.

Teorema 1.1. *Seja $d(v)$ o grau do vértice v em 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. Seja v_0 um vértice de Γ de grau máximo, isto é, $d(v_0) \geq d(v), \forall v \in \Gamma$.

Seja 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.

Claramente, a igualdade ocorre se Γ não tem arestas, caso em que $\alpha(\Gamma) = n$ e $d(v) = 0$, $\forall v \in \Gamma$, ou se Γ tem apenas 2 vértices, situação em que $\alpha(\Gamma) = 1$ e $d(v) = 1$, $\forall v \in \Gamma$.

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 $\alpha(\Gamma) = \alpha(\Gamma^-) + 1$, se v_0 havia sido contado para $\alpha(\Gamma)$, ou $\alpha(\Gamma) = \alpha(\Gamma^-)$, caso contrário. Assim, temos dois casos a analisar:

1^o caso. Se $\alpha(\Gamma) = \alpha(\Gamma^-) + 1$, então $\alpha(\Gamma) > \displaystyle\sum_{v\in\Gamma} \frac{1}{d(v)+1}$.

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

$$\sum_{v\in\Gamma}\frac{1}{d\,(v)+1}\leq\frac{1}{d\,(v_0)+1}+\sum_{v\in\Gamma^-}\frac{1}{d^-\,(v)+1}$$

$$<1+\sum_{v\in\Gamma^-}\frac{1}{d^-\,(v)+1}\leq 1+\alpha\left(\Gamma^-\right)=\alpha\,(\Gamma)\,.$$

2^o caso. Se $\alpha\,(\Gamma)=\alpha\,(\Gamma^-)$, então podemos mostrar que $\displaystyle\sum_{v\in\Gamma^-}\frac{1}{d^-\,(v)+1}\geq\sum_{v\in\Gamma}\frac{1}{d\,(v)+1}$ ou que, equivalentemente, $\displaystyle\sum_{v\in\Gamma^-}\left[\frac{1}{d^-\,(v)+1}-\frac{1}{d\,(v)+1}\right]\geq\frac{1}{d\,(v_0)+1}$, 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, $\frac{1}{d(v)(d(v)+1)}$ já que $d(v_0)\geq d(v)$, $\forall v\in\Gamma$, por hipótese.

Agora, assumimos $\alpha(\Gamma^-)\geq\displaystyle\sum_{v\in\Gamma^-}\frac{1}{d^-(v)+1}$ como hipótese de indução sobre a quantidade de vértices. Daí, $\alpha(\Gamma^-)\geq\displaystyle\sum_{v\in\Gamma^-}\frac{1}{d^-(v)+1}$ nos dá $\alpha(\Gamma)\geq\displaystyle\sum_{v\in\Gamma^-}\frac{1}{d^-(v)+1}\geq\sum_{v\in\Gamma}\frac{1}{d(v)+1}$. Isso prova a primeira parte do teorema.

Em seguida, se Γ é a união de cliques disjuntas $\Gamma_1,\Gamma_2,...,\Gamma_s$, então $\alpha(\Gamma)=s$ e, em cada Γ_i, teremos

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

Portanto, $\alpha(\Gamma)=\displaystyle\sum_{v\in\Gamma}\frac{1}{d(v)+1}$.

Neste momento, suponha que ocorra a igualdade $\alpha(\Gamma)=\displaystyle\sum_{v\in\Gamma}\frac{1}{d(v)+1}$. 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, $r = \alpha(\Gamma)$. 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 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 $\{v \in \Gamma^-; \exists(v, v_0)\} = \Gamma_i \cup \left\{v^0\right\}$, teríamos

$$\sum_{\substack{v\in\Gamma^- \\ \exists(v,v_0)}} \frac{1}{d(v)\,(d(v)+1)} = |\Gamma_i| \frac{1}{|\Gamma_i|\,(|\Gamma_i|+1)} + \frac{1}{d(v^0)\,(d(v^0)+1)}$$

$$> \frac{1}{|\Gamma_i|+1} > \frac{1}{|\Gamma_i|+2} \geq \frac{1}{d(v_0)+1},$$

pois $d(v_0) \geq |\Gamma_i|+1$. Mas isso é absurdo uma vez que (*) e (**) nos dá $\displaystyle\sum_{\substack{v\in\Gamma^- \\ \exists(v,v_0)}} \frac{1}{d(v)\,(d(v)+1)} = \frac{1}{d(v_0)+1}$.

Isso conclui essa demonstração. □

Esse teorema nos dá o seguinte

Corolário 1.1. *Nas notações da demonstração do teorema,* $\alpha(\Gamma) \geq \frac{|V(\Gamma)|^2}{|V(\Gamma)|+2|E(\Gamma)|}$, *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 , $\displaystyle\left(\sum_{v\in\Gamma} \frac{1}{d(v)+1}\right)\left(\sum_{v\in\Gamma} (d(v)+1)\right) \geq \left(\sum_{v\in\Gamma} 1\right)^2 = |V(\Gamma)|^2$.

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

Pelo teorema, $\displaystyle\alpha(\Gamma) \geq \sum_{v\in\Gamma} \frac{1}{d(v)+1}$. Logo, $\alpha(\Gamma) \geq \frac{|V(\Gamma)|^2}{|V(\Gamma)|+2|E(\Gamma)|}$.

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

□

Agora, associe a um grupo 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 1.1. *$a(G)$ 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 $a(G)$.

Definição 1.2. *Definimos a **classe de conjugação** contendo x como $x^G = \left\{y^{-1}xy; y \in G\right\}$.*

Definição 1.3. *O **centralizador de** x **em** G é dado por $C(x) = \left\{y \in G; y^{-1}xy = x\right\}$.*

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 relação $|C(x)| = d(x) + 1, \forall x \in G$, assumindo que Γ não possui loops.

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 1.2.

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. Temos

$$2\,|E(\Gamma)| = \sum_{x \in G} d(x) = \sum_{x \in G} (|C(x)| - 1)$$
$$= \sum_{\substack{classes \\ distintas}} \left|x^G\right| |C(x)| - |G| = k(G)\,|G| - |G|,$$

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

Pelo corolário, 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 maximal . Somando sobre as $k_G(A)$ G-classes distintas $a^G, a \in A$, e usando que $A = \dot{\bigcup\limits_{a \in A}} \left(a^G \cap A\right)$, temos

$$|A| = \sum_{a \in A} \left|a^G \cap A\right| \leq \max_{a \in A} \left|a^G\right| \cdot k_G(A)$$

$$= \left|a_0^G\right| \cdot k_G(A) \leq \frac{|G| \cdot k(G)}{|C(a_0)|} \leq \frac{|G| \cdot k(G)}{\min\limits_{a \in A} |C(a)|},$$

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, além de outros possíveis elementos. 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 e $A = G$, então ocorre a igualdade.

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

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

e assim, $|C(a)| = |A|, \forall a \in G$ e, então, $|a^G| = |b^G|, \forall a, b \in A$.

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

Temos ainda $|G| = |a^G| \, |C(a)| = 1 \cdot |A| = |A|$, que dá $G = A$.

Além disso, $|a^G| = 1, \forall a \in A$, dá que $A = G$ é abeliano.

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

□

Exemplo 1.1. *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 1.2. *No exemplo anterior, 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 $(1\ 2)(34)$ não é abeliano.

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, $a(S_4) = 10$.

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

Portanto, $\alpha(S_4) = a(S_4)$.

■

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

Lema 2.1. *Seja G um grupo finito não-abeliano 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 da seção anterior, 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 $|x^G| < |G|^{\frac{r+1}{2}}, \frac{|G|}{|C(x)|} < |G|^{\frac{r+1}{2}}, |C(x)| > |G|^{\frac{1-r}{2}}$.

b) Seja $Z(G) = \{x \in G; xy = xy, \forall y \in G\}$ o **centro** do grupo G. Relacionando com Γ, o centro representa o conjunto dos vértices com grau $n-1$, sendo n o 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. Novamente do teorema da seção anterior,

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

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

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

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

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

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

Na prova do item a), vimos que $\displaystyle\sum_{\substack{classes \\ distintas}} \left|x^G\right|^2 \leq \alpha(G)|G|$.

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

$\square$

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, $\alpha(G) > |G|^r - 1 \quad \mathrm{e} \quad \alpha(G) \geq \lfloor |G|^r \rfloor$.

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 $(1\ 2)(3\ 4)$.

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

A partir do último lema, 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 3.1. *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 anterior 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 $\alpha(G) \geq \left\lfloor |G|^{\frac{1}{3}} \right\rfloor$.

□

Corolário 3.1. *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 último teorema.

Como p é primo, $C(x)$ é abeliano e cíclico. Denotemos $C(x) = \left\{1, x, x^2, ..., x^{p-1}\right\}$, 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 3.1. *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, conseqüentemente, $h = 1$, absurdo. Logo, $x \in H$ e, portanto, $C(h) \subset H$.

■

Exemplo 3.2. *Outro exemplo de grupo G contendo subgrupo fechado para os centralizadores é um grupo de permutação 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, $C(P) = P$.

■

Referências

[1] OLIVEIRA, M. M. *Aplicações da Teoria dos Grafos à Teoria dos Grupos*. Fortaleza, 2008. Tese (Mestrado em Matemática) - Dept. de Matemática, Univ. Federal do Ceará.