



# p-grupos e Aplicações

Pedro Henrique Cavalcanti da Silva<sup>1</sup> Igor dos Santos Lima (Orientador)<sup>2</sup>

<sup>1</sup> Graduando em Matemática - UFG – CAC, Bolsista de Iniciação Científica - PIBIC, Catalão, Brasil, pedriw@gmail.com

<sup>2</sup> Doutor em Matemática pela Universidade Estadual de Campinas UNICAMP e Professor do Departamento de Matemática da – UFG – CAC igor.matematico@gmail.com



**Resumo:** Como sabemos, a ordem de um grupo traz consequências para sua estrutura, e quanto mais fatores primos a sua ordem possui, mais complicado pode ser o grupo. Assim, utilizando a conjugação de classes, entenderemos algumas propriedades particulares de p-grupos finitos. Hoje a teoria dos grupos é aplicável em outras áreas tanto das ciências afins quanto em outras da Matemática.

## I. Introdução

Usando a conjugação de classes de um elemento, conseguimos demonstrar uma equação na qual podemos retirar efeitos sobre a teoria de grupos. A aplicação desta equação chamada, de equação de classes nos ajuda a demonstrar algumas propriedades para p-grupos. Como por exemplo, todo p-grupo com ordem  $p^2$  é abeliano, ou um p-grupo não trivial, então o centro deste também é não trivial.

## II. Considerações Iniciais

Para tal demonstração, serão necessários alguns conceitos básicos de Álgebra. Seguem alguns conceitos:

- Dizemos que um conjunto “G” não vazio é grupo, se munido de uma operação binária “\*” bem definida. Se com “ $a \in G$ ” satisfaz as seguintes propriedades:
  - Possui Associatividade. “ $a*(b*c)=(a*b)*c$ ”
  - Existe Elemento Neutro. “ $a*e=e*a=a$ ”
  - Existe Elemento Inverso. “ $a*a^{-1}=a^{-1}*a=e$ ”.
- Dizemos que um subconjunto H, não vazio, de um grupo G é um subgrupo, se munido da mesma operação de G, respeita as mesmas propriedades.
- Dizemos centro, o subconjunto que contém todos os elementos que comutam com outros elementos.
- Pelo teorema de Lagrange temos que, a ordem de H divide a ordem de G.
- Sejam um Grupo G, H um subgrupo de G e  $a \in G$ . Os subconjuntos de G,  $aH=\{ah, h \in H\}$  e  $Ha=\{ha, h \in H\}$  são chamados, respectivamente, de classe lateral a esquerda e a direita de H.
- Seja G um grupo, H subgrupo de G, a um elemento de G. O grupo quociente,  $G/H$ , contém todas as classes laterais a direita de H por a.
- Dizemos que um grupo finito G é um p-grupo, se G possui ordem  $p^n$ , sendo p um número primo, e n um natural.
- Um homomorfismo é uma aplicação F de um grupo G em outro grupo G’ que satisfaz a seguinte situação, sendo “ $a, b \in G$ ”, sendo a operação de G “\*” e G’+ :
  - $F(a*b)=F(a)+F(b)$
  - Um homomorfismo injetor e sobrejetor é dito Isomorfismo.

## III. Equação de Classes

Dizemos que G sendo um grupo, “ $a, b \in G$ ”, dizemos que a é conjugado de b e indicamos “ $a \sim b$ ”, se existe “ $g \in G$ ” tal que “ $b= g^{-1}ag$ ”. Daqui, vamos chamar de Classe de Conjugação de “a”, todos os elementos que se relacionam com a da forma anterior.

A equação de classes, vem de uma bijeção da grupo quociente de G na classe de conjugação. Sendo esta bijeção  $\varphi(Hg)=g^{-1}ag$ . Desta bijeção, concluímos que a ordem deste grupo quociente é igual a ordem desta classe de conjugação. Ou seja, a ordem da Classe de Conjugação divide a ordem do Grupo.

$$\text{Assim } |G| = |Z(G)| + \sum_{a \in G} |C_a|.$$

## III. Aplicação da Equação de Classes em p-Grupos

- Se G é um p-grupo e  $|G| > 1$ , então  $Z(G)$  também é um p-grupo e  $|Z(G)| > 1$ .

Demonstração: Seja  $|G| = p^n > 1$ . Como  $Z(G) \leq G$ , do teorema de Lagrange,  $|Z(G)| |p^n$ , logo,  $\exists m \in \mathbb{Z}_+, 0 \leq m \leq n$ , tal que  $|Z(G)| = p^m$ . Para cada  $a \notin Z(G)$ ,  $|C_a|$  e da equação de classes,  $|C_a| |p^m$ ,  $\sum_{a \notin Z(G)} |C_a|$  é um múltiplo de p. Como  $p^n = |G| = |Z(G)| + \sum_{a \in G} |C_a|$ , temos que  $p \mid |Z(G)| \Rightarrow p \mid p^m \Rightarrow m \geq 1$ .

$$\text{Assim } |Z(G)| = p^m > 1.$$

- Se  $|G| = p^2$ , onde p é um primo positivo, então G é abeliano.

Demonstração: Seja G um grupo de ordem  $p^2$ . Então pelo que demonstramos anteriormente,  $|Z(G)|$  é igual a p ou  $p^2$  e portanto  $(G:Z(G))$  é igual a p ou 1. Logo o grupo quociente é cíclico. Se  $x \in Z(G)$  é um gerador deste grupo, segue que  $G = \langle x, Z(G) \rangle$  e como x comuta com cada elemento de  $Z(G)$ , temos que G é abeliano.

## IV. Referências Bibliográficas

- J.J.Rotman, Advanced Modern Algebra, Prentice Hall, revised 2nd ed., 2003.
- A. Garcia e Y. Lequain, Elementos de Algebra, IMPA, 2nd ed., 2003.
- N. O. Dantas, Estruturas Algébricas I, CESAD-UFS, 2009.
- C. Polcino Milies, Grupos Nilpotentes: Uma Introdução, IME-USP, 2003.

\* A impressão deste foi financiada pela FAPEG .