GRUPOS DE PERMUTAÇÕES E GRUPOS FINITOS SIMPLES

Lauro Maycon Fernandes Ferreira[1], Antonio Carlos Tamarozzi[2], Sônia Angelina Garcia Modesto[3]

[1]Aluno do Curso de Bacharelado em Matemática da UFMS; e-mail: laurorg94@hotmail.com. [2]Professor da UFMS, Campus de Três Lagoas, Departamentos de Ciências Exatas. [3]Professora da UFMS, Campus de Três Lagoas, Departamentos de Ciências Exatas.

RESUMO

A normalidade de subgrupos em um grupo finito foi uma propriedade descoberta por E. Galois em 1832, no estudo do grupo de permutações de raízes de equações polinomiais. A partir de então, este conceito foi explorado extensivamente agregando definições e propriedades que colaboraram para a descrição de vários conceitos de impacto na estrutura de grupos finitos. Neste trabalho apresentamos um desenvolvimento introdutório da Teoria dos Grupos de Permutações, com vistas a apresentar exemplos de grupos simples. Esta investigação propiciou contato com técnicas importantes para o desenvolvimento da Teoria dos Grupos, baseadas em subgrupos normais, centralizadores, equação das classes, p-grupos e o primeiro teorema de Sylow.
Palavras-chave: subgrupos normais; permutações; grupos solúveis.

GROUP OF PERMUTATIONS AND FINITE SIMPLE GROUPS

ABSTRACT

The normality of subgroups in a finite group has a property discovered by E. Galois in 1832, study-group of permutations of roots of polynomial equations. Since then, this concept was explored extensively by adding definitions and properties that contributed to the description of various concepts of impact on the structure of finite groups. This paper presents an introductory development of group theory of permutations, in order to present examples of simple groups. This research has provided important technical contact for the development of group theory, based on normal subgroups, centralizers,class equation, p-groups and Sylow first theorem.
Key words: normal subgroups, permutations, solvable groups

1. INTRODUÇÃO

A teoria de permutações iniciou com o estudo de Cauchy (1789-1857) publicado em 1815, cuja motivação principal era a de explorar as permutações de raízes de equações algébricas. Somente em 1844, Cauchy publicou um artigo principal que determina a teoria de permutações como um assunto de sua autoria. Ele introduz a notação de potências positivas e negativas para permutações (com a permutação na potência 0 (zero) sendo a identidade), define ordem de uma permutação e introduz a notação de ciclo, amplamente empregada nas referências (DEAN), (GARCIA; LEAQUIN, 1989; GONÇALVES, 1980).

Evariste Galois [1811-1832] foi o primeiro matemático a realmente entender que a solução algébrica de uma equação polinomial está relacionada com a estrutura do grupo de permutações relativas à equação. A existência de uma condição necessária e suficiente para a solução da equação de quinto grau com coeficientes racionais e por meio de radicais foi apresentada por Evariste Galois em 1832, na véspera de sua morte. A Teoria de Galois introduziu conceitos fundamentais para o desenvolvimento da Teoria dos Grupos, como subgrupos normais e a solubilidade, uma vez que a solução da equação algébrica está relacionada a existência de uma cadeia de subgrupos normais.

A Teoria de Galois destaca portanto a importância da existência de subgrupos normais para um determinado grupo. Os grupos simples são os grupos não abelianos que não admitem subgrupos normais não triviais. Galois estabeleceu a não resolução de equações algébricas de quinto grau, devido exatamente a simplicidade dos grupos de permutações de cinco elementos.

2. METODOLOGIA

Ao longo do trabalho desenvolvemos a teoria inicial dos grupos de permutações e as ferramentas da Teoria dos Grupos necessária para a compreensão de algumas das consequências do impacto da existência de subgrupos normais em Grupos Finitos.

Para o desenvolvimento do trabalho foram empregados técnicas e métodos tradicionalmente utilizados na demonstração de proposições da Teoria dos Grupos de Permutação e Grupos Finitos.

As principais referências bibliográficas consultadas foram: (BAUMSLAG, 1968; DEAN, 1978) para a revisão da teoria elementar dos Grupos, (GONÇALVES, 1980; HERSTEIN,1970) para Grupos de permutações, Grupos Solúveis , *p*-grupos finitos e os Teoremas de Sylow.

3. RESULTADOS E DISCUSSÃO

Dado um grupo *G*, não necessariamente finito, introduziremos a seguir algumas categorias de subgrupos de *G* que estão intrinsecamente relacionadas ao objetivo deste trabalho. Sem perda de generalidade e, com base na literatura, vamos admitir que a operação de *G* seja multiplicativa.

Consideremos o conjunto $Z(G)=\{a\in G / ax=xa, \forall\, x\in G\}$, dos elementos de *G* que comutam com todos os elementos de *G*. É fácil constatar que *Z(G)* é um subgrupo, chamado centro do grupo *G,* para o qual temos: *G* é abeliano, se, e somente se, *Z(G) = G.*

Considerando qualquer elemento $x\in G$, podemos considerar o subconjunto $C_G(x)=\{g\in G / xg=gx\}$ de *G*. Esse conjunto é um subgrupo de *G,* chamado centralizador de *x* em *G*. E ainda, $C_G(x)=G$, se, e somente se $x\in Z(G)$.

Dado *a* um elemento qualquer de *G*, o subgrupo gerado por *a* é o seguinte conjunto

$\langle a\rangle=\{a^k, k\in\mathbf{Z}\}$. O numero de elemento de $\langle a\rangle$ é chamando de ordem de *a*. Se $G=\langle a\rangle$, dizemos que *G* é um grupo cíclico, caso em que *a* é chamado gerador do grupo. Este subgrupo proporciona a verificação de resultados fortes na Teoria dos Grupos, como a seguinte aplicação do Teorema de Lagrange: Todo grupo de ordem prima é cíclico.

Dado um grupo finito *G*, uma das principais relações entre Z(*G*) e $C_G(x)$ é dada pela seguinte igualdade

$$|G| = |Z(G)| + \sum_{x\notin Z(G)} |C(x)| =$$

$$|Z(G)| + \sum_{x\notin Z(G)} |G : C_G(x)|$$

conhecida como a equação das classes.

Seja *S* um subconjunto não vazio de *G*, então podemos definir o conjunto
<S> = {$a_0\, a_1\, a_{2...}a_n$ / $n \in$ *IN* e $a_0, a_1, a_{2...}, a_n \in S$}. Este é o subgrupo de *G* gerado por S, que generaliza o caso <*a*>, em que S={*a*}.

Um subgrupo interessante que se pode observar a partir de *G* é o subgrupo gerado pelo conjunto $S=\left\{xyx^{-1}y^{-1} / x,\ y\in G\right\}$. Trata-se do subgrupo dos comutadores de *G*, que denotamos por *G'*, ou seja G'=$\langle S\rangle \le G$. Avaliando o tamanho de *G'*, podemos ter uma idéia do quanto *G* é abeliano.

Subgrupos normais

Um outro fato muito utilizado em teoria dos grupos é que sendo *H* um subgrupo de *G* o conjunto $N_G(H)=\{g\in G / g.H = Hg\}$ é um subgrupo de *G* , chamado normalizador de *H* em *G*. Se $N_G(H)=\{g\in G / gH = Hg\}$ = *G* então dizemos que *H* é um subgrupo normal de *G*, que é denotado por $H \lhd G$.

Enunciaremos, a seguir, uma sequência de resultados sobre a normalidade de subgrupos de um grupo *G*. As verificações dos resultados podem ser encontradas em (BAUMSLAG, 1968; HERSTEIN, 1970).

Proposição 1: Seja *G* um grupo e *N* um subgrupo de *G*. As afirmações seguintes são equivalentes:

(i) N é um subgrupo normal de *G;*

(ii) $aN = Na$, $\forall a\in G$;

(iii) $a.N.a^{-1}\subseteq N, \forall\ a\in G$;

(iv) $a.na^{-1}\in N, \forall a\in G, \forall n\in N.$

Proposição 2: Seja *G* um grupo, então:

(i) $Z(G)\lhd G$ e $G'\lhd G$;

(ii) $H\le Z(G)\Rightarrow H\lhd G$;

(iii) G/Z(G) é cíclico $\Rightarrow$ *G* é abeliano $\Leftrightarrow$ *Z(G) = G.*

Proposição 3: Seja *G* um grupo e N um subgrupo normal de *G*. Então:

(i) Subgrupos de *G/N* são da forma *H/N*, onde *H* é um subgrupo de *G*;

(ii) Se $N\le H$, então $H/N\lhd G/N \ \Leftrightarrow\ H\lhd G$.

Para verificar esta proposição basta, usarmos a definição de normalidade apresentada na proposição 1.

Teorema 1: (Teorema do homomorfismo). Sejam *G* e *J* grupos com identidades e e u respectivamente e $\psi: G\to J$ um homomorfismo. Então vale o seguinte:

(i) $\mathrm{Im}\psi=\psi(G)=\{\psi(g): g\in G\}$ é subgrupos de *J*.

(ii) $N(\psi)=\{g\in G:\psi(g)=u\}$ é subgrupo normal de *G* (chamado de núcleo do homomorfismo) e mais ψ é injetiva $\Leftrightarrow N(\psi)=\{e\}$.

(iii) $G/N(\psi)\approx \mathrm{Im}\psi$.

Proposição 4: Seja *G* um grupo, então *Aut(G)* é grupo para a operação de composição de funções $(\circ)$.

Definição: O automorfismo $I_g : G \to G,\ I_g(x) = gxg^{-1}$ é chamado *automorfismo interno* associado ao elemento $g \in G$ e o conjunto dos automorfismos internos será denotado por $I(G) = \{I_g \,/\, g \in G\}.$

Uma relação importante no grupo dos automorfismos de um grupo *G* é dada pela seguinte proposição.

Proposição 5: $I(G) \lhd Aut(G).$

Shumyatsky e Tamarozzi (2002) estenderam as técnicas de Thompson (1959) e apresentaram uma condição para um grupo finito que admite um automorfismo sem pontos fixos ser nilpotente.

Grupos de Permutações

Seja *X* um conjunto. Então o conjunto $S(X) = \{\sigma : X \to X \,/\, \sigma$ é bijetora}, munido da operação de composição de funções, é um grupo chamado de grupo das permutações sobre *X*. Se *X*={1, 2, ..., *n*}, então *S*(*X*) é chamado S_n , e uma permutação σ de S_n é denotada por $\sigma =$

$$\begin{pmatrix} 1 & 2 & 3 & ... & n \\ \sigma(1) & \sigma(2) & \sigma(3) & ... & \sigma(n) \end{pmatrix}.$$

Observação: Se *X*={1, 2, ..., n} então da analise combinatória elementar pode-se mostrar que $|S(X)| = n!$.

Definição: Seja σ uma permutação de S_n . Chamamos σ de *r*-ciclo se existir elementos $a_1, a_2, ..., a_r \in \{1, 2, ..., n\}$ tais que $\sigma(a_1) = a_2,\ \sigma(a_2) = a_3,\ ...,\ \sigma(a_{r-1}) = a_r,$ $\sigma(a_r) = a_1$, e para todo $j \in \{1, 2, ..., n\} - \{a_1, a_2, ..., a_r\},\ \sigma(j) = j$.

Denotamos esse *r*-ciclo por $(a_1\ a_2\ ...\ a_r)$.

Em um *r*-ciclo, o número *r* é chamado comprimento do ciclo onde $\{a_1, a_2, ..., a_r\}$ é o conjunto suporte de σ, e os 2-ciclos são chamados transposições.

Proposição 6: Seja $\sigma \in S_n$ uma permutação. Então σ pode ser escrita como um produto de ciclos disjuntos. E essa fatoração é única, a não ser pela ordem dos ciclos.

Seja σ um r-ciclo qualquer, então σ = $(a_1\ a_2\ ...\ a_r)$, podemos verificar facilmente que, $(a_1\ a_2) \circ (a_1\ a_3) \circ ... \circ (a_1\ a_{r-1}) \circ (a_1\ a_r) = \sigma$ ou seja σ pode ser fatorada como um produto de transposições. Se σ pode ser fatorada com um número par de transposições, então dizemos que σ é uma permutação par. Do contrário, σ é chamada uma permutação ímpar. A fatoração de uma permutação em transposições não é única, porém conserva-se a paridade, o que permite definirmos o subconjunto de S_n a seguir.

Seja A_n o conjunto de todas as permutações pares em S_n . O fechamento da composição para permutações pares e a propriedade $(ab)^{-1} = b^{-1}a^{-1}$, válida em qualquer grupo, asseguram que A_n é um subgrupo de S_n . Este é o grupo alternado de grau *n*. Pode-se mostrar que $|A_n| = \frac{n!}{2}$. Como $|S_n| = n!$, vemos que A_n é um subgrupo de S_n de índice 2, de onde segue que $A_n \lhd S_n$.

***p*-grupos finitos**

Dado um grupo finito G, se H é um subgrupo de G que é um *p*-grupo, dizemos que H é um *p*-subgrupo de G. O primeiro teorema de Sylow assegura a existência de *p*-subgrupos de Sylow em G para todo primo divisor de |*G*|. Para *p*-grupos finitos, a utilização da equação das classes, mencionada acima, possibilita os seguintes resultados:

Proposição 7: Seja *p* um número primo e G um grupo finito de ordem p^n, com $n \geq 1$. Então, $|Z(G)| \geq p$.

Proposição 8: Seja *G* um grupo de ordem *p* ou p^2, então *G* é abeliano.

Dado um grupo finito *G*, se *H* é um subgrupo de *G* que é um *p*-grupo, dizemos que *H* é um *p*-subgrupo de *G*. O primeiro teorema de Sylow assegura a existência de *p*-subgrupos de Sylow em G para todo primo divisor de $|G|$.

Primeiro Teorema de Sylow: Sejam *G* um grupo finito e *p* um número primo tal que p^m divide a ordem de *G*, para algum *m*. Então $\exists\, H \subseteq G$ onde $|H| = p^n$, para $0 \leq n \leq m$.

A simplicidade dos grupos A_n, $n \geq 5$

Agora vamos introduzir conceitos para mostramos a simplicidade dos grupos A_n, $n \geq 5$. Com este objetivo vamos introduzir o conceito de solubilidade. Como resultado particular teremos a não solubilidade dos grupos S_n, $n \geq 5$.

Definição: Um grupo *G* diz-se *solúvel* se existem subgrupos que satisfazem à cadeia $\{e\} \leq G_0 \leq G_1 \leq G_2 \leq ... \leq G_{n-1} \leq G_n = G$ tais que:

(i) $G_{i-1} \lhd G_i,\ \forall\ i \in \{1,2,...,n\}$

(ii) G_i / G_{i-1} é abeliano $\forall i \in \{1,2,...,n\}$.

É fácil verificar que a solubilidade é preservada para subgrupos e quocientes:

Proposição 9:a) Todo subgrupo de grupo solúvel é solúvel.

b) Todo quociente de um grupo solúvel é solúvel.

É imediato observar que todo grupo abeliano é solúvel. Mas temos o seguinte resultado interessante para os *p*-grupos finitos:

Proposição 10: Se *G* é um *p*-grupo então *G* é solúvel.

A importância de grupos solúveis para a Teoria dos Grupos, fica evidenciada, a partir de dois resultados famosos na teoria dos grupos finitos que enunciaremos a seguir. O primeiro provado por W. Burnside no início do século e o segundo, no início da década de 1960, por W-Feit, e J. Thompson.

Teorema 2: $p^a.q^b$ (Burnside). Todo grupo finito cuja ordem é divisível no máximo por dois primos é solúvel.

Teorema 3: (W. Feit & J. Thompson). Todo grupo de ordem impar é solúvel.

Proposição 11: a) O grupo S_n, $n \geq 2$ é gerado pelo conjunto de todas as transposições de S_n.

b) O grupo A_n, $n \geq 3$ é gerado pelo conjunto de todos 3-ciclos de S_n.

c) Sejam $a, b \in \{1,2,...,n\}, a \neq b$. Então para $n \geq 3$, $A_n = \langle \{(abi) \mid i = 1,2,...,n;\ i \neq a,\ b\} \rangle$.

Teorema 4: O grupo A_n é um grupo finito simples para $n \geq 5$.

Corolário 1: O grupo S_n tem como subgrupos normais apenas os subgrupos triviais e o grupo A_n, para $n \geq 5$.

Corolário 2: O grupo S_n, $n \geq 5$, não é solúvel.

Demonstração: Temos que $A_n \leq S_n$ e A_n é não solúvel que o subgrupo normal de A_n diferente dele mesmo é {*e*}, e $A_n / \{e\} = \{\{e\}\sigma \mid \sigma \in A_n\} = A_n$ que é não-abeliano, que contraria a definição de grupos solúveis. E assim pela proposição 9 S_n, $n \geq 5$, não é solúvel.

Podemos observar que o grupo A_4 tem como únicos subgrupos normais os subgrupos triviais e o grupo K, o grupo de Klein, onde $K = \{id,\ (1\ 2)\circ(3\ 4),\ (1\ 3)\circ(2\ 4),\ (1\ 4)\circ(2\ 3)\}$

. Enquanto que o grupo S_4 tem como subgrupos normais apenas os triviais, o grupo A_4 e o grupo de Klein.

4. CONCLUSÕES

A normalidade de subgrupos de um grupo finito foi uma propriedade descoberta por E. Galois em 1832, no estudo do grupo de permutações de raízes de equações polinomiais. A partir de então, este conceito foi explorado extensivamente agregando definições e propriedades que colaboraram para a descrição de vários conceitos de impacto na estrutura de grupos finitos. Os grupos finitos simples são os grupos irredutíveis quanto a normalidade e são alvo de investigações que possibilitam aplicações não apenas à Matemática mas para diversas outras áreas do conhecimento.

No trabalho desenvolvemos a teoria introdutória dos grupos de permutações com a finalidade principal de apresentar exemplos de grupos simples. O primeiro grupo simples é o grupo alternado de grau 5, cuja ordem é 60. Além da normalidade as conclusões do trabalho requereram o desenvolvimento de algumas técnicas e ferramentas para a Teoria dos Grupos, baseadas em subgrupos característicos, centralizadores, equação das classes, *p*-grupos e o primeiro teorema de Sylow.

REFERÊNCIAS

BAUMSLAG, B.; CHANDLER, B. **Theory and problems of Group Theory**. New York: McGrawhill, 1968.

DEAN, R. **Elementos de Álgebra Abstrata**. Rio de Janeiro: LTC, 1978.

GARCIA, A.; LEAQUIM, I. **Álgebra, um Curso de Introdução**. Rio de Janeiro: Impa, 1989.

GONÇALVES, A. **Introdução à Álgebra**. Rio de Janeiro: Impa, 1980.

HERSTEIN, I. **Tópicos de Álgebra**. São Paulo: Polígono, 1970.

SHUMYATSKY, P.; TAMAROZZI, A. On finite groups with fixed–point–free automorphisms. **Communications in Algebra**, v. 30, p. 2837–2842, 2002. http://dx.doi.org/10.1081/AGB-120003992

THOMPSON, J. Finite Groups with Fixed-Point-Free Automorphisms of Prime Order. **Proceedings of the National Academy of Sciences of the United States of America**, v. 45, n. 4, p. 578-581, 1959. http://dx.doi.org/10.1073/pnas.45.4.578