A SIMPLICIDADE DOS GRUPOS $A_n, n \geq 5$.

ELEMAR RAPACHI PUHL[1]; JULIANA BORGES PEDROTTI[2]; ANDREA MORGADO[3]

[1]*Universidade Federal de Pelotas – elemarrp@hotmail.com*
[2]*Universidade Federal de Pelotas – julianabpedrotti@gmail.com*
[3]*Universidade Federal de Pelotas – andrea.morgado@ufpel.edu.br*

1. INTRODUÇÃO

Problemas relacionados a resoluções de equações algébricas começam a aparecer desde cedo na vida escolar. Mesmo com o uso exaustivo dessas equações, pouco se sabe sobre a história, importância ou como se desenvolveram suas formas de resoluções por meio de solubilidade por radicais, ou seja, através de fórmulas envolvendo os coeficientes da equação em questão e operações de soma, subtração, multiplicação, divisão, potenciação e radiciação entre estes.

Em torno de 1830, surgiu um dos resultados mais importantes sobre resolução de equações algébricas: E. Galois provou a insolubilidade por meio de radicais de equações gerais de grau maior ou igual a cinco. Este trabalho, publicado em 1846 por Joseph Liouville, em Journal de Mathématiques, possibilitou grande avanço matemático na época, pois até então só se sabia que equações de grau 1, 2, 3 e 4 eram solúveis por radicais e que equações de grau 5 não eram solúveis.

Com a finalidade de pesquisar a famosa Teoria de Galois, criou-se o projeto de pesquisa Iniciação Científica em Teoria de Galois. Como nesta teoria unem-se dois importantes conceitos em Álgebra – os conceitos de Corpo e Grupo – foi necessário um estudo profundo destes.

Dentro do contexto de Grupos nosso trabalho visa apresentar um resultado que nos fornece uma classe de exemplos de grupos simples (ver Teorema 3.3) e, consequentemente, grupos não solúveis (ver página 4). Especificando, vamos mostrar que os grupos das permutações pares A_n, tal que $n \geq 5$, são grupos simples e, como um corolário deste resultado, segue que o grupo de permutações S_n, $n \geq 5$ não é solúvel.

2. METODOLOGIA

O desenvolvimento do trabalho se deu através de estudo contínuo, a partir do livro texto *Introdução à Álgebra* e demais referências, contando com encontros periódicos com a professora orientadora. Durante este processo foi priorizada a pesquisa individual para a resolução dos desafios surgidos. Por fim, houve a apresentação, através de seminários semanais, dos resultados estudados para a professora orientadora e os demais participantes do projeto. Nosso principal intuito nesse momento foi fomentar a discussão em grande grupo, com a finalidade de remate das dúvidas obtidas durante o trabalho individual.

3. RESULTADOS E DISCUSSÃO

Neste trabalho, temos por objetivo provar a simplicidade dos grupos A_n, $n \geq 5$, para tal necessitamos apresentar algumas definições e resultados anteriores que servem como base para a demonstração. Lembremos que se S é um conjunto finito, então podemos considerar o *grupo das permutações* $S_n = \{\sigma: S \to S: \sigma \text{ é } função\ bijetiva\}$, com a operação de composição e unidade dada por $e = Id_S$. Dizemos que uma permutação $\sigma \in S_n$ é um *r-ciclo de S_n*, $r \geq 2$, se existem elementos dois a dois distintos $i_1, i_2, \ldots, i_r \in \{1, 2, \ldots, n\}$, tais que:

$$\sigma(i_1) = i_2, \sigma(i_2) = i_3, \ldots, \sigma(i_{r-1}) = i_r, \sigma(i_r) = i_1$$

e

$$\sigma(j) = j, \ \forall j \in \{1, 2, \ldots, n\} \backslash \{i_1, i_2, \ldots, i_r\}.$$

Podemos denotar um r-ciclo por $\sigma = (i_1\, i_2 \ldots i_r)$. Por exemplo, a permutação em S_4 dada por $\sigma(1) = 3$, $\sigma(2) = 2$, $\sigma(3) = 4$ e $\sigma(4) = 1$ é um 3-ciclo, denotado por $\sigma = (134)$. Um 2-ciclo é também chamado de *transposição*.

Sejam $\sigma = (i_1\, i_2 \ldots i_r)$ e $\tau = (j_1\, j_2 \ldots j_s)$ dois ciclos de S_n. Dizemos que $\sigma\ e\ \tau$ são dois ciclos disjuntos, se $\{i_1, i_2, \ldots, i_r\} \cap \{j_1, j_2, \ldots, j_s\} = \emptyset$. Por exemplo, os ciclos de S_6 dados por $\sigma = (145)$ e $\tau = (236)$ são disjuntos.

Proposição 3.1 [GONÇALVES, 2012]**:** Nas condições anteriores, toda permutação $e \neq \sigma \in S_n$ pode ser escrita de modo único, a menos de ordem, como um produto de ciclos disjuntos.

Uma permutação σ em S_n, $n \geq 3$, é dita *permutação par* se σ é um produto de um número par de transposições. Temos que o conjunto das permutações pares de S_n, denotado por A_n, é um subgrupo de S_n, com ordem $n!/2$. Com base nessas definições temos o seguinte resultado, o qual é de suma importância para mostrar a simplicidade dos grupos A_n.

Proposição 3.2 [GONÇALVES, 2012]**:** Nas condições anteriores,

i. o grupo S_n, $n \geq 2$, é gerado pelo conjunto de todas as transposições de S_n;
ii. o grupo A_n, $n \geq 3$, é gerado pelo conjunto de todos os 3-ciclos de S_n. Em particular, o grupo A_n, $n \geq 3$, é gerado pelo conjunto de todos os 3-ciclos de S_n do tipo (abk), onde $a, b \in \{1, 2, \ldots, n\}$, $a \neq b$, são fixos e $1 \leq k \leq n$, $k \neq a$, $k \neq b$.

Com isso, podemos apresentar o resultado principal deste trabalho.

Teorema 3.3 [GARCIA, LEQUAIN, 2013]**:** Nas condições anteriores, o grupo A_n, $n \geq 5$, é simples, ou seja, seus únicos subgrupos normais são $\{e\}$ e A_n.

Demonstração:

Seja $N \trianglelefteq A_n$, $N \neq \{e\}$. Primeiramente, vamos mostrar que N contém um 3-ciclo e com isso provar que $N = A_n$. Como $N \neq \{e\}$, $\exists\ \sigma \in N$, tal que $\sigma \neq e$. Consideremos a ordem de σ dada por $m = \mathcal{O}(\sigma)$. Como $\sigma \neq e$, temos $m > 1$.

Seja um primo $p \in \mathbb{N}$ tal que $p|m$. Assim, $m = pq$ para algum $q \in \mathbb{N}$. Considere $\tau = \sigma^q \in N \subset A_n$, então $\tau \neq e$ e $\mathcal{O}(\tau) = p$. Pela Proposição 3.1, τ é um produto de ciclos disjuntos, digamos $\tau = \rho_1\rho_2 \dots \rho_s$.

Note que $p = \mathcal{O}(\tau) = \mathcal{O}(\rho_1\rho_2 \dots \rho_s) = mmc\{\mathcal{O}(\rho_1), \mathcal{O}(\rho_2), \dots, \mathcal{O}(\rho_s)\}$,o que implica $\mathcal{O}(\rho_i)|p$, $\forall\ i \in \{1,2,\dots,s\}$. Como $\rho_i \neq e$ $\forall\ i \in \{1,2,\dots,s\}$, segue que $\mathcal{O}(\rho_i) = p$. Logo, ρ_i é p-ciclo e $\tau = \rho_1\rho_2 \dots \rho_s$ onde todos os ρ_i é p-ciclo, $i \in \{1,2,\dots,s\}$.

Vamos dividir a demonstração em casos:

<u>CASO 1</u>: $p = 2$

Neste caso, todos os ρ_i's são transposições. Se considerarmos $s = 1$, então $\tau = \rho_1 \notin A_n$. Logo, $s \geq 2$ e, além disso, s é par, pois $\tau \in A_n$.

Escrevendo $\rho_1 = (ab)$ e $\rho_2 = (cd)$, então $\tau = (ab)(cd)\rho_3 \dots \rho_s$. Seja $u = (abc) \in A_n$, então $x = u\tau u^{-1}\tau^{-1} \in N$, pois $N \trianglelefteq A_n$. Assim,

$$\begin{aligned} x = u\tau u^{-1}\tau^{-1} &= (abc)(ab)(cd)\rho_3 \dots \rho_s(cba)\rho_s^{-1} \dots \rho_3^{-1}(cd)(ab) \\ &= (abc)(ab)(cd)\rho_3 \dots \rho_s\rho_s^{-1} \dots \rho_3^{-1}(cba)(cd)(ab) \\ &= (abc)(ab)(cd)(cba)(cd)(ab) \\ &= (ac)(bd) \end{aligned}$$

Logo, $(ac)(bd) = u\tau u^{-1}\tau^{-1} = x \in N$.

Lembremos que $n \geq 5$, então existe $k \in \{1,2,\dots,n\} \backslash \{a,b,c,d\}$. Seja $v = (akc) \in A_n$. Temos que $y = v(u\tau u^{-1}\tau^{-1})v^{-1} \in N$. Assim,

$$\begin{aligned} y = v(u\tau u^{-1}\tau^{-1})v^{-1} &= (akc)(ac)(bd)(cka) \\ &= (ak)(bd) \end{aligned}$$

Logo, $(ak)(bd) = v(u\tau u^{-1}\tau^{-1})v^{-1} = y \in N$.

Como $x,\ y \in N$, então $xy \in N$, pois $N \trianglelefteq A_n$. Logo,

$$xy = (ac)(bd)(ak)(bd) = (akc)$$

Portanto $xy = (akc) \in N$.

<u>CASO 2</u>: $p = 3$

Se $s = 1$, $\tau = \rho_1 \in N$ é um 3-ciclo. Seja $s \geq 2$ e $\rho_1 = (abc)$ e $\rho_2 = (def)$, então $\tau = (abc)(def)\rho_3 \dots \rho_s$. Considere $u = (bcd) \in A_n$, deste modo $u\tau u^{-1}\tau^{-1} \in N$. Assim, por cálculos análogos ao caso anterior, temos que $u\tau u^{-1}\tau^{-1} = (adbce)$. Logo, encontramos um 5-ciclo $u\tau u^{-1}\tau^{-1} = (adbce)$ em N. Portanto, o caso $p = 3$ está reduzido ao próximo caso:

<u>CASO 3</u>: $p > 3$

Seja $\rho_1 = (a_1a_2a_3 \dots a_p)$, então $\tau = (a_1a_2a_3 \dots a_p)\rho_2\rho_3 \dots \rho_s \in N$. Considere $u = (a_1a_2a_3) \in A_n$, deste modo $u\tau u^{-1}\tau^{-1} \in N$ pois $N \trianglelefteq A_n$. Assim, $u\tau u^{-1}\tau^{-1} = (a_1a_2a_4)$. Portanto, $u\tau u^{-1}\tau^{-1} = (a_1a_2a_4)$ é um 3-ciclo em N.

Assim sendo, provamos então que existe um 3-ciclo $(abc) \in N$. Logo, temos que $(bac) = (abc)^2 \in N$. Consideremos $\varphi = (ab)(ck) \in A_n$. Como $N \trianglelefteq A_n$ temos que

$$\varphi^{-1}(bac)\varphi = (ck)(ab)(bac)(ab)(ck) = (abk) \in N, \ \forall \, k \in \{1, 2, \dots, n\} \backslash \{a, b\}.$$

Pela Proposição 3.2, item (ii), segue que $N = A_n$. ■

Lembremos que um grupo G é dito *solúvel*, se existem subgrupos:

$$\{e\} = G_0 \leq G_1 \leq G_2 \leq \ldots \leq G_{n-1} \leq G_n = G,$$

tais que:

i. $G_{i-1} \trianglelefteq G_i$, para todo $i \in \{1, 2, \dots, n\}$;
ii. G_i/G_{i-1} é abeliano, para todo $i \in \{1, 2, \dots, n\}$.

Note que todo subgrupo de um grupo solúvel é solúvel. Logo, se o grupo $S_n, n \geq 5$ fosse solúvel, então o subgrupo A_n seria solúvel, ou seja, existiria uma cadeia $\{e\} = G_0 \leq G_1 \leq G_2 \leq \ldots \leq G_{n-1} \leq G_n = A_n$, tal que $G_{n-1} \trianglelefteq A_n$. Como $A_n, \ n \geq 5$ é simples, segue que $G_{n-1} = \{e\}$ e, sendo assim $A_n = {}^{A_n}/_{e}$, abeliano, o que é um absurdo. Dessa maneira, segue o seguinte corolário do Teorema 3.3:

Corolário 3.4: O grupo $S_n, n \geq 5$, não é solúvel.

4. CONCLUSÕES

Com estes resultados conseguimos uma infinidade de exemplos de grupos simples e não solúveis. A partir de agora vamos dar continuidade a pesquisa sobre Teoria de Galois. Dentro deste contexto, estudaremos aplicações dos resultados citados neste trabalho, por exemplo, utilizar a não solubilidade de S_5 para provar que o polinômio $f(x) = x^5 - 6x + 3 \in \mathbb{Q}[x]$ não é solúvel por meio de radicais sobre $\mathbb{Q}$.

5. REFERÊNCIAS BIBLIOGRÁFICAS

.

GARCIA, A.; LEQUAIN, Y. **Elementos de Álgebra.** 6º ed. Rio de Janeiro. IMPA, 2013.

GONÇALVES, A. **Introdução à Álgebra.** 5º ed. Rio de Janeiro: IMPA, 2012.

I.N. HERSTEIN. **Topics in Algebra 2nd Edition**. Wiley India Pvt. Limited, 2006.

MONTEIRO, L. H. J. **Elementos de Álgebra.** Elementos de Matemática. IMPA, 1969.

OWEN, J. BRISON. **Teoria de Galois**. Faculdade de Ciências da Universidade de Lisboa, Textos de Matemática, 1997.

STEWART, I. **Galois Theory 3rd Edition**. Chapman and Hall, 2000.