GRUPOS FINITOS: O TEOREMA DE CAYLEY

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

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

1. INTRODUÇÃO

Na área da Álgebra, um dos problemas de maior relevância ao longo da história foi o de encontrar soluções para equações polinomiais. Durante muito tempo, o principal intuito era o de encontrar fórmulas que envolvessem operações com os coeficientes da equação polinomial em questão (este método é chamado de solução por radicais). Até 1824 eram conhecidas soluções por radicais de equações de graus 1, 2, 3, e 4, e neste mesmo ano, N. H. Abel provou que a "equação geral" de grau 5 não era resolúvel por meio de radicais. Porém, não ficou estabelecido quando um polinômio de grau ≥ 5 é ou não resolúvel.

Em torno de 1843, tornaram-se públicos os trabalhos de E. Galois, o qual solucionou este problema de maneira geral, onde sua teoria consiste em caracterizar todos os polinômios os quais são solúveis por meio de radicais através de propriedades do grupo de automorfismos de um corpo. Além de resolver o problema de encontrar soluções de uma equação por meio de radicais, os trabalhos de Galois uniram duas teorias as quais são de extrema importância na área da Álgebra: a Teoria de Grupos e a Teoria de Corpos.

O Projeto de Pesquisa Iniciação Científica em Teoria de Galois foi criado com o intuito de estudar tal teoria. Para isso se fez necessário pesquisar mais profundamente as Teorias de Grupos e Anéis, com a finalidade de obter pré-requisitos para então estudar a importante Teoria de Galois.

O presente trabalho se propõe a apresentar o Teorema de Cayley, o qual surge como um corolário do Teorema de Representação para Grupos. Um dos problemas dentro da Teoria de Grupos é o de caracterizar o grupo segundo sua ordem. Neste sentido, o Teorema de Cayley nos mostra que todo grupo finito de ordem n é isomorfo a um subgrupo de $S_n = \{ f: S \to S \mid f \text{ é } função\ bijetiva\}$, onde S é um conjunto finito.

2. METODOLOGIA

Este trabalho se dá através de uma pesquisa em grupo, que vem sendo realizada desde o final de 2013, como um dos projetos de pesquisa na área de matemática da Universidade Federal de Pelotas. Este projeto tem como metodologia pesquisas em jornais, revistas e livros na área da Álgebra, guiados pela professora orientadora do projeto, onde cada integrante do grupo apresenta semanalmente um tópico em forma de seminário para os demais participantes.

3. RESULTADOS E DISCUSSÃO

Primeiramente, relembraremos algumas definições e resultados básicos dentro da teoria de Grupos, para então enunciarmos o Teorema de Representação e o Teorema de Cayley e darmos a demonstração destes.

Lembremos que um *grupo* é um conjunto G, distinto do vazio, munido de uma operação, a qual é associativa, possui elemento neutro e todo elemento do grupo possui inverso. Se G é um conjunto finito, então G é um grupo finito e a cardinalidade de G é chamado *ordem* de G, e denotamos por $|G|$. Um exemplo importante de grupos finitos se dá através da seguinte definição.

Definição 3.1 [Gonçalves, 2012]**:** Seja S um conjunto não vazio e considere o conjunto $G = \{ f: S \to S : f \text{ função bijetiva}\}$. Temos que G com a operação de composição de funções é um grupo, chamado *grupo de permutações do conjunto* S. Se S é um conjunto finito, dado por $S = \{1,2, \dots, n\}$, então G é denotado por S_n e é fácil ver que $|S_n| = n!$.

Se H é subconjunto não vazio de G, o qual é um grupo com a operação de G, então dizemos que H é um *subgrupo de* G, e denotamos $H \leq G$. Mais ainda, se $\mathrm{g^{-1}Hg} \subset \mathrm{H}$, onde $\mathrm{g^{-1}Hg} = \{\mathrm{g^{-1}hg: h} \in \mathrm{H}\}$, para todo $g \in G$, então dizemos que H é um *subgrupo normal de* G , e denotamos $H \trianglelefteq G$.

Note que se G é um grupo e $H \leq G$, podemos definir uma relação de equivalência em G, a qual é dada por $x \equiv y (mod H)$ se, e somente se, $xy^{-1} \in H$, para quaisquer $x, y \in G$. Neste caso, chamamos *de classe lateral à direita* de H em G ao conjunto:

$$\bar{x} = Hx = \{hx : h \in H\},$$

e definimos, o *índice de* H *em* G como sendo o número de classes laterais de H em G, o qual é denotado $[G: H]$. Se $[G: H] = n$, temos que $G = Hx_1 \cup \dots \cup Hx_n$, onde $x_1, \cdots, x_n \in G$, são os representantes das classes da relação $\equiv (mod\ H)$.

Se G é um grupo e H é um subgrupo normal de G, mediante a relação acima, definimos em $G/H = \{Hx: x \in G\}$, uma operação dada por $Hx \cdot Hy = Hxy$, para quaisquer $x, y \in G$. Temos que G/H é um grupo com essa operação.

Sejam G e G' grupos e $\psi: G \to G'$ uma função de G em G'. Dizemos que ψ é um *homomorfismo de grupos,* se $\psi(xy) = \psi(x)\psi(y)$, para quaisquer $x, y \in G$ Se $\psi: G \to G'$ é um homomorfismo bijetor, então dizemos que ψ é um isomorfismo e que os grupos G e G' são isomorfos. Se G e G' são grupos com elementos neutros $e \in G$ e $e' \in G'$, então dizemos que o *núcleo* de um homomorfismo $\psi: G \to G'$ é o conjunto dado por:

$$N(\psi) = \{x \in G : \psi(x) = e'\} .$$

Com base nessas definições, podemos então enunciar um teorema o qual é uma ferramenta muito usada para demonstrar resultados dentro da teoria de grupos e será de suma importância para a prova do Teorema de Representação.

Teorema 3.2 (1º Teorema do Homomorfismo) [Gonçalves, 2012]**:** Sejam G e G' grupos com identidades e e e', respectivamente, e $\psi: G \to G'$ um homomorfismo de grupos. Então:

(i) $Im(\psi) = \psi(G) = \{\psi(g): g \in G\}$ é um subgrupo de G';

(ii) $N(\psi) = \{g \in G: \psi(g) = e'\}$ é um subgrupo normal de G e mais, ψ é injetora $\Leftrightarrow N(\psi) = \{e\}$;

(iii) ${}^{G}/_{N(\psi)}$ é isomorfo a $Im(\psi)$.

Com essas definições, temos as ferramentas necessárias e suficientes para enunciar o Teorema da Representação para Grupos, no qual o Teorema de Cayley seguirá como um corolário.

Teorema 3.3 (Teorema da Representação) [Gonçalves, 2012]**:** Seja G um grupo e H subgrupo de G de índice $[G:H] = n$. Então, existe $N \subseteq H, N \trianglelefteq G$, tal que ${}^{G}/_{N}$ é um grupo isomorfo a um subgrupo do grupo S_n.

Mais ainda, N é o "maior" subgrupo normal em G que está contido em H.

Demonstração: Sejam $S = {}^{G}/_{H} = \{Hx_1, \dots, Hx_n\}$ e $\mathcal{P}(S)$ o grupo de permutações do conjunto S. Considere a seguinte função $\psi : G \to \mathcal{P}(S)$, dada por:

$\psi(g)(Hx_i) = Hx_i g^{-1}$, para quaisquer $g \in G$ e $Hx_i \in S$.

Note que se $g \in G$ é tal que $\psi(g)(Hx_i) = \psi(g)(Hx_j)$, para $i, j \in \{1, \cdots, n\}$, então: $\psi(g)(Hx_i) = \psi(g)(Hx_j) \Leftrightarrow Hx_i g^{-1} = Hx_j g^{-1} \Leftrightarrow Hx_i = Hx_j$, ou seja, $\psi(g)$ é uma função injetiva, para todo $g \in G$. Portanto, $\psi(g): S \to S$ é uma bijeção, já que $|S| = n$. Logo, $\psi(g) \in \mathcal{P}(S) = \{f: S \to S: f \text{ é } bijeção\}$, para todo $g \in G$, provando assim que a aplicação ψ é bem definida.

Observemos que ψ é um homomorfismo, cujo núcleo é dado por:

$N(\psi) = \bigcap_{x \in G} H^x$, onde $H^x = \{x^{-1}hx: h \in H\}$, para todo $x \in G$.

De fato:

Se $g, h \in G$, então $\psi(gh)(Hx_i) = Hx_i(gh)^{-1} = Hx_i h^{-1} g^{-1} = \big(\psi(g) \circ \psi(h)\big)(Hx_i)$, para todo $Hx_i \in S$, logo ψ é um homomorfismo. Mais ainda, se $g \in N(\psi)$, então $\psi(g) = Id_S$, ou seja, $Hx_i g^{-1} = \psi(g)(Hx_i) = Id_S(Hx_i) = Hx_i$, para todo $Hx_i \in S$, o que implica $g \in H^{x_i}$, para todo $i \in \{1, \cdots, n\}$. Como $G = Hx_1 \cup \dots \cup Hx_n$, dado $x \in G$, então existe $j \in \{1, \cdots, n\}$ tal que $H^x = H^{x_j}$. Portanto, $g \in \bigcap_{x \in G} H^x$. Reciprocamente, seja $g \in \bigcap_{x \in G} H^x$. Em particular, $g \in H^{x_i}$, para todo $i \in \{1 \cdots, n\}$. Então, $\psi(g)(Hx_i) = Hx_i$, para todo $Hx_i \in S$, ou seja, $\psi(g) = Id_S$ e, logo , $g \in N(\psi)$.

Consideremos o subgrupo normal de G, dado por:

$N = N(\psi) = \bigcap_{x \in G} H^x \subset H^e = \{e^{-1}he : h \in H\} = H$.

Pelo Teorema do Isomorfismo G/N é isomorfo a imagem de ψ, a qual é um subgrupo de $P(S) \simeq S_n$.

Para provar a última afirmação, resta mostrar que se $L \trianglelefteq G$ e $L \subseteq H$, então $L = L^x \subseteq H^x, \ \forall\, x \in G$. De fato, para todo $x \in G$, segue diretamente da definição de subgrupo normal que $L^x \subset L$, já que $L \trianglelefteq G$, reciprocamente, se $l \in L$, então temos $l = x^{-1}xlx^{-1}x \in L^x$, já que $xlx^{-1} \in L$, pois $L \trianglelefteq G$. Portanto, $N = \bigcap_{x \in G} H^x$ é o "maior" subgrupo normal de G contido em H.

Corolário 3.4 (Teorema de Cayley) [Gonçalves, 2012]**:** Se G é um grupo de ordem n, então G é isomorfo a um subgrupo do S_n.

Demonstração: Note que se G é um grupo de ordem n, e se consideramos o subgrupo normal de G dado por $H = \{e\}$, então o Teorema de Cayley segue diretamente do Teorema de Representação com $N = \{e\}$.

4. CONCLUSÕES

Com este trabalho conseguimos enunciar um importante resultado de caracterização de grupos finitos de ordem finita n, já que vimos que todo grupo de ordem finita é isomorfo a um subgrupo do S_n. No que segue, daremos continuidade à pesquisa em Teoria de Galois.

5. REFERÊNCIAS BIBLIOGRÁFICAS

CRUZ, K. B., **Introdução Á Teoria de Galois.** 14 de março de 2014. Monografia (Trabalho de Conclusão de Curso). Curso de Licenciatura e Bacharelado em Matemática, Universidade Federal de São Carlos.

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

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

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

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.