TEOREMA DA CORRESPONDÊNCIA DE GALOIS

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

Na história da Matemática o problema de encontrar soluções de equações polinomiais é certamente um dos mais significativos. Durante muito tempo matemáticos tentaram encontrar formas de resoluções de tais equações por meio de solubilidade por radicais, ou seja, fórmulas envolvendo os coeficientes das equações em questão utilizando as operações de soma, subtração, multiplicação, divisão, potenciação e radiciação.

Até o século XVII já eram conhecidas as soluções por radicais das equações de grau 1, 2, 3 e 4. Em 1824, N. Abel demonstrou que equações polinomiais de grau 5 não eram em geral solúveis por radicais. Por volta de 1840, tornaram-se públicos os resultados de E. Galois, o qual demonstrou que equações de grau maior ou igual a 5 não são solúveis por radicais em geral. Estes resultados proporcionaram grandes avanços dentro da Matemática e a famosa "Teoria de Galois" é estudada até hoje em cursos de bacharelado e mestrado em Matemática, entre outros. Outro fator importante é que os resultados de E. Galois unem dois conceitos importantes de estruturas algébricas: o conceito de *grupo* e o conceito de *corpo*.

Com o intuito de estudar tal teoria dentro do curso de Licenciatura em Matemática criou-se no final de 2013 o projeto de pesquisa "Iniciação Científica em Teoria de Galois". Para estudar tais resultados fez-se necessário trabalhar com as Teorias de Grupos e Corpos. Como os alunos envolvidos não tinham experiência com esses conteúdos foi de fundamental importância estudar e aprofundar esses conceitos para compreender a Teoria de Galois.

Este trabalho visa apresentar e dar uma ideia da demonstração do importante Teorema da Correspondência de Galois, o qual dada uma extensão de corpos $M \supset K$ estabelece uma relação entre os subcorpos intermediários da extensão $M \supset K$ e os subgrupos do grupo de automorfismos $Aut_K M$ (ver página 3).

2. METODOLOGIA

Este trabalho se deu através do projeto de pesquisa Iniciação Científica em Teoria de Galois criado em 11 de novembro de 2013 no Departamento de Matemática e Estatística da UFPel. Seu desenvolvimento se deu através de estudo contínuo, a partir do livro texto "Introdução à Álgebra" [G] 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 apresentar o Teorema da Correspondência de Galois. Para tal, carecemos exibir algumas definições e resultados que servem como suporte para melhor entendimento do mesmo. Tais definições e resultados podem ser encontrados em [G], [H], [O] e [S]. É importante salientar que neste trabalho vamos considerar extensões finitas $L \supset K$ tal que $\mathbb{C} \supset L \supset K \supset \mathbb{Q}$.

Lembremos primeiramente que um corpo L é uma *extensão* do corpo K se $L \supset K$. Dada uma extensão $L \supset K$, temos que as operações do corpo L induzem em L uma estrutura de K-espaço vetorial. Se a dimensão de L como K-espaço vetorial é finita então dizemos que a extensão $L \supset K$ é *finita*. É possível provar que se $M \supset L \supset K$ são corpos tais que $dim_L M$ e $dim_K L$ são finitas, então $dim_K M$ é finita e

$$dim_K M = (dim_L M)(dim_K L) \qquad \textbf{(3.1)}$$

Além disso, um elemento $\alpha \in L \supset K$ é dito *algébrico sobre* K se existe um polinômio $f(x) \in K[x]\backslash\{0\}$ tal que $f(\alpha) = 0$. Se para todo $\alpha \in L$, temos que α *algébrico* sobre K então $L \supset K$ diz-se uma *extensão algébrica*.

Se $f(x) \in K[x]\backslash\{0\}$, chamamos de *corpo de decomposição de* $f(x)$ *sobre* K, denotado por $L = Gal(f, K)$, ao menor subcorpo de $\mathbb{C}$ que contém K e todas as raízes de $f(x)$ em $\mathbb{C}$. É provado em [G, página 93] que se $\alpha_1, \alpha_2, \dots, \alpha_n$ são as raízes de $f(x)$ em $\mathbb{C}$, então:

$$Gal(f, K) = K[\alpha_1, \dots \alpha_n] = \left\{ \sum_{fin} a_{j_1, j_2, \dots, j_n} \alpha_1^{j_1} \alpha_2^{j_2} \dots \alpha_n^{j_n} : a_{j_1, j_2, \dots, j_n} \in \mathbb{Q}, j_1, j_2, \dots, j_n \in \mathbb{N} \right\}.$$

Dizemos que uma extensão finita $L \supset K$ é uma *extensão galoisiana* se existe $f(x) \in K[x]$ tal que $L = Gal(f, K)$. Por exemplo, basta considerar $K = \mathbb{Q}[\sqrt[3]{2}]$ e $L = Gal(x^3 - 2, \mathbb{Q})$. Uma extensão algébrica $L \supset K$ é dita *normal* se para todo polinômio irredutível $g(x) \in K[x]$ sobre K, que possui uma raíz $\alpha \in L$, então $g(x)$ possui todas as suas raízes complexas em L. Por exemplo, basta considerar $K = \mathbb{Q}$ e $L = \mathbb{Q}[\sqrt{2}]$.

A seguir enunciaremos alguns resultados acerca da equivalência entre as definições de extensões galoisianas e extensões normais, os quais serão usados no decorrer do trabalho.

Proposição 3.2 [G, Página 172]: Seja $L \supset K$ uma extensão finita. Então as seguintes afirmações são equivalentes:

(1) $L \supset K$ galoisiana;
(2) $L \supset K$ normal;
(3) Para todo $\alpha \in L\backslash K$ existe $\sigma \in Aut_K L$ tal que $\sigma(\alpha) \neq \alpha$;
(4) $dim_K L = |Aut_K L|$.

Seja $M \supset K$ uma extensão finita. Dizemos que L é um *corpo intermediário* de $M \supset K$, se L é um subcorpo de M contendo K, ou seja, $M \supset L \supset K$. A partir de agora se $G = Aut_K M = \{f: M \longrightarrow M : f \text{ é } automorfismo\ de\ M\ sobre\ K\}$, então usaremos as seguintes notações:

$$\mathcal{J}(M, K) = \{L: corpo\ intermediário\ de\ M \supset K\} \qquad \mathcal{T}(G) = \{H: H\ subgrupo\ de\ G\}.$$

Se $H \in \mathcal{T}(G)$ então $L = \{a \in M: \gamma(a) = a \; \forall \; \gamma \in H\}$ é um corpo intermediário de $M \supset K$. Esse corpo L é chamado de *corpo fixo* de H. Considere agora as seguintes correspondências:

$$\psi: \mathcal{J}(M,K) \longrightarrow \mathcal{T}(G) \qquad \theta: \mathcal{T}(G) \longrightarrow \mathcal{J}(M,K)$$
$$L \longmapsto \psi(L) = Aut_L M \qquad H \longmapsto \theta(H) = \{a \in M: \gamma(a) = a \; \forall \; \gamma \in H\}$$

Observemos algumas propriedades dessas correspondências:

(1) $\psi(K) = Aut_K M = G$;

(2) $\psi(M) = Aut_M M = \{Id_M\}$;

(3) $\theta(\{Id_M\}) = \{a \in M: Id_M(a) = a\} = M$;

(4) $\theta(G) = \{a \in M: \gamma(a) = a \; \forall \; \gamma \in G\} \supseteq K$.

E pela Proposição 3.2 temos ainda que: $\theta(G) = K \Leftrightarrow M \supset K$ galoisiana.

(5) Se $L_1, L_2 \in \mathcal{J}(M,K)$ e $L_1 \subseteq L_2$ então $\psi(L_2) \leq \psi(L_1)$;

(6) Se $H_1, H_2 \in \mathcal{T}(G)$ e $H_1 \leq H_2$ então $\theta(H_1) \supseteq \theta(H_2)$;

(7) Para todo $L \in \mathcal{J}(M,K)$ tem-se $(\theta \circ \psi)(L) \supseteq L$;

(8) Para todo $H \in \mathcal{T}(G)$ tem-se $(\psi \circ \theta)(H) \geq H$.

Podemos agora enunciar o principal resultado deste trabalho, o qual vamos exibir uma ideia da demonstração apenas do item (c).

Teorema 3.3 [G, Página 181]: Se $M \supset K$ é uma extensão galoisiana, então:
a) Para todo $L \in \mathcal{J}(M,K)$ tem-se $dim_L M = |\psi(L)|$ e $dim_K L = [G: \psi(L)]$;
b) Para todo $H \in \mathcal{T}(G)$ tem-se $dim_{\theta(H)} M = |H|$ e $dim_K \theta(H) = [G:H]$;
c) $\psi \circ \theta = Id_{\mathcal{T}(G)}$ e $\theta \circ \psi = Id_{\mathcal{J}(M,K)}$;
d) Para todo $L \in \mathcal{J}(M,K)$, $L \supset K$ galoisiana se, e somente se, $\psi(L) = Aut_L M \trianglelefteq G$;
e) Se $L \in \mathcal{J}(M,K)$ e $L \supset K$ galoisiana então $dim_K L = |Aut_K L|$ e $G/_{\psi(L)} \simeq Aut_K L$.

Demonstração:

c) Queremos provar que $\psi \circ \theta = Id_{\mathcal{T}(G)}$ e $\theta \circ \psi = Id_{\mathcal{J}(M,K)}$, ou seja, $(\psi \circ \theta)(H) = Id_{\mathcal{T}(G)}(H) = H$ e $(\theta \circ \psi)(L) = Id_{\mathcal{J}(M,K)}(L) = L$, quaisquer que sejam $H \in \mathcal{T}(G)$ e $L \in \mathcal{J}(M,K)$.

Pelos itens (7) e (8) acima temos que:

$$H \subset \psi\big(\theta(H)\big) \text{ e } L \subset \theta\big(\psi(L)\big).$$

Neste caso, resta então provar:

$$\psi\big(\theta(H)\big) \subset H \text{ e } \theta\big(\psi(L)\big) \subset L.$$

Primeiramente provemos que $\psi\big(\theta(H)\big) \subset H$. Pelo item (a), escolhendo $L = \theta(H)$ temos que

$$[G: \psi(\theta(H))] = dim_K \theta(H)$$

e pelo item (b) temos

$$dim_K \theta(H) = [G:H]$$

Logo, pelo Teorema de Lagrange

$$|G|/_{|\psi(\theta(H)|} = [G:\psi(\theta(H)] = [G:H] = |G|/_{|H|}.$$

Logo, $|H| = |\psi(\theta(H)|$ e, como $H \leq \psi(\theta(H))$, segue que $H = \psi(\theta(H))$.

Portanto, $\psi \circ \theta = Id_{\mathcal{T}(G)}$.

Analogamente, pelo item (b), escolhendo $H = \psi(L)$ temos que $dim_{\theta(\psi(L))}M = |\psi(L)|$ e pelo item (a), temos $dim_L M = |\psi(L)|$.

Assim, $dim_{\theta(\psi(L))}M = dim_L M$. Logo, utilizando o resultado **(3.1)**, segue que

$$dim_L M = \left(dim_{\theta(\psi(L))}M\right)\left(dim_L \theta\left(\psi(L)\right)\right) \Longrightarrow$$

$$dim_L M = (dim_L M)\left(dim_L \theta\left(\psi(L)\right)\right) \Longrightarrow$$

$$dim_L \theta\left(\psi(L)\right) = 1$$

ou seja, $\theta\left(\psi(L)\right) = L$.

Portanto, $\theta \circ \psi = Id_{\mathcal{J}(M,K)}$.

4. CONCLUSÕES

Este projeto de pesquisa Iniciação Científica em Teoria de Galois nos proporcionou um maior desenvolvimento do raciocínio lógico-matemático, uma melhora na familiarização com apresentações em público e a iniciação à pesquisa na área de Matemática, especificamente na área da Álgebra. Com este trabalho conseguimos alcançar todos os objetivos, tais como estudar o Teorema da Correspondência de Galois e provar que o polinômio $f(x) = x^5 - 6x + 3 \in \mathbb{Q}[x]$ não é solúvel por meio de radicais sobre $\mathbb{Q}$.

Foram apresentados os trabalhos: “A Simplicidade dos Grupos A_n, $n \geq 5$” e “Grupos Finitos: o Teorema de Cayley”, sendo duas apresentações no XXIV Congresso de Iniciação Científica da UFPel e outras duas na 14ª Mostra da Produção Universitária da FURG, ambos em 2015. Houve também duas apresentações de divulgação do projeto, em 2014 e 2015, na XVI e XVII Semana Acadêmica do Curso de Licenciatura em Matemática.

5. REFERÊNCIAS BIBLIOGRÁFICAS

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

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

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

[O] OWEN, J. B. **Teoria de Galois**. Faculdade de Ciências da Universidade de Lisboa, Textos de Matemática, 1997.

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