CORRESPONDÊNCIA DE GALOIS

Angelina Carrijo de Oliveira
Universidade Federal de Uberlândia
angelina.carrijo@gmail.com

Victor Gonzalo Lopez Neuman
Universidade Federal de Uberlândia
gonzalo@famat.ufu.br

RESUMO

Neste trabalho estudamos a Teoria de Galois e demonstramos o Teorema Fundamental de Galois. Através de exemplos, mostra-se como encontrar de forma explícita os subcorpos de um corpo de decomposição através do conhecimento dos subgrupos do Grupo de Galois a ele associado. Define-se também a noção de polinômio solúvel por meio de radicais e provamos um critério para que as raízes de um polinômio sejam expressas por meio de radicais.

ABSTRACT

In this work, we study the Galois Theory and demonstrate the Fundamental Theorem of Galois Theory. Across examples, it is shown how to find explicitly subfields of a decomposition field through knowledge of the subgroups of the Galois group associated to it. It also defines the notion of polynomial soluble by radicals and prove the Galois's criterion for solvability of polynomials by radicals.

Palavras-chave: Grupo de Galois, extensões algébricas, radicais.

1 INTRODUÇÃO

O estudo das equações algébricas, ou equações polinomiais numa variável, levou ao aparecimento da Álgebra. A resolução das equações cúbicas e quárticas foram talvez a maior contribuição à Álgebra desde que os babilônicos, quatro milênios antes, aprenderam a completar o quadrado para equações quadráticas. O objetivo deste trabalho é estudar a teoria de Galois e aplicá-la na resolução de equações polinomiais e mostrar um critério que verifica quando as raízes de um polinômio podem ser expressas por meio de radicais utilizando o Teorema de correspondência de Galois.

Para entender a Teoria de Galois é necessário ter uma base sobre extensões algébricas. Lembrando que este é um tema estudado na graduação, faremos unicamente uma breve introdução deste, sem demonstrações. Em seguida, faremos o estudo da Teoria de Galois, começando pelas extensões galoisianas e normais, para depois enunciar e demonstrar o Teorema de correspondência de Galois. Na seção 5 encontramos a estrutura de corpos de decomposição de um polinômio específico, utilizando como ferramenta o Teorema Fundamental de Galois, que coloca em relação corpos e grupos.

Cabe lembrar que a maioria das demonstrações foram extendidas para melhor compreensão do leitor. Inclusive, algumas demonstrações foram feitas de forma diferente às encontradas na literatura. As principais referência utilizadas para o desenvolvimento do texto foram [1] e [5].

2 EXTENSÕES ALGÉBRICAS

Todos os corpos considerados estão contidos em $\mathbb{C}$.

Definição 2.1: *Sejam K um corpo e $f(x) \in K[x]$. O menor corpo que contém K e todas as raízes de $f(x)$ é chamado de corpo das raízes de $f(x)$, ou corpo de decomposição de $f(x)$, denotado por $Gal(f, K)$.*

Definição 2.2: *Sejam K um corpo e $f(x) \in K[x] \setminus \{0\}$. Dizemos que $f(x)$ é irredutível em $K[x]$ se as duas condições seguintes são satisfeitas:*

(a) $f(x) \notin K^* = K \setminus \{0\}$;

(b) $f(x)$ *não possui fatoração não-trivial em* $K[x]$, *isto é:*

$$\forall g(x), h(x) \in K[x] \text{ tais que } f(x) = g(x)h(x), \text{ então } g(x) \in K^* \text{ ou } h(x) \in K^*.$$

Definição 2.3: *Seja $L|K$ uma extensão de corpos, em particular L é um K-espaço vetorial. A dimensão de L como K-espaço vetorial é chamada de grau da extensão, que denotaremos por $[L : K]$. Se $[L : K] < \infty$, então dizemos que a extensão é finita, caso contrário dizemos que $L|K$ é uma extensão infinita.*

Definição 2.4: *Seja L um corpo. Todo isomorfismo φ de L em L é chamado automorfismo de L. Denotamos por $AutL$ o conjunto de todos os automorfismos de L. Se K é um subcorpo de L e φ é um automorfismo de L tal que $\varphi(\alpha) = \alpha$, para todo $\alpha \in K$, dizemos que φ fixa K e o conjunto de todos os automorfismos de L que fixam K é chamado $Aut_K L$. É fácil provar que $Aut_K L$ é um grupo.*

Proposição 2.1: *Sejam K um corpo, $f(x) \in K[x]$ e $\alpha \in \mathbb{C}$ uma raiz de $f(x)$. Então:*

a) α é uma raiz de multiplicidade 1 ou raiz simples se, e somente se, $f'(\alpha) \neq 0$ e $f(\alpha) = 0$.

b) Se $f(x)$ é irredutível então todas as raízes de $f(x)$ são simples.

Demonstração. Ver referência [4, Capítulo V, Proposição 2].

■

Teorema 2.1: *(Teorema do elemento primitivo) Seja $L|K$ uma extensão de corpos tal que $[L : K] < \infty$. Então, existe $\alpha \in L$ tal que $L = K[\alpha]$.*

Demonstração. Ver referência [4, Capítulo V, Teorema 3].

■

Corolário 2.1: *Seja $L|K$ uma extensão de corpos tal que $[L : K] < \infty$. Então $[L : K] \geq |Aut_K L|$, com $|Aut_K L|$ denotando o número de elementos de $Aut_K L = \{\sigma \in AutL : \sigma(\lambda) = \lambda, \forall \lambda \in K\}$.*

Demonstração. Ver referência [4, Capítulo V, Corolário 1].

■

3 TEORIA DE GALOIS ELEMENTAR

3.1 EXTENSÕES GALOISIANAS E NORMAIS

Definição 3.1: *Sejam $L|K$ uma extensão de corpos e $\alpha \in L$. Dizemos que α é algébrico sobre K se existe $f(x) \in K[x]$ tal que $f(\alpha) = 0$. A extensão $L|K$ é algébrica se todo elemento de L é algébrico sobre K.*

Proposição 3.1: *Sejam $L|K$ uma extensão de corpos e $\alpha \in L$ algébrico sobre K e seja $f(x) \in K[x]$, mônico, de menor grau tal que $f(\alpha) = 0$. O polinômio $f(x)$ é o único polinômio mônico irredutível em $K[x]$ tal que $f(\alpha) = 0$, o qual denotaremos por $f(x) = irr(\alpha, K)$.*

Demonstração. Suponha que $f(x)$ não é irredutível. Então existem polinômios $g(x), h(x) \in K[x]$ não constantes, tais que $f(x) = g(x)h(x)$. Como α é raiz de $f(x)$, então $g(\alpha)h(\alpha) = 0$. Isto é, α é raiz de $g(x)$ ou de $h(x)$. Mas isto não é possível pela minimalidade de $f(x)$. Logo $f(x)$ é irredutível.

É fácil ver que se α é raiz de algum polinômio, este será múltiplo de $f(x)$, pela divisão euclidiana e a minimalidade do grau de $f(x)$. Assim, $f(x)$ é o único polinômio mônico irredutível em $K[x]$ tal que $f(\alpha) = 0$.

■

Definição 3.2: *Seja L uma extensão de K. Se existe $f(x) \in K[x]$ tal que $L = Gal(f, K)$, dizemos que $L|K$ é uma extensão galoisiana.*

Definição 3.3: *Seja $L|K$ uma extensão algébrica. Dizemos que $L|K$ é normal se para todo $f(x) \in K[x]$, irredutível sobre K tal que possui uma raiz $\alpha \in L$, então $f(x)$ possui todas as suas raízes em L.*

Observação 3.1: *Mostraremos no Corolário 3.2 que se uma extensão $L|K$ é finita, então ser extensão galoisiana é equivalente a ser extensão normal.*

Exemplo 1: *As raízes do polinômio x^3-2 são $\sqrt[3]{2}$, $\xi\sqrt[3]{2}$, $\xi^2\sqrt[3]{2}$; onde ξ é raiz de x^2+x+1 (observe que $\xi^3 = 1$). Assim $\mathbb{Q}[\xi, \sqrt[3]{2}] = Gal(x^3 - 2, \mathbb{Q})$, isto é $\mathbb{Q}[\xi, \sqrt[3]{2}]|\mathbb{Q}$ é uma extensão galoisiana, e pelo Corolário 3.2, também uma extensão normal.*

Definição 3.4: *Sejam K, K' corpos e $\sigma : K \longrightarrow K'$ um isomorfismo de K sobre K'. Se $f(x) \in K[x]$, com $f(x) = a_0 + a_1x + \cdots + a_nx^n$, então definimos*

$$f^\sigma(x) = a'_0 + a'_1x + \cdots + a'_nx^n \in K'[x],$$

onde $a'_i = \sigma(a_i)$ para $i = 1, 2, \ldots, n$.

Proposição 3.2: *Sejam K, K' corpos, $\sigma : K \longrightarrow K'$ um isomorfismo de corpos e $h(x) \in K[x]$ um polinômio irredutível sobre K.*

Se α é uma raiz de $h(x)$ em $\mathbb{C}$ e β é raiz de $h^\sigma(x)$ em $\mathbb{C}$, então existe um único isomorfismo $\widehat{\sigma} : K[\alpha] \longrightarrow K'[\beta]$ tal que a função $\widehat{\sigma}(\alpha) = \beta$ e $\widehat{\sigma}|_K = \sigma$.

Demonstração. Sejam α uma raiz qualquer de $h(x) \in K[x]$ e β uma raiz de $h^\sigma(x) \in K'[x]$. Como $h(x)$ é irredutível em $K[x]$, então $h^\sigma(x)$ é irredutível em $K'[x]$. Sabemos que $K[\alpha]$ e $K'[\beta]$ são corpos de grau $grau(h(x)) = grau(h^\sigma(x)) = r$ sobre K, segue que:

1) $K[\alpha] = \{a_0 + a_1\alpha + \cdots + a_{r-1}\alpha^{r-1} : a_i \in K\}$ e $\{1, \alpha, \alpha^2, \ldots, \alpha^{r-1}\}$ é uma base do espaço vetorial $K[\alpha]$ sobre o corpo K.

2) $K'[\beta] = \{a'_0 + a'_1\beta + \cdots + a'_{r-1}\beta^{r-1} : a'_i \in K'\}$ e $\{1, \beta, \beta^2, \ldots, \beta^{r-1}\}$ é uma base do espaço vetorial $K'[\beta]$ sobre o corpo K'.

Verifiquemos que $\widehat{\sigma} : K[\alpha] \longrightarrow K'[\beta]$ definido por

$$\widehat{\sigma}(a_0 + a_1\alpha + \cdots + a_{r-1}\alpha^{r-1}) = \sigma(a_0) + \sigma(a_1)\beta + \cdots + \sigma(a_{r-1})\beta^{r-1}$$

é um isomorfismo de corpos, tal que $\widehat{\sigma}(\alpha) = \beta$ e $\widehat{\sigma}|_K = \sigma$.

Devemos provar então que:

a) $\widehat{\sigma}$ é um homomorfismo;

Perceba que para $f(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} \in K[x]$. Temos que

$$\widehat{\sigma}(f(\alpha)) = \widehat{\sigma}(a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}) = \sigma(a_0) + \sigma(a_1)\beta + \cdots + \sigma(a_{n-1})\beta^{n-1} = f^{\sigma}(\beta).$$

Sejam $f(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$ e $g(x) = b_0 + b_1x + \cdots + b_{n-1}x^{n-1}$ e seja $t(x) = f(x) + g(x)$.

Daí,

$$\widehat{\sigma}(f(\alpha) + g(\alpha)) = \widehat{\sigma}(t(\alpha)) = t^{\sigma}(\beta).$$

Por outro lado,

$$t^{\sigma}(x) = f^{\sigma}(x) + g^{\sigma}(x)$$

ou seja,

$$t^{\sigma}(\beta) = f^{\sigma}(\beta) + g^{\sigma}(\beta) = \widehat{\sigma}(f(\alpha)) + \widehat{\sigma}(g(\alpha)).$$

Devemos também mostrar que $\widehat{\sigma}(f(\alpha)g(\alpha)) = \widehat{\sigma}(f(\alpha))\widehat{\sigma}(g(\alpha)) = f^{\sigma}(\beta)g^{\sigma}(\beta)$.

De fato, sabemos que

$$f(x)g(x) = q(x)h(x) + R(x), \quad grau(R(x)) < r \tag{1}$$

Daí, $f(\alpha)g(\alpha) = R(\alpha)$, pois $h(\alpha) = 0$, assim $\widehat{\sigma}(f(\alpha)g(\alpha)) = \widehat{\sigma}(R(\alpha)) = R^{\sigma}(\beta)$.

Por outro lado, aplicando σ na equação (1) obtemos:

$f^{\sigma}(x)g^{\sigma}(x) = q^{\sigma}(x)h^{\sigma}(x) + R^{\sigma}(x)$

Daí, $f^{\sigma}(\beta)g^{\sigma}(\beta) = R^{\sigma}(\beta)$, pois $h^{\sigma}(\beta) = 0$. Logo, $\widehat{\sigma}(f(\alpha)g(\alpha)) = f^{\sigma}(\beta)g^{\sigma}(\beta)$.

Portanto, $\widehat{\sigma}$ é um homomorfismo.

b) $\widehat{\sigma}$ é injetor;

Como $K[\alpha]$ é um corpo e $\widehat{\sigma} \neq 0$, segue que $Ker\{\widehat{\sigma}\} = \{0\}$, logo $\widehat{\sigma}$ é injetor.

c) $\widehat{\sigma}$ é sobrejetor;

De fato, seja $b_0 + b_1\beta + \cdots + b_{r-1}\beta^{r-1} \in K'[\beta]$.

Como σ é um isomorfismo então existem $a_0, a_1, \ldots, a_{r-1} \in K$ tais que $\sigma(a_j) = b_j$, $j = 0, \ldots, r-1$. Então,

$\widehat{\sigma}(a_0 + a_1\alpha + \cdots + a_{r-1}\alpha^{r-1}) = \sigma(a_0) + \sigma(a_1)\sigma(\alpha) + \cdots + \sigma(a_{r-1})\sigma(\alpha^{r-1}) =$

$\sigma(a_0) + \sigma(a_1)\beta + \cdots + \sigma(a_{r-1})\beta^{r-1} = b_0 + b_1\beta + \cdots + b_{r-1}\beta^{r-1}$.

Logo $\widehat{\sigma}$ é sobrejetor.

Assim, $\widehat{\sigma}$ é um isomorfismo.

d) $\widehat{\sigma}(\alpha) = \beta$ e $\widehat{\sigma}|_K = \sigma$.

Como $\alpha \in K[\alpha]$, então $\alpha = 0 + 1\alpha$.

Assim, $\widehat{\sigma}(\alpha) = \sigma(0) + \sigma(1)\beta = \beta$, logo $\widehat{\sigma}(\alpha) = \beta$.

E ainda, $\widehat{\sigma}(a_0) = \sigma(a_0)$, logo $\widehat{\sigma}|_K = \sigma$.

Agora mostremos a unicidade:
Seja $\varphi : K[\alpha] \longrightarrow K'[\beta]$ tal que $\varphi(\alpha) = \beta$ e $\varphi|_K = \sigma$.
Então:
$\varphi(a_0 + a_1\alpha + \cdots + a_{r-1}\alpha^{r-1}) = \varphi(a_0) + \varphi(a_1)\varphi(\alpha) + \cdots + \varphi(a_{r-1})\varphi(\alpha^{r-1}) =$
$a'_0 + a'_1\beta + \cdots + a'_{r-1}\beta^{r-1} = \widehat{\sigma}(a_0 + a_1\alpha + \cdots + a_{r-1}\alpha^{r-1})$.

■

Proposição 3.3: *Sejam $L|K$ uma extensão, $\sigma \in Aut_K L$ e $\alpha \in L$, então $\sigma(\alpha)$ é raiz de $irr(\alpha, K)$.*

Demonstração. Seja $f(x) = irr(\alpha, K) = x^n + b_{n-1}x^{n-1} + \cdots + b_0$. Então $f(\alpha) = 0$.
Sabemos que $\sigma|_K = id$. Aplicando σ em $f(\alpha)$, temos:

$$0 = \sigma(f(\alpha)) = \sigma(\alpha)^n + b_{n-1}\sigma(\alpha)^{n-1} + \cdots + b_0 = f(\sigma(\alpha)).$$

Logo $\sigma(\alpha)$ é também uma raiz de $f(x)$.

■

Proposição 3.4: *Sejam K, K' corpos e $\sigma : K \longrightarrow K'$ um isomorfismo e $\alpha \in \mathbb{C}$ uma raiz qualquer em $f(x) \in K[x]$. Então existe β raiz de $f^\sigma(x)$ em $\mathbb{C}$ e existe um isomorfismo $\sigma_1 : K[\alpha] \longrightarrow K'[\beta]$ tal que $\sigma_1(\alpha) = \beta$ e $\sigma_1|_K = \sigma$.*

Demonstração. Seja $f(x) = f_1(x)^{m_1} f_2(x)^{m_2} \cdots f_k(x)^{m_k}$, onde $f_1(x), \ldots, f_k(x)$ são os distintos fatores irredutíveis de $f(x)$ em $K[x]$.
Assim, $f^\sigma(x) = f_1^\sigma(x)^{m_1} f_2^\sigma(x)^{m_2} \cdots f_k^\sigma(x)^{m_k}$, onde $f_1^\sigma(x), \ldots, f_k^\sigma(x)$ são os distintos fatores irredutíveis de $f^\sigma(x)$ em $K'[x]$.
Se α é raiz de $f(x)$ podemos assumir que α é raiz de $f_1(x)$, irredutível sobre K.
Assim, se β é qualquer raiz do polinômio $f_1^\sigma(x)$, irredutível sobre K', considerando $h(x) = f_1(x)$, segue da Proposição 3.2 que existe um isomorfismo $\sigma_1 : K[\alpha] \longrightarrow K'[\beta]$ tal que $\sigma_1(\alpha) = \beta$ e $\sigma_1|_K = \sigma$.

■

Teorema 3.1: *Sejam K, K' corpos e $\sigma : K \longrightarrow K'$ um isomorfismo, $f(x) \in K[x]$ e $\alpha_1, \alpha_2, \ldots, \alpha_r$ as distintas raízes de $f(x)$ em $\mathbb{C}$. Se $L = Gal(f, K)$ e $L' = Gal(f^\sigma, K')$ então existe $\widehat{\sigma} : L \longrightarrow L'$ um isomorfismo tal que $\widehat{\sigma}|_K = \sigma$ e $\widehat{\sigma}(\alpha_1), \widehat{\sigma}(\alpha_2), \ldots, \widehat{\sigma}(\alpha_r)$ são as raízes distintas de $f^\sigma(x)$ em $\mathbb{C}$.*

Demonstração. Se $f(x) \in K[x]$ possui uma única raiz α_1, então temos $f(x) = (x - \alpha_1)^m$ em $\mathbb{C}[x]$, mas isto implica que $\alpha_1 \in K$ (ver o coeficiente de x^{m-1} em $f(x)$) e portanto $\sigma(\alpha_1) \in K'$ é a única raiz de $f^\sigma(x)$ em $\mathbb{C}$ e teremos $L = K$, $L' = K'$ e $\widehat{\sigma} = \sigma : L \longrightarrow L'$.
Agora se $f(x) = f_1(x)^{m_1} \cdots f_k(x)^{m_k}$ onde $f_i(x) \in K[x]$ são os distintos polinômios irredutíveis sobre K temos que $f^\sigma(x) = f_1^\sigma(x)^{m_1} \cdots f_k^\sigma(x)^{m_k}$ onde $f_i^\sigma(x) \in K'[x]$ são os distintos polinômios irredutíveis sobre K'.
Sabemos que o número r de raízes distintas de $f(x)$ em $\mathbb{C}$ é igual à soma dos graus dos polinômios $f_1(x), \ldots, f_k(x)$ e portanto temos como consequência que o número de raízes distintas de $f^\sigma(x)$ em $\mathbb{C}$ é também igual a r.
Sejam $\beta_1, \beta_2, \ldots, \beta_r$ as distintas raízes em $\mathbb{C}$ do polinômio $f^\sigma(x) \in K'[x]$, e sejam $K_1 = K[\alpha_1]$, $K_2 = K_1[\alpha_2], \ldots, K_r = K_{r-1}[\alpha_r]$ e portanto $L = K[\alpha_1, \ldots, \alpha_r] = K_r$.
Pela Proposição 3.4, existe $\beta \in \{\beta_1, \ldots, \beta_r\}$ e existe um isomorfismo $\sigma_1 : K[\alpha_1] \longrightarrow K'[\beta]$ tal que $\sigma_1(\alpha_1) = \beta$ e $\sigma_1|_K = \sigma$. Notemos $\beta_1 = \beta$, $K_1 = K[\alpha_1]$ e $K'_1 = K'[\beta_1]$.
Como $f(x) \in K[x]$ e $\sigma_1|_K = \sigma$, segue imediatamente que $f(x) \in K_1[x]$ e $f^{\sigma_1}(x) \in K'_1[x]$. Novamente pela Proposição 3.4, para os corpos K_1, K'_1 e $\sigma_1 : K_1 \longrightarrow K'_1$ existe $\beta \in \{\beta_2, \ldots, \beta_k\}$ (que chamaremos de β_2) e existe um isomorfismo $\sigma_2 : K_1[\alpha_2] \longrightarrow K'_1[\beta_2]$ tal que $\sigma_2(\alpha_2) = \beta_2$ e $\sigma_2|_{K_1} = \sigma_1 : K_1 \longrightarrow K'_1$.
Observe que σ_2 é um isomorfismo e $\alpha_1 \neq \alpha_2$ implica que $\beta_1 = \sigma_2(\alpha_1) \neq \sigma_2(\alpha_2) = \beta_2$.

Como $\sigma_1|_K = \sigma$ segue que $\sigma_2|_K = \sigma$ e $\sigma_2(\alpha_1) = \beta_1, \sigma_2(\alpha_2) = \beta_2$ e $\sigma_2 : K[\alpha_1, \alpha_2] \longrightarrow K'[\beta_1, \beta_2]$ é um isomorfismo.

Supondo que existe $\sigma_{k-1} : K[\alpha_1, \ldots, \alpha_{k-1}] \longrightarrow K'[\beta_1, \ldots, \beta_{k-1}]$ isomorfismo tal que $\sigma_{k-1}(\alpha_i) = \beta_i$, $i = 1, 2, \ldots, k-1$ e $\sigma_{k-1}|_K = \sigma$ temos que $f(x) \in K_{k-1}[x]$ e $f^{\sigma_{k-1}}(x) = f^{\sigma}(x)$.

Aplicando a Proposição 3.4 para os corpos $K_{k-1} = K[\alpha_1, \ldots, \alpha_{k-1}]$ e $K'_{k-1} = K'[\beta_1, \ldots, \beta_{k-1}]$ com $\sigma_{k-1} : K_{k-1} \longrightarrow K'_{k-1}$ temos que existe β (que denotaremos por β_k) raiz de f^{σ} e um isomorfismo $\sigma_k : K_{k-1}[\alpha_k] \longrightarrow K'_{k-1}[\beta_k]$ tal que $\sigma_k|_{K_{k-1}} = \sigma_{k-1}$ e $\sigma_k(\alpha_k) = \beta_k$.

Daí, segue que existe $\sigma_k : K[\alpha_1, \ldots, \alpha_k] \longrightarrow K'[\beta_1, \ldots, \beta_k]$ isomorfismo tal que $\sigma_i(\alpha_i) = \beta_i$, para todo $i \in \{1, 2, \ldots, k\}$ e $\sigma_k|_K = \sigma$.

Como $L = K_r = K[\alpha_1, \ldots, \alpha_r]$ o teorema segue imediatamente.

■

Corolário 3.1: *Seja $L|K$ uma extensão galoisiana e sejam M, M' subcorpos de L contendo K. Se $\sigma : M \longrightarrow M'$ é um isomorfismo tal que $\sigma(a) = a$ para todo $a \in K$ então existe $\sigma' \in Aut_K L$ tal que $\sigma'|_M = \sigma$.*

Demonstração. Segue imediatamente do Teorema 3.1.

■

Corolário 3.2: *Seja $L|K$ uma extensão finita. Então esta extensão é galoisiana se, e somente se, esta extensão for normal.*

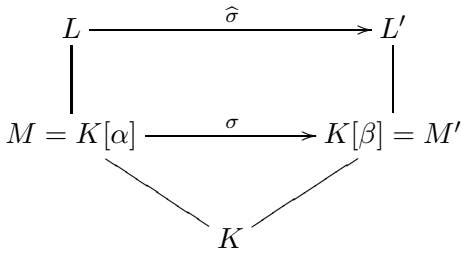
Demonstração. ($\Leftarrow$) Suponha que $L|K$ é normal. Como $L|K$ é finita, então pelo Teorema 2.1 existe $u \in L$ tal que $L = K[u]$. Como $L|K$ é normal segue que, se u é raiz de $h(x) = irr(u, K)$, então todas as raízes de $h(x)$ estão em L, o que implica que $L = Gal(h, K)$, ou seja, $L|K$ é galoisiana.

($\Rightarrow$) Suponhamos que $L|K$ é galoisiana com $L = Gal(f, K)$, seja $g(x) \in K[x]$ um polinômio irredutível tal que existe $\alpha \in L$, $g(\alpha) = 0$.

Mostremos que para todo $\beta \in \mathbb{C}$, se $g(\beta) = 0$ então $\beta \in L$.

Seja $\beta \neq \alpha$ uma raiz de $g(x)$ em $\mathbb{C}$. Sabemos pela Proposição 3.2 que existe um isomorfismo $\sigma : K[\alpha] \longrightarrow K[\beta]$ tal que $\sigma(\alpha) = \beta$ e $\sigma(a) = a$, para todo $a \in K$.

Sejam $M = K[\alpha], M' = K[\beta]$, $L' = Gal(f, M')$ e sejam $\gamma_1, \ldots, \gamma_n$ raízes de f. Então, $L = K[\gamma_1, \ldots, \gamma_n] \subset K[\beta][\gamma_1, \ldots, \gamma_n] = M'[\gamma_1, \ldots, \gamma_n] = L'$. Logo $L \subset L'$ e pelo Teorema 3.1 existe um isomorfismo $\widehat{\sigma}$: $L \longrightarrow L'$ que extende σ: $M \longrightarrow M'$. Como $L \subset L'$, então $L = L'$.



■

Corolário 3.3: *Se $L|K$ é uma extensão galoisiana então:*

a) $[L : K] = |Aut_K L|$.

b) Seja $\alpha \in L$, se $\alpha \notin K$ então existe $\sigma \in Aut_K L$ tal que $\sigma(\alpha) \neq \alpha$.

Demonstração. a) Como $L|K$ é galoisiana, então L é gerado, sobre K, por um número finito de elementos algébricos sobre K, logo $L|K$ é uma extensão finita. Pelo Teorema 2.1, existe $\alpha \in L$ tal que $L = K[\alpha]$. Seja $h(x) = irr(\alpha, K)$, para cada raiz β de $h(x)$, temos que $\beta \in L$, pois $L|K$ é extensão normal. Como $[K[\beta] : K] = grau(h(x))$, então $L = K[\beta]$. Pela Proposição 3.2, existem tantos automorfismos de L, quantas raízes do polinômio

$h(x)$ (com $K = K'$ e $\sigma = id$). Assim, $[L : K] = grau(h(x)) \leq |Aut_K L|$ e pelo Corolário 2.1, temos $[L : K] = |Aut_K L|$.

b) Seja $\alpha \in L, \alpha \notin K$. Se $g(x) = irr(\alpha, K)$ segue que $grau(g(x)) = r \geq 2$. Pela Proposição 3.3, existe $\beta \neq \alpha$ tal que $g(\beta) = 0$. Pelo Corolário 3.2, $\beta \in L$, pois L é normal.

Agora pela Proposição 3.2, existe um isomorfismo $\sigma : K[\alpha] \longrightarrow K[\beta]$ tal que $\sigma(a) = a$, para todo $a \in K$ e $\sigma(\alpha) = \beta \neq \alpha$. Pelo Corolário 3.1, existe $\widehat{\sigma} \in Aut_K L$, $\widehat{\sigma}|_{K[\alpha]} = \sigma$ finalizando assim a demonstração.

■

Teorema 3.2: *Se $K \subset M \subset L$ são extensões finitas e $L|K$ é galoisiana, então as seguintes afirmações são equivalentes:*

a) $M|K$ *é galoisiana.*

b) $\sigma(M) \subset M$, *para todo* $\sigma \in Aut_K L$.

c) $Aut_M L \lhd Aut_K L$, *onde* $H \lhd G$ *indica que* H *é subgrupo normal de* G.

Demonstração. (a) $\Rightarrow (b)$ Seja $u \in L$ tal que $M = K[u]$. Se $M|K$ é galoisiana segue do Corolário 3.2 que $M|K$ é normal.

Se $h(x) = irr(u, K)$ e $\sigma \in Aut_K L$, sabemos que $v = \sigma(u)$ é também raiz de $h(x)$ e como $M|K$ é normal temos $v = \sigma(u) \in M$, ou seja, $\sigma(K[u]) \subset K[u] = M$.

(b) $\Rightarrow (a)$ Seja $u \in L$ tal que $M = K[u]$ e seja $h(x) = irr(u, K)$.

Vamos mostrar que se $\sigma(M) \subset M$ para todo $\sigma \in Aut_K L$, então $M = Gal(h, K)$.

Sejam v uma raiz de $h(x)$ e $M' = K[v]$. Pela Proposição 3.2, existe um isomorfismo $\sigma_0 : M \longrightarrow M'$ tal que $\sigma_0(u) = v$ e $\sigma_0(a) = a$, para todo $a \in K$.

Assim pelo Teorema 3.1, existe $\sigma \in Aut_K L$ tal que $\sigma|_M = \sigma_0$. Como $\sigma(M) \subset M$ e $u \in M$ temos $v = \sigma(u) \in M$.

(b) $\Rightarrow (c)$ Sejam $\sigma \in Aut_K L$ e $\gamma \in Aut_M L$.

Vamos mostrar que se $\sigma(M) \subset M$, então $\sigma^{-1} \circ \gamma \circ \sigma \in Aut_M L$.

Seja $m \in M$, então $m' = \sigma(m) \in M$ e $\gamma(m') = m'$, logo

$(\sigma^{-1} \circ \gamma \circ \sigma)(m) = \sigma^{-1}(\gamma(m')) = \sigma^{-1}(m') = m$, isto é $\sigma^{-1} \circ \gamma \circ \sigma \in Aut_M L$.

(c) $\Rightarrow (b)$ Suponha por absurdo que existe $\sigma \in Aut_K L$ e $u \in M$ tal que $\sigma(u) = v \notin M$.

Como $L|K$ é galoisiana, existe f tal que $L = Gal(f, K) \subset Gal(f, M) \subset L$, logo $L|M$ é galoisiana. Temos pelo Corolário 3.3 item (b) que existe $\gamma \in Aut_M L$ tal que $\gamma(v) \neq v$.

Assim $(\sigma^{-1} \circ \gamma \circ \sigma)(u) = \sigma^{-1}(\gamma(v)) \neq \sigma^{-1}(v) = u$ ou seja $(\sigma^{-1} \circ \gamma \circ \sigma) \notin Aut_M L$, o que contraria a hipótese $Aut_M L \lhd Aut_K L$.

■

Teorema 3.3: *Seja $L|K$ uma extensão finita. Então as seguintes afirmações são equivalentes:*

a) $L|K$ *é galoisiana.*

b) $L|K$ *é normal.*

c) Para todo $\alpha \in L - K$ *existe* $\sigma \in Aut_K L$ *tal que* $\sigma(\alpha) \neq \alpha$.

d) $[L : K] = |Aut_K L|$.

Demonstração. (a) $\Leftrightarrow (b)$ Segue do Corolário 3.2.

(a) $\Rightarrow (c)$ Segue do Corolário 3.3.

(c) $\Rightarrow (d)$ Pelo Corolário 2.1, temos $[L:K] \geq |Aut_K L|$.

Suponha por absurdo que $[L:K] > |Aut_K L|$.

Seja $Aut_K L = \{\varphi_1, \varphi_2, \ldots, \varphi_n\}$ onde $\varphi_1 = id_L$ é o automorfismo identidade de L.

Se $[L:K] > n$ então, existem $u_1, u_2, \ldots, u_n, u_{n+1} \in L$ linearmente independentes sobre o corpo K. Considere agora o sistema linear homogêneo com n equações e $(n+1)$ incógnitas $x_1, x_2, \ldots, x_{n+1} \in L$:

$$\begin{cases} \varphi_1(u_1)x_1 + \varphi_1(u_2)x_2 + \cdots + \varphi_1(u_{n+1})x_{n+1} &= 0 \\ \varphi_2(u_1)x_1 + \varphi_2(u_2)x_2 + \cdots + \varphi_2(u_{n+1})x_{n+1} &= 0 \\ \vdots & \\ \varphi_n(u_1)x_1 + \varphi_n(u_2)x_2 + \cdots + \varphi_n(u_{n+1})x_{n+1} &= 0 \end{cases} \tag{2}$$

Como o número de equações de (2) é menor que o número de incógnitas então (2) admite solução não trivial.

Seja agora $(x_1, x_2, \ldots, x_{n+1}) = (a_1, a_2, \ldots, a_{n+1})$ uma solução não trivial de (2) com o maior número de incógnitas iguais a zero. Reordenando se necessário, denotaremos por $a_1, a_2, \ldots, a_r$ os $a_i's$ não nulos dessa solução.

Multiplicando por a_1^{-1} se necessário, podemos assumir que $a_1 = 1$. Assim $1, a_2, \ldots, a_r$ não nulos são tais que $(1, a_2, \ldots, a_r, 0, \ldots, 0)$ é uma solução de (2) com um número máximo de zeros. Então temos $\varphi_i(u_1) + \varphi_i(u_2)a_2 + \cdots + \varphi_i(u_r)a_r = 0$ para todo $i \in \{1, 2, \ldots, n\}$.

Como $\varphi_1 = id_L$ e $u_1, u_2, \ldots, u_r, \ldots, u_n$ são linearmente independentes sobre K então segue que existe $a_i \in L$ tal que $a_i \notin K$. Seja $a_r \notin K$. Assim por (c) existe $\sigma \in Aut_K L$ tal que $\sigma(a_r) \neq a_r$.

Daí segue que $(\sigma \circ \varphi_i)(u_1) + (\sigma \circ \varphi_i)(u_2)\sigma(a_2) + \cdots + (\sigma \circ \varphi_i)(u_r)\sigma(a_r) = 0$ para todo $i \in \{1, 2, \ldots, n\}$.

Como $Aut_K L$ é um grupo e $\sigma \in Aut_K L$ segue que :

$Aut_K L = \{\varphi_1, \varphi_2, \ldots, \varphi_n\} = \{\sigma\varphi_1, \sigma\varphi_2, \ldots, \sigma\varphi_n\}$.

Portanto $\sigma\varphi_i = \varphi_k$ para algum k e temos

$$\varphi_k(u_1) + \varphi_k(u_2)\sigma(a_2) + \cdots + \varphi_k(u_r)\sigma(a_r) = 0, \forall k \in \{1, 2, \ldots, n\}$$

por outro lado

$$\varphi_k(u_1) + \varphi_k(u_2)a_2 + \cdots + \varphi_k(u_r)a_r = 0, \forall k \in \{1, 2, \ldots, n\}.$$

Daí segue que:

$$\varphi_k(u_2)(\sigma(a_2) - a_2) + \cdots + \varphi_k(u_r)(\sigma(a_r) - a_r) = 0, \forall k \in \{1, 2, \ldots, n\}.$$

Como $\sigma(a_r) - a_r \neq 0$ temos uma solução $(0, \sigma(a_2) - a_2, \ldots, \sigma(a_r) - a_r, \ldots)$ que contradiz a maximalidade de zeros da solução $(1, a_2, \ldots, a_r, 0, \ldots, 0)$.

(d) $\Rightarrow (a)$ Suponhamos $L|K$ extensão finita e $[L:K] = |Aut_K L|$. Vamos provar que $L|K$ é galoisiana.

Sejam $L = K[u]$ e $h(x)$ definido por $h(x) = irr(u, K)$ então para todo $\sigma \in Aut_K L$ tem-se $\sigma(u)$ é raiz de $h(x)$ e por outro lado para cada raiz $\beta \in L$ de $h(x)$, existe um único $\sigma \in Aut_K L$ tal que $\sigma(u) = \beta$.

Logo, $|Aut_K L| = n$, com n o número de raízes de $h(x)$ em L. Agora se $[L:K] = |Aut_K L|$ então $grau(h(x)) = [L:K] = |Aut_K L| = n$.

Daí segue que L contém todas as raízes de $h(x)$, ou seja, $L = Gal(h, K)$.

■

Proposição 3.5: *Seja $L|K$ uma extensão galoisiana e seja $f(x) \in K[x]$ o polinômio de grau n, tal que $L = Gal(f, K)$. Então $G = Aut_K L$ é isomorfo a um subgrupo de S_n (grupo de permutações de n elementos).*

Demonstração. Seja $B = \{u_1, u_2, \ldots, u_n\}$ o conjunto de todas as raízes de $f(x)$. Como $L = Gal(f, K)$, temos $B \subset L = K[B]$. Sabemos, pela Proposição 3.3, que todo automorfismo $\sigma \in G = Aut_K L$ envia uma raiz de $f(x)$ em outra raiz de $f(x)$.

Assim, como B é finito e σ injetivo, segue que $\sigma_0 = \sigma|_B : B \longrightarrow B$ define uma permutação do conjunto B.

Se S_B denota o grupo das permutações do conjunto B então basta mostrar que $Aut_K L$ é isomorfo a um subgrupo de S_B, pois $S_B \cong S_n$.

Define-se ψ da seguinte forma:

$$\begin{array}{rccc} \psi: & G & \longrightarrow & S_B \\ & \sigma & \longmapsto & \sigma_0 = \sigma_{|_B} \end{array}$$

A função ψ é um homomorfismo de grupos, pois $\psi(\sigma \circ \tau) = (\sigma \circ \tau)|_B = \sigma|_B \circ \tau|_B$.

Obviamente ψ é injetiva, pois se todas as raízes de $f(x)$ são fixadas por $\sigma \in G$, então $\sigma = id_L$. Isto é, $G \cong \psi(G)$ é subgrupo de $S_B \cong S_n$.

■

Proposição 3.6: *Sejam K um corpo, $a \in K$ e $L = Gal(x^n - a, K)$. Suponha que K contém uma raiz ζ primitiva n-ésima da unidade, então $G = Aut_K L$ é um grupo abeliano.*

Demonstração. Seja $\alpha = \sqrt[n]{a} \in \mathbb{C}$ e ζ uma raiz primitiva n-ésima da unidade tal que $\zeta \in K$, então $\alpha, \alpha\zeta, \alpha\zeta^2, \ldots, \alpha\zeta^{n-1}$ são as n raízes distintas de $x^n - a$ em $\mathbb{C}$.

Sabemos que $L = K[\zeta, \alpha] = K[\alpha]$, pois $\zeta \in K$. Assim pela Proposição 3.3, se $\sigma, \tau \in Aut_K L$, então $\sigma(\alpha) = \alpha\zeta^i$ para algum i, e $\tau(\alpha) = \alpha\zeta^j$, para algum j. Daí, segue que :

$$(\sigma \circ \tau)(\alpha) = \sigma(\alpha\zeta^j) = \sigma(\alpha)\zeta^j = \alpha\zeta^{i+j},$$

$$(\tau \circ \sigma)(\alpha) = \tau(\alpha\zeta^i) = \tau(\alpha)\zeta^i = \alpha\zeta^{j+i}.$$

Assim $\sigma \circ \tau(\alpha) = \tau \circ \sigma(\alpha)$, para todo $\sigma, \tau \in Aut_K L$. Como $L = K[\alpha]$, então $\sigma \circ \tau = \tau \circ \sigma$, para todo $\sigma, \tau \in Aut_K L$.

■

3.2 CORRESPONDÊNCIA DE GALOIS

A partir desta seção denotaremos $G = Aut_K L$ o grupo de automorfismos de L que fixam K. Este grupo G é chamado de Grupo de Galois da extensão $L|K$.

Definição 3.5: *Seja $L|K$ uma extensão finita. Dizemos que M é um corpo intermediário de $L|K$ se M é um subcorpo de L contendo K, ou seja, $K \subset M \subset L$.*

Proposição 3.7: *Seja H subgrupo de $G = Aut_K L$, então o conjunto*

$$M = \{a \in L : \gamma(a) = a, \forall \gamma \in H\}$$

formado pelos elementos de L fixados pelos elementos de H é um corpo intermediário de $L|K$. Notaremos $M = L^H$.

Demonstração. De fato,

- $0, 1 \in K \subset L^H$.

- Se $x, y \in L^H$, para todo $\gamma \in H$ temos $\gamma(x-y) = \gamma(x) - \gamma(y) = x - y$, então $x - y \in L^H$.
- Se $x, y \in L^H$, para todo $\gamma \in H$ temos $\gamma(xy^{-1}) = \gamma(x).\gamma(y^{-1}) = \gamma(x).\gamma(y)^{-1} = xy^{-1}$ então $xy^{-1} \in L^H$.

Isto é, L^H é um corpo intermediário da extensão $L|K$. Esse corpo L^H é chamado de *corpo fixo de* H.

■

Assim temos uma correspondência entre subgrupos de $Aut_K L$ e os corpos intermediários da extensão $L|K$ da seguinte forma: Dado um subgrupo H de $G = Aut_K L$ obtemos um corpo intermediário L^H da extensão $L|K$.

Por outro lado, dado M um corpo, com $K \subset M \subset L$, obtemos o grupo $Aut_M L$. Temos uma inclusão natural $Aut_M L \subset Aut_K L$, pois se um automorfismo de L fixa M então ele fixará também $K \subset M$.

Temos as seguintes propriedades imediatas:

1. $G = Aut_K L$.
2. $Aut_L L = \{id_L\}$.
3. $L^{\{id_L\}} = \{a \in L : id_L(a) = a\} = L$.
4. $K \subset L^G = \{a \in L : \gamma(a) = a, \forall \gamma \in G\}$.
5. Pelo Teorema 3.3 item (c), temos:

$$L^G = K \iff L|K \text{ é uma extensão galoisiana.}$$

Proposição 3.8: *De acordo com as notações acima, temos:*

a) Se M_1, M_2 são corpos tais que $K \subset M_1 \subset M_2 \subset L$ então $Aut_{M_2} L \subset Aut_{M_1} L$.

b) Se $H_1 \subset H_2$ são subgrupos de $Aut_K L$ então $L^{H_2} \subset L^{H_1}$.

c) Para todo corpo intermediário M com $K \subset M \subset L$, tem-se $M \subset L^{Aut_M L}$.

d) Para todo subgrupo H de $Aut_K L$, tem-se $H \subset Aut_{(L^H)} L$.

Demonstração. a) Considere os corpos $K \subset M_1 \subset M_2 \subset L$. Seja $\gamma \in Aut_{M_2} L$. Como $M_1 \subset M_2$, então γ fixa M_1 e daí $\gamma \in Aut_{M_1} L$.

b) Sejam os grupos $H_1 \subset H_2 \subset G$, $\gamma \in H_1$ e $a \in L^{H_2}$. Como $\gamma \in H_1 \subset H_2$, então $\gamma(a) = a$. Logo $a \in L^{H_1}$.

c) Seja M um corpo intermediário da extensão $L|K$. Por definição os elementos de $Aut_M L$ fixam M, logo $M \subset L^{Aut_M L}$.

d) Seja H um subgrupo de G. Então um elemento $\gamma \in H \subset G$ é um automorfismo de L que fixa L^H, logo $H \subset Aut_{(L^H)} L$.

■

Considerando os corpos $K \subset M_1 \subset M_2 \subset L$ e os grupos $\{id_L\} \subset H_1 \subset H_2 \subset G = Aut_K L$, temos as correspondências abaixo:

$$\begin{array}{ccccccc} K & \subset & M_1 & \subset & M_2 & \subset & L \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \\ Aut_K L & \supset & Aut_{M_1} L & \supset & Aut_{M_2} L & \supset & \{id_L\} \end{array}$$

e

$$\begin{array}{ccccccc} & & G & \supset & H_1 & \supset & H_2 & \supset & \{id_L\} \\ & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\ K & \subset & L^G & \subset & L^{H_1} & \subset & L^{H_2} & \subset & L \end{array}$$

Agora vamos demonstrar o Teorema Fundamental de Galois:

Teorema 3.4: *(Teorema Fundamental de Galois) Se $L|K$ é uma extensão galoisiana, então:*

a) Para todo corpo intermediário M, com $K \subset M \subset L$, tem-se $[L : M] = |Aut_M L|$ e $[M : K] = (G : Aut_M L)$ (o índice de $Aut_M L$ em G).

b) Para todo subgrupo H de G, tem-se $[L : L^H] = |H|$ e $[L^H : K] = (G : H)$ (o índice de H em G).

c) $Aut_{L^H} L = H$ e $L^{Aut_M L} = M$.

d) Para todo corpo intermediário M, com $K \subset M \subset L$ temos que a extensão $M|K$ é galoisiana se, e somente se $Aut_M L$ é subgrupo normal de G.

e) Para todo corpo intermediário M, com $K \subset M \subset L$, se $M|K$ é galoisiana então $[M : K] = |Aut_K M|$ e $G/Aut_M L \cong Aut_K M$.

Demonstração. a) Seja M um corpo intermediário da extensão $L|K$. Como $L|K$ é galoisiana, então $L|M$ também é galoisiana. Pelo Teorema 3.3, segue que: $[L : M] = |Aut_M L|$ e como $[L : K] = |Aut_K L| = [L : M][M : K]$, temos $[M : K] = |G|/|Aut_M L| = (G : Aut_M L)$.

b) Seja H subgrupo de G e $M = L^H$. Sabemos pelo item (a) que :

$$[L : M] = |Aut_M L| \quad \text{e} \quad [M : K] = (G : Aut_M L)$$

Por outro lado, pela Proposição 3.8 item (d), tem-se : $H \subset Aut_M L$, então $[L : M] = |Aut_M L| \geq |H|$.

Utilizaremos um argumento semelhante ao usado na demonstração do Teorema 3.3. Suponha $H = \{\gamma_1 = Id_M, \gamma_2, \ldots, \gamma_n\}$ e por absurdo suponha $|Aut_M L| > |H|$. Logo $[L : M] > n$.

Assim, existem $(n+1)$ vetores $u_1, u_2, \ldots, u_n, u_{n+1} \in L$ linearmente independentes sobre o corpo M. Considere agora o sistema linear homogêneo com n equações e $(n+1)$ incógnitas $a_1, a_2, \ldots, a_{n+1} \in L$:

$$\begin{cases} \gamma_1(u_1)a_1 + \gamma_1(u_2)a_2 + \cdots + \gamma_1(u_{n+1})a_{n+1} = 0 \\ \gamma_2(u_1)a_1 + \gamma_2(u_2)a_2 + \cdots + \gamma_2(u_{n+1})a_{n+1} = 0 \\ \vdots \\ \gamma_n(u_1)a_1 + \gamma_n(u_2)a_2 + \cdots + \gamma_n(u_{n+1})a_{n+1} = 0 \end{cases} \tag{3}$$

Então existe uma solução não nula $(a_1, a_2, \ldots, a_{n+1}) \in L^{n+1}$. Tomemos uma solução não trivial de (3) com o maior número de zeros possível nas coordenadas $(a_1, a_2, \ldots, a_{n+1})$, assim denotaremos por $a_1, a_2, \ldots, a_r$ os $a_i s$ não nulos dessa solução, isto é, reorganizando podemos supor

$$a_1 \neq 0, a_2 \neq 0, \ldots, a_r \neq 0, a_{r+1} = 0, \ldots, a_{n+1} = 0.$$

Multiplicando o sistema por a_1^{-1} se necessário, podemos assumir $a_1 = 1$. Temos que a solução $(1, a_2, \ldots, a_r, 0, \ldots, 0) \in L^{n+1}$, com $1, a_2, \ldots, a_r$ não nulos, é uma solução de (3) com um número máximo de zeros. A primeira equação é :

$$u_1 + u_2a_2 + \cdots + u_ra_r = 0, \text{ pois } \gamma_1 = id.$$

Como $\{u_1, u_2, \ldots, u_r\}$ é LI sobre M, então nem todos os a_j são elementos de M.

Logo reorganizando novamente os valores, podemos supor $a_2 \notin M = L^H$. Assim, existe $\gamma \in H$ tal que $\gamma(a_2) \neq a_2$.

Aplicando γ ao sistema (3) temos:

$$\begin{cases} \gamma(\gamma_1(u_1)) + \gamma(\gamma_1(u_2)a_2) + \cdots + \gamma(\gamma_1(u_r)a_r) &= 0 \\ \gamma(\gamma_2(u_1)) + \gamma(\gamma_2(u_2)a_2) + \cdots + \gamma(\gamma_2(u_r)a_r) &= 0 \\ \vdots \\ \gamma(\gamma_n(u_1)) + \gamma(\gamma_n(u_2)a_2) + \cdots + \gamma(\gamma_n(u_r)a_r) &= 0 \end{cases} \tag{4}$$

Mas como $\gamma \in H$ e $H = \{\gamma_1, \ldots, \gamma_n\}$ então $\{\gamma\gamma_1, \ldots, \gamma\gamma_n\} = H$, ou seja, o sistema (4) é uma permutação de (3):

$$\begin{cases} \gamma_1(u_1) + \gamma_1(u_2)\gamma(a_2) + \cdots + \gamma_1(u_r)\gamma(a_r) &= 0 \\ \gamma_2(u_1) + \gamma_2(u_2)\gamma(a_2) + \cdots + \gamma_2(u_r)\gamma(a_r) &= 0 \\ \vdots \\ \gamma_n(u_1) + \gamma_n(u_2)\gamma(a_2) + \cdots + \gamma_n(u_r)\gamma(a_r) &= 0 \end{cases} \tag{5}$$

Subtraindo o sistema (3) de (5), temos:

$$\begin{cases} 0 + \gamma_1(u_2)(a_2 - \gamma(a_2)) + \cdots + \gamma_1(u_r)(a_r - \gamma(a_r)) &= 0 \\ 0 + \gamma_2(u_2)(a_2 - \gamma(a_2)) + \cdots + \gamma_2(u_r)(a_r - \gamma(a_r)) &= 0 \\ \vdots \\ 0 + \gamma_n(u_2)(a_2 - \gamma(a_2)) + \cdots + \gamma_n(u_r)(a_r - \gamma(a_r)) &= 0 \end{cases}$$

Como $a_2 \neq \gamma(a_2) \Longrightarrow a_2 - \gamma(a_2) \neq 0$ e

$$(0, (a_2 - \gamma(a_2)), (a_3 - \gamma(a_3)), \cdots, (a_r - \gamma(a_3)), 0, \cdots, 0)$$

é uma solução de (3) com no máximo $r - 1$ coeficientes não nulos.

Logo, temos uma contradição com a minimalidade de r de coeficientes não nulos.

Portanto $|Aut_M L| = |H|$, ou seja, $H = Aut_M L$ e obtemos o que queríamos.

c) Pelo item (b), já temos que $H = Aut_M L = Aut_{L^H} L$. Resta provar que $L^{Aut_M L} = M$.

Seja M um corpo intermediário da extensão $L|K$. Notemos $H = Aut_M L$.

Como H fixa M, então $M \subseteq L^H \subseteq L$, ou seja, $[L : M] = [L : L^H][L^H : M]$.

Pelo item (b), $[L : L^H] = |H|$ e pelo item (a), $[L : M] = |H|$.

Logo, $[L^H : M] = 1$, isto é $L^H = M$.

d) Segue imediatamente do Teorema 3.2, $M|K$ galoisiana se, e somente se, $Aut_M L \lhd Aut_K L = G$.

e) Sabemos do item (a) que $(G : Aut_M L) = [M : K]$, resta provar que para todo corpo intermediário M da extensão $L|K$, tal que $L|M$ seja galoisiana, temos que:

$$G/Aut_M L \cong Aut_K M.$$

De fato, como $M|K$ é galoisiana, pelo Teorema 3.2, temos que para todo $\sigma \in G = Aut_K L$ tem-se $\sigma_0 = \sigma|_M \in Aut_K M$ portanto, podemos definir:

$$\begin{array}{rccc} \Phi: & G & \longrightarrow & Aut_K M \\ & \sigma & \longmapsto & \sigma_0 = \sigma_{|_M}. \end{array}$$

Vemos que Φ é homomorfismo de grupos. De fato, sejam $\sigma, \tau \in G$, então $\phi(\sigma \circ \tau) = (\sigma \circ \tau)|_M = \sigma|_M \circ \tau|_M = \phi(\sigma) \circ \phi(\tau)$.

Observe também que: $\sigma \in Ker(\Phi) \Leftrightarrow \Phi(\sigma) = id_M \Leftrightarrow \sigma|_M = id_M \Leftrightarrow \sigma \in Aut_M L$.

Por outro lado, como $L|M$ é uma extensão galoisiana, então pelo Teorema 3.1, para todo $\sigma_0 \in Aut_K M$, existe $\sigma \in Aut_K L$, tal que $\sigma|_M = \sigma_0$, logo ϕ é sobrejetor. Pelo Teorema de homomorfismo (ver [2, Teorema 3, p.125]), temos:

$$G/Aut_M L \cong Aut_K M.$$

■

O seguinte diagrama ilustra a correspondência de Galois:

$$\begin{array}{ccccc} L^{id} & = & L & \longleftrightarrow & \{id_L\} & = & \mathrm{Aut}_L L \\ & & | & & | & & \\ L^H & = & M & \longleftrightarrow & H & = & \mathrm{Aut}_M L \\ & & | & & | & & \\ L^G & = & K & \longleftrightarrow & G & = & \mathrm{Aut}_K L \end{array}$$

4 SOLUBILIDADE POR MEIO DE RADICAIS

Definição 4.1: *Dizemos que uma extensão finita $L|K$ é uma extensão radical sobre o corpo K se existem $\alpha_1, \alpha_2, \ldots, \alpha_n \in L$, tais que:*

a) $K = K_0 \subset K_0[\alpha_1] = K_1 \subset K_1[\alpha_2] = K_2 \subset \cdots \subset K_{i-1}[\alpha_i] = K_i \subset \cdots \subset K_n = L$.

b) Para todo $i \in \{1, 2, \ldots, n\}$ *existe* $n_i \in \mathbb{N}$ *tal que* $\alpha_i^{n_i} \in K_{i-1}$.

Exemplo 2: *Observe que* $L = \mathbb{Q}[\sqrt{2}, \sqrt[3]{3-\sqrt{2}}]|\mathbb{Q}$ *é uma extensão radical sobre* $\mathbb{Q}$, *pois* $\mathbb{Q} \subset \mathbb{Q}[\sqrt{2}] \subset \mathbb{Q}[\sqrt{2}][\sqrt[3]{3-\sqrt{2}}] = L$ *e* $(\sqrt{2})^2 \in \mathbb{Q}$, $(\sqrt[3]{3-\sqrt{2}})^3 \in \mathbb{Q}[\sqrt{2}]$.

Definição 4.2: *Seja* $f(x) \in K[x]$ *e* $L = Gal(f, K)$. *Dizemos que* $f(x)$ *é um polinômio solúvel por meio de radicais sobre* K *se existe uma extensão radical* $M|K$ *tal que temos* $K \subset L \subset M$.

Observação 4.1: *Se um polinômio é solúvel por meio de radicais sobre* K, *de acordo com esta definição vemos que as raízes de* $f(x)$ *poderão realmente ser escritas como combinações algébricas de expressões radicais. Prossigamos agora com a definição de grupo solúvel que, na realidade, é o análogo de extensão radical através da correspondência de Galois.*

Definição 4.3: *Um grupo* G *é dito solúvel se existem subgrupos* G_j, *com* $j = 0, 1, 2, \ldots, k$ *tais que :*

$$\{id\} = G_0 \subset G_1 \subset \cdots \subset G_{k-1} \subset G_k = G,$$

onde cada G_j *é um subgrupo normal de* G_{j+1} *e* G_{j+1}/G_j *é abeliano.*

Note que se G *é um grupo simples (ou seja, se os únicos subgrupos normais de* G *são* $\{id\}$ *e* G*) e* G *é solúvel, então também será abeliano, mais ainda, será cíclico de ordem primo.*

Proposição 4.1: *Seja* $L|K$ *uma extensão radical sobre* K. *Então existe uma extensão* $K \subset L \subset M$ *tal que* M *é radical e galoisiana sobre* K.

Demonstração. Como $L|K$ é uma extensão radical podemos escrever

$$K = L_0 \subset L_1 \subset \cdots \subset L_{r-1} \subset L_r = L$$

onde

$$L_i = L_{i-1}[\alpha_i] \text{ e } \alpha_i \text{ é raiz de } x^{n_i} - a_i \in L_{i-1}[x].$$

Seja $n = n_1 \cdot n_2 \cdot \ldots \cdot n_r$ e ζ uma raiz primitiva n-ésima da unidade. Substituindo, se necessário, L por $L[\zeta]$ e K por $K[\zeta]$ podemos assumir que $K \subset L$ e K contém as raízes n-ésimas da unidade.

Desta forma os elementos da forma $\alpha_1(\zeta^{n/n_1})^i$, $0 \leq i \leq n_1$ são todos raízes de $x^{n_1} - a_1 \in K[x]$, logo $K = L_0 \subset L_1 = L_0[\alpha_1] = Gal(x^{n_1} - a_1, K)$. Considere agora $L_2 = L_1[\alpha_2]$, onde α_2 é raiz de $x^{n_2} - a_2 \in L_1[x]$.

Considere o polinômio

$$g_2(x) = (x^{n_1} - a_1) \cdot \prod_{\sigma \in Aut_K L_1} (x^{n_2} - \sigma(a_2)) \in L_1[x].$$

Observe que todo $\sigma \in Aut_K L_1$ permuta as raízes de $\prod_{\sigma \in Aut_K L_1} (x^{n_2} - \sigma(a_2))$. Assim, pelo Teorema 3.3 item (c), temos que $g_2(x) \in K[x]$.

Definimos $L_2^* = Gal(g_2(x), K)$. Observe que $K \subset L_2 \subset L_2^*$, por definição $L_2|K$ é uma extensão galoisiana e

$$L_2^* = L_1\left[\sqrt[n_2]{\sigma(a_2)}\,;\, \sigma \in Aut_K L_1\right],$$

ou seja, L_2^* é radical sobre L_1. Concluímos assim que $L_2|K$ é uma extensão galoisiana e radical.

Por indução suponha que $L_i^* = Gal(g_i(x), K)$, onde $K \subset L_i \subset L_i^*$ e $L_i^*|K$ é uma extensão galoisiana e radical. Veja que $L_{i+1} = L_i[\alpha_{i+1}] \subset L_i^*[\alpha_{i+1}]$, onde α_{i+1} é raiz de $x^{n_{i+1}} - a_{i+1} \in L_i[x] \subset L_i^*[x]$.

Novamente pelo Teorema 3.3 item (c), temos que

$$g_{i+1}(x) = g_i(x) \cdot \prod_{\sigma \in Aut_K L_i^*} (x^{n_{i+1}} - \sigma(a_{i+1})) \in K[x].$$

Definimos $L_{i+1}^* = Gal(g_{i+1}(x), K)$. Como $g_i(x)$ é um fator de $g_{i+1}(x)$, então $L_i^* \subset L_{i+1}^*$. Como α_{i+1} é raiz de um dos fatores de $g_{i+1}(x)$, então $L_{i+1} \subset L_i^*[\alpha_{i+1}] \subset L_{i+1}^*$.

Por definição, $L_{i+1}^*|K$ é uma extensão galoisiana e radical pois

$$L_{i+1}^* = L_i^*\left[\sqrt[n_{i+1}]{\sigma(a_{i+1})}\,;\, \sigma \in Aut_K L_i^*\right].$$

Por indução, na etapa $i + 1 = r$, obtemos a extensão desejada $M = L_r^*$.

■

Teorema 4.1: *(Correspondência de Galois) Sejam K um corpo, $f(x) \in K[x]$ e $L = Gal(f, K)$. Temos que $f(x)$ é solúvel por meio de radicais sobre K se, e somente se, o grupo $G = Aut_K L$ é solúvel.*

Demonstração. ($\Longrightarrow$)

Pela Proposição 4.1, existem $K \subset L \subset M$ tal que M é radical e galoisiana sobre K.

Assim, como $L|K$ é normal segue pelo Teorema 3.4, que:

$$G = Aut_K L \cong Aut_K M / Aut_L M$$

Portanto será suficiente provarmos que $Aut_K M$ é solúvel.

Seja $n = n_1 \cdot n_2 \ldots n_r$ tal que $M = K[\alpha_1, \ldots, \alpha_r]$ e $\alpha_i^{n_i} \in K_{i-1}$, $K_i = K_{i-1}[\alpha_i]$ como nas notações anteriores. Seja ζ uma raiz primitiva n-ésima da unidade, $M^* = M[\zeta]$ e $K^* = K[\zeta]$. Para $\sigma \in Aut_K M$, considere $\sigma^* \in Aut_{K^*} M^*$ satisfazendo $\sigma^*|_M = \sigma$ e $\sigma^*(\zeta) = \zeta$.

Claramente se $\sigma \neq \tau$ temos $\sigma^* \neq \tau^*$ e portanto a função abaixo

$$\begin{array}{rccc} \Phi : & Aut_K M & \longrightarrow & Aut_{K^*} M^* \\ & \sigma & \mapsto & \sigma^* \end{array}$$

define um homomorfismo injetivo. Daí segue que $Aut_K M \cong \Phi(Aut_K M) \leq Aut_{K^*} M^*$ e portanto $Aut_K M$ será solúvel se $Aut_{K^*} M^*$ for solúvel.

Assim podemos assumir que K contém uma raiz primitiva n-ésima da unidade.

Agora, se $M = K[\alpha_1, \alpha_2, \ldots, \alpha_r]$ é uma extensão radical sobre K, $n = n_1.n_2 \ldots n_r$, onde $\alpha_i^{n_i} \in K_{i-1}$, e K contém uma raiz primitiva n-ésima da unidade, vamos provar por indução sobre r que $Aut_K M$ é um grupo solúvel.

Se $r = 1$, então $M = K[\alpha_1]$, $\alpha_1^{n_1} = a_1 \in K$ e como K contém uma raiz primitiva n_1-ésima da unidade, segue que $M = Gal(x^{n_1} - a_1, K)$ e $Aut_K M$ é um grupo abeliano, pela Proposição 3.6.

Pela hipótese de indução $Aut_{K_1} M$ é solúvel, onde $M = K_1[\alpha_2, \alpha_3, \ldots, \alpha_r]$.

Como $K_1 = Gal(x^{n_1} - a_1, K)$ é normal sobre K, a função :

$$\begin{array}{rccc} \psi : & Aut_K M & \longrightarrow & Aut_K K_1 \\ & \sigma & \mapsto & \sigma|_{K_1} = \sigma_1 \end{array}$$

define um homomorfismo de grupos cujo núcleo é $Ker(\psi) = Aut_{K_1} M$.

Assim, pelo Teorema de homomorfismos (ver [2, Teorema 3, p.125]), temos:

$$Aut_K M / Aut_{K_1} M \cong \psi(Aut_K M) \subseteq Aut_K K_1.$$

Como $Aut_K K_1$ é abeliano e por indução $Aut_{K_1} M$ é solúvel então temos que $Aut_K M$ é solúvel e isto demonstra o teorema.

($\Longleftarrow$) Ver [1, Teorema 10.18].

■

5 EXEMPLO

Vamos aplicar essa teoria para encontrar a estrutura de subcorpos do corpo de decomposição do polinômio $x^4 - 4x^3 - 4x^2 + 8x - 2$, através da sua ligação com o grupo de Galois do mesmo.

Observe que as raízes de $x^4 - 4x^3 - 4x^2 + 8x - 2$ são

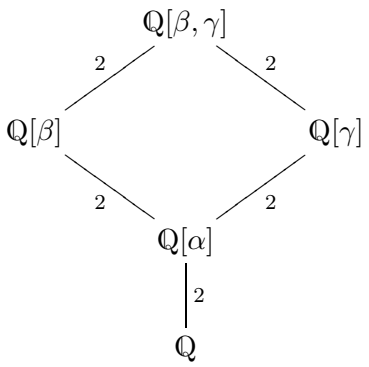
$$x_{1,3} = 1 + \sqrt{2} \pm \sqrt{3 + \sqrt{2}}$$

e

$$x_{2,4} = 1 - \sqrt{2} \pm \sqrt{3 - \sqrt{2}}.$$

Denotemos, $\alpha = \sqrt{2}$, $\beta = \sqrt{3 - \alpha}$ e $\gamma = \sqrt{3 + \alpha}$. Observe que, $L = Gal(f, \mathbb{Q}) = \mathbb{Q}[\beta, \gamma]$.

Como primeira etapa calculamos o grau da extensão e obtemos o seguinte diagrama:



De fato, pelo Critério de Eisenstein (ver [3, Capítulo III, Teorema III.2.8]), para $p = 2$, sabemos que $x^2 - 2$ é irredutível em $\mathbb{Q}[x]$. Logo, $[\mathbb{Q}[\alpha] : \mathbb{Q}] = 2$, (ver [4, Capítulo V, Proposição 3]).

Observando que β e γ são raízes de $x^2 - 3 + \alpha$ e $x^2 - 3 - \alpha$, respectivamente, prova-se por absurdo que $x^2 - 3 + \alpha$ e $x^2 - 3 - \alpha$ são irredutíveis sobre $\mathbb{Q}[\alpha]$. Por exemplo, se $x^2 - 3 + \alpha$ não for irredutível sobre $\mathbb{Q}[\alpha]$, então possui uma raiz em $\mathbb{Q}[\alpha]$ da forma $a + b\alpha$, com $a, b \in \mathbb{Q}$. Assim

$$\begin{aligned} 0 &= (a + b\alpha)^2 - 3 + \alpha \\ &= (a^2 + 2b^2 - 3) + (2ab + 1)\alpha \,. \end{aligned}$$

Logo $a^2 + 2b^2 - 3 = 0$ e $2ab + 1 = 0$. Substituindo $b = -1/2a$ na primeira igualdade, obtemos

$$a^2 + 2\left(-\frac{1}{2a}\right)^2 - 3 = 0 \quad \Longrightarrow \quad 2a^4 - 6a^2 + 1 = 0 \,.$$

Como esta equação não possui raízes racionais, o polinômio $x^2 - 3 + \alpha$ é irredutível sobre $\mathbb{Q}[\alpha]$. De forma similar, prova-se que $x^2 - 3 - \alpha$ é irredutível sobre $\mathbb{Q}[\alpha]$. Assim, $[\mathbb{Q}[\beta] : \mathbb{Q}[\alpha]] = [\mathbb{Q}[\gamma] : \mathbb{Q}[\alpha]] = 2$.

Resta provar que $[\mathbb{Q}[\beta, \gamma] : \mathbb{Q}[\beta]] = 2$. De fato, como γ é raiz de $x^2 - 3 - \alpha$, então $[\mathbb{Q}[\beta, \gamma] : \mathbb{Q}[\beta]] \leqslant 2$. Suponha que $[\mathbb{Q}[\beta, \gamma] : \mathbb{Q}[\beta]] = 1$, neste caso $\gamma \in \mathbb{Q}[\beta]$ chegando a uma contradição com argumentos aritméticos novamente.

Pelo Teorema Fundamental de Galois, $|Aut_{\mathbb{Q}} L| = 8$. Utilizando a Proposição 3.2 em cada degrau do diagrama 6, encontramos todos os automorfismos de L que fixam $\mathbb{Q}$:

$$\begin{array}{ccc} \mathbb{Q}[\beta,\gamma] & \xrightarrow{\sigma} & \mathbb{Q}[\beta,\gamma] \\ \downarrow & & \downarrow \\ \mathbb{Q}[\beta] & \xrightarrow{\psi} & \mathbb{Q}[\beta] \\ \downarrow & & \downarrow \\ \mathbb{Q}[\alpha] & \xrightarrow{\varphi} & \mathbb{Q}[\alpha] \\ \downarrow & & \downarrow \\ \mathbb{Q} & \xrightarrow{id} & \mathbb{Q} \end{array} \tag{6}$$

Obtemos assim todos os elementos do grupo de Galois $G = Aut_{\mathbb{Q}} L$. Analisando os elementos do grupo, chegamos à conclusão que $Aut_{\mathbb{Q}} L \cong D_8$, ou seja

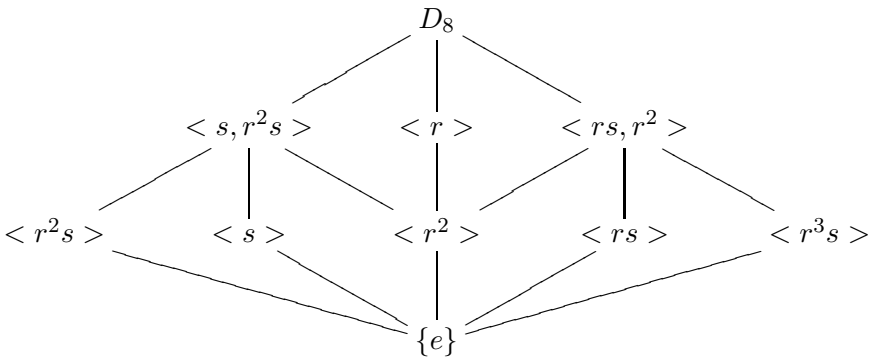
$$G = \left\langle r, s \mid r^4 = e, s^2 = e, rs = sr^3 \right\rangle,$$

onde r e s são os automorfismos definidos a seguir:

$$\begin{aligned} r: \quad \alpha &\longmapsto -\alpha \\ \beta &\longmapsto -\gamma \\ \gamma &\longmapsto \beta \end{aligned}$$

$$\begin{aligned} s: \quad \alpha &\longmapsto -\alpha \\ \beta &\longmapsto \gamma \\ \gamma &\longmapsto \beta \end{aligned}$$

A estrutura de subgrupos H_i de D_8 é representada pelo seguinte diagrama:



Para cada subrupo H calculamos o subcorpo L^H correspondente. Por exemplo:

Seja $x \in L$. Temos que, $L = \langle 1, \alpha, \beta, \gamma, \alpha\beta, \alpha\gamma, \beta\gamma, \alpha\beta\gamma \rangle$, ou seja, um elemento de L é da forma

$$x = a_0 + a_1\alpha + a_2\beta + a_3\gamma + a_4\alpha\beta + a_5\alpha\gamma + a_6\beta\gamma + a_7\alpha\beta\gamma.$$

Assim, se $x \in L^{<r^2>}$ então, $x = r^2(x)$, onde

$$r^2(x) = a_0 + a_1\alpha - a_2\beta - a_3\gamma - a_4\alpha\beta - a_5\alpha\gamma + a_6\beta\gamma + a_7\alpha\beta\gamma.$$

Logo,

$$2a_2\beta + 2a_3\gamma + 2a_4\alpha\beta + 2a_5\alpha\gamma = 0,$$

isto é,

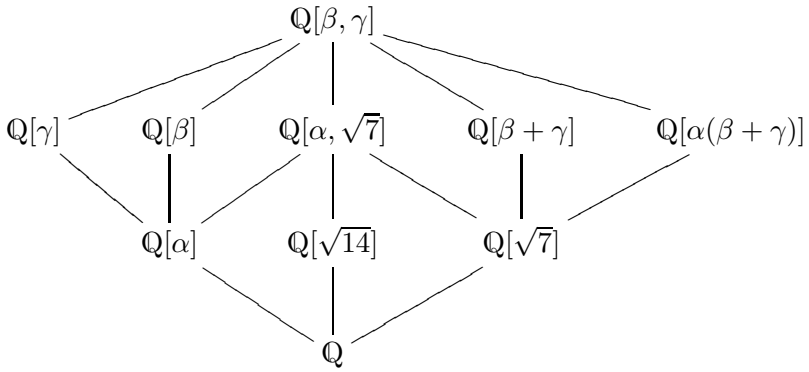
$$a_2 = a_3 = a_4 = a_5 = 0.$$

Daí, $x = a_0 + a_1\alpha + a_6\beta\gamma + a_7\alpha\beta\gamma$.

Portanto, $L^{<r^2>} = \mathbb{Q}[\alpha, \beta\gamma]$ e como $\beta\gamma = \sqrt{3^2 - \alpha^2} = \sqrt{9-2} = \sqrt{7}$, então

$$L^{<r^2>} = \mathbb{Q}[\sqrt{2}, \sqrt{7}].$$

De forma similar achamos os outros corpos intermediários e pelo Teorema 3.4, obtemos a seguinte estrutura de corpos intermediários da extensão $\mathbb{Q}[\beta, \gamma]|\mathbb{Q}$:



O que conclui este exemplo. Este método pode ser aplicado sempre que for possível calcular o grupo de Galois.

6 CONCLUSÃO

Sabe-se que qualquer polinômio de grau menor ou igual a quatro é solúvel por meio de radicais. Neste trabalho demonstramos que um polinômio $f(x)$ de grau n é solúvel por meio de radicais se seu grupo de Galois G, é solúvel. Mostramos também que o grupo G pode ser visto como subgrupo de S_n, (grupo de permutações de n elementos). Sabe-se que para

$n \leq 4$, S_n é solúvel, razão pela qual existem métodos algébricos para encontrar as raízes de polinômios de grau menor ou igual a 4 através de radicais (*Bhaskara, Cardano, Ferrari*).

Ninguém conseguiu encontrar um método geral para achar as raízes de um polinômio de grau ≥ 5 por meio de radicais, pois em geral, o grupo de Galois de um polinômio de grau 5 é isomorfo a A_5 ou S_5 e os grupos A_n e S_n não são solúveis para $n \geq 5$. Mesmo assim, em alguns casos é possível que o grupo de Galois de um polinômio de grau ≥ 5 seja solúvel; nesses casos é possível achar as raízes do polinômio por meio de radicais.

AGRADECIMENTOS

O segundo autor agradece à Fundação de Amparo à Pesquisa do estado de Minas Gerais (FAPEMIG) pelo auxílio financeiro recebido.

REFERÊNCIAS

[1] J. Bewersdorff: *Galois Theory for Beginners*. Rhode Island, AMS, 2006.

[2] H. H. Domingues e G. Iezzi: *Álgebra Moderna*. São Paulo, Atual Editora, 1982.

[3] A. Garcia e Y. Lequain: *Elementos de Ágebra*. IMPA, 2008.

[4] A. Gonçalves: *Introdução à Álgebra*. IMPA, 2009.

[5] R. M. T. Portugal: *Introdução à Teoria de Galois*. Universidade Federal de Uberlândia, 2010.