Revista Eletrônica Paulista de Matemática

ISSN 2316-9664
Volume 9, jul. 2017

A insolubilidade da quíntica e o Teorema Fundamental de Galois

The insolubility of the quintic and the Galois Fundamental Theorem.

José Rafael Borges Zampiva
Universidade Federal de São Carlos - CCET-DM-Ufscar
rafaelbzampiva@gmail.com

Resumo

Historicamente, a primeira vez que os números foram tratados por suas propriedades algébricas foi por Évariste Galois (25 Outubro 1811 - 31 Maio 1832), mais especificamente, uma forma rudimentar do que conhecemos hoje como teoria de Grupos. Em sua teoria, podemos associar a cada grupo de raizes de polinômios uma estrutura de corpo, o que resolveria o famoso problema da impossibilidade de uma fórmula para se resolver a quíntica. No presente trabalho, usamos o Teorema Fundamental da Teoria de Galois, que é usado para demonstrar a impossibilidade de se resolver a quíntica em termos de radicais. Tal fato é feito usando-se a solubilidade e simplicidade de grupos para uma aplicação de solução por radicais para uma quíntica em específico.
Palavras-chave: Quíntica. Grupos solúveis. O polinômio geral. Teoria de Galois. Teorema Fundamental da Teoria de Galois.

Abstract

Historically, the first time the numbers were treated for their algebraic properties was by Évariste Galois (25 October 1811 - 31 May 1832), more specifically, a rudimentary form of than we know today as group theory. In his theory we can associate with each group of roots of polynomials a structure of field, which would solve the famous problem of the impossibility of a formula to solve the quintic. In the present work we use the fundamental theorem of the Galois Theory, which is used to demonstrate the impossibility of solving the quantum in terms of radicals. This is done by using the solubility and simplicity of groups for a radical solution application to a specific quintic.
Keywords: Quintic. Soluble groups. The general polynomial. Galois theory. Fundamental Theorem of Galois Theorem.

1 Alguns resultados básicos

Aqui apresentamos alguns resultados básicos que serão utilizados ao longo o texto e cujas demonstrações podem ser encontradas em Garcia e Lequain (2003), Stewart (2015) e Martin (2010).

Teorema 1 (Lagrange)**.** *A ordem de um subgrupo de um grupo finito é sempre um divisor da ordem do grupo.*

Demonstração. A demonstração pode ser encontrada em: Garcia e Lequain (2003). □

Teorema 2. *Seja $K(\alpha):K$ uma extensão algébrica simples de corpo, e seja $\psi(x)$ o polinômio minimal de α sobre K. Então $K(\alpha):K$ é isomorfo a $\dfrac{K[x]}{\langle\psi(x)\rangle}$. O isomorfismo pode ser escolhido de modo a associar x a α.*

Demonstração. Ora, considere a seguinte função

$$\begin{array}{rccc} \varphi: & \dfrac{K[x]}{\langle\psi(x)\rangle} & \longrightarrow & K(\alpha) \\ & \overline{p}(x) & \longmapsto & \varphi(\overline{p}(x)) = p(\alpha). \end{array}$$

De modo análogo à demonstração do teorema anterior, temos que φ está bem definida e é um isomorfismo. Nota-se que $p(\alpha)=0$ se, e somente se, $\psi(x)|p(x)$. Temos ainda que φ é a identidade, quando restrito a K. □

Corolário 3. *Suponha que $K(\alpha):K$ e $K(\beta):K$ sejam extensões simples, tais que α e β tenham o mesmo polinômio minimal $\psi(x)\in K[x]$. Então, estas duas extensões são isomorfas, e o isomorfismo de corpos maiores pode ser entendido como uma função de α para β.*

Demonstração. Ora, pelo Teorema (2) temos que ambas as extensões são isomorfas a $\dfrac{K[x]}{\langle\psi(x)\rangle}$, e que tais isomorfismos φ, ϕ associam x a α e x a β, respectivamente. Assim, $\phi\varphi^{-1}$ é um isomorfismo de $K(\alpha)$ em $K(\beta)$. E temos o desejado. □

Teorema 4. *Suponha que K e L sejam subcorpos de $\mathbb{C}$ e que $\iota: K\longrightarrow L$ é um isomorfismo. Sejam $K(\alpha)$ e $L(\beta)$ extensões algébricas simples de K e L, respectivamente, tais que $\psi_\alpha(x)$ é o polinômio minimal de α sobre K, e $\psi_\beta(x)$ é o polinômio minimal de β sobre L. Além disso, suponha que $\psi_\beta(x)=\iota(\psi_\alpha(x))$. Então, existe um isomorfismo $\Upsilon: K(\alpha)\longrightarrow L(\beta)$ tal que $\Upsilon|_K=\iota$ e $\Upsilon(\alpha)=\beta$.*

Demonstração. A demonstração pode ser encontrada em: Stewart (2015). □

Proposição 5. *Seja $K(\alpha):K$ uma extensão simples. Se esta, é transcendente, então $[K(\alpha):K]=\infty$. Se a extensão é algébrica, então $[K(\alpha):K]=\partial\psi(x)$, em que $\psi(x)$ é o polinômio minimal de α sobre K e $\partial\psi(x)$ é definido como o grau de $\psi(x)$.*

Demonstração. A demonstração pode ser encontrada em: Stewart (2015). □

Lema 6. *$L:K$ é uma extensão finita se, e somente se, L é algébrico sobre K e existem $\alpha_1,\ldots,\alpha_n\in L$, $n\in\mathbb{N}$, tais que $L=K(\alpha_1,\ldots,\alpha_n)$.*

Demonstração. A demonstração pode ser encontrada em: Stewart (2015). □

Lema 7. *Suponha que $\iota : K \longrightarrow K'$ é um isomorfismo de subcorpos de $\mathbb{C}$. Seja $f(x) \in K[x]$ e $Gal(f(x),K)$ o corpo de decomposição para $f(x)$. Considere também L qualquer extensão de corpo de K' tal que $\iota(f(x))$ decompõe-se linearmente sobre L. Então, existe um monomorfismo $\Upsilon : Gal(f(x),K) \longrightarrow L$, tal que $\Upsilon|_K = \iota$.*

Demonstração. Observe o seguinte diagrama

$$\begin{array}{ccc} K & \longrightarrow & Gal(f(x),K) \\ \iota \downarrow & & \downarrow \Upsilon \\ K' & \longrightarrow & L \end{array}$$

em que Υ precisa ser encontrada. A construção de Υ será feita por indução no grau de $f(x)$. Ora, tome $f(x) \in Gal(f(x),K)$ e obtemos:

$$f(x) = k(x-\beta_1)...(x-\beta_n).$$

Se $\psi_1(x)$ é o polinômio minimal de α_1, sobre K, então $\psi_1(x)$ é claramente um fator irredutível de $f(x)$. Ou seja, $\iota(\psi(x))$ divide $\iota(f(x))$, o qual se decompõe sobre L, ou seja,

$$\iota(\psi(x)) = (x-\alpha_1)...(x-\alpha_r),$$

sobre L, em que $\alpha_1,...,\alpha_r \in L$. Como $\iota(\psi(x))$ é irredutível sobre K', este é o polinômio minimal de α_1 sobre K'. Assim, pelo Teorema (4), existe um isomorfimo

$$\Upsilon : K(\beta_1) \longrightarrow K'(\alpha_1),$$

tal que $\Upsilon_1|_K = \iota$ e $\Upsilon_1(\beta_1) = \alpha_1$. Deste modo, $Gal(f(x),K)$ é o corpo de decomposição sobre $K(\beta_1)$ do polinômio $\Phi : \dfrac{f(x)}{(x-\beta_1)}$. Por indução, existe um monomorfismo $\Upsilon : Gal(f(x),K) \longrightarrow L$ tal que $\Upsilon|_{K(\beta_1)} = \Upsilon_1$. Então, $\Upsilon|_K = \iota$. □

Definição 8. *O Grupo de Galois $\Gamma(L:K)$ de uma extensão $L:K$ é o grupo de todos os K-automorfismos de L com a composição de funções.*

Observação 9. *Também é comum denotarmos o Grupo de Galois da extensão $L:K$ como $Gal(L:K)$.*

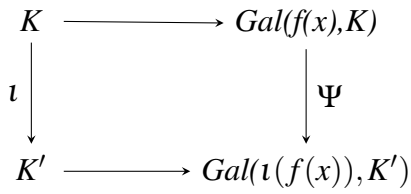
Proposição 10. *Sejam M um corpo intermediário e H um subgrupo de $\Gamma(L:K)$. Então $M \subseteq M^{*\dagger}$ e $H \subseteq H^{\dagger *}$.*

Demonstração. A demonstração pode ser encontrada em: Stewart (2015). □

Teorema 11. *Seja $\iota : K \longrightarrow K'$ um isomorfismo. Seja $Gal(f(x),K)$ o corpo de decomposição de $f(x)$ sobre K, e seja $Gal'(\iota(f(x)),K')$ o corpo de decomposição de $\iota(f(x))$ sobre K'. Então, existe um isomorfismo $\Psi : Gal(f(x),K) \longrightarrow Gal'(\iota(f(x)),K')$ tal que $\Psi|_K = \iota$.*

Demonstração. Em outras palavras, devemos mostrar que as extensões $Gal(f(x),K) : K$ e $Gal'(\iota(f(x)),K') : K'$ são isomorfas.

Observa-se o seguinte diagrama



Devemos assim encontrar Ψ de modo que o diagrama acima comute. Ora, pelo Lema (7), sabemos que existe um monomorfismo $\Upsilon : Gal(f(x),K) \longrightarrow Gal(\iota(f(x)),K')$ tal que $\Upsilon|_K = \iota$. Temos claramente que, $\Upsilon(Gal((f(x)),K)$ é o corpo de decomposição de $\iota(f(x))$ sobre K', e está contido em $Gal(\iota(f(x)),K')$. Como $Gal(\iota(f(x)),K')$ é também o corpo de decomposição de $\iota(f(x))$ sobre K', temos por definição que

$$\Upsilon(Gal(f(x),K) = Gal(\iota(f(x)),K'),$$

de onde obtemos que Υ é sobrejetora. Ou seja, Υ é um isomorfismo e basta tomarmos, $\Psi = \Upsilon$. E obtemos o desejado. □

Teorema 12. *Uma extensão de corpo $L : K$ é normal e finita se, e somente se, L é um corpo de decomposição para algum polinômio sobre K.*

Demonstração. Suponha que $L : K$ seja normal e finita. Ora, pelo Lema (6), $L = K(\alpha_1, ..., \alpha_s)$ para certos α_j algébricos sobre K. Seja $\psi_j(x)$ o polinômio minimal de α_j sobre K, e $\psi(x) = \psi_1(x)...\psi_s(x)$. Cada $\psi_j(x)$ é irredutível sobre K e tem um zero, $\alpha_j \in L$. Usando a hipótese de que $L : K$ é normal, temos que cada ψ_j decompõe-se linearmente sobre L. E, assim, $\psi(x)$ decompõe-se linearmente sobre L. Como L é gerado por K e pelos zeros de $\psi(x)$, este é o corpo de decomposição de $\psi(x)$ sobre K.

Suponha agora que L seja o corpo de decomposição para algum polinômio $g(x)$ sobre K. A extensão $L : K$ é assim, obviamente, finita. Devemos mostrar ainda que é normal. Para fazermos isto, precisamos tomar uma polinômio irredutível $f(x)$ sobre K, com um zero em L, e mostrar que este se decompõe linearmente em L. Consideremos $L \subseteq M$ um corpo de decomposição para $f(x)g(x)$ sobre K. Suponhamos que α_1 e α_2 são zeros de $f(x)$ em M. Por irredutibilidade, $f(x)$ é o polinômio minimal de α_1 e α_2 sobre K.

Mostremos que

$$[L(\alpha_1) : L] = [L(\alpha_2) : L].$$

Consideremos os seguintes subcorpos: $K, L, K(\alpha_1), L(\alpha_1), K(\alpha_2), L(\alpha_2)$ de M tais que,

$$K \subseteq K(\alpha_1) \subseteq L(\alpha_1) \subseteq M,$$
$$K \subseteq K(\alpha_2) \subseteq L(\alpha_2) \subseteq M.$$

Claramente, temos $K \subseteq K(\alpha_j)$ e $L \subseteq L(\alpha_j)$, com $j = 1,2$ e $K \subseteq L \subseteq M$. Fazendo agora, um simples cálculo dos graus dessas torres. Para $j = 1$ ou 2,

$$[L(\alpha_j) : L] \cdot [L : K] = [L(\alpha_j) : K] = [L(\alpha_j) : K(\alpha_j)] \cdot [K(\alpha_j) : K]. \quad (1)$$

Pela Proposição (5), $[K(\alpha_1) : K] = [K(\alpha_2) : K]$. Claramente, $L(\alpha_j)$ é o corpo de decomposição de $g(x)$ sobre $K(\alpha_j)$, e pelo Corolário (3), $K(\alpha_1)$ é isomorfo a $K(\alpha_2)$. Assim, pelo Teorema (11), as extensões $L(\alpha_j) : K(\alpha_j)$ são isomorfas para $j = 1,2$. Ou seja, possuem o mesmo grau. Substituindo em (1) e fazendo os devidos cancelamentos, obtemos

$$[L(\alpha_1):L] = [L(\alpha_2):L].$$

Agora, precisamos mostrar que $L:K$ é normal. Ora, se $\alpha_1 \in L$, então $[L(\alpha_1):L] = 1$, e analogamente, $[L(\alpha_2):L] = 1$ e $\alpha_2 \in L$. Logo, $L:K$ é normal. □

Lema 13. *Um polinômio $f(x) \neq 0$ sobre um corpo K possui um zero com multiplicidade maior ou igual a 1 em uma corpo de decomposição se, e somente se, $f(x)$ e $f'(x)$ possuem um fator comum de grau maior ou igual a 1.*

Demonstração. Suponha que $f(x)$ possua um zero repetido em uma corpo de decomposição L. Então sobre L temos,

$$f(x) = (x-\alpha)^2 g(x), \text{ onde } \alpha \in L. \text{ Então,}$$

$$f'(x) = (x-\alpha)((x-\alpha)g'(x) + 2g(x), \text{ ou seja,}$$

$f(x)$ e $f'(x)$ possuem $(x-\alpha)$ como fator comum em $L[x]$. E assim, $f(x)$ e $f'(x)$ possuem um fator comum em $K[x]$.

Agora suponha que $f(x)$ não possua zeros repetidos. Mostraremos por indução no grau de $f(x)$ que $f(x)$ e $f'(x)$ são primos entre si. Se $\partial f(x) = 1$ então, é imediato, que $f(x)$ e $f'(x)$ são primos entre si. Suponha que o resultado valha para todo polinômio com $\partial h(x) < n$, e vamos mostrar que o resultado vale para polinômios de grau n.

De fato, suponha que $\partial f(x) = n$ com $f(x) = (x-\alpha)g(x)$, em que $(x-\alpha) \nmid g(x)$. Então

$$f'(x) = (x-\alpha)g'(x) + g(x).$$

Ora, se um fator de $g(x)$ divide $f'(x)$, então também é verdade que ele divide $g'(x)$, já que não divide $(x-\alpha)$. Mas, por indução, $g(x)$ e $g'(x)$ são primos entre si. E assim, $f(x)$ e $f'(x)$ são primos entre si. Seguindo o resultado. □

Proposição 14. *Se K é um subcorpo de $\mathbb{C}$, então todo polinômio irredutível sobre K é separável.*

Demonstração. Ora, pelo Lema (13), temos que um polinômio irredutível $f(x)$ sobre K é separável se, e somente se, $f(x)$ e $f'(x)$ têm um fator comum de grau maior ou igual a 1. Como $f(x)$ é irredutível, o fator comum entre estes deve ser $f(x)$. Mas, $f'(x)$ tem um grau menor que o grau de $f(x)$, e o único múltiplo de $f(x)$ de grau menor é 0, ou seja, $f'(x) = 0$. Portanto, se

$$f(x) = a_0 + xa_1 + ... + x^n a_n,$$

temos que $na_n = 0$, para todos os inteiros $n > 0$. Para subcorpos de $\mathbb{C}$, isto é, equivalente a $a_n = 0$, para todo $n \in \{1, 2, \cdot, n\}$. □

Teorema 15 (Dedekind)**.** *Seja G um monóide multiplicativo, K um corpo e $\sigma_1, ..., \sigma_n : G \longrightarrow K$ homomorfismos distintos. Então, eles são linearmente independentes sobre K, isto é, os únicos elementos $a_1, ..., a_n \in K$ tais que:*

$$a_1\sigma_1(x) + ... + a_n\sigma_n(x) = 0, \tag{2}$$

para $x \in G$ são $a_1 = a_2 = ... = a_n = 0$.

Demonstração. A demonstração pode ser encontrada em: Martin (2010). □

Lema 16. *Se G é um grupo com elementos distintos $g_1, ..., g_n$ e se $g \in G$ então as g_j variáveis de 1 até n dos elementos gg_j percorrem todo o grupo G.*

Demonstração. A demonstração pode ser encontrada em: Martin (2010). □

Teorema 17. *Seja G um subgrupo finito do grupo de automorfismos de um corpo K, e seja K_0 o corpo fixo de G. Então $[K : K_0] = |G|$.*

Demonstração. A demonstração pode ser encontrada em: Stewart (2015). □

Teorema 18. *Suponhamos que $L : K$ seja uma extensão normal e finita, e que $K \subseteq M \subseteq L$. Seja τ um K-monomorfismo de M em L. Então, existe um K-automorfismo σ de L tal que $\sigma|_M = \tau$.*

Demonstração. Como $L : K$ é uma extensão normal e finita, o Teorema (12) nos diz que L é o corpo de decomposição de algum polinômio $f(x)$ sobre K. Portanto, este também é o corpo de decomposição de $f(x)$ sobre M e de $\tau(f(x))$ sobre $\tau(M)$. Mas, $\tau|_K$ é a identidade, então $\tau(f(x)) = f(x)$. Conseguimos o seguinte diagrama:

$$\begin{array}{ccc} M & \xrightarrow{\tau} & L \\ \tau \downarrow & & \downarrow \sigma \\ \tau(M) & \longrightarrow & L \end{array}$$

Onde σ precisa ser encontrada. Ora, pelo Teorema (11) existe um isomorfismo $\Upsilon : L \longrightarrow L$ tal que $\Upsilon|_M = \tau$. Deste modo, $\Upsilon = \sigma$ que estamos procurando, sendo este um automorfismo de L, e como $\sigma|_K = \tau|_K$ e este é a identidade, onde σ é um K-automorfismo de L. □

Proposição 19. *Suponhamos que $L : K$ seja uma extensão normal e finita e α, β sejam os zeros em L do polinômio irredutível p sobre K. Então, existe um k-automorfismo σ de L tal que,*

$$\sigma(\alpha) = \beta.$$

Demonstração. Aplicando o Corolário (3), temos a existência de um isomorfismo $\tau : K(\alpha) \longrightarrow K(\beta)$, de modo que $\tau|_K$ é a identidade e $\tau(\alpha) = \beta$. Usando agora o Teorema (18), conseguimos estender τ a um k-automorfismo σ de L. □

Teorema 20. *Se $L : K$ é uma extensão finita com grupo de Galois G, tal que K é um corpo fixo de G, então $L : K$ é normal.*

Demonstração. A demonstração pode ser encontrada em: Stewart (2015). □

2 A Correspondência de Galois

Apresentamos aqui o Teorema de Galois, tão importante para o entendimento do presente trabalho. Seja $L : K$ uma extensão com Grupo de Galois G, que consiste de todos os K-automorfismos de L. Seja $\mathscr{F}$ o conjunto dos corpos intermediários, ou seja, o conjunto dos subcorpos M tais que $K \subseteq M \subseteq L$. E seja $\mathscr{G}$ o conjunto de todos os subgrupos H de G. Definimos as seguintes funções:

$$\begin{array}{rccc} * : & \mathscr{F} & \longrightarrow & \mathscr{G} \\ \dagger : & \mathscr{G} & \longrightarrow & \mathscr{F} \end{array}$$

Definidas como segue: Se $M \in \mathscr{F}$, então M^* é o grupo de todos os M-automorfismos de L. Se $H \in \mathscr{G}$, então $H^\dagger$ é o corpo fixo de H. Já observamos, pela Proposição (10) que, $M \subseteq M^{*\dagger}$ e $H \subseteq H^{\dagger *}$, ou seja, que $*$ e $\dagger$ são inclusões reversas.

Antes de enunciarmos e provarmos o teorema fundamental, provemos o seguinte Lema.

Lema 21. *Suponhamos que $L : K$ é uma extensão de corpo, M é um corpo intermediário, e τ é um K-automorfismo de L. Então $(\tau(M))^* = \tau M^* \tau^{-1}$.*

Demonstração. A demonstração pode ser encontrada em: Stewart (2015). □

Teorema 22 (Teorema Fundamental da Teoria de Galois). *Se $L : K$ é uma extensão normal finita, com Grupo de Galois G, e se $\mathscr{F}, \mathscr{G}, *, \dagger$ são definidas como acima, então:*

i) O Grupo de Galois tem ordem $[L : K]$;

ii) As funções $*$ e $\dagger$ são mutuamente inversas, e geram um correspondência bijetiva entre $\mathscr{F}$ e $\mathscr{G}$;

iii) Se M é um corpo intermediário, então

$$\begin{aligned} [L : M] &= |M^*|, \\ [M : K] &= \frac{|G|}{|M^*|}; \end{aligned}$$

iv) Um corpo intermediário M é uma extensão normal de K se, e somente se, M^* é um subgrupo normal de G;

v) Se um corpo intermediário M é uma extensão normal de K, então o Grupo de Galois de $M : K$ é isomorfo ao grupo quociente $\dfrac{G}{M^*}$

Demonstração. A demonstração pode ser encontrada em: Stewart (2015). □

3 Solubilidade e simplicidade de grupos

Com a intensão de aplicar a Correspondência de Galois, precisamos ter em mãos alguns conceitos teóricos da teoria dos grupos. Assumiremos familiaridade com a Teoria Elementar de Grupos: subgrupos, subgrupos normais, grupos quocientes, conjugados e agora, adicionaremos os Teoremas Fundamentais do Isomorfismo e o Grupo de Permutações.

3.1 Grupo de Permutação

Definição 23. *Seja X um conjunto qualquer diferente do vazio. Uma permutação de X é uma função bijetora de X em X.*

Teorema 24. *O conjunto de todas as permutações de um conjunto X, com X diferente do vazio, forma um grupo com a composição de funções com a operação de composição de funções.*

Proposição 25. $|S_n| = n!$.

Demonstração. Basta observar que existem $n!$ maneiras de se combinar n elementos. □

Observação 26 (Notação de ciclos para uma permutação)**.** *Considera-se α o seguinte elemento de S_6:*

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 3 & 6 & 1 & 2 \end{pmatrix}.$$

Podemos reescrever α como $\alpha = (1,5)(2,4,6)$.

Esta notação é feita do seguinte modo: Abrimos parenteses e colocamos o menor elemento. E, em seguida, o elemento no qual ele é levado, separando os dois por uma vírgula, fechamos os parêntes e então o último elemento é levado no primeiro.

No caso de α, 1 é levado em 5, e 5 é levado em 1. Caso um elemento não esteja nos parênteses, isto significa que ele é levado nele mesmo. Abrimos então parêntes novamente e repetimos o processo com o próximo menor elemento da permutação.

Exemplo 27. *Considere o seguinte elemento de S_9:*

$$\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 7 & 3 & 8 & 6 & 1 & 4 & 9 & 2 \end{pmatrix}.$$

Reescrevendo β em ciclos, temos: $\beta = (1,5,6)(2,7,4,8,9)$.

Exemplo 28. *Os elementos de S_3 podem ser reescritos como segue*

$$\varepsilon,\ (1,2),\ (2,3),\ (1,3),\ (1,2,3)\ e\ (1,3,2),$$

em que ε é a identidade.

Definição 29. *Seja k um inteiro positivo. Uma permutação do tipo $(a_1a_2a_3...a_k)$, ou seja, uma permutação escrita em apenas um parêntese, é chamada de permutação cíclica. E um ciclo com apenas dois elementos é chamado de transposição.*

Teorema 30. *Todo elemento de S_n é um produto de transposições.*

Demonstração. Dado $\gamma \in S_n$ e reescrevendo γ em sua notação de ciclos, notamos que:

$$(a_{r_0}, a_{r_1}, ..., a_{r_s}) = (a_{r_0}, a_{r_s}), (a_{r_0}, a_{r_{s-1}}), ..., (a_{r_0}, a_{r_1}),$$

e obtemos o desejado. □

Teorema 31. *As transposições $(1,2),(1,3),...,(1,n)$ juntas geram S_n.*

Demonstração. De fato, $(a,b) = (1,a)(1,b)(1,a)$. Sendo $a,b \in \mathbb{N}_n$, considere $\alpha = (1,a)$ e $\beta = (1,b)$ e $\gamma = (1,a)$. Logo, temos:

$$\gamma\beta\alpha(1) = \gamma\beta(a) = \gamma(a) = 1$$

$$\gamma\beta\alpha(a) = \gamma\beta(1) = \gamma(b) = b$$

$$\gamma\beta\alpha(b) = \gamma\beta(b) = \gamma(1) = a.$$

Logo $(a,b) = (1,a)(1,b)(1,a)$ (Observa-se que 1 vai nele mesmo, ou seja, ele não é representado em (ab)).

Pelo Teorema 30, temos:

$$(a_1a_2a_3...a_k)=(a_1a_k)(a_1a_{k-1})...(a_1a_3)(a_1a_2).$$

Escolhendo qualquer transposição no segundo termo, temos que ele pode ser escrito da seguinte forma: $(a,b) = (1,a)(1,b)(1,a)$. Logo $(1,2),(1,3),...,(1,n)$ geram S_n. □

Teorema 32. *As transposições* $(1,2),(2,3),(3,4),...,(n-1,n)$ *juntas geram* S_n.

Demonstração. Temos pelo Teorema (31) que $(1,2),(1,3),...,(1,n)$ geram S_n. Consideremos k, tal que $1 \leq k \leq n$, temos então:

$(1,k) = (k-1,k)(k-2,k-1)...(3,4)(2,3)(1,2)(2,3)(3,4)...(k-2,k-1)(k-1,k)$. De fato, notemos que se considerarmos $\alpha_1 = (1,2)$, $\alpha_2 = (2,3)$, $\alpha_3 = (3,4)$, ..., $\alpha_{k-1} = (k-1,k)$, temos:

$$(1,k) = (\alpha_{k-1},\alpha_{k-2},\cdot,\alpha_3,\alpha_2,\alpha_1,\alpha_2,\alpha_3,...,\alpha_{k-2},\alpha_{k-1})(x)=\varphi(x), \text{ daí:}$$

$\varphi(k)=(\alpha_{k-1},\alpha_{k-2},...,\alpha_3,\alpha_2,\alpha_1,\alpha_2,\alpha_3,...,\alpha_{k-2},\alpha_{k-1})(k)$. Ou seja, $\varphi(k) = 1$ e $\varphi(1) = k$.

Mostremos que $\varphi(n) = n$, para todo $n \in \{2,3,...,k-2,k-1\}$. Considera-se agora:

$$\varphi(n)=(\alpha_{k-1},\ ...\ ,\alpha_n,\alpha_{n-1},...,\alpha_2,\alpha_1,\alpha_2,\alpha_{n-1},\alpha_n,\ ...\ ,\alpha_{k-1})(n).$$

Logo, n apenas aparecerá em α_{n-1} e α_n. Sendo que $\alpha_n(n) = n+1$ não está em α_{n-1}. Logo, $\alpha_{n-1}(n+1) = n+1$. E isso se repetirá até que se "encontre"o α_n novamente, ou seja, $\alpha_n(n+1) = n$. Logo, $\varphi(n) = n$. □

Observação 33. *Notemos que pelo Teorema* (30) *qualquer permutação pode ser escrita como produto de transposições, sendo esta quantidade de transposições ímpar ou par.*

Considera-se o polinômio

$$P = P(x_1,x_2,\ ...x_n)=(x_1-x_2)(x_1-x_3)...(x_1-x_2)(x_2-x_3)...(x_{n-1}-x_n).$$

Note que o polinômio P consiste de todos os fatores $(x_i - x_j)$ *com* $1 \leq i \leq n$, $1 \leq j \leq n$ *e* $i \leq j$.

Definição 34. *Seja* α *uma permutação de* S_n *e P o polinômio* $P = P(x_1,x_2,\ ...x_n)$. *Denotamos por* αP *todos os fatores* $(x_{\alpha(i)} - x_{\alpha(j)})$ *com* $1 \leq i \leq n, 1 \leq j \leq n$ *e* $i \leq j$.

Observação 35. *: Na Definição* (34)*,* α *reordena os fatores de P trocando o sinal de alguns destes.*

Definição 36. *Seja* α *uma permutação de* S_n *e* $P = P(x_1,x_2,...x_n)$ *se* $\alpha P = P$*, então* α *é positivo e seu sinal e* $+1$. *Caso* $\alpha P = -P$*, então* α *é negativo e seu sinal é* -1.

Definição 37. *Seja* α *uma permutação de* S_n. *Se* α *é positivo, então* α *é par. Caso contrário,* α *é ímpar.*

Definição 38. A_n *é o conjunto de todas as permutações pares de* S_n.

Teorema 39. $|A_n| = \dfrac{n!}{2}$.

Demonstração. Esta demonstração pode ser encontrada em um livro de álgebra, indicamos Garcia e Lequain (2003). □

Exemplo 40. *Expressar cada um dos seguintes elementos de S_8 como produto de permutações cíclicas disjuntas e também como produto de transposições.*

Ora,

$$a)\ \begin{pmatrix}1&2&3&4&5&6&7&8\\7&6&4&1&8&2&3&5\end{pmatrix} = (1734)(26)(58) = (14)(13)(17)(26)(58)$$

$b)\ (4,5,6,8)(1,2,4,5) = (1,2,5)(4,6,8) = (1,5)(1,2)(4,8)(4,6).$

$c)\ (6,2,4)(2,5,3)(8,7,6)(4,5) = (2,5,6,8,7)(3,4) = (2,7)(2,8)(2,6)(2,5)(3,4).$

Algumas destas permutações pertencem a A_8?

Sim, apenas b), pois é par.

Proposição 41. *Se $k = 2n$, para algum $n \in \mathbb{N}$ então $(a_1a_2a_3...a_k) = (a_1a_k)(a_1a_{k-1})\cdot(a_1a_3)(a_1a_2)$, em que o número de transposições do segundo termo é ímpar. De modo análogo, se $k = 2n+1$, para algum $n \in \mathbb{N}$, então o número de transposições do segundo termo é par.*

Proposição 42. *Se $\alpha, \beta \in S_n$, então o sinal de $\alpha\beta$ é o produto usual dos sinais de α e β.*

Exemplo 43. *Seja $P = (x_1,x_2)$ e $\alpha = (1,2)$. Discutir o sinal de α.*

Considera-se P=(x_1,x_2) e $\alpha = (1,2)$, temos então:

$$P = (x_1 - x_2),\ \alpha P = (x_{\alpha(1)} - x_{\alpha(2)}) = (x_2 - x_1) = -(x_1 - x_2) = -P$$

Portanto, o sinal de α é negativo. Nota-se que:

$$(1,a) = (2,a)(1,2)(2,a),\ \text{para } n \geq 2.$$

Como sabemos, o sinal de $(1,2)$ é -1, ou seja, pouco importa o sinal de $(2,a)$, pois o sinal de $(1,a)$ será sempre negativo.

Temos agora que:

$(a,b) = (1,a)(1,b)(1,a)$, e como o sinal de $(1,a)$ e $(1,b)$ são negativos, temos que o sinal de qualquer transposição é negativa.

Concluimos que se um elemento de S_n pode ser escrito com um número par de transposições, ele terá o valor positivo. Caso seja escrito com um número ímpar, ele terá o valor negativo.

Exemplo 44. *Calcular $\alpha P = (x_1,x_2,x_3,x_4)$ quando $\alpha = (1,4,3)$ e quando $\alpha = (2,3)(4,1,2)$.*

Ora, quando $\alpha = (1,4,3)$, temos:

$$P = (x_1,x_2,x_3,x_4) = (x_1 - x_2)(x_1 - x_3)(x_1 - x_4)(x_2 - x_3)(x_2 - x_4)(x_3 - x_4).\ \textit{Portanto,}$$

$$\alpha P = (x_{\alpha(1)} - x_{\alpha(2)})(x_{\alpha(1)} - x_{\alpha(3)})(x_{\alpha(1)} - x_{\alpha(4)})(x_{\alpha(2)} - x_{\alpha(3)})(x_{\alpha(2)} - x_{\alpha(4)})(x_{\alpha(3)} - x_{\alpha(4)}),$$

o que implica em:

$$\alpha\ P = (x_4 - x_2)(x_4 - x_1)(x_4 - x_3)(x_2 - x_1)(x_2 - x_3)(x_1 - x_3).$$

Considera-se agora α=$(23)(412)$, nota-se que $(23)(412)$=(1234), assim:

$$\alpha\ P = (x_{\alpha(1)} - x_{\alpha(2)})(x_{\alpha(1)} - x_{\alpha(3)})(x_{\alpha(1)} - x_{\alpha(4)})(x_{\alpha(2)} - x_{\alpha(3)})(x_{\alpha(2)} - x_{\alpha(4)})(x_{\alpha(3)} - x_{\alpha(4)}),$$

o que implica em:

$$\alpha\, P = (x_3 - x_4)(x_3 - x_2)(x_4 - x_1)(x_4 - x_2)(x_4 - x_1)(x_2 - x_1).$$

Concluímos, assim, que $(1,4,3)$ *é par e* $(1,2,3,4)$ *é ímpar.*

Exemplo 45. *Se* α, $\beta \in S_n$, *mostrar que* $\alpha\beta\alpha^{-1}\beta^{-1}$ *sempre pertence a* A_n *e que* $\alpha\beta\alpha^{-1}$ *pertence a* A_n *sempre que* β *é uma permutação par.*

Se uma permutação qualquer pertence a A_n, *temos que tal permutação é par, ou seja, temos que a permutação possui o sinal positivo. Deste modo, dividiremos em quatro casos:*

1. α *e* β *pares, ou seja, ambos positivos.*
2. α *par e* β *ímpar, ou seja, positivo e negativo, respectivamente.*
3. α *ímpar e* β *par, ou seja, negativo e positivo, respectivamente.*
4. α *e* β *ímpares, ou seja, ambos negativos.*

Sabendo que o sinal de um produto de permutações é o produto dos sinais das permutações, temos então que $\alpha\beta\alpha^{-1}\beta^{-1}$ *sempre será positivo em qualquer caso, ou seja, será sempre par.*

Logo, temos que $\alpha\beta\alpha^{-1}\beta^{-1}$ *sempre pertence a* A_n. *E, quando* β *é par, temos então que* $\alpha\beta\alpha^{-1}$ *será sempre par, ou seja, sempre pertence a* A_n.

Exemplo 46. *Encontrar a ordem da permutação* $\alpha = (1,7,3,4)(2,6)(5,8)$.

Observa-se que:

$$(1,7,3,4)(2,6)(5,8)(1,7,3,4)(2,6)(5,8) = (1,7,3,4)(1,7,3,4) = (1,3)(4,7) = \alpha^2;$$

$$(1,3)(4,7)(1,7,3,4)(2,6)(5,8) = (1,4,3,7)(2,6)(5,8) = \alpha^3;$$

$$(1,4,3,7)(2,6)(5,8)(1,7,3,4)(2,6)(5,8) = \varepsilon.$$

Portanto, concluímos que a ordem de α *é quatro.*

3.2 Grupos solúveis

Definição 47. *Seja* H *um subgrupo normal de* G. *Denotamos* H *subgrupo normal de* G *por* $H \lhd G$.

Definição 48. *Um grupo* G *é solúvel se este tem uma sequência finita de subgrupos,*

$$\{e\} = G_0 \subseteq G_1 \subseteq \ldots \subseteq G_n = G, \tag{3}$$

tais que

i) $G_i \lhd G_{i+1}$, *para* $i = 0,1,\ldots,n-1$;

ii) $\dfrac{G_{i+1}}{G_i}$ *é abeliano para* $i = 0,1,\ldots,n-1$.

Observação 49. *Claramente, a normalidade não é transitiva, ou seja, se $G_i \lhd G_{i+1} \lhd G_{i+2}$ não, necessariamente, temos $G_i \lhd G_{i+2}$.*

Exemplo 50. *1. Todo grupo abeliano é solúvel.*

2. *S_3 é solúvel. De fato, temos que $|S_3| = 2 \cdot 3$, e $\sigma = (1,2,3) \in S_3$, com $|\langle\sigma\rangle| = 3$. Logo, o quociente de S_3 pelo gerado por σ possui ordem 2, sendo assim é cíclico. Como todo grupo cíclico é abeliano, obtemos o resultado.*

3. *S_4 é solúvel. Ora, a sequência*

$$\{e\} \lhd \mathscr{V} \lhd A_4 \lhd S_4,$$

em que A_4 é o grupo alternante de ordem 12 e $\mathscr{V}$ é o grupo quarto de Klein, com $\mathscr{V} = \{e,(1,2)(3,4),(1,3)(2,4),(1,4)(2,3)\}$ e, portanto, um produto direto de dois grupos cíclicos de ordem 2. Os grupos quocientes são:

$$\frac{\mathscr{V}}{\{e\}} \cong \mathscr{V} \text{ abeliano de ordem 4;}$$
$$\frac{A_4}{\mathscr{V}} \cong \mathbb{Z}_3 \text{ abeliano de ordem 3;}$$
$$\frac{S_4}{A_4} \cong \mathbb{Z}_2 \text{ abeliano de ordem 2.}$$

Lema 51 (Segundo e Terceiro Teoremas do Isomorfismo)**.** *Sejam G, H e A grupos*

i) Se $H \lhd G$ e $A \subseteq G$, então $H \cap A \lhd A$ e

$$\frac{A}{H \cap A} \cong \frac{HA}{H}$$

ii) Se $H \lhd G$, e $H \subseteq A \lhd G$ então $H \lhd A$, $\frac{A}{H} \lhd \frac{G}{H}$ e

$$\frac{G/H}{A/H} \cong \frac{G}{A}.$$

Demonstração. Consulte Garcia e Lequain (2003). □

Teorema 52. *Sejam G um grupo, $H < G$ e $N \lhd G$, assim:*

i) Se G é solúvel, então H é solúvel;

ii) Se G é solúvel, então G/H é solúvel;

iii) Se N e G/N são solúveis então G é solúvel.

Demonstração. Ora,

i) Seja $\{e\} = G_0 \subseteq G_1 \subseteq ... \subseteq G_r = G$ uma sequência de subgrupos normais de G, com quociente G_{i+1}/G_i abeliano. Tomemos $H_i = G_i \cap H$. Pela parte *i)* do Lema (51), temos que H tem uma sequência dada por

$$\{e\} = H_0 \subseteq H_1 \subseteq ... \subseteq H_r = H.$$

Temos ainda que $G_i \subseteq G_{i+1}$, ou seja, $G_i \cap G_{i+1} = G_i$, daí

$$\frac{H_{i+1}}{H_i} \cong \frac{G_{i+1} \cap H}{G_i \cap H} = \frac{G_{i+1} \cap H}{(G_i \cap G_{i+1}) \cap H} = \frac{G_{i+1} \cap H}{G_i \cap (G_{i+1} \cap H)} \cong \frac{G_i(G_i \cap H)}{G_i}. \tag{4}$$

A última parte da equação (4) decorre da parte *i)* do Lema (51). Mas, temos que $\frac{G_i(G_i \cap H)}{G_i}$ é um subgrupo de $\frac{G_{i+1}}{G_i}$ que é abeliano. Logo $\frac{H_{i+1}}{H_i}$ é abeliano para todo $i = 0, 1, ..., n-1$, e assim, H é solúvel.

ii) Definimos G_i como anteriormente. Então, em G/N temos a sequência

$$\frac{N}{N} = \frac{G_0 N}{N} \lhd \frac{G_1 N}{N} \lhd ... \lhd \frac{G_r N}{N} = \frac{G}{N}.$$

Nota-se que $G_i \subseteq G_{i+1}$ e daí $G_i G_{i+1} = G_{i+1}$ (produto de grupos). Temos um quociente típico

$$\frac{G_{i+1}N/N}{G_i N/N},$$

que pela parte *i)* do Lema (51) é isomorfo à

$$\frac{G_{i+1}N}{G_i N} \cong \frac{G_{i+1}(G_i N)}{G_i N} \overset{(*)}{\cong} \frac{G_{i+1}}{G_{i+1} \cap (G_i N)} \overset{(**)}{\cong} \frac{G_{i+1}/G_i}{(G_{i+1} \cap (G_i N))/G_i}.$$

$(*)$ e $(**)$ seguem do item *i)* e *ii)* do Lema (51), respectivamente. E, assim, obtemos um quociente dos grupos abelianos $\frac{G_{i+1}}{G_i}$, assim, abeliano. Logo, G/N é solúvel.

iii) Temos, por hipótese, que existem as duas sequências

$$\begin{gathered} \{e\} = N_0 \lhd N_1 \lhd ... \lhd N_r = N; \\ \frac{N}{N} = \frac{G_0}{N} \lhd \frac{G_1}{N} \lhd ... \lhd \frac{G_s}{N} = \frac{G}{N} \end{gathered}$$

com coeficientes abelianos. Considera-se a sequência de G dada pela combinação delas:

$$\{e\} = N_0 \lhd N_1 \lhd ... \lhd N_r = N = G_0 \lhd G_1 \lhd ... \lhd G_s = G.$$

Os quocientes são $\frac{N_{i+1}}{N_i}$, que são abelianos, ou $\frac{G_{i+1}}{G_i}$ isomorfo a $\frac{G_{i+1}/N}{G_i/N}$ também abeliano. Portanto, G é solúvel.

□

Definição 53. *Um grupo G é simples se seus subgrupos normais são apenas $\{e\}$ e G.*

Teorema 54. *Um grupo solúvel é simples se, e somente se, é cíclico e de ordem prima.*

Demonstração. Suponha G um grupo solúvel, portanto, G possui uma sequência $\{e\} = G_0 \lhd G_1 \lhd ... \lhd G_n = G$, devemos supor $G_{i+1} \neq G_i$. Assim, G_{n-1} é um subgrupo normal próprio de G. Mas G é simples, logo $G_{n-1} = \{e\}$ e $G_n/G_{n-1} = G$, que é abeliano. Mas, todo subgrupo de um grupo abeliano é normal, e todo elemento de G gera um subgrupo cíclico. Assim, G deve ser cíclico com subgrupos próprios não triviais. Logo, G tem ordem prima.

Agora, se G é cíclico, dado $g \in G$ temos que $\langle g \rangle = G$, com $|G| = p$, para p primo. Daí, dado $H < G$, temos que $|H| \leq |G|$ e, pelo Teorema de Lagrange (1) $|H||p$, ou seja, $|H| = 1$ ou $|H| = p$. Ou seja, $H = \{e\}$ ou $H = G$. □

Proposição 55. *Se $n \geq 3$, então os 3-ciclos geram A_n.*

Demonstração. De fato, tome $(1ab) = (1a)(1b)$ e pelo que vimos na Observação (26), nota-se que $(1ab) = (1b)(1a)$. Como o sinal de uma transposição é ímpar, isto é, -1. Daí, segue que o sinal de $(1ab)$ é +1. Logo, $(1ab)$ é par. Como $(1ab) = (1b)(1a)$ e as transposições geram S_n, temos o resultado desejado. □

Teorema 56. *Se $n \geq 5$, então o grupo alternante A_n de grau n é simples.*

Demonstração. Suponha que $N \lhd A_n$ em que $\{e\} \neq N$. A demonstração será feita do seguinte modo: observamos primeiro que se N contém um 3-ciclo, então contém todos os 3-ciclos e como os 3-ciclos geram A_n, temos que $N = A_n$. Segundo, mostraremos que N deve conter um 3-ciclo. Daí, teremos como essencial o fato de $n \geq 5$.

Suponha, então, que N contenha um 3-ciclo. Sem perda de generalidade, suponha que seja (123). Assim, para qualquer $k > 3$, o ciclo $(32k)$ é uma permutação par, de fato, $(32k) = (3k)(32)$ e como toda transposição é ímpar, temos que a composição de duas delas é par. Logo,

$$(32k)^{-1} = (k23)(123)(32k) = (1k2), \text{ de fato,}$$

$$(123)(32k) = (1k3) \text{ e } (k23)(1k3) = (k21) = (1k2),$$

que, por fim, pertence a N. Portanto, N contém $(1k2)^2 = (12k)$, para todo $k \geq 3$. Afirmamos que A_n é gerado por todos os 3-ciclos da forma $(12k)$. Se $n = 3$, temos a afirmação verdadeira. Caso, $n > 3$, temos que para todos $a, b > 2$ a permutação $(1ab) = (1b)(1a)$ é par, mesmo argumento, usado acima para o caso $(32k)$. Portanto, pertence a A_n e, assim, A_n contém

$$(1ab) = (12b)(12a)(12b)^{-1}, \text{ de fato,}$$

como $(12b)^{-1} = (b21)$, temos:

$$(12a)(b21) = (2ab) \text{ e } (12b)(12a) = (1ab).$$

A_n é gerado por todos os ciclos $(12k)$, isto mostra que $N = A_n$.

Mostremos agora que N contém ao menos um 3-ciclo, faremos isso pela análise de casos:

1. Suponha que N contenha um elemento $x = abc...$, em que $a, b, c, ...$ sejam ciclos disjuntos e,

$$a = (a_1...a_m), \text{ com } m \geq 4.$$

Consideremos $t = (a_1 a_2 a_3)$. Então, N contém $t^{-1}xt$. Como, t comuta com $b, c, ...$ (pois são ciclos disjuntos) segue que, $t^{-1}xt = (t^{-1}at)bc... = z$ (digamos), então, N contém, $zx^{-1} = (a_1 a_3 a_m)$, que é um 3-ciclo.

2. Suponhamos, agora, que N contenha um elemento envolvendo ao menos dois 3-ciclos. Sem perda de generalidade, N contém:

$$x = (123)(456)y, \text{ em que } y \text{ fixa } 1, 2, ..., 6.$$

Consideremos $t = (234)$. Então, N contém,

$$(t^{-1}xt)x^{-1} = ((342)(123)(456)y(234))y^{-1}(654)(321) = (12436).$$

Assim, pelo caso anterior, N contém um 3-ciclo.

3. Suponhamos que N contenha um elemento de x da forma $(ijk)p$, em que, p é um produto de 2-ciclos disjuntos, digamos $p = (ab)(cd)$, de (ijk). Então, N contém

$$x^2 = ((ijk)p)^2 = (ijk)p(ijk)p = (ijk)(ijk)pp = (ijk)(ijk) = (kij) = (ijk).$$

(Nota-se que a inversa de uma transposição é ela mesma, daí $(ab)^{-1} = (ab)$ e, assim, $(ab)^2 = e$).

4. Resta apenas o caso em que todo elemento de N é um produto disjunto de 2-ciclos. (Isto ocorre, na verdade, apenas quando A_n é A_4, dado pelo grupo quatro de Klein). Mas, como $n \geq 5$, podemos assumir que N contém,

$$x = (12)(34)p, \text{ em que } p \text{ fixa } 1, 2, 3, 4.$$

Se considarmos, $t = (234)$, teremos que N contém $(t^{-1}xt)x^{-1} = (14)(23)$ e se $u = (145)$, N contém, $u^{-1}(t^{-1}xtx^{-1})u = (45)(23)$. Assim, N contém, $(45)(23)(14)(23) = (145)$, contradizendo o fato de termos assumido que todo elemento de N é um produto de 2-ciclos disjuntos.

Portanto, se $n \geq 5$ então A_n é simples. □

Galois provou que A_5 é o menor grupo simples não-abeliano.

Corolário 57. *O grupo simétrico S_n de grau n é não solúvel para $n \geq 5$.*

Demonstração. Se S_n fosse solúvel e $A_n < S_n$, então A_n seria solúvel. Como A_n é simples pelo Teorema (56) e, portanto, de ordem prima. Mas, $|A_n| = \dfrac{n!}{2}$ e não é primo se $n \geq 5$, o que é um absurdo. Portanto, S_n não é solúvel se $n \geq 5$. □

3.3 Teorema de Cauchy

Definição 58. *Elementos a e b de um grupo G são conjugados em G, se existe $g \in G$ tal que, $a = gbg^{-1}$.*

Temos que a conjugação é, claramente, uma relação de equivalência e isso nos dá uma partição do conjunto G. Logo, se $C_1, ..., C_r$ são as classes de equivalência da conjugação, temos que:

$$|G| = \{e\} + |C_2| + ... + |C_r|, \text{ que é a equação de classes para } G.$$

Definição 59. *Se G é um grupo e $x \in G$, então o centralizador $C_G(x)$ de x em G é o conjunto de todos os $g \in G$ para os quais $gx = xg$.*

Proposição 60. *Seja G um grupo e $x \in G$, então $C_G(x) < G$.*

Demonstração. $e \in C_G(x)$, pois, $ex = xe$, para todo $x \in G$. Assim, $C_G(x) \neq \varnothing$. Tomemos agora, $g_1, g_2 \in C_G(x)$. Daí $g_1x = xg_1$ e $g_2x = xg_2$, ou seja, $g_1xg_1^{-1} = x$ e $g_2xg_2^{-1} = x$, daí $g_2xg_2^{-1} = g_1xg_1^{-1}$ e assim, $xg_2^{-1}g_1 = g_2^{-2}g_1x$. Portanto, $g_2^{-1}g_1 \in C_G(x)$. □

Lema 61. *Se G é um grupo e $x \in G$, então o número de elementos na classes de conjugação de x é o índice de $C_G(x)$ em G.*

Demonstração. A seguinte equação $g^{-1}xg = h^{-1}xh$ é válida se, e somente se, $hg^{-1}x = xhg^{-1}$, ou seja, $hg^{-1} \in C_G(x)$, isto é, h e g estão na mesma classe lateral de $C_G(x)$ em G. O número destas classes laterais é o índice de $C_G(x)$ em G, donde segue o resultado do lema. □

Corolário 62. *O número de elementos em uma classe de conjugação de um grupo finito G divide a ordem do grupo G.*

Definição 63. *O centro $Z(G)$ de um grupo G é o conjunto de todos os elementos de G, tais que $xg = gx$, $\forall g \in G$.*

Exemplo 64. *O centro de G é um subgrupo normal de G. Muitos grupos têm um centro trivial, por exemplo, $Z(S_3) = \{e\}$. Nota-se, porém, que se G é abeliano, temos daí que $Z(G) = G$.*

Lema 65. *Se A é um grupo finito abeliano cuja ordem é divisível por um primo p, então A tem um elemento de ordem p.*

Demonstração. Usaremos indução em $|A|$. Se $|A|$ é primo, temos que ó resultado é trivial, ou seja, existe $g \in A$ tal que $|\langle g \rangle|$ divide $|A|$ e, assim, $\langle g \rangle = A$. Caso contrário, considera-se $M < A$ com $M \subsetneq A$ cuja ordem m é máximal. Se $p|m$ podemos usar a indução, suponha então que $p \nmid m$. Seja $b \in A \setminus M$ e seja B um subgrupo cíclico gerado por$b$, ou seja, $B = \langle b \rangle$. Então, $MB < A$ sendo que MB é maior que M e pela maximalidade de M temos que $MB = A$, usando a parte *i)* do Teorema (51), temos

$$|MB| = \frac{|M||B|}{|M \cap B|}, \text{ e daí,}$$

se $|B| = r$ temos que $p|r$,mas B é cíclico. Ou seja, o elemento $b^{\frac{r}{p}}$ tem ordem p, o que demonstra o lema. □

Definição 66. *Seja p um primo. Um grupo finito G é um p-grupo se sua ordem é uma potência de p.*

Teorema 67. *Se $G \neq \{e\}$ é um p-grupo, então G possui um centro não trivial.*

Demonstração. Suponha $|G| = p^n$ e como sabemos G pode ser particionado pela conjugação, como $|G| < \infty$, suponha

$$|G| = \{e\} + |C_1| + |C_2| + ... + |C_r|, \tag{5}$$

daí temos:

$$p^n = \{e\} + |C_1| + |C_2| + ... + |C_r|.$$

Como cada $|C_i|||G|$ temos que $|C_i| = p^{n_i}$, para algum $n_i \geq 0$. Assim, p divide o lado direito da equação (5). Então, pelo menos $p-1$ valores de $|C_i|$ são iguais a 1. Mas, se x pertence a uma classe de conjugação com, pelo menos, um elemento, então $g^{-1}xg = x$, $\forall g \in G$, ou seja, $xg = gx$. Assim, $x \in Z(G)$. Logo, $Z(G) \neq 0$. □

Lema 68. *Se G é um p-grupo de ordem p^n, então G possui uma série de subgrupos normais*

$$\{e\} = G_0 \subseteq G_1 \subseteq G_2 \subseteq ... \subseteq G_n = G, \text{ tal que, } |G_i| = p^i, \text{ para todo } i = 0, 1, ..., n.$$

Demonstração. Faremos por indução sobre n. Se $n = 0$, é claro, o resultado segue. Caso contrário, seja $Z = Z(G) \neq \{e\}$. Pelo Teorema (67), como Z é um grupo abeliano de ordem p^m possui um elemento de ordem p. O subgrupo cíclico K gerado por um elemento possui ordem p e $K \lhd G$, sendo $K \subseteq Z$. Agora, G/K é um p-grupo de ordem p^{n-1} e, por indução, temos uma série de subgrupos normais

$$K/K = G_1/K \subseteq G_2/K \subseteq ... \subseteq G_n/K, \text{ onde } |G_i/K| = p^{i-1}.$$

Mas, então $|G_i| = p^i$ e $G_i \lhd G$, se tivermos que $G_0 = \{e\}$, então o resultado segue. □

Corolário 69. *Todo p-grupo finito é solúvel.*

Demonstração. O quociente G_{i+1}/G_i das séries usados no Lema (68), são de ordem p. Logo, cíclicos e, portanto, abelianos. E o resultado segue. □

Definição 70. *Se G é um grupo finito de ordem $p^\alpha r$, em que p é primo e $mdc(p,r) = 1$, então um Sylow p-subgrupo, ou ainda, p-subgrupo de Sylow de G é um subgrupo de G de ordem p^α.*

Teorema 71 (Teorema de Sylow)**.** *Seja G um grupo finito de ordem $p^\alpha r$ em que p é primo e não divide r. Então:*

i) G possui pelo menos um subgrupo de ordem p^α;

ii) Todos os p-subgrupos de Sylow de mesma ordem são conjugados entre si;

iii) Qualquer p-subgrupo de G está contido em um p-subgrupo de ordem p^α;

iv) O número de subgrupos de G de ordem p_α é congruente a 1 módulo p.

Demonstração. Consultar Garcia e Lequain (2003). □

Teorema 72 (Teorema de Cauchy)**.** *Se um primo p divide a ordem de um grupo G, então G possui um elemento de ordem p.*

Demonstração. O Teorema de Sylow (Teorema (71)) nos garante que $\exists\, H < G$ com $|H| = p^\alpha$ se $|G| = p^\alpha r$ com $mdc(p,r) = 1$. Pelo Lema (68) H tem um subgrupo L normal de ordem p. Daí, qualquer elemento desse subgrupo L possui ordem p, claro, tal elemento não é a identidade. O que termina a Demonstração. □

4 Solução por radicais

O objetivo desta seção é usar a correspondência de Galois para encontrar uma condição que deve ser satisfeita por qualquer equação polinomial para que esta seja solúvel por radicais, digamos: O Grupo de Galois associado deve ser um grupo solúvel. Nós, então, construiremos uma equação polinomial quíntica cujo Grupo de Galois não seja solúvel, o que mostra que a equação quíntica não é solúvel por radicais.

Uma condição suficiente para que uma equação seja solúvel por radicais é que o Grupo de Galois associado a equação seja também solúvel, tal resultado será melhor discutido na próxima seção.

4.1 Extensões por Radicais

Precisamos ter cuidado na formalização da ideia de solubilidade por radicais. Começaremos do ponto de vista de extensões de corpos.

Informalmente, uma extensão por radical é obtida por uma sequência de adjunções de raízes n-ésimas, para vários n. Por exemplo, a expressão a seguir é radical:

$$\sqrt[3]{11}\sqrt[5]{\frac{7+\sqrt{3}}{2}}+\sqrt[4]{1+\sqrt[3]{4}}. \tag{6}$$

Para encontrarmos uma extensão de $\mathbb{Q}$ que contenha este elemento, deveremos adicionar, gradualmente, os elementos

$$\alpha=\sqrt[3]{11},\ \beta=\sqrt{3},\ \gamma=\sqrt[5]{\frac{(7+\beta)}{2}},\ \delta=\sqrt[3]{4} \text{ e } \xi=\sqrt[4]{1+\delta}.$$

O que nos sugere a seguinte definição:

Definição 73. *Uma extensão $L:K$ é radical se $L=K(\alpha_1,...,\alpha_m)$, em que para cada $j=1,...,m$ existe um inteiro n_j, tal que*

$$\alpha_j^{n_j}\in K(\alpha_1,...,\alpha_m)\ (j\geq 2).$$

Os elementos α_j formam uma sequência radical para $L:K$. O grau radical do radical α_j é n_j.

Por exemplo, a expressão em (6) está contida em uma extensão radical da forma $\mathbb{Q}(\alpha,\beta,\gamma,\delta,\xi)$ de $\mathbb{Q}$, em que $\alpha^3=11$, $\beta^2=3$, $\gamma^5=\frac{(7+\beta)}{2}$, $\delta^3=4$ e $\xi^4=1+\delta$.

Claramente, qualquer extensão radical está contida em alguma extensão radical. É razoável pensarmos que: Um polinômio deve ser considerado solúvel por radicais se todos os seus zeros são expressões radicais sobre o corpo base.

Definição 74. *Seja $f(x)$ um polinômio sobre um subcorpo K de $\mathbb{C}$, e seja $Gal(f(x),K)$ o corpo de decomposição de $f(x)$ sobre K. Dizemos que $f(x)$ é solúvel por radicais se existe um corpo M, que contém $Gal(f(x),K)$, tal que $M:K$ é uma extensão radical.*

Note que não exigimos que a extensão ao corpo de decomposição $Gal(f(x),K)$ seja expresso por radicais, mas é esperado que tudo expresso pelo mesmos radicais esteja dentro do corpo de decomposição. Se $M:K$ é radical L é um corpo intermediário, então $L:K$ não precisa ser radical.

Nota-se também que requeremos que todos os zeros de $f(x)$ sejam expressos por radicais. É possível que alguns zeros sejam expressos por radicais, enquanto outros não. Ora, simplesmente tomemos o produto de dois polinômios, um solúvel por radicais e outro não. Todavia, se um polinômio irredutível $f(x)$ tem um zero expresso por radicais, então todos os zeros devem ser expressos, por um argumento baseado no Corolário (3).

Lema 75. *Se $L:K$ é uma extensão radical em $\mathbb{C}$ e M é fecho normal de $L:K$, então $M:K$ é radical.*

Demonstração. Seja $L=K(\alpha_1,...,\alpha_r)$ com $\alpha_i^{n_i}\in K(\alpha_1,...,\alpha_{i-1})$. Lembrando que por hipótese $L:K$ é uma extensão radical, seja $\psi_i(x)$ o polinômio minimal de α_i sobre K. Então, $L\subseteq M$ é o corpo de decomposição de $\prod_{i=1}^{r}\psi_i(x)$. Para todo zero β_{ij} de $\psi_i(x)$ em M, pelo Corolário (3), existe um isomorfismo $\sigma:K(\alpha_i)\longrightarrow K(\beta_{ij})$. Assim, temos pela Proposição (19) que σ estende a um K-automorfismo $\tau:M\longrightarrow M$. Como α_i é radical sobre K, então β_{ij} também é. Portanto, $M:K$ é radical. □

Lema 76. *Seja K um subcorpo de $\mathbb{C}$ e seja L o corpo de decomposição para x^p-1 sobre K, com p primo. Então, o Grupo de Galois de $L:K$ é abeliano.*

Demonstração. Ora, a derivada de x^p-1 é, claramente, px^{p-1}, que é primo com x^p-1. Logo, pelo Lema (13), o polinômio não tem zeros múltiplos em L. Claramente, seus zeros formam um subgrupo multiplicativo, este grupo possui ordem prima p, e como os zeros são distintos, ele é cíclico. Seja ξ um gerador deste grupo. Então, $L=K(\xi)$ e qualquer K-automorfismo de L é determinado por seu efeito em ξ. Além disso, K-automorfismos permutam os zeros de x^p-1. Portanto, qualquer K-automorfismo de L é da forma

$$\alpha_j:\xi\longmapsto\xi^j$$

e é unicamente determinado por esta condição. Mas, então $\alpha_i\alpha_j$ e $\alpha_j\alpha_i$ levam, ambos, ξ em ξ^{ij}. Portanto, o Grupo de Galois é abeliano. □

Lema 77. *Seja K um subcorpo de $\mathbb{C}$ em que x^n-1 se decompõe linearmente. Sejam $a\in K$ e L um corpo de decomposição para x^n-a sobre K. Então, o Grupo de Galois de $L:K$ é abeliano.*

Demonstração. Seja α um zero qualquer de x^n-a. Como x^p-1 se decompõe linearmente em K, o zero de x^n-a é $\xi\alpha$, onde ξ é um zero de x^n-1 em K. Como $L=K(\alpha)$, qualquer K-automorfismo de L é determinado por seu efeito em α. Dados dois K-automorfismos

$$\Phi:\alpha\longmapsto\xi\alpha \text{ e } \Psi:\alpha\longmapsto\eta\alpha, \text{ com } \xi \text{ e } \eta\in K,$$

então,

$$\Phi\Psi(\alpha)=\xi\eta\alpha=\eta\xi\alpha=\Psi\Phi(\alpha).$$

E, como anteriormente, o Grupo de Galois é abeliano. □

Lema 78. *Se existe uma torre finita de subcorpos, podemos refinar (se for necessário aumentar o comprimento) de modo a fazermos todos os n_j primos.*

Demonstração. Para j fixado, escreve-se $n_j=p_1...p_K$ com p_l primos. Seja $\beta_l=\alpha_j^{p_1\cdots p_l}$. Então $\beta_{l+1}^{p_l+1}\in K_j(\beta_l)$ e o resto segue facilmente. □

Lema 79. *Se K é um subcorpo de $\mathbb{C}$ e $L:K$ é normal e radical, então $\Gamma(L:K)$ é solúvel.*

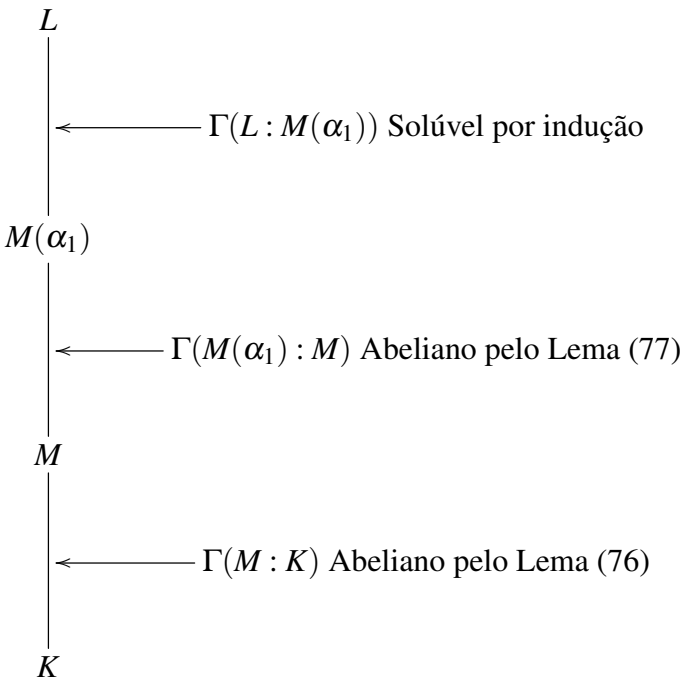
Demonstração. Suponha que $L = K(\alpha_1,...,\alpha_n)$ com $\alpha_j^{n_j} \in K(\alpha_1,...,\alpha_{j-1})$. Pelo Lema (78), devemos assumir que n_j é primo para todo j. Em particular, existe um primo p tal que $\alpha_1^p \in K$.

Provaremos o resultado por indução em n, usando a hipótese adicional de que todos os n_j são primos. O caso $n = 0$ é trivial, donde começa a indução.

Se $\alpha_1 \in K$, então $L = K(\alpha_2,...,\alpha_n)$ e $\Gamma(L:K)$ é solúvel por indução.

Podemos assumir que $\alpha_1 \notin K$. Seja $\psi(x)$ o polinômio minimal de α_1 sobre K. Como $L:K$ é normal, $\psi(x)$ se decompõe linearmente em L, pois $K \subseteq \mathbb{C}$, e $\psi(x)$ não tem zeros repetidos em L. Como $\alpha_1 \notin K$, o grau de $\psi(x)$ é no mínimo 2. Seja β um zero em $\psi(x)$ diferente de α_1, e consideremos $\xi = \dfrac{\alpha_1}{\beta}$. Então, $\xi^p = 1$ e $\xi \neq 1$. Portanto, ξ tem ordem p no grupo multiplicativo de L, como os elementos $1, \xi, \xi^2, ..., \xi^{p-1}$ são raízes p-ésimas distintas da unidade em L. Portanto, $x^p - 1$ se decompõe linearmente em L.

Seja $M \subseteq L$ o corpo de decomposição de $x^p - 1$ sobre K, isto é, $M = K(\xi)$. Consideremos a cadeia de subcorpos $K \subseteq M \subseteq M(\alpha_1) \subseteq L$. Podemos ilustrar o resto da demonstração pelo seguinte diagrama:



Observa-se que $L:K$ é finita e normal e, portanto, também o é $L:M$. Assim, o Teorema (22) se aplica à $L:K$ e à $L:M$.

Como $x^p - 1$ se decompõe linearmente em M e $\alpha_1^p \in M$, a demonstração do Lema (77) implica que $M(\alpha_1)$ é um corpo de decomposição para $x^p - \alpha_1^p$ sobre M. Portanto, $M(\alpha_1):M$ é normal, e pelo Lema (77) $\Gamma(M(\alpha_1):M)$ é abeliano. Apliquemos o Teorema de Galois (22) à $L:M$ para deduzirmos que

$$\Gamma(M(\alpha_1):M) \cong \frac{\Gamma(L:M)}{\Gamma(L:M(\alpha_1}.$$

Agora, $L = M(\alpha_1)(\alpha_2,...,\alpha_n)$, e então $L:M(\alpha_1)$ é um extensão normal radical. Por indução, $\Gamma(L:M(\alpha_1))$ é solúvel. Portanto, pelo item *iii)* do Teorema (52), $\Gamma(L:M)$ é solúvel.

Como M é o corpo de decomposição para $x^p - 1$ sobre K, a extensão $M : K$ é normal. Pelo Lema (76), temos que $\Gamma(M : K)$ é abeliano. Agora, o Teorema de Galois (22) aplicado à $L : K$ garante que

$$\Gamma(M : K) \cong \frac{\Gamma(L : K)}{\Gamma(L : M)}.$$

Por fim, o Teorema de Galois (22), mostra-nos que $\Gamma(L : K)$ é solúvel, completando a indução. □

Teorema 80. *Se K é um subcorpo de $\mathbb{C}$ e $K \subseteq L \subseteq M$, com $M : K$ uma extensão radical, então o Grupo de Galois de $L : K$ é solúvel.*

Demonstração. Seja K_0 um corpo fixo de $\Gamma(L : K)$ e $N : M$ o fecho normal de $M : K_0$. Então, $K \subseteq K_0 \subseteq L \subseteq M \subseteq N$. Como $M : K_0$ é radical o Lema (75) implica que $N : K_0$ é uma extensão normal radical, de onde, pelo Lema (79), $\Gamma(N : K_0)$ é solúvel.

Apartir do Teorema (20), conseguimos que a extensão $L : K_0$ é normal. E assim, pelo Teorema de Galois (22)

$$\Gamma(L : K_0) \cong \frac{\Gamma(N : K_0}{\Gamma(N : L)}.$$

Obtemos, daí que $\Gamma(L : K_0)$ é solúvel. Mas, $\Gamma(L : K) = \Gamma(L : K_0)$. E, portanto, $\Gamma(L : K)$ é solúvel. □

Definição 81. *Seja $f(x)$ um polinômio sobre K, com corpo de decomposição $Gal(f(x), K)$ sobre K. O Grupo de Galois de $f(x)$ sobre K é o grupo $Gal(Gal(f(x), K) : K)$.*

Observação 82. *Seja G o Grupo de Galois de um polinômio $f(x)$ sobre K, e seja o grau de $f(x)$ igual a n. Se $\alpha \in Gal(f(x), K)$ é um zero de $f(x)$, então $f(\alpha) = 0$. Logo, para todo $g \in G$ temos $f(g(\alpha)) = g(f(\alpha)) = 0$.*

Portanto, cada elemento $g \in G$ induz uma permutação g' do conjunto de raízes de $f(x)$ em $Gal(f(x), K)$. Segue $g \longmapsto g'$ é um monomorfismo de grupo de G no grupo de S_n de todas as permutações de zeros de $f(x)$.

Podemos, assim, reescrever o Teorema (80)*, como segue:*

Teorema 83. *Seja $f(x)$ um polinômio sobre um subcorpo K de $\mathbb{C}$. Se $f(x)$ é solúvel por radicais, então o Grupo de Galois de $f(x)$ sobre K é solúvel.*

Lema 84. *Sejam p um primo e $f(x)$ um polinômio irredutível de grau p sobre $\mathbb{Q}$. Suponhamos que $f(x)$ tenha precisamente dois zeros não reais em $\mathbb{C}$. Então, o grupo de Galois de $f(x)$ sobre $\mathbb{Q}$ é isomorfo ao grupo simétrico S_p.*

Demonstração. O Teorema Fundamental da Álgebra nos garante que $\Gamma(f(x), \mathbb{Q}) \subseteq \mathbb{C}$. Seja G o Grupo de Galois de $f(x)$ sobre $\mathbb{Q}$, considerado como grupo de permutação nos zeros de $f(x)$. Estes, são distintos pela Proposição (14). Logo, G é isomorfo a um subgrupo de S_p. Quando construímos o corpo de decomposição de $f(x)$, primeiro adicionamos um elemento de grau p, então $[Gal(f(x) : \mathbb{C}) : \mathbb{Q}]$ é divisível por p. Pelo Teorema de Galois, p divide a ordem de G. Pelo Teorema de Cauchy (72), G tem um elemento de ordem p. Mas, os únicos elementos de S_p de ordem p são os p-ciclos. Portanto, G contém os p-ciclos.

Como conjugação dos complexos é um $\mathbb{Q}$-automorfismo de $\mathbb{C}$, temos a indução de um $\mathbb{Q}$-automorfismo de $Gal(f(x),\mathbb{C})$. Isto, deixa $p-2$ zeros reais de $f(x)$ fixados enquanto transpõe os zeros não reais. Assim, G contém um 2-ciclo.

Devemos assumir que G contém o 2-ciclo (12) e o p-ciclo $(1,2,...,p)$ e estes geram todo o conjunto S_p. O que demonstra o resultado. □

Teorema 85. *O polinômio $x^5-6x+3 \in \mathbb{Q}[x]$ é não solúvel por radicais.*

Demonstração. Ora, $f(x)=x^5-6x+3$ é irredutível por Eisenstein para $p=3$. 5 é primo e pelo Lema (84) o Grupo de Galois de $f(x)$ sobre $\mathbb{Q}$ é S_5 e já sabemos, pelo Corolário (57), que S_n para $n \geq 5$ é não solúvel. Assim, pelo Teorema (83), $f(x)=0$ é não solúvel por radicais.

Mostremos que $f(x)$ tem exatamente três zeros reais, cada um de multiplicidade 1. Ora,

$$f(-2)=-17,\ f(-1)=8,\ f(0)=3,\ f(1)=-2 \text{ e } f(2)=23.$$

Assim, pelo Teorema de Rolle (Consultar um livro de Cálculo) os zeros de $f(x)$ são separados pelos zeros de $f'(x)$. Além disso, $f'(x)=5x^4-6$, que tem como zeros $\pm\sqrt[4]{\frac{6}{5}}$.

Temos que $f(x)$ e $f'(x)$ são primos entre si, então $f(x)$ não tem zeros repetidos (segue também por irredutibilidade) e, então, $f(x)$ tem no máximo três zeros reais. Mas, $f(x)$ certamente tem no mínimo 3 zeros reais, já que uma função contínua definida nos reais não muda de sinal, exceto se passar pelo zero (eixo x). Portanto, $f(x)$ tem precisamente 3 zeros reais, e o resultado segue. □

5 O polinômio geral

O chamado polinômio "geral"é na verdade um polinômio muito especial. É um polinômio cujos coeficientes não satisfaz algumas relações algébricas. Esta propriedade faz com que seja mais fácil de trabalhar do que, digamos, polinômios sobre $\mathbb{Q}$; e, em particular, é mais fácil de calcular o seu *Grupo de Galois*. Como resultado, podemos mostrar que nem todo polinômio quíntico é solúvel por radicais sem assumir a teoria do grupo. Efetivamente isso implica que não existe uma fórmula geral através do qual todas as equações de quinto grau podem ser resolvidas em termos de radicais. Uma vez que este não, a priori, exclui a possibilidade de que podem existir soluções por radicais de todos os polinômios de quinto grau que não podem ser reunidos sob uma fórmula geral.

Verifica-se que o *Grupo de Galois* do polinômio geral de grau n é todo o grupo simétrico S_n. Isto mostra imediatamente a insolubilidade da quíntica geral. O conhecimento da estrutura de S_2, S_3, S_4 pode ser utilizado para encontrar métodos de resolução da equação quadrática, cúbica, ou quártica.

5.1 Graus transcendentes

Até o presente momento não trabalhamos com as extensões transcendentes, ao invés disso assumimos a finitude das extensões como foco central da teoria. Considereramos agora esta classe maior de extensões.

Definição 86. *Um extensão $L:K$ é finitamente gerada se $L=K(\alpha_1,...,\alpha_n)$, em que n é finito.*

Notemos que α_i podem ser algébricos ou transcendentes sobre K.

Definição 87. *Se $t_1,...,t_n$ são elementos transcendentes sobre um corpo K, todos em alguma extensão L de K, então eles são independentes se há um polinômio não trivial p sobre K (em n indeterminadas) tal que $p(t_1,...,t_n) = 0$ em L.*

Lema 88. *Se $L : K$ é finitamente gerada, então existe um corpo intermediário M tal que*

i) $M = K(\alpha_1,...,\alpha_r)$, em que os α_i são elementos transcendentes e independentes sobre K;

ii) $L : M$ é uma extensão finita.

Demonstração. Sabemos que $L = K(\beta_1,...,\beta_n)$, pois $L : K$ é corpo finitamente gerado. Se todos os β_j são algébricos sobre K, então $L : K$ é finita pela generalização do Lema (6) e, devemos considerar $M = K$. Ora, caso contrário, algum dos β_i é transcendente sobre K. Chamemos este de α_1. Se $L : K(\alpha_1)$ não é finita, existe algum β_k trancendente sobre $K(\alpha_1)$, chamemos o mesmo de α_2. Continuamos esse processo, de tal modo que $L : M$ é finita. Logo, por construção, os α_j são elementos transcendentes sobre K. □

Lema 89. *Com a mesma notação do Lema* (88) *item i). Se existir outro corpo intermediário de $N = K(\beta_1,...,\beta_s)$, tal que $\beta_1,...,\beta_s$ são elementos transcendentes independentes sobre K e $L : N$ seja finita, devemos ter $s = r$.*

Demonstração. Ora, como $[L : K]$ é finito, temos pelo Lema (88) que β_1 é algébrico sobre M. Portanto, existe uma equação polinomial $p(\beta, \alpha_1,..., \alpha_r) = 0$. Assim, algum α_j, sem perda de generalidade, digamos α_1 aparece na equação. Então, α_1 é algébrico sobre $K(\beta_1, \alpha_2,..., \alpha_r)$ e $L : K(\beta_1, \alpha_2,..., \alpha_r)$ é finita. Indutivamente, conseguimos substituir α_j por β_j, e deste modo, $L : K(\beta_1,...,\beta_r)$ é finita. Se $s > r$, temos que β_{r+1} deve ser algébrico sobre $K(\beta_1,...,\beta_r)$, o que é uma contradição. Portanto, $r \leq s$. Analogamente, conseguimos que $s \leq r$. E assim, temos que $s = r$. □

Exemplo 90. *Consideremos $K(t, \alpha, u) : K$, em que, t é transcendente sobre K, $\alpha^2 = t$ e u é transcendente sobre $K(t, \alpha)$. Assim, $M = K(t, u)$, em que t e u são elementos transcendentes independentes sobre K e portanto, $K(t, \alpha, u) = M(\alpha) : M$ é finita. Deste modo, vemos que o grau de transcendência é* 2.

Proposição 91. *Uma extensão finitamente gerada $L : K$ tem grau de transcendência r se, e somente se, existe um corpo intermediário M tal que L é uma extensão finita de M e $M : K$ é isomorfa a $K(t_1,...,t_r) : K$.*

Demonstração. Suponhamos que $L : K$ seja finitamente gerada. Assim, pelo Lema (88), temos que existe M, um corpo intermediário, ou seja, $K \subseteq M \subseteq L$, e elementos $t_1,..,t_r$ transcendentes e independentes, tais que $M = K(t_1,..,t_r)$ e $L : M$ é finita. Neste caso, r é o grau de transcendência de $L : K$.

Suponhamos, agora, que $L : K$ é finitamente gerada, M é corpo intermediário de L e K, $L : M$ seja uma extensão finita e $M : K$ é isomorfa a $K(t_1,...,t_r) : K$. Assim, consideremos φ o isomorfismo de M em $K(t_1,...,t_r)$. Logo, $K(\beta_1,...,\beta_r) \subseteq M$. Seja $\beta \in M \setminus K(\beta_1,...,\beta_r)$, logo, existe $\alpha = \varphi(\beta) \in K(t_1,...,t_r)$. Se α é algébrico, então $\alpha \in K$ e $\beta \in K$, o que é absurdo.

Portanto, α é transcendente, ou seja, existe um polinômio não constante, tal que $\alpha = p(t_1,...,t_r)$. Assim, $\beta = (\varphi^{-1}p)(\beta_1,...,\beta_r) \in K(\beta_1,...,\beta_r)$. Portanto, $M = K(\beta_1,...,\beta_r)$ e pelo Lema (89), r é o grau de transcendência de $L : K$. □

5.2 Polinômios simétricos

Seja K um corpo e suponha que o polinômio de $K[x]$, $f(x) = x^n - s_1x^{n-1} + s_2x^{n-1} - ... + (-1)^n s_n$, se fatore na extensão $L : K$. Expandindo o lado direito acima e comparando com os coeficientes de $f(x)$, obtemos as *relações de Girard:*

$$\begin{aligned} s_1 &= r_1 + ... + r_n \\ s_2 &= r_1r_2 + ... + r_{n-1}r_n \\ s_3 &= r_1r_2r_3 + ... + r_{n-2}r_{n-1}r_n \\ &\vdots \\ s_n &= r_1r_2...r_n \end{aligned}$$

As funções $s_j = s_j(r_1, ..., r_n)$ são invariantes por qualquer permutação das raízes:

$$s_j = s_j(r_1, ..., r_n) = s_j(r_{\sigma(1)}, ..., r_{\sigma(n)}) \text{ com } \sigma \in S_n.$$

Por exemplo: $t = r_1^2 + ... + r_n^2$, daí

$$t = (r_1 + ... + r_n)^2 - 2(r_1r_2 + ... + r_{n-1}r_n) = s_1^2 - 2s_2.$$

Definição 92. *Seja $f \in K[x]$, tal que K é um corpo com raízes $r_1, ..., r_n$, e os coeficientes s_j são polinômios nas variáveis $r_1, ..., r_n$. Os polinômios s_j são chamados de polinômios simétricos elementares.*

Definição 93. *Um polinômio $g \in F[r_1, .., r_n]$ é simétrico em $r_1, .., r_n$ se for fixo por ação, ou seja, $\sigma g = g$, onde, $\sigma g(r_1, .., r_n) = g(r_{\sigma(1)}, .., r_{\sigma(n)})$, para todo $\sigma \in S_n$.*

Teorema 94. *Todo polinômio simétrico em $r_1, ..., r_n$ pode ser expresso como um polinômio nos polinômios simétricos elementares $s_1, ..., s_n$. Além disso, um polinômio simétrico em $r_1, ..., r_n$, com coeficientes inteiros pode ser expresso como um polinômio em $s_1, ..., s_n$, com coeficientes inteiros.*

Demonstração. Vamos definir o grau do monômio $r_1^{i_1}r_2^{i_2}...r_n^{i_n}$ como sendo a n-upla $(i_1, ..., i_n)$. Introduzindo a ordem lexicográfica $(i_1, ..., i_n) > (j_1, ..., j_n)$ se o primeiro elemento não nulo (caso exista na sequência $i_1 - j_1, i_2 - j_2, ..., i_n - j_n$ for positiva) definimos o grau de um polinômio não nulo f como o máximo dos graus dos seus monômios. Será denotado por ∂f.

Seja f um polinômio simétrico e $Ar_1^{i_1}r_2^{i_2}...r_n^{i_n}$ o seu monômio de maior grau. Como f é simétrico, todos os monômios obtidos desse monômio de maior grau, pela permutação das variáveis, são monômios de f, de modo que, necessariamente, $i_1 > i_2 > ... > i_n$.Tomando

$$f_1 = As_1^{i_1-i_2}s_2^{i_2-i_3}...s_{n-1}^{i_{n-1}-i_n}s_n^{i_n}.$$

Obtemos que f_1 é simétrico e

$$\partial f_1 = (i_1 - i_2)\partial s_1 + ... + i_n\partial s_n = (i_1, i_2, ..., i_n),$$

ou seja: O polinômio $f - f_1$ é simétrico, com $\partial(f - f_1) < \partial f$. Repetimos o processo com $f - f_1$ no lugar de f e, em um número finito de passos chegaos ao polinômio nulo. □

Exemplo 95. *Tomar o polinômio $f = r_1^2r_2^2 + r_1^2r_3^2 + r_2^2r_3^2$ cujo grau é $\partial f = (2, 2, 0)$. Então, $f_1 = s_1^0s_2^2s_3^0$, ou seja,$f_1 = (r_1r_2 + r_1r_3 + r_2r_3)^2$ e podemos calcular*

$$f - f_1 = 2(r_1^2r_2r_3 + r_1r_2^2r_3 + r_1r_2r_3^2).$$

Vemos que $\partial(f - f_1) = (2, 1, 1)$. Tomamos $f_2 = 2s_1s_2^0s_3 = 2s_1s_3$ e, claramente, $f - f_1 = f_2$. Logo, $f = f_1 + f_2$, ou seja, $f = s_2^2 + 2s_1s_3$.

5.3 O polinômio geral

Seja K um corpo qualquer e sejam $t_1,...,t_n$ elementos transcendentes sobre K. O grupo simétrico S_n pode atuar como um grupo de K-automorfismos de $K(t_1,...,t_n)$, definindo $\sigma(t_i) = t_{\sigma(i)}$, para $\sigma \in S_n$. Podemos extender assim qualquer expressão racional Φ pela definição:

$$\sigma(\Phi(t_1,...,t_n)) = \Phi(t_{\sigma(1)},...,t_{\sigma(n)}),$$

deste modo temos que σ extendido é um K-automorfismo.

Exemplo 96. *Tomemos S_n e $\sigma = (1,2,4)$ onde $\sigma \in S_4$. Temos daí $\sigma(t_1) = t_2$, $\sigma(t_2) = t_4$, $\sigma(t_3) = t_3$ e $\sigma(t_4) = t_1$. E se $\Phi(t_1,t_2,t_3,t_4) = \dfrac{t_1^5 t_4}{t_2^4 - 7t_3}$, então*

$$\sigma(\Phi(t_1,t_2,t_3,t_4)) = \sigma\left(\frac{t_1^5 t_4}{t_2^4 - 7t_3}\right) = \frac{t_2^5 t_1}{t_4^4 - 7t_3}.$$

Claramente elementos distintos de S_n originam K-automorfismos distintos.

Teorema 97. *Sejam F o corpo fixo de S_n, K um corpo qualquer e $t_1,...,t_n$ os elementos transcendentes de K. Então, $F = K(s_1,...,s_n)$, para $s_r = s_r(t_1,...,t_n)$, são os polinômios elementares simétricos.*

Demonstração. Afirmação:

$$[K(t_1,...,t_n) : K(s_1,...,s_n)] \leq n!.$$

Por indução em n, consideremos a exntesão dupla

$$K(s_1,...,s_n) \subseteq K(s_1,...,s_n,t_n) \subseteq K(t_1,...,t_n).$$

Agora, $f(t_n) = 0$, em que,

$$f(t) = t^n - s_1 t^{n-1} + ... + (-1)^n s_n, \text{ e tal que,}$$

$$[K(s_1,...,s_n,t_n) : K(s_1,...,s_n)] \leq n.$$

Se considerarmos $s'_1,...,s'_{n-1}$ o polinômio elementar simétrico em $t_1,...,t_{n-1}$ e definirmos $s'_0 = 1$, então $s_j = t_n s'_{j+1} + s'_j$, e, portanto, $K(s_1,...,s_n,t_n) = K(t_n,s'_1,...,s'_{n-1})$.

Por indução

$$[K(t_1,...,t_n : K(s_1,...,s_n,t_n] = [K(t_n)(t_1,...,t_{n-1}) : K(t_n)(s'_1,...,s'_{n-1}] \leq (n-1)!$$

e, assim, pela Lei da Torre (generalizado), o passo de indução segue.

Agora, $K(s_1,..,s_n)$ é claramente o corpo fixo F de S_n. Pelo Teorema (17), obtemos $[K(t_1,...,t_n : F] = |S_n| = n!$ e, assim obtemos, $F = K(s_1,...,s_n)$. □

Corolário 98. *Todo polinômio simétrico em $t_1,...,t_n$ sobre K pode ser escrito como uma expressão racional em $s_1,...,s_n$.*

Demonstração. Polinômios simétricos estão no corpo fixo de F. □

Lema 99. *Com a notação acima, $s_1,...,s_n$ são elementos transcendentes independentes sobre K.*

Demonstração. Como $K(t_1,...,t_n)$ é uma extensão finita de $K(s_1,...,s_n)$ temos que ambos possuem o mesmo grau de transcendência, digamos n. Portanto, os s_j são independentes, pois, caso contrário, $[K(s_1,...,s_n:K] < n$, o que é absurdo. □

Definição 100. *Seja K um corpo e sejam $s_1,...,s_n$ elementos transcendentes sobre K. O polinômio geral de grau n sobre K é o polinômio*

$$t^n - s_1 t^{n-1} + s_2 t^{n-2} - ... + (-1)^n s_n \text{ sobre o corpo } K(s_1,...,s_n).$$

Enunciaremos a seguir dois Teoremas, mas que não provaremos:

Teorema 101. *Sejam K um corpo qualquer, g um polinômio geral de grau n sobre K (na verdade sobre $K(s_1,..,s_n)$) e L o corpo de decomposição de g sobre $K(s_1,...,s_n)$. Então, os zeros $t_1,...,t_n$ de g em L são elementos independentes transcendentes sobre K, e o Grupo de Galois de $L : K(s_1,...,s_n)$ é isomorfo ao grupo S_n.*

Teorema 102. *Se K é um corpo de característica zero e $n \geq 5$, então a polinomial geral de grau n sobre K (na verdade sobre $K(s_1,...,s_n)$) é não solúvel por radicais.*

5.4 Extensões cíclicas

Definição 103. *Consideremos $L : K$ uma extensão normal e finita com Grupo de Galois G. A norma de um elemento $a \in L$ é $N(a) = \tau_1(a)\tau_2(a)...\tau_n(a)$, em que $\tau_1, \tau_2, ..., \tau_n$ são elementos de G.*

Temos que $N(a)$ pertence ao corpo fixo de G pelo Lema (16), e, se a extensão é também separável, temos que $N(a) \in K$.

Teorema 104 (Teorema 90 de Hilbert)**.** *Seja $L : K$ uma extensão normal finita com Grupo de Galois cíclico G, gerado por um elemento τ. Então, $a \in L$ tem norma 1 se, e somente se, $a = \dfrac{b}{\tau(b)}$, para algum $b \in L$, em que $b \neq 0$.*

Demonstração. Consideremos $|G| = n$. Se $a = \dfrac{b}{\tau(b)}$ e $b \neq 0$, então

$N(a) = a\tau(a)\tau^2(a)...\tau^{n-1}(a) = \dfrac{b}{\tau(b)}\dfrac{\tau(b)}{\tau^2(b)}\dfrac{\tau^2(b)}{\tau^3(b)}...\dfrac{\tau^{n-1}(b)}{\tau^n(b)} = 1$, já que, $\tau^n = e$.

Reciprocamente, suponhamos que $N(a) = 1$. Consideremos $c \in L$, e definamos

$$\begin{aligned} d_0 &= a_0 \\ d_1 &= (a\tau(a))\tau(c) \\ &\vdots \\ d_j &= [a\tau(a)...\tau^j(a)]\tau^j(c), \text{ para } 0 \leq j \leq n-1. \end{aligned}$$

Então, $d_{n-1} = N(a)\tau^{n-1}(c) = \tau^{n-1}(c)$. E mais, $d_{j+1} = a\tau(d_j)$, para $0 \leq j \leq n-2$. Definamos $b = d_0 + d_1 + ... + d_{n-1}$, afirmamos que podemos podemos escolher c de modo a tornarmos $b \neq 0$. Suponhamos por absurdo, que não consigamos isto, ou seja, $b = 0$ para todas as escolhas de c. Assim, para $c \in L$,

$$\lambda_0\tau^0(c) + \lambda_1\tau(c) + ... + \lambda_{n-1}\tau^{n-1}(c) = 0, \text{ em que } \lambda_j = a\tau(a)...\tau^j(a), \text{ pertece a } L.$$

Logo os τ^j automorfismos distintos são linearmente dependentes sobre L, contrariando o Teorema (15). Assim, podemos escolher c tal que $b \neq 0$. Deste modo,

$$\begin{aligned} \tau(b) &= \tau(d_0) + ... + \tau(d_{n-1}) \\ &= \left(\frac{1}{a}\right)(d_1 + ... + d_{n-1}) + \tau^n(c) \\ &= \left(\frac{1}{a}\right)(d_1 + ... + d_{n-1}) = \frac{b}{a}. \end{aligned}$$

Portanto, $a = \dfrac{b}{\tau(b)}$, como afirmamos. □

Teorema 105. *Suponhamos que $L : K$ seja uma extensão normal finita cujo Grupo de Galois, G, é cíclico de ordem p, gerado por τ. Assumamos que a característica de K é 0 ou, primo com p, e que $t^p - 1$ se decompõe linearmente sobre K. Então, $L : K(\alpha)$, em que α é um zero de um polinômio irredutível $t^p - a$ sobre K para algum $a \in K$.*

Demonstração. Os p zeros de $t^p - 1$ de um grupo H, grupos este que é cíclico, pois, possuem ordem prima. Sabemos que um grupo cíclico consiste de potências de um elemento. Assim, os zeros de $t^p - 1$ são potências de algum $\beta \in K$, em que, $\beta^p = 1$. Logo, $N(\beta) = \beta...\beta = 1$, uma vez que, $\beta \in K$, e, portanto, $\tau^2(\beta) = \beta$. Pelo Teorema (104), temos que $\beta = \dfrac{a}{\tau(\alpha)}$, para algum $\alpha \in L$. Assim,

$$\tau(\alpha) = \beta^{-1}\alpha\tau^2(\alpha) = \beta^{-2}\alpha...\tau^j(\alpha) = \beta^{-j}\alpha, \text{ e } a = \alpha^p \text{ é fixado por } G.$$

Logo, está em K. Agora, como $K(\alpha)$ é o corpo de decomposição para $t^p - a$ sobre K, então K-automorfismos $e, \tau, ..., \tau^{p-1}$ mapeiam α em elementos distintos. Então eles são os p distintos K-automorfismos de $K(\alpha)$. Pelo Teorema Fundamental da Teoria de Galois (Teorema (22)), o grupo de $[K(\alpha) : K] \geq p$. Mas, $[L : K] = |G| = p$, então $L = K(\alpha)$.

Portanto, $t^p - a$ é o polinômio minimal de α sobre K, caso contrário, deveríamos ter $[K(\alpha) : K] < p$. Sendo um polinômio minimal, $t^p - a$ é irredutível sobre K. □

Teorema 106. *Se K é um corpo de característica zero, e $L : K$ é uma extensão normal finita com Grupo de Galois solúvel G, então existe uma extensão R de L tal que $R : K$ é radical.*

Demonstração. Todas as extensões são separáveis já que K tem característica 0. Usaremos indução em $|G|$. O resultado é claro quando $|G| = 1$. Se $|G| \neq 1$, tomamos o subgrupo normal maximal H de G. Este existe, já que G é finito. Portanto, G/H é simples, e como H é maximal, temos que este é também solúvel pelo item *ii)* do Teorema (52). Agora, pelo Teorema (54), G/H é cíclico e de ordem prima p.

Seja N o corpo de decomposição de $t^p - 1$ sobre L. Então, $N : K$ é normal, e pelo Teorema (12), L é um corpo de decomposição sobre K para algum polinômio f. Assim, N é o corpo de decomposição sobre L de $(t^p - 1)f$, o que implica que $N : K$ é normal pelo Teorema (12).

Pelo Lema (77), o Grupo de Galois de $N : L$ é abeliano e pelo Teorema Fundamental (Teorema (22)), $\Gamma(L : K)$ é isomorfo a $\dfrac{\Gamma(N : K)}{\Gamma(N : L)}$. Assim, pelo Teorema (52) $\Gamma(N : K)$ é solúvel. Seja M o subcorpo de N gerado por K e os zeros de $t^p - 1$. Então, $N : M$ é normal. Agora, $M : K$ é claramente radical, e como $L \subseteq N$, temos que o resultado desejado providenciará um extensão R de N, tal que, $R : M$ é radical.

Afirmamos que, o Grupo de Galois de $N : M$ é isomorfo a um subgrupo de G. Mapeamos qualquer M-automorfismo τ de N por $\tau|L$. Como $L : K$ é normal, $\tau|L$ é um K-automorfismo de L, e existe um homomorfismo de grupos $\Phi : \Gamma(N : M) \longrightarrow \Gamma(L : K)$.

Se $\tau \in Ker(\Phi)$, então τ fixa todos os elementos de M e L, o que gera N. Portanto, $\tau = e$, e assim, Φ é um monomorfismo, o que implica que $\Gamma(N : M)$ é isomorfo a um subgrupo J de $\Gamma(L : K)$.

Se $J = \Phi(\Gamma(N : M))$ é um subgrupo próprio de G, então por indução, existe uma extensão R de N, tal que $R : M$ é radical. A única possibilidade restante é que $J = G$. Então, podemos encontrar um subgrupo $I \lhd \Gamma(N : M)$ de índice p, digamos, $I = \Phi^{-1}(H)$. Consideremos o corpo fixo de $I^{\dagger}$. Então, $[P : M] = p$, pelo Teorema Fundamental (Teorema (22)), $P : M$ é normal, e ainda pelo Teorema, $t^p - 1$ se decompõe linearmente em M. Pelo Teorema (105), $P = M(\alpha)$, em que $\alpha^p = a \in M$. Mas, $N : P$ é uma extensão normal com Grupo de Galois solúvel de ordem menor do que $|G|$, e então, por indução, existe uma extensão R de N tal que $R : P$ é radical. Ora, $R : M$ é radical e o resultado está provado. □

E para finalizar:

Teorema 107. *Sobre um corpo de característica zero, um polinômio é solúvel por radicais se, e somente se, este tem Grupo de Galois solúvel.*

Demonstração. Segue do Teorema (106) e do Teorema (83). □

6 Referências Bibliográficas

GARCIA, A.; LEQUAIN, Y. **Elementos de Álgebra.** 2. ed. Rio de Janeiro: Instituto Nacional de Matemática Pura e Aplicada, 2003.

MARTIN, P. A. **Grupos, corpos e teoria de Galois.** São Paulo: Editora Livraria da Fïsica, 2010.

STEWART, I. N. **Galois theory.** 5. ed, Boca Raton, Fla: CRC Press, 2015.