Introdução a Teoria de Galois

Palavras-Chave: Corpo, Extensão de corpo, Extensão Algébrica, Polinômios, Anéis.
Autores:
Brener Costa dos Santos, IMECC - UNICAMP;
Prof. Dr. Pietro Speziali (orientador), IMECC - UNICAMP.

1 Introdução

O intuito desse estudo é entender a razão pela qual não podemos encontrar uma fórmula que resolva equações de polinômios de grau maior ou igual a 5. Fórmulas como a de Bhaskara e de Cardano são conhecidas para encontrar as soluções de polinômios de grau 2, 3 e 4. Sem entrar em detalhes, essas fórmulas resolutivas são ditas "por radicais"pois envolvem apenas operações elementares nos coeficientes do mesmo polinômios: soma, multiplicação, e e estração de raízes. No entanto, por muito tempo restou em aberto o problema permaneceu em aberto por cerca de três séculos para polinômios de grau 5, a saber

$$ax^5 + bx^4 + cx^3 + dx^2 + ex + f = 0. \tag{1}$$

Surpreendendo as expectativas de alguns grandes matemáticos do século 19, como Lagrange, a resposta ao problema, nesse caso, foi negativa; mais precisamente, vale o seguinte resultado.

Teorema 1.1 (Abel-Ruffini) *Um polinômio $f(x)$ de grau maior igual a 5 não pode ser resolvido por radicais.*

Vamos agora detalhar um exemplo simples, para exemplificar o que a "resolução por radicais"comporta. Tomemos polinômio de grau 2, $ax^2 + bx + c = 0$, cuja solução é dada pela fórmula de Bhaskara:

$$x = \frac{-b \pm \sqrt{\Delta}}{2a}, \quad \text{onde} \quad \Delta = b^2 - 4ac.$$

A busca de soluções para equações de grau arbitrário levou a criação da Álgebra moderna, com a Teoria de Grupos e Corpos, que estão juntas na assim chamada Teoria de Galois. O foco deste projeto é entender um nível elementar de Teoria de Galois, em especial o seguinte célebre Teorema:

Teorema 1.2 *Um polinômio $f(x)$ solúvel por radicais se e somente se seu grupo de Galois é solúvel.*

Para compreendermos o teorema acima é necessário elucidar alguns conceitos fundamentais de álgebra e entender algumas estruturas como grupos, anéis, em especial os anéis de polinômios, corpos e extensão de corpos.

2 Desenvolvimento da Pesquisa

A pesquisa em primeiro momento foi focada em entender os conceitos fundamentais de álgebra em sua totalidade ao longo do semestre, para posteriormente entendermos o Teorema de Abel-Ruffini e o Teorema Fundamental de Galois.

Foram usadas as bibliografias [1] e [2] para o estudo dos conceitos de anel, domínio, corpo, homomorfismo, ideais, corpo de frações de um domínio, polinômios em uma variável e grupos. No segundo momento, usufruimos das bibliografias [3] e [4] para enteder a fundo os problemas da quíntica, corpos, extensões, corpo de decomposição e introduzir a teoria de Galois.

3 Estruturas álgebricas

Vamos introduzir o conceito de grupos e seus resultados mais importantes, a fim de entender a relação entre a teoria de grupos com os corpos e termos traquejo suficiente para entender o Teorema 1.2.

Definição 3.1 (Grupo) *Um grupo é um par $(G, \cdot)$ onde G é um conjunto e $\cdot : G \times G \to G$ é uma operação binária em G que, para todo $a, b, c \in G$, satisfaz:*

(i) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ *(Associatividade)*

(ii) $\exists e \in G$ *tal que* $a \cdot e = e \cdot a = a$ *(Elemento neutro)*

(iii) $\exists a^{-1} \in G$ *tal que* $a \cdot a^{-1} = a^{-1} \cdot a = e$ *(Elemento inverso)*

Quando $a \cdot b = b \cdot a$ dizemos que o grupo é abeliano (comutativo).

Vamos exemplificar alguns grupos:

1. Os inteiros $\mathbb{Z}$ são um grupo com respeito à operação $+$. Aqui, o elemento neutro é 0. Para cada $a, b \in \mathbb{Z}$, temos que $a + b \in \mathbb{Z}$.

2. Seja X um conjunto e $G = \mathrm{Perm}(X) = \{f : X \to X \mid f \text{ é uma bijeção}\}$. Tal f é chamado de permutação de X. G é um grupo com respeito à operação de composição, i.e.,

$$(f \circ g)(x) = f(g(x)) \quad \text{para cada } x \in X.$$

Se f e g são permutações de X, então $f \circ g$ também é uma permutação. Aqui, o elemento neutro é a identidade de X, denotada por id_X. No caso em que X é um conjunto finito de n elementos, G é denotado por S_n e é chamado de grupo simétrico.

Definição 3.2 (Homomorfismo) *Sejam (H,*), (G,κ) grupos, onde * e κ são operações binárias, dada $f : H \to G$, se vale $f(a * b) = f(a) * f(b)$ $\forall a, b \in H$, então f é homomorfismo. Veja que f preserva a estrutura de grupo.*

Definição 3.3 (Isomorfismo) *Dado G, H grupos se tivermos f homomorfismo e este for bijetivo, então temos um isomorfismo.*

Grupos isomorfos são "iguais". Como possuem mesma estrutura então conhecendo um grupo o outro também o é. Veja que com isso iremos apenas considerar grupos diferentes aqueles que não são isomorfos. Inclusive escrevemos $G\tilde{=}H$ nesses casos.

A ausência de uma fórmula geral para resolver equações de quinto grau é uma consequência do fato de que o grupo S_5, que é o grupo das permutações do conjunto $\{1, 2, 3, 4, 5\}$, não é solúvel.

Seja G um grupo de ordem p^n. Se H é um subgrupo maximal de G, então H é normal em G e $|G|/|H| = p$.

Definição 3.4 (Grupo Solúvel) *Um grupo G é solúvel se existir uma cadeia de subgrupos*

$$\langle e \rangle = H_0 \subseteq H_1 \subseteq H_2 \subseteq \cdots \subseteq H_n = G$$

tal que cada grupo quociente H_{i+1}/H_i é abeliano.

Definição 3.5 (Anel) *Um anel é um par $(A, +, \cdot)$ onde A é um conjunto e $+$ e $\cdot$ são operações binárias em A, que satisfazem as seguintes propriedades:*

- *$(A, +)$ é um grupo abeliano.:*
- *$(A, \cdot)$ é um semigrupo, isto é:*

  (i) A operação $\cdot$ é associativa.

- *A operação $\cdot$ distribui sobre $+$, isto é:*

  (ii) Para todo $a, b, c \in A$,

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

e

$$(a + b) \cdot c = a \cdot c + b \cdot c.$$

Quando $(A, \cdot)$ é um grupo, isto é, cada elemento $a \in A$ possui inverso com relação a operação $\cdot$ temos um corpo.

Exemplos de anéis são $\mathbb{Z}$ e as matrizes. Exemplos de corpos são $\mathbb{Q}, \mathbb{R}, \mathbb{C}$.

Vamos enfatizar os anéis de polinômios e listar alguns resultados importantes.

Definição 3.6 (Anel de Polinômios) *Seja R um anel. O anel de polinômios sobre R, denotado por $R[x]$, é o anel formado pelos polinômios com coeficientes em R, onde a adição é a adição de polinômios e a multiplicação é a multiplicação de polinômios.*

O importante é que polinômios tenham fatoração única. Como geralmente trabalhamos com o anel base $\mathbb{Z}$, que é um domínio de fatorização única, não precisamos nos preocupar,pois

Definição 3.7 (Domínio) *Um anel R é um domínio integral (ou simplesmente domínio) quando, para todo $a, b \in R$, $ab = 0 \implies a = 0$ ou $b = 0$.*

Teorema 3.1 *Se R é um domínio de fatorização única, entao $R[x]$ também é.*

Isso resume algumas das propriedades necessárias para anéis, embora algumas definições gerais, como a definição de máximo divisor comum em qualquer anel e alguns teoremas relacionados, não tenham sido abordadas

4 Corpos, Extensões e Teoria de Galois

Antes de falarmos do teorema de Galois, precisamos discorrer sobre alguns resultados importantes de corpos e extensões. Corpos são importantes, pois os espaços vetoriais são feitos partindo deles.

Definição 4.1 (Extensão de Corpo) *Sejam $\mathbb{F}, \mathbb{K}$ corpos, se $\mathbb{F} \subseteq \mathbb{K}$, também denotado por K/F, é denominado extensão de corpo.*

Um exemplo fácil de verificar isso são os $\mathbb{C}$(complexos) como entensão de $\mathbb{R}$.

Como K é um espaço vetorial sobre F, ele tem uma dimensão sobre o mesmo. Escrevemos $[K : F]$ para essa dimensão e chamamos ela de grau da extensão K/F. Nesse projeto nos restringimos a trabalhar com extensões finitas.

Definição 4.2 *Seja K/F uma extensão. Dizemos que $\alpha \in K$ é algébrico sobre F quando existe $f \in F[x]$ tal que $f(\alpha) = 0$. Se todo elemento de K é algébrico, então dizemos que K é algébrico sobre F e K/F é uma extensão algébrica.*

Como exemplo, temos $\mathbb{C} = \mathbb{R}[i]$, onde dado $z \in \mathbb{C}$, temos $z = a + bi$, com $a, b \in \mathbb{R}$. Veja que i é algébrico sobre $\mathbb{R}$, tome $p(x) = x^2 - 1$.

Ou ainda $\mathbb{Q}(\sqrt{2})$, veja que $\sqrt{2}$ é algébrico sobre $\mathbb{Q}$,tome $p(x) = x^2 - 2$.

Definição 4.3 *Se K é uma extensão de F, o grupo de Galois de K/F é o grupo formado pelos F-automorfismos de K. Esse grupo é denotado por* $\mathrm{Gal}(K/F)$.

Assumimos que nossos polinômios são separáveis. Para grau 2, 3, ou 4, exigimos que o corpo F não tenha característica 2 ou 3 é suficiente para garantir a separabilidade. Seja $f(x) \in F[x]$ separavel e irredutível sobre F, e K o corpo de decomposição sobre F de f. Defina $f(x) = (x-\alpha_1)\cdots(x-\alpha_n) \in K[x]$. Se $n = \deg(f)$, note que n divide $[K : F] = |\mathrm{Gal}(K/F)|$, Como $[F(\alpha_1) : F] = n$. O grupo de Galois $\mathrm{Gal}(K/F)$ é isomorfo a um subgrupo de S_n, com S_n sendo o grupo de permutações das raizes de f.

Quando conseguimos associar o grupo de permutações das raízes de $f(x)$, encontramos uma fórmula que resolve o polinômio.

Definição 4.4 *Uma extensão de corpo K de F é uma extensão radical se $K = F(a_1, \ldots, a_r)$, tal que existem inteiros $n_1, \ldots, n_r$ com $a_1^{n_1} \in F$ e $a_i^{n_i} \in F(a_1, \ldots, a_{i-1})$ para todo $i > 1$. Se $n_1 = \cdots = n_r = n$, então K é chamada uma extensão n-radical de F.*

Definição 4.5 *Se $f(x) \in F[x]$, então f é solúvel por radicais se existe uma extensão radical L/F tal que f se decompõem em L.*

Lema 4.1 *Se K é uma extensão de F, $\alpha \in K$ é algébrico sobre F e $\tau \in \mathrm{Gal}(K/F)$, então τ permuta as raízes de $\min(F, \alpha)$.*

Definição 4.6 *Uma extensão K de F é dita Galois quando $F = F(\mathrm{Gal}(K/F))$.*

Proposição 4.1 *Se K é uma extensão Galois de F, então $[K : F] = |\mathrm{Gal}(K/F)|$.*

Da proposição 4.1, segue corolário

Corolário 4.1 *Se K/F é uma extensão e $\alpha \in K$ é algébrico sobre F, então $|\mathrm{Gal}(F(\alpha)/F)|$ é igual ao número de raízes distintas de $\min(F, \alpha)$ em $F(\alpha)$. Assim, $\mathrm{Gal}(F(\alpha)/F)$ é Galois se, e somente se, $\min(F, \alpha)$ tem n raízes distintas em $F(\alpha)$, onde $n = \deg(\min(F, \alpha))$.*

Portanto, há duas maneiras pelas quais $F(\alpha)/F$ pode não ser uma extensão de Galois. Ou algumas das raízes de $\min(F, \alpha)$ não estão contidas em $F(\alpha)$ ou o polinômio possui raízes repetidas.

Teorema 4.1 (Teorema Fundamental da Teoria de Galois) *Seja K uma extensão de Galois finita de F. Então há uma bijeção entre os corpos L tais que $K \supseteq L \supseteq F$ e os subgrupos de G, dada por $L \mapsto \mathrm{Gal}(K/L)$ e sua inversa por $H \mapsto F(H)$. Além disso, se L corresponde a H, temos $[K : L] = |H|$ e $[L : F] = |G|/|H|$. Além disso, H é normal em G se, e somente se, L é Galois sobre F. Quando isso ocorre, $\mathrm{Gal}(K/F) \cong G/H$.*

5 Conclusão

Como discorrido nas seções anteriores, concluímos que não é possível associar uma fórmula geral para polinômios de grau maior ou igual a 5, pois não podemos garantir que o grupo $F(\alpha)/F$ seja uma extensão de Galois.

Referências

[1] Lequain, Arnaldo Yves Garcia *Elementos de álgebra*, IMPA (2022).

[2] Gonçalves, Adilson *Introdução à Álgebra*, IMPA, (1979).

[3] Morandi, Patrick *Field and Galois Theory*, Graduate texts in Mathematics, Springer (1996).

[4] Rotman, Joseph *Galois Theory*, Universitext, Springer (1998).