XXVIII Congresso {virtual} de Iniciação Científica da Unicamp 2020

Grupos, Corpos, Teoria de Galois e Aplicações

Lucas Henrique Martins da Silva e Prof. Dr. Plamen Emilov Kochloukov

Resumo. Este trabalho apresenta um resumo das atividades desenvolvidas por mim, sob orientação do Prof. Plamen e financiamento da Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP) no período compreendido entre 1º de agosto de 2019 e 30 de setembro de 2020[1].

A teoria de Galois é uma área que caracteriza determinadas extensões de corpos a partir de grupos de automorfismos. Se uma extensão de corpos K/k é separável e normal (dita extensão de Galois), há uma correspondência injetiva entre os subgrupos do grupo de automorfismos k-lineares e os corpos fixos, que inverte a inclusão e, se a extensão K/k é finita, a correspondência é bijetiva; em suma, o teorema fundamental da teoria de Galois afirma que tal mapa é um funtor contravariante entre a categoria dos subgrupos de $\mathrm{Gal}(K/k)$ com morfismo de inclusão e a categoria dos corpos intermediários de K/k com o mesmo tipo de morfismo, ou que a correspondência é um anti-isomorfismo de reticulados.

Além do tópico principal – teoria de corpos e de Galois –, esta Iniciação Científica abordou os tópicos preliminares de grupos, anéis e polinômios. Com a bagagem adquirida, foram vistas aplicações a problemas clássicos, como construções com régua e compasso, o teorema de Abel-Ruffini e o teorema fundamental da álgebra ($\mathbb{C}$ é algebricamente fechado).

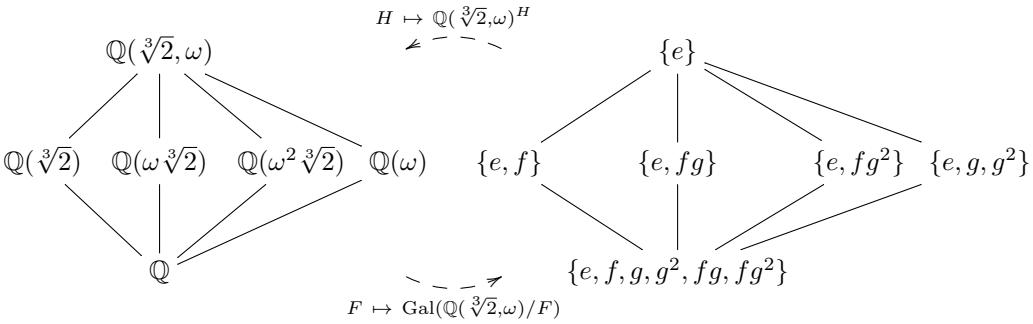

Figura 1. Correspondência de Galois entre a extensão de corpos $\mathbb{Q}(\sqrt[3]{2},\omega)/\mathbb{Q}$ e o grupo de Galois associado

[1]Processo FAPESP 2019/17092-1.

Preliminares

Para estudar a teoria de corpos e a teoria de Galois, os conceitos preliminares são fundamentais. Os grupos são caracterizados como conjuntos munidos de uma operação binária associativa, com elemento neutro e admitindo inverso; os anéis compatibilizam grupos comutativos com a noção de produto e, no caso específico dos corpos, comutatividade do produto e inverso multiplicativo para cada elemento não-nulo. É de principal interesse o estudo de polinômios com coeficientes sobre um corpo.

Além das definições, os fatos mais relevantes utilizados são o 1º teorema do isomorfismo, o fato de que $R/\mathfrak{p}$ é anel de integridade para $\mathfrak{p}$ ideal primo e $R/\mathfrak{m}$ é corpo para $\mathfrak{m}$ ideal maximal, quando R é anel comutativo. Além disso, $F[x]$ é anel principal e, quando $p \in F[x]$ é irredutível, $F[x]/\langle p \rangle$ é um corpo que contém uma raiz de p; a saber, a classe de equivalência $[x]$. Em especial, para a teoria de solubilidade por radicais, fatos básicos sobre grupos cíclicos e a solubilidade do grupo simétrico $\mathfrak{S}_n$ são necessários.

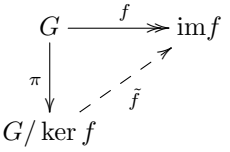

Figura 2. Diagrama do 1º teorema do isomorfismo

Extensões algébricas

Sejam K e k corpos. Dizemos que K é extensão de k se $K \supset k$; neste caso, dizemos que K/k é uma extensão de corpos. Se $\alpha \in K$ é raiz de um polinômio sobre k, i.e., $\exists p \in k[x] : \ p(\alpha) = 0$, dizemos que α é *algébrico* sobre k. Se todo elemento de K é algébrico sobre k, dizemos que K/k é uma extensão algébrica. Além disso, o ideal de aniquiladores de um elemento algébrico α tem como gerador um único polinômio mônico irredutível (pois $k[x]$ é anel principal); dessa forma, a noção de polinômio mínimo de um elemento é bem definida. Dado um elemento $\alpha \in K$ algébrico com polinômio mínimo p_α, há um isomorfismo entre o menor corpo $k(\alpha)$ que contém k e α (dito corpo de adjunção) e $k[x]/\langle p_\alpha \rangle$. Com este fato, sempre é possível construir uma extensão em que um polinômio qualquer tem uma raiz (comparando com a estrutura de $k[x]/\langle p_\alpha \rangle$).

No contexto de espaços vetoriais, é uma verificação direta o fato de que K é um k-espaço vetorial com as operações usuais. De fato, isso dá mais uma motivação para pensar em uma extensão como dois elementos – toda extensão tem algumas estruturas associadas.

Se $\dim_k K$ é finita, dizemos que a extensão K/k é finita. Em geral, denotamos esta dimensão (chamada de grau da extensão) por $[K : k]$. Consequentemente, sendo $n := [K : k]$, $\forall \alpha \in K : \ \{1, \alpha, \ldots, \alpha^n\}$ não pode ser linearmente independente e assim todo elemento é algébrico. As extensões finitas são de interesse central na teoria de Galois. Considerando as bases dos espaços vetoriais, é possível estabelecer uma bijeção e o seguinte teorema:

Teorema 1 (Lei da Torre). *Sejam E/K e K/F extensões de corpos. Então*

$$[E : F] = [E : K][K : F].$$

Exemplo 2. A extensão $\mathbb{C}/\mathbb{R}$ é algébrica: fazendo o caminho inverso da fórmula quadrática, todo elemento de $\mathbb{C}$ satisfaz uma equação do segundo grau com coeficientes em $\mathbb{R}$. Além disso, como $\{1, i\}$ é base de $\mathbb{C}$ em relação aos reais, é extensão finita de grau 2.

Exemplo 3. Seja $S = \{ \sqrt[n]{2} : n \in \mathbb{N} \wedge n \geq 2\}$ o conjunto de todas as raízes n-ésimas de 2. Seja $K := \mathbb{Q}(S) \subset \mathbb{R}$, i.e., o menor subcorpo dos reais que contém todas as raízes n-ésimas (reais) de 2. Essa extensão é algébrica: notando que $\mathbb{Q}(S) = \bigcup_{n=2}^{\infty} \mathbb{Q}(\sqrt[2]{2}, \ldots, \sqrt[n]{2})$, e que cada corpo na união é uma extensão finita (e portanto algébrica) de $\mathbb{Q}$, conclui-se que $\mathbb{Q}(S)$ é algébrico. Por outro lado, se $n := [\mathbb{Q}(S) : \mathbb{Q}] < \infty$, basta tomar $p \nmid n$ primo. Dessa forma, pela lei da torre, teríamos $n = [\mathbb{Q}(S) : \mathbb{Q}(\sqrt[p]{2})] \underbrace{[\mathbb{Q}(\sqrt[p]{2}) : \mathbb{Q}]}_{=p} \implies p \mid n$, contradição. Obtemos então uma extensão algébrica mas que não é finita.

Imersões e corpos de decomposição

A correspondência entre k e $k[x]/\langle p\rangle$ dada por $c \mapsto [c]$ tem por imagem um corpo; isto é, k pode ser identificado naturalmente com um subcorpo de $k[x]/\langle p\rangle$. Este fato mostra que, em muitas vezes, é mais interessante trabalhar com extensões de corpos a menos de isomorfismo (visto que, rigorosamente, $k \not\subseteq k[x]/\langle p\rangle$). Desta forma, definimos a noção de imersão: dizemos que um corpo F está *imerso* em E se houver um homomorfismo injetivo $f : F \to E$ (observe que, como F é corpo, basta que $\ker f \neq F$ para satisfazer injetividade). Como os polinômios tem papel fundamental no estudo de corpos, se $\sigma : F \to E$ é uma imersão e $p \in F[x]$, podemos definir $\sigma p \in E[x]$ como o polinômio obtido aplicando o mapa em cada coeficiente.

Exemplo 4. O mapa $\sigma : \mathbb{C} \to \mathbb{C}$ dado por $a+bi \mapsto a-bi$, chamado *conjugação*, é uma imersão do conjunto dos complexos em si mesmo. Neste caso, se $p = (3+2i)x + 7i$, então $\sigma p \stackrel{\text{def}}{=} \sigma(3+2i)x + \sigma(7i) = (3-2i)x - 7i$.

É fácil notar que, se $f(\alpha) = 0$, então $\sigma f(\sigma(\alpha)) = 0$; isto é, imersões levam raízes em raízes. De fato, a recíproca é verdadeira: se α é raiz de p e $\beta \in E$ é raiz de σp, então há uma extensão $\tau : F(\alpha) \to E$ da imersão σ que leva α em β. As imersões entre corpos dizem muito sobre suas estruturas.

Um tipo específico de imersão é central na teoria de Galois: seja E/F uma extensão de corpos. Se $\sigma : E \to E$ é um isomorfismo de corpos, chamamos σ de *automorfismo*. Além disso, se σ é F-linear (equivalentemente $\sigma(F) = F$), chamamos σ de automorfismo de E sobre F e denotamos o conjunto (que é grupo com a composição de funções) de todos os automorfismos de E sobre F por $\mathrm{Aut}(E/F)$. Dado $H \leq \mathrm{Aut}(E/F)$ subgrupo, definimos $E^H := \{x \in E : \forall h \in H(\ h(x) = x)\}$, dito *corpo fixo* de H que de fato é corpo.

Paralelamente, definamos a noção de corpo de decomposição: seja $p \in F[x]$ um polinômio. Seja E/F uma extensão tal que p se decompõe em fatores lineares. Se, sempre que $E \supseteq K \supseteq F$ e K é um corpo em que p se decompõe em fatores lineares tem-se $E = K$, então E é dito um *corpo de decomposição* de p. De fato, E existe (via corpo de adjunção), e é único a menos de isomorfismo. Com estes fatos, é possível definir as duas características que definem uma extensão de Galois.

Extensões separáveis, normais e de Galois

Seja E/F uma extensão algébrica. Dizemos que um elemento $\alpha \in E$ é *separável* se seu o seu polinômio mínimo se divide em fatores lineares **distintos** no corpo de decomposição; equivalentemente, um elemento é separável se, e só se existem $\deg p_\alpha$ imersões de $F(\alpha)$ a E estendendo a identidade; se todo elemento de E é separável, dizemos que a extensão é separável. Em característica 0, utilizando o teste da multiplicidade de uma raíz via derivada formal, toda extensão é separável; as minúcias ocorrem em característica p. Com estes fatos, separando nos casos de corpos finitos e infinitos, é possível demonstrar o seguinte teorema:

Teorema 5 (Teorema do Elemento Primitivo). *Seja E/F uma extensão separável e finita. Então há $\gamma \in E$ tal que $E = F(\gamma)$.*

Além disso, se uma extensão algébrica E/F é tal que, para todo $p \in F[x]$ irredutível: p é irredutível em $E[x]$ ou p se divide em fatores lineares em $E[x]$, então E/F é dita extensão *normal*. Equivalentemente, introduzindo a noção de fechamento algébrico (menor extensão algebricamente fechada), uma extensão é normal se toda imersão $E \hookrightarrow \overline{E}$ que estende a identidade em F é um automorfismo de E sobre F. É possível demonstrar que uma extensão é normal se e somente se é o corpo de decomposição de um conjunto de polinômios; em especial, se E/F é finita e normal, então é o corpo de decomposição de algum polinômio em F.

Uma extensão normal e separável é chamada extensão de Galois. Se E/F é de Galois, denotamos $\mathrm{Aut}(E/F)$ por $\mathrm{Gal}(E/F)$. Além disso, se $E \supseteq K \supseteq F$, então E/K é de Galois.

A correspondência de Galois

A correspondência de Galois é o cerne da teoria. Todos os outros resultados dependem da dualidade subgrupo/corpo intermediário.

Teorema 6 (Teorema Fundamental da Teoria de Galois). *Seja E/F uma extensão finita e de Galois. Então o mapa $K \mapsto \mathrm{Gal}(E/K)$ entre os corpos intermediários de E/F e os subgrupos de $\mathrm{Gal}(E/F)$ é uma bijeção tal que $K \subseteq K' \implies \mathrm{Gal}(E/K') \leq \mathrm{Gal}(E/K)$.*

Demonstração. Será apresentado um esboço da demonstração. O mapa é injetivo: se $E \neq E'$ mas $\mathrm{Gal}(K/E) = \mathrm{Gal}(K/E')$, tem-se $E = K^{\mathrm{Gal}(K/E)} = K^{\mathrm{Gal}(K/E')} = E'$, contradição; logo o mapa é injetivo. Além disso, se $E \subseteq E'$, então todo automorfismo sobre E' deixa E fixo; isto é, $\mathrm{Gal}(K/E') \leq \mathrm{Gal}(K/E)$. Este fato é verdadeiro para extensões de Galois que não são finitas.

Para demonstrar que é sobrejetivo, considere $H \leq \mathrm{Gal}(K/F)$. Queremos, naturalmente, que $K^H \mapsto H$. Como Gal(K/F) é grupo finito (pois K/F é finita e separável), temos $H = \{\sigma_1, \ldots, \sigma_n\}$, e pelo Teorema do Elemento Primitivo (5), temos $K = F(\alpha)$ para algum $\alpha \in K$. Defina $f(t) = (t - \sigma_1\alpha)\cdots(t - \sigma_n\alpha)$. Observe que $\sigma f = f$ para todo $\sigma \in H$. Ou seja, os coeficientes de f estão no corpo fixo K^H. Além disso, como $H \subseteq \mathrm{Gal}(K/F)$, temos $F \subseteq K^H$. Portanto $K \supseteq K^H(\alpha) \supseteq F(\alpha) = K$ e, portanto, $K = K^H(\alpha)$. Como α é raiz de f (pois H tem elemento identidade), de grau n, tem-se $[K^H(\alpha) : K^H] = [K : K^H] \leq n$. Mas K tem n imersões sobre K^H até uma extensão algebricamente fechada (as imersões de H) que são, portanto, automorfismos (extensão normal). Tem-se $[K : K^H] = n$, $H = \mathrm{Gal}(K/K^H)$ e portanto $K^H \mapsto H$, o que finaliza a demonstração. □

Como toda extensão de Galois é normal e, portanto, corpo de decomposição, os automorfismos podem ser vistos como permutações das raízes. Dessa forma, se a extensão é o corpo de decomposição de um polinômio de grau n, o grupo de Galois está imerso em $\mathfrak{S}_n$.

Exemplo 7. Considere o corpo de decomposição K de $x^3 - 2$ sobre $\mathbb{Q}$. As raízes do polinômio são dadas por $\{\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}\}$ e portanto $K = \mathbb{Q}(\sqrt[3]{2}, \omega)$. Tomando $f, g \in \mathrm{Gal}(K, \mathbb{Q})$ tais que $f(\sqrt[3]{2}) = \sqrt[3]{2} \wedge f(\omega) = \omega^2$ e $g(\sqrt[3]{2}) = \omega\sqrt[3]{2} \wedge g(\omega) = \omega$, obtemos o diagrama da figura 1, com $f \leftrightarrow (12) \wedge g \leftrightarrow (123)$, ciclos de $\mathfrak{S}_3$.

Aplicações

Uma das mais evidentes aplicações da teoria de corpos e a teoria de Galois é o estudo da natureza de equações polinomiais (via corpo de de decomposição) e a solubilidade por radicais. Para grau ≤ 4, os resolventes de Lagrange classificam bem as equações polinomiais.

Em relação aos clássicos de construção com régua e compasso, basta notar que o corpo dos números construtíveis é o conjunto de todos os números reais que são elemento de alguma torre quadrática real sobre $\mathbb{Q}$. Esta caracterização trivialmente implica que todo número construtível é algébrico sobre $\mathbb{Q}$, cujo grau é potência de 2. Portanto, problemas como a duplicação do cubo (que implica na construtibilidade de $\mathbb{Q}[\sqrt[3]{2}]$) tornam-se triviais, visto que 3 não é potência de 2.

Quanto à solubilidade de corpos, a nomenclatura de grupos pode ser naturalmente identificada com extensões de corpos (e, de fato, dá uma razão para tais nomes). Um polinômio $p \in F[x]$ dito solúvel por radicais se há uma torre radical (cada extensão é a adjunção de uma raiz da extensão anterior) que contém o corpo de decomposição E de p. Utilizando fatos sobre grupos solúveis, é possível concluir que se p é solúvel e E/F é de Galois, então $\mathrm{Gal}(E/F)$ é solúvel. Para o teorema de Abel-Ruffini (em característica 0), basta notar que, tratando os coeficientes como variáveis (polinômios simétricos elementares), o grupo de Galois associado a um polinômio genérico de grau n é isomorfo a $\mathfrak{S}_n$, que não é solúvel para $n \geq 5$. De forma mais prática, com um pouco da análise real e os teoremas de Sylow, é possível demonstrar que polinômios "comuns" como $t^5 - 4t + 2 \in \mathbb{Q}[t]$ não são solúveis por radicais. Desta mesma forma, notando que todo polinômio real de grau ímpar tem raiz, que todo número complexo tem raiz quadrada e com os teoremas de Sylow temos o seguinte fato:

TEOREMA 8 (Teorema Fundamental da Álgebra). $\mathbb{C}$ *é algebricamente fechado.*

DEMONSTRAÇÃO. Considere $E/\mathbb{C}$ uma extensão finita. Então $E/\mathbb{R}$ é extensão finita e, pelo Teorema do Elemento Primitivo, seja $E = \mathbb{R}(\gamma)$; seja K o corpo de decomposição de γ. A fim de contradição, assuma que $[E : \mathbb{C}] > 1$ (e, consequentemente, $[K : \mathbb{C}] > 1$).

Observe que $[K : \mathbb{R}] = [K : \mathbb{C}]\overbrace{[\mathbb{C} : \mathbb{R}]}^{=2}$ e, então, 2 divide $|\mathrm{Gal}(K/\mathbb{R})|$. Tome então, pelo primeiro teorema de Sylow, um 2-subgrupo maximal (maior grau possível) $H \leq \mathrm{Gal}(K/\mathbb{R})$; por construção, $[K : K^H] = |\mathrm{Gal}(K/K^H)|$ e portanto, pela Fórmula da Torre e pela maximalidade de H, $[K^H : \mathbb{R}]$ é ímpar. Mas, implicitamente, pelo Teorema do Elemento Primitivo, o polinômio irredutível do elemento que gera K^H sobre $\mathbb{R}$ não pode ter grau > 1 (porque todo polinômio real de grau ímpar tem uma raiz real). Portanto $[K^H : \mathbb{R}] = 1$, i.e., $K^H = \mathbb{R}$ e portanto $\mathrm{Gal}(K/\mathbb{R})$ é um 2-grupo $\implies$ $\mathrm{Gal}(K/\mathbb{C})$ é 2-grupo. Mas então, novamente pelo primeiro teorema de Sylow, se $|\mathrm{Gal}(K/\mathbb{C})| = 2^n$, há um 2-subgrupo H' de ordem 2^{n-1}. Então $[K^{H'} : \mathbb{C}] = 2$ e então $K^{H'}/\mathbb{C}$ é uma extensão quadrática. Mas como o corpo de decomposição é dado por $\mathbb{C}(\sqrt{D})$ para $D \in \mathbb{C}$ discriminante do polinômio mínimo de qualquer elemento primitivo, temos $K^{H'} = \mathbb{C} \implies [K^{H'} : \mathbb{C}] = 1$, contradição. Portanto nossa hipótese de $[E : \mathbb{C}] > 1$ é falsa; em especial, sendo $f \in \mathbb{C}[t]$ qualquer, a extensão E dada pelo corpo de decomposição de f é igual a $\mathbb{C}$. Ou seja, $\mathbb{C}$ é corpo de decomposição de todos os seus polinômios $\therefore \mathbb{C}$ é algebricamente fechado. □

Conclusão

A teoria de Galois é não-trivial. Historicamente, levou ao estudo aprofundado de grupos e, ainda hoje, tem aplicações em teoria dos números, topologia algébrica (ex.: grupos de monodromia) e inúmeras áreas, tendo um papel fundamental na formação matemática, principalmente dentro da álgebra.

Agradecimentos

Agradeço ao Prof. Plamen pela paciência, tempo e trabalho dedicados a mim. Agradeço aos meus colegas mais próximos que estiveram me apoiando e agradeço à FAPESP pelo financiamento à pesquisa.