14º Congresso de Inovação, Ciência e Tecnologia do IFSP - 2023

Números algébricos, reticulados e aplicações

CLEBER LUIZ DE OLIVEIRA SANTOS[1], ROBSON RICARDO DE ARAUJO[2]

[1]Graduando em Licenciatura em Matemática, Bolsista FAPESP, IFSP, Câmpus Cubatão, cleber.luiz@aluno.ifsp.edu.br.
[2]Professor de Ensino Básico, Técnico e Tecnológico, IFSP, Câmpus Catanduva, robson.ricardo@ifsp.edu.br.

Área de conhecimento (Tabela CNPq): 1.01.01.05-5 Algebra Comutativa

RESUMO: A teoria algébrica dos números, é uma área tradicional da matemática que utiliza métodos e conceitos da álgebra abstrata para investigar estruturas algébricas relacionadas a números algébricos e inteiros algébricos, entre outros tópicos. Esta teoria estuda propriedades e relações entre esses números, explorando suas características através de abordagens matemáticas mais abstratas. Embora seja uma subárea da matemática pura e tenha se desenvolvido principalmente para fins teóricos, ela tem sido aplicada em contextos práticos nas últimas décadas, com destaque para sua relevância na criptografia, pois fornece fundamentos matemáticos sólidos para o desenvolvimento de sistemas seguros, garantindo a proteção e a privacidade de informações sensíveis nas comunicações digitais.

PALAVRAS-CHAVE: corpos de números; anéis de inteiros; corpos quadráticos; corpos ciclotômicos.

Algebraic numbers, lattices and applications

ABSTRACT: The algebraic number theory is a traditional area of mathematics that utilizes methods and concepts from abstract algebra to investigate algebraic structures related to algebraic numbers and algebraic integers, among other topics. This theory studies properties and relationships among these numbers, exploring their characteristics through more abstract mathematical approaches. While it is a subfield of pure mathematics and has primarily developed for theoretical purposes, it has been applied in practical contexts in recent decades, notably in its relevance to cryptography. It provides a solid mathematical foundation for the development of secure systems, ensuring the protection and privacy of sensitive information in digital communications.

KEYWORDS: number fields; rings of integers; quadratic fields; cyclotomic fields.

INTRODUÇÃO

A teoria algébrica dos números é uma área clássica da matemática que, através de métodos e conceitos da álgebra abstrata, investiga estruturas matemáticas envolvendo números algébricos e inteiros algébricos, entre outros tópicos. Historicamente, é possível identificar estudos sobre as propriedades dos números desde tempos antigos, mas essa teoria experimentou um notável desenvolvimento a partir do século XVII, especialmente após Pierre de Fermat conjecturar que a equação $x^n + y^n = z^n$ não

possui soluções inteiras para qualquer $n > 3$. Esse resultado ficou conhecido como o Último Teorema de Fermat e só foi comprovado na década de 1990 (Samuel, 1970). Apesar de ser considerada uma subárea da matemática pura e de ter se desenvolvido para finalidades teóricas, nas últimas décadas a teoria dos números algébricos têm sido bastante utilizada para fins práticos, com destaque ao seu relevante uso em criptografia (Stewart; Tall, 2015).

O objetivo geral deste trabalho é apresentar uma introdução abrangente aos fundamentos da teoria dos números algébricos, bem como aos aspectos básicos de sua conexão com a teoria de reticulados e algumas de suas aplicações. Através desse estudo, espera-se expor as principais técnicas e proposições dessa área, possibilitando assim que ele avance em seus estudos acadêmicos nessa área ou áreas relacionadas. Além disso, o objetivo é capacitá-lo a contribuir de forma direta e original no progresso dessas áreas ou na obtenção de novos resultados em matemática pura ou em áreas aplicadas, como teoria da informação, códigos e criptografia.

Também apresentaremos uma visão geral sobre os conceitos fundamentais da teoria algébrica dos números, como o de normas e traços de corpos de números, investigar aneis de inteiros de algumas extensões de corpos quadráticos e corpos ciclotômicos, os quais são aplicados à teoria da Informação e à teoria dos códigos corretores de erros (Araujo, 2015). Para a continuação deste trabalho até o final do ano, temos como objetivo avançar em algumas possíveis aplicações à reticulados, sua realização geométrica via mergulho de Minkowski e introduzir o estudo das curvas elípticas e dos espaços projetivos, aplicando tais conhecimentos às equações diofantinas.

MATERIAIS E MÉTODOS

Por se tratar de um estudo em matemática pura, esse trabalho foi feito apenas com estudo através de leituras em livros, artigos e textos físicos e digitais. Para bem desenvolver esse trabalho, foram feitas leituras críticas de diversos itens da bibiografia, reflexões a respeito das ferramentas e propriedades observadas, discussões com o orientador sobre os destaques e as dúvidas surgidas e produção de textos com as principais conclusões e resultados obtidos dos estudos teóricos.

RESULTADOS E DISCUSSÃO

O principal objeto que orienta a teoria dos números algébricos, como o nome sugere, são os números algébricos. Um número é chamado **algébrico** quando é raiz de um polinômio não nulo, que nesse caso, terá coeficientes racionais. Esse elemento não pertence ao corpo dos racionais, já que dessa forma, todo número será algébrico e não ganharemos boas propriedades com essa definição. Utilizamos esse conceito para construir corpos de números, isto é, extensões finitas do corpo dos racionais. Ou seja, precisamos construir um corpo K a partir de $\mathbb{Q}$, que contenha um elemento α, onde $\alpha \notin \mathbb{Q}$ (K será o menor corpo contendo $\mathbb{Q}$ e α).

Chamaremos de $\mathbb{Q}[\alpha]$, com $\alpha \in \mathbb{C}$, como sendo o conjunto das aplicações de α nos polinômios $p(x) \in \mathbb{Q}[x]$. Isto é, $\mathbb{Q}[\alpha] = \{p(\alpha)|p(x) \in \mathbb{Q}[x]\}$.

Usando o homomorfismo de avaliação de α, isto é, $\epsilon_\alpha : \mathbb{Q}[x] \longrightarrow \mathbb{C}$ que leva $f(x) \longmapsto f(\alpha)$, sabemos que se α é transcendente, implica $\langle Ker\epsilon_\alpha \rangle = 0 \implies \mathbb{Q}[x] \cong \mathbb{Q}[\alpha]$ que é um anel. Mas se α for algébrico, implica $\langle Ker\epsilon_\alpha \rangle = \langle irr(\alpha, \mathbb{Q}) \rangle$, onde $irr(\alpha, \mathbb{Q})$ é o polinômio irredutível de menor grau no qual α é raiz. Assim, vemos que $\mathbb{Q}[\alpha]$ é um corpo, já que $irr(\alpha, \mathbb{Q})$ é um polinômio irredutível. Neste caso, denotamos $\mathbb{Q}[\alpha] = \mathbb{Q}(\alpha)$.

Enxergamos $\mathbb{Q}(\alpha)$ como sendo um espaço vetorial sobre $\mathbb{Q}$ com base $\{1, \alpha, ..., \alpha^{n-1}\}$. O grau da extensão de $\mathbb{Q}(\alpha)$ sobre $\mathbb{Q}$, será denotado por $[\mathbb{Q}(\alpha) : \mathbb{Q}]$, que nesse caso, é igual a n. E por ter dimensão finita, $\mathbb{Q}(\alpha)$ é um corpo de número.

A partir dessa construção, podemos definir alguns parâmetros desses corpos para complementar a teoria e nos dar vantagens de trabalhar com eles. Os primeiros a ser definidos, são os conjugados e discriminantes desses corpos. Os conjugados de $\alpha \in K = \mathbb{Q}(\theta)$, para θ algébrico, denotado por $\sigma_i(\alpha)$, $i = 1, 2, .., n$, são os n monomorfismos distintos que permuta as n raízes do polinômio irredutível que zera θ. Ou seja, se $\alpha = a_0 + a_1\theta + ... + a_n\theta^{n-1}, a_i \in \mathbb{Q}$, então $\sigma_i(\alpha) = a_0 + a_1\theta_i + ... + a_n\theta_i^{n-1}$, onde θ_i é uma outra raíz do $irr(\theta, \mathbb{Q})$.

Com essa noção, se $\{\alpha_1, ..., \alpha_n\}$ é uma base de K, então define-se o **discriminante dessa base** como sendo $\Delta[\alpha_1, ..., \alpha_n] = \{det[\sigma_i(\alpha_j)]\}^2$. Se pegarmos uma outra base $\{\beta_1, ..., \beta_n\}$, temos o discriminante desta nova base como $\Delta[\beta_1, ..., \beta_n] = [det(c_{ik})]^2\Delta[\alpha_1, ..., \alpha_n]$. Essa afirmação anterior mostra uma das vantagens de trabalhar com inteiros algébricos, que são os elementos do corpo de número que são raízes de polinômios com coeficientes inteiros. Esse conjunto forma um anel denominado anel de inteiros algébricos de $K = \mathbb{Q}(\theta)$, e é denotado por $\mathcal{O}_K$. Esse conjunto, por ser um anel, forma um grupo aditivo que possui uma base com n elementos, chamados grupos abelianos livres, igual a dimensão de K sobre $\mathbb{Q}$, e com isso, podemos usar um resultado que diz respeito sobre o determinante da troca de base desses grupos ser ± 1. Assim, o determinante de outra base que era $\Delta[\beta_1, ..., \beta_n] = [det(c_{ik})]^2\Delta[\alpha_1, ..., \alpha_n]$ para corpos de números, passa a ser $\Delta[\beta_1, ..., \beta_n] = \pm\Delta[\alpha_1, ..., \alpha_n]$ e, como Δ é o quadrado de um racional, implica que em anéis de inteiros o discriminante é único, sendo um ótimo parâmetro a ser usado para caracterizar certas estruturas.

Outros parâmetros que podemos definir de corpos de números, é a norma e traço. Para algum $\alpha \in K$ define-se a **norma** de α como sendo $N_K(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha)$, e definimos o **traço** de α como sendo $T_K(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha)$. Essas definições são úteis para calcular discriminantes, ou posteriormente, para identificar certos elementos que nos dirá se esses conjuntos possui uma fatoração única semelhante ao anel dos inteiros. O cálculo do discriminante pode ser feita da forma: dada $\{\alpha_1, ..., \alpha_n\}$ uma base de K, então $\Delta[\alpha_1, ..., \alpha_n] = det(T_K(\alpha_i\alpha_j))$.

Com essas medidas e definições, podemos exemplificar com corpos conhecidos, como é o caso dos corpos quadráticos e ciclotômicos. Os corpos quadráticos são corpos de números que possui grau 2 sobre $\mathbb{Q}$, ou seja, $K = \mathbb{Q}(\sqrt{d}$, onde d é um livre de quadrados, isto é, que não é divisível pelo quadrado de um número primo. O anel de inteiros de $\mathbb{Q}(\sqrt{d})$ é $\mathbb{Z}[\sqrt{d}]$, se $d \not\equiv 1 \pmod 4$ ou $\mathbb{Z}[\frac{1}{2} + \frac{1}{2}\sqrt{d}]$ se $d \equiv 1 \pmod 4$ e sua norma e traço são dados por $N_K(r + s\sqrt{d}) = r^2 - ds^2$ e $T_K(r + s\sqrt{d}) = 2r$.

Já os corpos ciclotômicos é um corpo da forma $\mathbb{Q}(\zeta)$, onde $\zeta = e^{\frac{2\pi i}{p}}$, para p primo impar, é uma n-ésima raíz primitiva da unidade. O anel $\mathcal{O}$ de inteiros de $\mathbb{Q}(\zeta)$ é $\mathbb{Z}[\zeta]$, sua norma é $N_K(\zeta) = N_K(\zeta^i) = \zeta.\zeta^2...\zeta^{p-1}$ que, para p ímpar, implica $N_K(\zeta^i) = 1$ e o traço desse corpo de número, usamos um argumento similar, já que $T_K(\zeta) = T_K(\zeta^i) = \zeta + \zeta^2 + ... + \zeta^{p-1}$ e $f(\zeta) = 1 + \zeta + ... + \zeta^{p-1}$, temos que $T_K(\zeta^i) = -1$. Já para um elemento qualquer de $\mathbb{Q}(\zeta)$, o traço é facilmente calculado pela expressão $T_K\left(\sum_{i=0}^{p-2} a_i\zeta^i\right) = pa_0 - \sum_{i=0}^{p-2} a_i$. A norma é mais complicado em geral, mas um caso útil é $N_K(1 - \zeta) = \prod_{i=1}^{p-2}(1 - \zeta^i)$ que pode ser calculado pondo $t = 1$ no polinômio minimal $irr(\zeta, \mathbb{Q}) = f(t) = t^{p-1} + ... + t + 1$. Daí $N_K(1 - \zeta) = p$.

CONCLUSÕES

Este trabalho tratou da extensão de corpos a partir do corpo dos números racionais, das vantagens de trabalhar com os aneis de inteiros e de algumas das propriedades incluídas na teoria. Nele foi discutido os principais resultados da teoria, desde a construção de corpos de números e do anel de inteiros, até a forma de calcular seus principais parâmetros, como norma, traço e discriminante de corpos quadráticos e ciclotômicos. Foi visto também, algumas condições para essas estruturas apresentarem uma fatoração única semelhante ao conjunto dos números inteiros, possibilitando diversas aplicações, como na construção de reticulados e conciliar tal teoria em estudos de curvas elípticas e espaços projetivos.

CONTRIBUIÇÕES DOS AUTORES

O Autor 1 (orientando) realizou o estudo de maneira independente e elaborou a escrita deste trabalho. Autor 2 (orientador) deu suporte e sanou todas as dúvidas em encontros assíncronos realizados periodicamente. Todos os autores revisaram e concordaram a submissão deste trabalho.

AGRADECIMENTOS

Agradecemos à comissão organizadora do 14º Congresso de Inovação, Ciência e Tecnologia do IFSP pela oportunidade de apresentação deste trabalho e a FAPESP por tornar viável a realização dessa pesquisa através do fomento da bolsa de Iniciação Científica, Projeto nº 2022/12667-9.

REFERÊNCIAS

ARAUJO, R. R. d. *Anéis de inteiros de corpos de números e aplicações.* Dissertação (Mestrado), 2015.

SAMUEL, P. *Algebraic Theory of Numbers.* [S.l.]: Hermann, 1970.

STEWART, I.; TALL, D. *Algebraic Number Theory and Fermat's Last Theorem.* [S.l.]: CRC Press, 2015.