

Matemática

Elementos Primitivos em Corpos Finitos

Conrado Rigotti de Carvalho - 8º módulo de Matemática, UFLA, bolsista PIBIC/CNPq

José Alves Oliveira - Orientador DMM, UFLA - Orientador(a)

Resumo

A teoria de corpos finitos, em especial o estudo de elementos primitivos em tais estruturas, é indispensável para diversas áreas como a teoria de códigos corretores de erros, combinatória e criptografia. Este trabalho tem por objetivo explorar a ideia de elementos primitivos, uma categoria de elementos especiais em corpos finitos. Um elemento primitivo de um corpo finito é definido como sendo o gerador do grupo multiplicativo cíclico que contém todos os elementos não nulos do corpo, isto é, dado um corpo finito F_q onde q é uma potência de um número primo, o conjunto de elementos não nulos de F_q formam um grupo para a operação multiplicação. Será explorada, de maneira concisa, a base teórica necessária para a definição de elementos primitivos, incluindo conceitos e resultados preliminares sobre grupos que contribuem para a demonstração do teorema que comprova que o grupo formado pelos elementos não nulos do corpo finito é, na verdade, um grupo cíclico, e alguns resultados importantes para corpos finitos, que garantem sua existência e unicidade.

Palavras-Chave: Elementos Primitivos, Corpos Finitos, Grupos Finitos.

Instituição de Fomento: CNPq

Link do pitch: <https://youtu.be/radi66ECMGw>