UNIVERSIDADE FEDERAL DE UBERLÂNDIA

Bacharelado em Matemática

Luís Henrique da Silva Pinheiro

Relatório parcial do trabalho:

Elementos primitivos e normais em corpos finitos

UBERLÂNDIA

Fevereiro de 2020

Introdução

A teoria dos corpos finitos é um ramo da matemática que veio a tona nos últimos cinquenta anos por causa de suas diversas aplicações em vários segmentos da ciência, entre eles, análise combinatória, teoria dos códigos, criptografia, entre outros. Muitas figuras proeminentes na história da matemática contribuíram para o desenvolvimento desta teoria, entre eles podemos citar: Pierre de Fermat (1601- 1665); Leonhard Euler (1707-1783); Joseph-Louis Lagrange (1736-1813); AndrienMarie Legendre (1752-1833); entre outros. Além disso, segundo R. Lidil e H. Niederreiter, autores de uma das referências que utilizaremos [1], tal teoria começou com os trabalhos de Carl Friedrich Gauss (1777-1855) e Evariste Galois (1811- 1832), contudo, só veio a se tornar interessante para os matemáticos aplicados nas últimas décadas.

Conceitos principais

Para que se possa entender melhor este tema, explicaremos aqui mesmo, de forma breve, o significado destes conceitos. Começamos com a definição de corpo finito, este é qualquer coleção finita e não vazia de elementos, munida de duas operações binárias entre esses elementos, uma que se comporta como a adição, e outra que se comporta como a multiplicação, e quando falamos adição e multiplicação estamos nos referindo àquelas definidas entre números reais. Veremos no decorrer do trabalho, por exemplo, que se retirarmos de um corpo finito, o elemento neutro da adição, os elementos que sobram formam um grupo cíclico com a multiplicação, interessante não? Consequentemente, como todo grupo cíclico, ele passa a ter um gerador deste grupo. Ora, estes elementos, geradores destes grupos assim formados, é exatamente o que chamamos de 'elementos primitivos'. Já a definição de 'elemento normal' é um pouquinho mais elaborada. Primeiro, começamos com um corpo finito de característica p, com q elementos (q é um natural não nulo). Veremos também que p deverá ser um número natural primo, e que o fato de p ser a característica deste corpo implica que a cardinalidade q deverá ser uma potência de p. Levando isso em conta, escolha um natural não nulo n, e considere uma extensão F de grau n do corpo inicial. Da teoria de corpos finitos sabemos que esta extensão é um corpo que contém o primeiro,

e que pode ser visto como um espaço vetorial de dimensão n (finita) sobre ele, é para a base deste espaço que olharemos agora. Um elemento x do corpo F é chamado 'elemento normal' quando o conjunto $\{ x , x^q , x^{q^2} , ... , x^{q^{n-1}} \}$ é uma base para este espaço vetorial, estas bases assim formadas são chamadas bases normais sobre corpos finitos.

Relevância

O interesse de bases normais sobre corpos finitos decorre tanto da curiosidade puramente matemática quanto das aplicações práticas. Com o desenvolvimento da teoria de codificação e o surgimento de vários sistemas criptográficos utilizando corpos finitos, o trabalho nesta área resultou em vários projetos de implementação de hardware's e software's. Estes produtos são baseados em esquemas de multiplicação usando bases normais para representar corpos finitos, assim é necessário desenvolver uma aritmética de corpos finitos para que se possa construir os algorítimos apropriados. É claro que as vantagens de se utilizar uma representação de base normal são conhecidas há muitos anos. A complexidade do desenho de hardware de tais esquemas de multiplicação é fortemente dependente da escolha das bases normais usadas. Por isso, é essencial encontrar bases normais de baixa complexidade.

Objetivos

O objetivo por trás deste trabalho é, em primeiro lugar, permitir que o estudante do curso de bacharelado em matemática, inscrito para realizar este trabalho, através de leitura, reflexão, resolução de exercícios, discussão com orientador e produção de texto lógico formal, se aprofunde no desenvolvimento de suas habilidades de pesquisa e autonomia para se tornar mais apto a seguir carreira acadêmica, já que este é seu intento. E em segundo lugar, mas não menos importante, criar um texto matemático que apresente o tema de forma agradável, apresentando um breve esboço da teoria dos corpos finitos, e mostrando como ela pode ser acessível a estudantes a nível de graduação, e como ela pode ser aplicada para tratar de elementos primitivos e normais. Em terceiro lugar, uma vez que o aluno adquira certa maturidade no tema de estudo, possa

colaborar nos projetos nos quais o orientador esteja trabalhando no momento.

Metodologia

O aluno estudará a estrutura de corpos finitos, polinômios sobre corpos finitos e somas exponenciais utilizando como referência o texto [1, Finite fields] e como livros de apoio os textos [2, Abstract algebra] e [3, Tópicos de álgebra]. O aluno apresentará semanalmente um seminário de uma hora com o material estudado durante a semana. Elementos primitivos e normais serão estudados a partir dos artigos de referências [4], [5], [6] e [7]. Além disso serão realizadas reuniões semanais de uma hora com o orientador para esclarecer dúvidas do aluno. Nos últimos meses da orientação o aluno irá participar dos projetos de pesquisa nos quais o orientador estará trabalhando. Serão também realizadas revisões bibliográficas para acrescentar conhecimentos atualizados. Mensalmente o aluno irá apresentar os resultados básicos a alunos de graduação que estudam temas similares.

Avanço do trabalho até aqui

Até o presente momento o aluno avançou nos estudos seguindo o cronograma proposto, estudou o primeiro capítulo: Estrutura de corpos finitos, dentro do qual viu os tópicos: Caracterização dos corpos finitos, Raízes de polinômios irredutíveis, Traços, normas e bases, Raízes da unidade e polinômios ciclotômicos, Representação de elementos de corpos finitos e Teorema de Wedderburn. E também, o segundo capítulo: Polinômios sobre corpos finitos, onde viu os tópicos: Ordem de polinômios e polinômios primitivos, Polinômios irredutíveis, Construção de polinômios irredutíveis, Polinômios linearizados e Binômios e trinômios. Tendo cumprido portanto, aproximadamente 50% do cronograma.

A partir daqui o aluno continuará seguindo com o cronograma, o próximo capítulo a ser estudado será: Somas exponenciais, dentro do qual verá os tópicos: Caracteres, Somas de Gauss, Somas de Jacobi e Soma de caracteres com argumentos polinomiais. Em seguida, verá o capítulo: Elementos primitivos e normais, no qual passará por:

Caracterização de elementos primitivos, Número de elementos primitivos em corpos finitos, Ação do anel de polinômios sobre um corpo finito, Caracterização de elementos normais e Número de elementos normais em corpos finitos. E por fim passará para as conclusões do trabalho, reunindo todos os conhecimentos e iniciando uma breve exploração do artigos citados.

Referências

[1] R. LIDL and H. Niederreiter, "Finite fields," *Cambridge University Press, Reino Unido*, 1997.

[2] P. A. Grillet, "Abstract algebra," *Springer, New York*, 2007.

[3] I. N. Hernstein, "Tópicos de álgebra," *Universidade de São Paulo, São Paulo*, 1970.

[4] H. W. Lenstra and R. J. Schoof, "Primitive normal bases for finite fields," *Mathematics of Computation*, 1987.

[5] S. D. Cohen, "Pairs of primitive elements in fields of even order," *Finite fields and their applications*, 2014.

[6] R. K. Sharma and Anju, "Existence of some special primitive normal elements over finite fields," *Finite Fields and Their Applications*, 2017.

[7] R. K. Sharma and Anju, "On primitive normal elements over finite fields," *Asian-European Journal of Mathematics*, 2018.