CARACTERES SOBRE CORPOS FINITOS E APLICAÇÕES

LUCAS REIS[A] E SAVIO RIBAS[B]

1. Introdução

No minicurso **Caracteres sobre Corpos Finitos e Aplicações**, pretendemos introduzir conceitos e resultados básicos da Teoria de Caracteres e aplicá-los sobre Corpos Finitos, além de apresentar algumas de suas diversas aplicações.

Pretendemos cobrir todo o básico da teoria de caracteres sobre grupos abelianos (com foco em corpos finitos), demonstrando todos os resultados de forma que o minicurso seja quase totalmente autocontido, com poucos pré-requisitos acerca da teoria básica de corpos finitos.

Um caracter em um grupo abeliano multiplicativo G é um homomorfismo

$$\chi : G \to \mathbb{C}.$$

Se $G = \mathbb{F}_q$ (additivamente) ou $G = \mathbb{F}_q^*$ (multiplicativamente), onde $\mathbb{F}_q$ é o corpo com q elementos, temos um caracter sobre um corpo finito.

Existem diversas referências que podem cobrir o básico sobre caracteres como, por exemplo, a "bíblia" de corpos finitos [6].

2. Temas a serem abordados

Caracteres formam uma poderosa ferramenta em Álgebra e Combinatória e podem ser aplicados em diversos problemas de existência e contagem de elementos, especialmente em corpos finitos. Caracteres são amplamente utilizados também em Teoria dos Números, em especial na Teoria do Crivo e no Teorema dos Números Primos em Progressão Aritmética (ver, por exemplo, [3]). No minicurso, abordaremos alguns dos problemas sobre corpos finitos, que podem ser adequados para um público-alvo em nível básico ou intermediário. Dentre as sugestões, podemos destacar alguns problemas clássicos:

- **Lei da Reciprocidade Quadrática:** Sejam p um número primo e $a \in \mathbb{Z}$. Definimos o símbolo de Legendre como:

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{se } x^2 \equiv a \pmod{p} \text{ tem solução em } \mathbb{Z}_p^*, \\ 0, & \text{se } p \mid a, \\ -1, & \text{caso contrário.} \end{cases}$$

É possível mostrar que $(\frac{a}{p})$ é uma função completamente multiplicativa em a, formando, portanto, um caracter módulo p. A Lei da Reciprocidade Quadrática afirma que se p e q são primos ímpares distintos então

$$\left(\frac{q}{p}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

Em outras palavras, a Lei da Reciprocidade Quadrática relaciona a existência de soluções de $x^2 \equiv q \pmod{p}$ com a existência de soluções de $y^2 \equiv p \pmod{q}$. É possível também determinar os valores de $(\frac{-1}{p})$ e $(\frac{2}{p})$. No minicurso, vamos demonstrar a Lei da Reciprocidade Quadrática (veja [6, Capítulo 5]).

Com ideias análogas e um pouco mais de trabalho, é possível estudar as equações de grau superior, como as cúbicas $x^3 \equiv a \pmod{p}$ e biquadráticas $x^4 \equiv a \pmod{p}$, mas não abordaremos essa parte no minicurso.

- **Equações Diagonais:** Uma equação diagonal sobre um corpo finito $\mathbb{F}_q$ é uma equação da forma

$$c_1 x_1^{k_1} + \cdots + c_s x_s^{k_s} = b,$$

onde $k_1, \ldots, k_s \in \mathbb{Z}_{>0}$, $c_1, \ldots, c_s \in \mathbb{F}_q^*$ e $b \in \mathbb{F}_q$. O problema a ser tratado aqui é a enumeração das soluções da equação diagonal. No minicurso, vamos estudar o número de soluções, fornecendo cotas inferiores e superiores (veja [6, Capítulo 6]).

- **Problema de Waring sobre corpos finitos:** Seja $g(k, q)$ o menor inteiro positivo s tal que todo elemento $b \in \mathbb{F}_q$ possa ser escrito como soma de no máximo s potências k-ésimas em $\mathbb{F}_q$. O problema de determinar ou estimar $g(k, q)$ é chamado de Problema de Waring.

No minicurso, vamos estimar $g(k,q)$ (veja [7, Capítulos 6 e 7 e suas referências internas]).

- **Polinômios primitivos com traço prescrito:** Seja $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in \mathbb{F}_q[x]$. Definimos o *traço* de $p(x)$ como $\mathrm{Tr}(p(x)) = a_{n-1}$. Dizemos que um elemento α em uma extensão $\mathbb{F}_{q^n}$ é *primitivo* se $\langle\alpha\rangle = \mathbb{F}_{q^n}^*$, e nesse caso seu traço $\mathrm{Tr}_{q^n/q}(\alpha)$ será definido como o traço do seu polinômio mínimo. Equivalentemente,

$$\mathrm{Tr}_{q^n/q}(\alpha) = \alpha^{q^{n-1}} + \alpha^{q^{n-2}} + \cdots + \alpha^q + \alpha.$$

  Dizemos que $p(x)$ é *primitivo* se $p(x)$ for o polinômio mínimo de um elemento primitivo. No minicurso, vamos mostrar que, com raras exceções (q,n), dado $c \in \mathbb{F}_q$ existem polinômios primitivos $p(x)$ com $\mathrm{Tr}(p(x)) = c$, ou equivalentemente, existe elemento primitivo $\alpha \in \mathbb{F}_{q^n}$ com $\mathrm{Tr}_{q^n/q}(\alpha) = c$ (veja [1]).
- **Teorema da Base Normal Primitiva:** Este é um resultado profundo na teoria estrutural de corpos finitos e foi provado em completa generalidade somente após ser tratado via caracteres. Uma extensão $\mathbb{F}_{q^n}$ de $\mathbb{F}_q$ pode ser vista como um $\mathbb{F}_q$-espaço vetorial de dimensão n, possuindo, portanto, uma base. Uma base é dita *normal* se for da forma $\{\beta, \beta^q, \beta^{q^2}, \ldots, \beta^{q^{n-1}}\}$. Uma base normal primitiva é uma base normal como acima, onde $\langle\beta\rangle = \mathbb{F}_{q^n}^*$. O Teorema da Base Normal Primitiva afirma que para todo q potência de primo e todo inteiro positivo n, existe uma base normal primitiva de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$. No minicurso, vamos demonstrar este teorema (veja [2, 5]).

3. Público-alvo

O nível do minicurso é **intermediário**, adequado a estudantes em final de graduação, mestrado ou início de doutorado.

4. Pré-Requisitos

O minicurso será quase totalmente autocontido. Serão considerados pré-requisitos apenas os seguintes resultados básicos sobre corpos finitos, mas que serão relembrados rapidamente na Aula 1:

- Existência e "unicidade" de corpos finitos com q elementos, onde q é potência de primo;

- o grupo multiplicativo $\mathbb{F}_q^*$ é cíclico de ordem $q-1$;
- Extensão de corpos finitos;
- A extensão $\mathbb{F}_{q^n}$ de $\mathbb{F}_q$ pode ser vista como um espaço vetorial de dimensão n sobre $\mathbb{F}_q$.

5. Objetivos

5.1. **Objetivo Geral.**

- O objetivo deste minicurso é o de introduzir conceitos e resultados básicos da Teoria de Caracteres sobre Corpos Finitos e apresentar algumas de suas diversas aplicações.

5.2. **Objetivos Específicos.**

- Apresentar os conceitos e resultados básicos da teoria de caracteres;
- Apresentar as somas de Gauss e de Jacobi;
- Aplicar os caracteres sobre corpos finitos;
- Aplicar os caracteres às equações diagonais;
- Aplicar os caracteres ao problema de Waring;
- Aplicar os caracteres aos polinômios primitivos com traço prescrito;
- Demonstrar o Teorema da Base Normal Primitiva.

6. Conteúdo programático

O minicurso consta de 5 aulas, cada uma com duração de 50 minutos.
A seguir temos um resumo do programa a ser ministrado.

6.1. **Aula 1: Resultados básicos sobre caracteres e somas de caracteres.**

(i) Revisão sobre corpos finitos;
(ii) Caracteres de um grupo abeliano: definição e exemplos;
(iii) O grupo dual;
(iv) Relações de ortogonalidade;
(v) Somas de Gauss;
(vi) Somas de Jacobi.

6.2. **Aula 2: A Lei da Reciprocidade Quadrática e caracteres sobre corpos finitos.**

(i) Símbolo de Legendre;
(ii) Lei da Reciprocidade Quadrática via caracteres;
(iii) Corpos Finitos: somas de caracteres aditivos e multiplicativos.

6.3. **Aula 3: Equações Diagonais e o Problema de Waring.**

(i) Equações diagonais;
(ii) Problema de Waring sobre corpos finitos; e/ou
(iii) Vamos mencionar também alguns resultados de artigos listados na Subseção 6.3 de [7]).

6.4. **Aula 4: Polinômios primitivos com traço prescrito.**

(i) Polinômios primitivos com traço prescrito [1].

6.5. **Aula 5: O Teorema da Base Normal Primitiva.**

(i) O Teorema da Base Normal Primitiva [2, 5].

Observação. Os resultados principais a serem demonstrados nas Aulas 4 e 5 requerem uma pequena parte de verificação computacional. Apesar de não discutirmos todos os detalhes, falaremos um pouco sobre os algoritmos de busca usados nas suas demonstrações que podem ser implementados em Softwares básicos como o SageMATH.

References

[1] S.D. Cohen. Primitive elements and polynomials with arbitrary trace. *Discrete Math.*, 83(1): 1–7, 1990.
[2] S.D. Cohen and S. Huczynska. The primitive normal basis theorem – without a computer. *J. London Math. Soc.*, 67(1): 41–56, 2003.
[3] H. Davenport. Multiplicative Number Theory. *Graduate Texts in Mathematics*, second edition, Springer-Verlag, 1980.
[4] W. Diffie and M. Hellman. New directions in cryptography. *IEEE Trans. Information Theory*, 22(6): 644–654, 1976.
[5] H.W. Lenstra Jr and R.J. Schoof. Primitive normal bases for finite fields. *Math. Comp.*, 48(177): 217–231, 1987.
[6] R. Lidl and H. Niederreiter. *Finite Fields*, volume 20 of *Enyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, second edition, 1997.

[7] G.L. Mullen, D. Panario; Handbook of Finite Fields, *Boca Raton: Taylor and Francis*, 2013.

(A) Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, São Carlos, SP 13560-970, Brazil

Email address: lucasreismat@gmail.com

(B) Departamento de Matemática, Instituto de Ciências Exatas e Biológicas, Universidade Federal de Ouro Preto, Ouro Preto, MG 35400-000, Brazil.

Email address: savio.ribas@ufop.edu.br