Revista de Divulgação Científica em
Ciências Exatas e Tecnológicas
PORANDU
Vol. x, n. y, 2018, pg. z-w

Fundamentos de Geometria de Galois e aplicação em códigos

Resumo.Este trabalho incide no estudo da geometria de Galois e aplicações em códigos corretores de erros. Serão exploradas e estudadas, os seguintes temas: planos projetivos finitos, a teoria de códigos e as relações existentes entre a geometria de Galois. A Geometria de Galois é definida como sendo espaços projetivos sobre corpos finitos. Já a teoria dos códigos dedica-se a detectar e a corrigir erros que são introduzidos quando são transmitidas as mensagens. Por meio de dois modelos estudados de planos projetivos, um de ordem dois e outro de ordem três foi feita a compreensão dessa geometria. A partir disso, houve uma discussão em torno da existência de planos projetivos de outras ordens. Mediante o exposto, foi desenvolvida a conexão entre a geometria de Galois e a teoria de códigos.

Palavras-chave. Geometrias finitas, planos projetivos, códigos corretores de erros.

Abstract. This work focuses on the study of Galois geometry and applications in brokers errors codes. Will be explored and studied the following topics: finite projective planes, coding theory and the relations between the Galois geometry. Galois geometry is defined as projective spaces over finite fields. Already the theory of codes is dedicated to detect and correct errors that are introduced when they are transmitted messages. Through two models studied projective plans, one of order two and one of three order was made to understand this geometry. From this, there was a discussion around the existence of projective planes of other orders. By the above, the connection between the Galois geometry and coding theory.

1 Introdução

O estudo da geometria de Galois teve como um dos pioneiros o matemático italiano Gino Fano (1871-1952), no entanto, o termo geometria de Galois aparece pela primeira vez em um artigo do também matemático italiano Beniamino Segre (1903-1977) em que ele se refere ao plano projetivo finito como plano de Galois (matemático francês 1811-1832), com o objetivo de enfatizar que uma abordagem analítica da geometria projetiva finita é baseada em corpos finitos de Galois e suas extensões.

As geometrias de Galois são definidas em espaços com um número finito de pontos e retas, e atualmente essa teoria está relacionada com aplicações em algumas áreas da matemática, como por exemplo, teoria de códigos, criptografia, teoria de grupos e combinatória.

Já os códigos corretores de erros são cruciais para armazenamento e transmissão de informação. A proposta desse texto é falar em linhas gerais dessa teoria, enfatizando na conexão entre planos projetivos finitos e a teoria de códigos. Para tal entendimento, será explorado um código, a partir de um plano projetivo de ordem dois.

Assim, o presente trabalho teve por objetivos gerais, pesquisar e desenvolver estudos na geometria de Galois e aplicação em códigos corretores de erros, e propiciar a integração entre as áreas científicas, geometria, álgebra, computação.

2 Planos projetivos finitos

Um plano projetivo finito consiste em um conjunto de pontos, um conjunto de retas e uma relação entre pontos e retas chamada incidência, que satisfaça o seguinte sistema axiomático, onde $n > 1$.

Axiomas:

A_1: Existe pelo menos quatro pontos não colineares três a três.

A_2: Existe pelo menos uma reta incidente em n+1 pontos distintos.

A_3: Dados dois pontos distintos, existe exatamente uma reta incidente em ambos.

A_4: Dados duas retas distintas, existe pelo menos um ponto incidente com ambas.

O axioma A_4 nos garante a não existência de retas paralelas nesse sistema axiomático, o que difere essa geometria da euclidiana. Note que nessa geometria as retas podem ser representadas também por curvas.

Agora apresentaremos alguns teoremas que são essenciais para o entendimento dessa geometria:

Teorema 1: Num plano projetivo de ordem n, cada reta incide em exatamente $n + 1$ pontos.

Teorema 2: Num plano projetivo de ordem n, cada ponto é incidente em $n + 1$ retas.

Teorema 3: Um plano projetivo de ordem n, tem exatamente $n^2 + n + 1$ pontos e $n^2 + n + 1$ retas.

A partir desses resultados, juntamente com os axiomas, conseguimos construir exemplos de planos projetivos.

Exemplo: Consideremos o plano projetivo de ordem 2. Pelos teoremas 1 e 2 sabemos que cada reta incide em 3 pontos e cada ponto incide em 3 retas. Além disso, o teorema 3 nos garante a existência de exatamente 7 pontos e de 7 retas. Diante disso, obtemos o seguinte modelo:

A construção desse modelo foi feita por meio de aplicações dos axiomas e teoremas sobre plano projetivo.

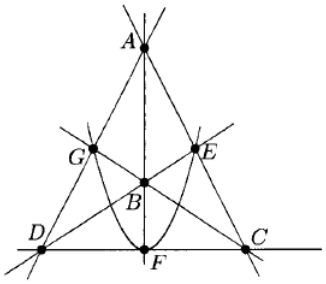

Figura 1: um possível modelo para o plano projetivo de ordem 2

Exemplo: Considere agora o plano projetivo de ordem 3. De modo análogo a construção do modelo anterior, sabemos que cada reta incide em 4 pontos e cada ponto incide em 4 retas. Tendo 13 pontos e 13 retas, segue um possível modelo:

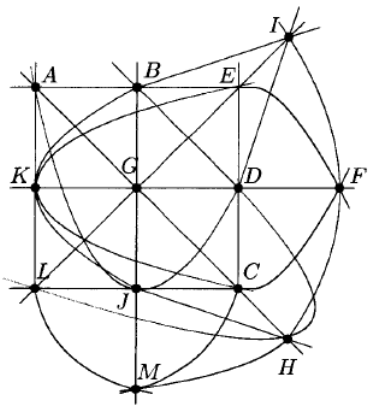

Figura 2: modelo para o plano projetivo de ordem 3

Apresentamos acima dois planos projetivos, um de ordem 2 e outro de ordem 3. Será que existem outros? Raposo (2014) apresenta alguns resultados que nos ajudam a responder essa questão.

Teorema 4: Existe um plano projetivo de ordem q para cada potência de primo q.

É fácil perceber que esse teorema diz respeito às ordens de planos projetivos que certamente existem. Já o próximo teorema irá nos garantir quais ordens de planos projetivos não existem.

Teorema 5: (Teorema de Bruck-Ryser). Seja n um número inteiro positivo. Se n $\equiv$ 1 ou 2 (mod 4), e não é a soma de dois quadrados, então não existe plano projetivo de ordem n.

Para que possamos discutir sobre a existência de planos projetivos de quaisquer ordens, considere os planos projetivos de ordem menor que 15. É fácil ver que existem as ordens 2, 3, 4, 5, 7, 8, 9, 11 e 13 existem, garantidos pelo teorema 4. Já com o teorema 5 concluímos que os planos projetivos de ordens 6 e 14 não existem. Embora tenhamos feito essa análise pautada nos teoremas 4 e 5, a respeito das ordens 10 e 12 não podemos afirmar nada.

3 Códigos corretores de erros

Um código corretor de erros é, em essência, um modo organizado de acrescentar algum dado adicional a cada informação que se queira transmitir ou armazenar, que permita, ao recuperar a informação, detectar e corrigir erros. A Teoria de Códigos é um campo de investigação atual e muito ativo, tanto do ponto de vista científico quanto tecnológico.

A Teoria de Códigos Corretores de Erros foi fundada pelo matemático C. E. Shannon, do Laboratório Bell, num trabalho publicado em 1948. Inicialmente, os maiores interessados em Teoria de Códigos foram os matemáticos que a desenvolveram consideravelmente nas décadas de 50 e 60.

A fim de fazer a conexão dos planos projetivos finitos com os códigos precisaremos recorrer à alguns resultados da teoria de códigos para que possamos utilizar elas a diante.

Assumiremos alguns resultados da álgebra, na qual não entraremos em detalhes (corpo, espaço vetorial, dimensão, etc.).

Seja A um conjunto finito com q elementos ($|A| = q$), um código corretor de erros, C, de comprimento n é um subconjunto de A^n. Cada elemento de C é chamado palavra-código (no alfabeto A).

Se o conjunto A for um corpo finito e C for um subespaço vetorial de dimensão k de A^n, teremos que $|C| = q^k$.

Agora apresentaremos uma sequência de definições que nos serão úteis para o entendimento da conexão entre a teoria de códigos e os planos projetivos finitos.

Definição: Um código linear binário, de comprimento n, é um subespaço vetorial de F_2.

Definição: Uma matriz geradora G para um código linear C é uma matriz cujas linhas formam uma base para C.

Dizemos que a matriz geradora está na forma padrão se G=[$I_(kxk)$ $B_(k(n-k))$].

Agora já temos as definições necessárias para abordar o exemplo de códigos a partir dos planos projetivos.

4 Relação entre planos projetivos e códigos

Para que possamos compreender a relação existente entre os planos projetivos finitos e os códigos iremos expor um exemplo de como obter um código a partir de um plano projetivo, por meio da matriz de incidência do plano projetivo finito.

Uma matriz de incidência de um plano projetivo é uma matriz quadrada de ordem n^2+n+1 onde as retas e os pontos são representados respectivamente pelas colunas e linhas da matriz, de tal forma que colocamos 1 se o ponto pertence à reta e 0 se não pertence.

Dos planos projetivos finitos, já sabemos que o menor plano é o de ordem $n = 2$ que tem 7 pontos e 7 retas. Onde não há retas paralelas; na verdade, cada par de retas compartilha um único ponto e cada par de pontos é contido por uma única reta. Além de que cada reta contém 3 pontos e cada ponto está em 3 retas.

Exemplo: Tomando o plano projetivo de ordem 2, a relação de incidência pode ser representada pela seguinte tabela de incidência:

	ABF	ACE	ADG	BCG	BDE	CDF	EFG
A	1	1	1	0	0	0	0
B	1	0	0	1	1	0	0
C	0	1	0	1	0	1	0
D	0	0	1	0	1	1	0
E	0	1	0	0	1	0	1
F	1	0	0	0	0	1	1
G	0	0	1	1	0	0	1

Tabela 1: tabela de incidência do plano projetivo de ordem 2

Recorrendo a tabela 1 obtemos a seguinte matriz de incidência: Matriz de incidência do plano projetivo de ordem 2:

$$M_2 = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$

Observação: a utilização do índice 2 é unicamente pelo fato de estarmos nos referindo ao plano projetivo dessa ordem.

Nossa intenção com essa matriz de incidência é obter uma matriz geradora para o código correspondente. Mas não queremos essa matriz geradora de qualquer forma, procuramos por conveniência obter ela em sua forma padrão. Fazendo então operações elementares com a matriz M_2 iremos obter uma matriz linearmente independente (L.I.):

$$G_2 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

Além de L.I. essa matriz também é geradora do código C_2, logo forma uma base do código. Contudo, temos que esse código possui $2^4 = 16$ palavras código, de tal forma que as palavras código são obtidas das combinações das linhas de G_2:

0000000
1000011
0100101
0010110
0001111
1100110
1010101
1001100
0110011
0101010
0011001
1110000
1101001
1011010
0111100
1111111

Desse exemplo, podemos ver como produzir códigos corretores de erros a partir de um plano projetivo.

Referências

[1] A. P. Z. RAPOSO, *Geometrias Finitas*. Dissertação de Mestrado em Matemática para o ensino, Escola de Ciências e Tecnologia, Universidade de Évora, 2014.

[2] C. C. LAVOR, M. M. S. ALVES, R. M. SIQUEIRA, and S. I. R. COSTA, "Notas em Matemática Aplicada; v. 21. in: Uma Introdução à Teoria de Códigos.," São Carlos, SP : SBMAC, 2006.

[3] L. B. Lima, *Contribuições em codificação no espaço projetivo e proposta de códigos quânticos de subespaços na grassmanniana*. Tese doutorado em engenharia elétrica, Faculdade de Engenharia Elétrica e de Computação, Unicamp, Campinas, 2017.

[4] L. LOVÁSZ, J. PELIKÁN, and K. VESZTERGOMBI, *Matemática Discreta*. Textos Universitários SBM, 2 ed., 2013.

[1, 2, 3, 4]