Revista de Divulgação Científica em
Ciências Exatas e Tecnológicas
PORANDU
Vol. 3, n. 1, 2019, pg. 17-24

Fundamentos de Geometria de Galois e aplicação em códigos

G. S. ROMAN[1,*], L. B. LIMA [1,†] .

[1] Universidade Federal de Mato Grosso do Sul, CPAQ, MS, Brasil,

Submetido em 15/11/2018; Aceito em 13/12/2018; Publicado em 06/09/2019

Resumo. Este trabalho incide no estudo da geometria de Galois e aplicações em códigos corretores de erros. Serão estudados os seguintes temas: planos projetivos finitos, a teoria de códigos e as relações existentes com 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 mensagens. Por meio de dois modelos de planos projetivos, um de ordem dois e outro de ordem três, foi feita a compreensão dessa geometria. A partir disso, discutimos a existência de planos projetivos de outras ordens. Mediante o exposto, discutimos a conexão entre a geometria de Galois e a teoria de códigos, através do plano projetivo de ordem dois.

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

Abstract. This work focuses on the study of Galois geometry and applications in brokers error codes. The following topics will be studied: finite projective plans, code theory and existing relations with Galois geometry. Galois geometry is defined as projective spaces over finite fields. Code theory is dedicated to detecting and correcting errors that are introduced when messages are transmitted. By means of two models of projective planes, one of order two and the other of order three, the understanding of this geometry was made. From this, we discuss the existence of projective plans of other orders. Through the above, we discuss the connection between Galois geometry and code theory, through the projective plan of order two.

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

*gaby-roman2011@hotmail.com
†leandro.lima@ufms.br

analítica da geometria projetiva finita é baseada em corpos finitos de Galois e suas extensões. Para maiores detalhes, veja [1] e suas referências. E para detalhes históricos sobre Galois e sua teoria, veja [2].

Segundo Evens [3], Évariste Galois, pode ser considerado como um meteoro, que riscou o firmamento matemático com brilho intenso e matinal, para depois, súbita e pateticamente, extinguir-se em morte prematura, deixando material de valor extraordinário para ser trabalhado pelos matemáticos das gerações futuras.

Tal material, teve seu início de produção durante a adolescência de Galois, quando este, passou a construir uma teoria com aplicações sobretudo à teoria das equações algébricas. Um dos resultados mais salientes desta teoria é a impossibilidade de resolução por meio de radicais de equações gerais de grau maior ou igual a cinco. Para uma leitura mais profunda sobre o assunto, recomendamos as referências [4, 5, 6].

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. Os pormenores sobre teoria de códigos e criptografia podem ser encontrados, por exemplo, em [7, 8, 9, 10, 11, 12].

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.

Por fim, o presente trabalho tem, por objetivos gerais, apresentar a conexão existente entre a geometria de Galois e a aplicação em códigos corretores de erros, elucidando assim a integração entre áreas científicas distintas como geometria, álgebra e computação.

2 Planos projetivos finitos

Iremos ao longo desta secção enunciar os principais resultados sobre planos projetivos que nos ajudam a compreender esta geometria. Finalizaremos com uma breve discussão sobre a existência de planos projetivos. Todos os resultados e demonstrações dos teoremas apresentados nessa seção podem ser encontradas em [13], assim como nas referências clássicas já citadas.

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 $n > 1$.

Sistema Axiomático 2.1. *:*

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

Teorema 2.2. *Num plano projetivo de ordem n, cada ponto é incidente em* $n + 1$ *retas.*

Teorema 2.3. *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.

Consideremos o plano projetivo de ordem 2. Pelos teoremas (2.1) e (2.2) sabemos que cada reta incide em 3 pontos e cada ponto incide em 3 retas. Além disso, o teorema (2.3) nos garante a existência de exatamente 7 pontos e de 7 retas. Diante disso, obtemos o seguinte modelo:

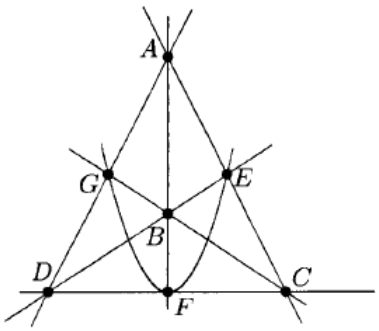

Figura 1: Um possível modelo para o plano projetivo de ordem 2
Fonte: [13], pp.69 - figura 3.15

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

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:

Apresentamos acima dois planos projetivos, um de ordem 2 e outro de ordem 3, os detalhes da construação de ambos exemplos podem ser encontrados em [13].

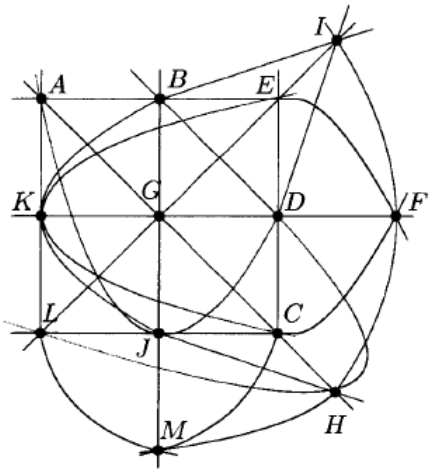

Figura 2: Modelo para o plano projetivo de ordem 3
Fonte: [13], pp.71 - figura 3.16

Diante disso, uma pergunta natural é: será que existem outroas ordens de planos projetivos? Em [13] temos alguns resultados que nos ajudam a responder essa questão.

Teorema 2.4. *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 2.5. *(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 (2.4). Já com o teorema (2.5) concluímos que os planos projetivos de ordens 6 e 14 não existem. Embora tenhamos feito essa análise pautada nos teoremas (2.4) e (2.5), 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. Para uma visão geral sobre teoria de códigos, veja [14].

A teoria de Códigos Corretores de Erros foi fundada pelo matemático *C. E. Shannon*, do Laboratório Bell, num trabalho publicado em 1948 [15]. Posteriormente, em 1949, junto com o também matemático *W. Weaver*, publicaram um livro contendo o artigo original de *Shannon*, entendível para não-especialistas. 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, todos esses resultados podem ser encontrados em [13]. Assumiremos alguns resultados da álgebra, na qual não entraremos em detalhes (corpo, espaço vetorial, dimensão, etc.), mas todas as definições necessárias estão em [13].

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 3.1. *Designamos por F_2 o conjunto $\{0, 1\}$ munido pelas operações de adição e multiplicação definidas pelas tabelas seguintes:*

$+$	0	1
0	0	1
1	1	0

$\times$	0	1
0	0	0
1	0	1

Além disso, esse conjunto satisfaz as condições de corpo. Este corpo é menos conhecido, mas é extremamente útil na teoria dos códigos.

Definição 3.2. *Um código linear binário, de comprimento n, é um subespaço vetorial de F_2.*

Definição 3.3. *Uma matriz geradora G para um código linear C é uma matriz cujas linhas formam uma base para C.*

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.

Vamos considerar o seguinte exemplo, tomando o plano projetivo de ordem 2, sua 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

As linhas dessa tabela representam os pontos, e as colunas representam as retas do plano projetivo de ordem 2. Um 1 na linha i e coluna j significa que o ponto está incidindo na reta da posição j, enquanto um 0 significa que eles não são incidentes. Recorrendo a tabela (1) para obter a matriz de incidência referente ao plano projetivo de ordem 2. 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. Desse modo, segue que:

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

Observação 4.1. *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.

5 Considerações Finais

Neste trabalho, o objetivo foi apresentar e elucidar sobre a conexão existente entre a teoria de códigos e a teoria de Galois, por meio de aplicações em códigos corretores de erros. Apresentamos exemplos de como obter um código a partir de um plano projetivo. Ainda que a teoria de Galois clássica tem um aspecto maravilhosamente fechado e perfeito, sua relação com diferentes áreas abre novos horizontes e a leva à vanguarda da investigação.

Referências

[1] B. SEGRE, "On Galois geometries," in *Proc. Intern. Congr. Mathematicians*, (Cambridge, 1958), pp. 488–499, 1960.

[2] P. NEUMANN, "The mathematical writings of Èvariste Galois," *European Mathematical Society*, 2011.

[3] H. EVES, "Introdução à história da matemática, tradução: Higino H. Domingues. 3. reimpressão," *Campinas. Ed. da UNICAMP*, 2008.

[4] H. EDWARDS, *Galois Theory.* Springer, 1998.

[5] I. STEWART, *Galois Theory.* Chapman and Hall, 1989.

[6] J. H. (Editor), *Handbook of Algebra*, vol. 5. Elsevier, 2008.

[7] B. F. C. CARSTENSEN and G. ROSENBERG, *Abstract Algebra. Apliccations to Galois Theory, Algebraic Geometry and Cryptography, Sigma series in Pure Mathematics 11.* De Gruyter, 2011.

[8] N. KOBLITZ, *Algebraic Methods of Criptography.* Springer, 1998.

[9] S. I. R. COSTA, R. M. SIQUEIRA, C. C. LAVOR, and M. M. S. ALVES, "Uma Introdução à Teoria de Códigos," *Sociedade Brasileira de Matemática Aplicada e Computacional, Sção Carlos-SP*, 2006.

[10] R. G. AYOUB, "Paolo ruffini's contributions to the quintic," *Archive for history of exact sciences*, vol. 23, no. 3, pp. 253–277, 1980.

[11] C. GREITHER and D. K. HARRISON, "A galois correspondence for radical extensions of fields," *Journal of Pure and Applied Algebra*, vol. 43, no. 3, pp. 257–270, 1986.

[12] B. M. KIERNAN, "The development of galois theory from lagrange to artin," *Archive for History of Exact Sciences*, vol. 8, no. 1-2, pp. 40–154, 1971.

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

[14] R. HILL, *A First Course in Coding Theory.* Oxford University Press, 1986.

[15] C. E. SHANNON, "A Mathematical Theory of Communication," *The Bell System Technical Journal*, vol. 27, pp. 379–423, 7 1948.