Revista Sergipana de Matemática e Educação Matemática

https://doi.org/10.34179/revisem.v11i1.24519

OS PRIMOS DISCRETOS DO PLANO AFIM

THE DISCRETE COUSINS OF THE AFFINE PLANE

Emerson Luiz do Monte Carmelo
Universidade Estadual de Maringá - UEM
elmcarmelo@uem.br

Mateus Barbosa Kopp Webber
Universidade Estadual de Maringá - UEM
mateus.kopp@hotmail.com

Pedro Ricardo Pereira Melo
Universidade Estadual de Maringá - UEM
pedroricardopereiramelo14@gmail.com

Comunicado por M. Alegri

Resumo

As geometrias finitas formam elos fundamentais entre a geometria clássica, a álgebra abstrata e a análise combinatória. Este artigo de divulgação tenta capturar um breve retrato deste caráter multidisciplinar de certas estruturas geométricas sobre conjuntos finitos. Combinando uma abordagem axiomática com argumentos combinatórios, discutimos condições de incidência e paralelismo que caracterizam os planos afins finitos, "os primos eremitas" do aclamado plano afim euclidiano. Apresentamos a construção de tais planos a partir de corpos de Galois. Além da sua importância matemática, convém mencionar que geometrias finitas emergem em aplicações contemporâneas, como na teoria de códigos corretores de erros, em planejamentos de experimentos estatísticos, além de jogos lúdicos.

Palavras-chave: Geometria finita, plano afim, independência de axiomas, bijeções, aritmética modular.

Abstract

This open access article is licensed under
a Creative Commons Attribution-NonCommercial 4.0.

Finite geometries form fundamental links between classical geometry, abstract algebra, and combinatorics. This popularization article attempts to capture a brief portrait of this multidisciplinary character of certain geometric structures on finite sets. Combining an axiomatic approach with combinatorial arguments, we discuss incidence and parallelism conditions that characterize finite affine planes, the "hermit cousins" of the acclaimed Euclidean affine plane. We present the construction of such planes from Galois fields. In addition to their mathematical importance, it is worth mentioning that finite geometries emerge in contemporary applications such as error-correcting codes theory, statistical experiment design, as well as in recreational games.

Keywords: finite geometry, affine plane, axiom independence, bijections, modular arithmetic.

1 Introdução

A Geometria euclidiana prevaleceu como referência principal até o Renascimento, moldando nossa compreensão do espaço como algo contínuo e infinito. Entretanto, artistas do século XV, ao tentarem retratar o mundo com fidelidade naturalista, perceberam que a intuição euclidiana não bastava para explicar como retas paralelas parecem convergir num ponto de fuga. Nascia ali a semente da Geometria projetiva. Apesar de motivada pela arte, foi apenas em 1822 que esta geometria se consolidou devido aos estudos sistemáticos de Jean-Victor Poncelet, sinalizando que a hegemonia de Euclides não era inabalável.

O ponto central dessa ruptura foi o famoso 5° postulado de Euclides, cujo enunciado segue:

> "Se uma reta, ao cortar duas outras, forma ângulos internos no mesmo lado cuja soma é menor do que dois ângulos retos, então as duas retas, se continuadas, encontrar-se-ão no lado onde estão os ângulos cuja soma é menor do que dois ângulos retos."

Tal postulado é equivalente ao axioma das paralelas:

> "Por um ponto exterior a uma reta passa uma única paralela" (ver [2]).

Alvo de discussões e polêmicas que perduraram por mais de 2.000 anos, acreditou-se que este postulado dependesse dos demais, frustrando muitas tentativas de demonstração feitas por grandes matemáticos, como o lendário Gauss. A reviravolta veio no século XIX, quando o russo Nikolai Lobachevsky concebeu uma geometria tão peculiar como impactante. Ele mostrou ser possível criar um sistema lógico consistente em que,

por um ponto fora de uma reta, passam infinitas paralelas. Recomendamos a leitura de [5] sobre este marco na história da Matemática e suas consequências.

Ao fim do século XIX, a necessidade de testar a independência de sistemas axiomáticos levou ao surgimento das Geometrias finitas. Matemáticos como Kirkman, Von Staudt, Fano, Veblen começaram a explorar estruturas com quantidade finita de pontos por meio axiomático ou utilizando ferramentas algébricas como coordenadas homogêneas sobre corpos finitos.

Entretanto, a área ganhou uma nova dimensão no final da década de 1930. O matemático indiano R.C. Bose revolucionou o campo ao introduzir um enfoque combinatório. Bose [3] percebeu que pontos e retas poderiam ser vistos como "blocos" de um delineamento experimental, transformando tais geometrias em uma ferramenta poderosa não apenas para a matemática pura, mas também para a Estatística.

Se o universo é contínuo e infinito, parece fazer sentido considerar as geometrias finitas como herméticas. No entanto, tais geometrias sustentam invisivelmente a fundamentação de tecnologias essenciais na vida moderna. Aplicações vitais na verificação e transmissão de informações, na construção de códigos corretores de erros (que garantem a integridade de dados digitais), em planejamentos estatísticos e na criptografia moderna ilustram o uso de tais geometrias. Ao leitor interessado, consultar [10].

Além do rigor matemático e dos desenvolvimentos tecnológicos, uma aplicação surpreendentemente tátil das geometrias finitas aparece em jogos de cartas atuais, cujas propriedades de incidência suportam o núcleo das regras. O popular jogo "Dobble" (ou "Spot It!") é uma aplicação direta de um plano projetivo finito (ver [6, 11]), enquanto o jogo "SET" depende essencialmente da estrutura de um espaço afim de quatro dimensões sobre um corpo de três elementos (anel dos inteiros módulo 3).

Este artigo de divulgação visa meramente despertar o leitor para um assunto pouco conhecido pela comunidade matemática brasileira. Sob um olhar teórico, geometrias finitas apresentam um caráter multidisciplinar, pois argumentos frequentemente interligam conceitos geométricos, combinatórios e algébricos. Este trabalho tenta passar um pouco deste aspecto. Iniciamos na Seção 2 com uma breve discussão sobre alguns axiomas basilares. Na Seção 3, exploramos axiomas independentes por meio de modelos. Na Seção 4, descrevemos algumas propriedades de planos afins e uma construção de tais planos usando aritmética modular.

2 Alguns fundamentos das Geometrias finitas

Nesta seção, visamos discutir alguns fundamentos e exemplos de geometrias finitas. Há uma vasta literatura em inglês sobre o tópico, mas recomendamos [4] por sua abordagem axiomática e introdutória. Na nossa língua materna, [8] apresenta um enfoque

mais axiomático, enquanto [9, 12] também discutem uma visão combinatória.

Iniciamos com um conjunto finito não vazio X, cujos elementos são chamados de *pontos*. Seja $\mathcal{L}$ uma família não vazia de subconjuntos de X, cujos elementos são chamados de *retas*. Geralmente, adotamos letras maiúsculas P, Q, R para nos referirmos a pontos, e minúsculas r, s, t, para retas.

Definição 2.1. Um *espaço* $S = (X, \mathcal{L})$ é formado pelo conjunto de pontos X e pela família de retas $\mathcal{L}$ que satisfazem os axiomas "previsíveis":

A: cada reta tem pelo menos dois pontos;

B: dados dois pontos distintos, existe no máximo uma reta que os contém.

Por simplicidade, a definição acima difere ligeiramente daquela usada no livro [4], a saber, "espaço linear parcial". A partir de agora, investigamos quais regras fundamentais são necessárias para construir alguns espaços e como a intuição geométrica se comporta quando confrontamos a geometria euclidiana com certas geometrias finitas.

Exemplo 2.2. Consideremos dois axiomas adicionais.

1. Cada reta tem 2 pontos;
2. Cada ponto incide em duas retas.

Uma rápida análise confirma que o espaço $S_1 = (X_1, \mathcal{L}_1)$ formado por $X_1 = \{0, 1, 2, 3\}$ e pelo conjunto de retas $\mathcal{L}_1 = \{\{0, 1\}, \{1, 2\}, \{2, 3\}, \{0, 3\}\}$ satisfaz ambos os axiomas acima. Para visualizarmos uma geometria, cada reta pode ser representada por um segmento de reta ou por uma curva diferencial ligando seus pontos. Segue abaixo uma possível representação de S_1.

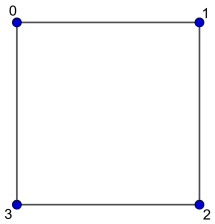


Figura 1: Representação de S_1.

Exemplo 2.3. O modelo apresentado no Exemplo 2.2 não é o único a satisfazer os axiomas propostos. De fato, selecionamos o espaço $S_2 = (X_2, \mathcal{L}_2)$ definido por $X_2 = \{0, 1, 2, 3, 4, 5\}$ e pelas retas $\mathcal{L}_2 = \{\{0, 1\}, \{1, 2\}, \{2, 3\}, \{3, 4\}, \{4, 5\}, \{0, 5\}\}$. É imediato verificar que esta estrutura também atende às condições exigidas.

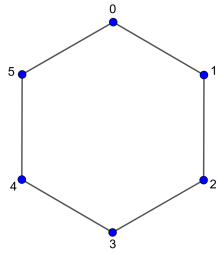


Figura 2: Representação de S_2.

Há diversas maneiras de definirmos paralelismo na geometria euclidiana: por meio de ângulos ou por distâncias (ver [2]). Como não há ordem entre os elementos de uma reta (um singelo conjunto), um espaço finito não suporta conceitos correlatos como ângulo e distância. Lembremos da inofensiva afirmação: duas retas distintas e paralelas não se interceptam. Com o mesmo tratamento a um espaço $S = (X, \mathcal{L})$, diremos que duas retas r, s em $\mathcal{L}$ são *paralelas*, e denotaremos por $r//s$, se $r = s$ ou $r \cap s = \emptyset$. Caso contrário, tais retas são *concorrentes*.

Retornando ao espaço $S_1 = (X_1, \mathcal{L}_1)$, constatamos que $\{0, 1\}//\{2, 3\}$ e $\{1, 2\}//\{0, 3\}$. Neste caso, quando dispomos as retas paralelas num mesmo conjunto, criamos naturalmente uma partição do conjunto de pontos. Aqui o paralelismo comporta-se como esperado.

Ao analisarmos o espaço $S_2 = (X_2, \mathcal{L}_2)$, a reta $\{0, 1\}$ é naturalmente paralela a $\{3, 4\}$. Contudo, a definição obriga que $\{0, 1\}$ também seja paralela às retas $\{2, 3\}$ e $\{4, 5\}$, ferindo a nossa intuição. Mais preocupante, como a reta $\{2, 3\}$ não é paralela a $\{3, 4\}$, o paralelismo não induz uma relação de equivalência.

Dito isso, há alguma condição que torna o paralelismo em uma relação de equivalência? Se sim, será que o espaço S_1 satisfaz tal condição?

Os dois exemplos acima abrem portas para observações importantes. A transição da geometria clássica para a finita exige que abandonemos a dependência visual do "desenho" contínuo para abraçarmos a geometria finita. Neste contexto, não nos importa a continuidade da reta, mas sim a relação de "pertinência": um ponto incide em uma reta, e uma reta contém um ponto. É claro que uma boa representação ajuda na elucidação e entendimento, mas devemos sempre ficar atentos aos conjuntos.

A intuição geométrica, frequentemente moldada pela tradição euclidiana, nos condiciona a aceitar como verdade absoluta que "por um ponto fora de uma reta, passa uma única reta paralela". No entanto, o universo das geometrias finitas oferece um terreno fértil para desafiarmos tais dogmas. Ao ajustarmos os axiomas, podemos construir estruturas onde a unicidade dá lugar à multiplicidade. Tal flexibilidade aparece no exemplo seguinte.

Exemplo 2.4. Ilustraremos uma geometria regida pelos seguintes axiomas:

1. Dados dois pontos distintos, existe uma única reta que os contém.
2. Dada uma reta t e um ponto $P \notin t$, existem exatamente **três** retas passando por P que são paralelas a t.

Para tanto, seja o espaço $S_3 = (X_3, \mathcal{L}_3)$ definido por $X_3 = \{0, 1, 2, 3, 4, 5\}$ e

$$\mathcal{L}_3 = \{\{u, v\} : u, v \in X,\ u \neq v\}.$$

Ou seja, há 6 pontos e as retas são formadas por todos os subconjuntos de dois elementos de X_3. Tal estrutura corresponde a um grafo completo sobre 6 vértices [10].

O primeiro axioma é trivialmente satisfeito pela própria construção das retas. Sobre o segundo axioma, para fixarmos a ideia, escolhemos a reta $t = \{0, 1\}$ e o ponto $P = 2$. As retas que incidem em $P = 2$ conectam-no aos demais pontos do espaço em:

$$r_1 = \{2, 0\}, \quad r_2 = \{2, 1\}, \quad r_3 = \{2, 3\}, \quad r_4 = \{2, 4\}, \quad r_5 = \{2, 5\}.$$

As retas r_1 e r_2 interceptam t nos pontos 0 e 1, respectivamente, e portanto são concorrentes a t. Por outro lado, as retas r_3, r_4 e r_5 são disjuntas de t. Portanto, identificamos exatamente três retas, r_3, r_4, r_5, que passam por 2 e são paralelas a $t = \{0, 1\}$. A simetria da estrutura garante que o resultado é válido para qualquer escolha de reta e um ponto não pertencente a ela.

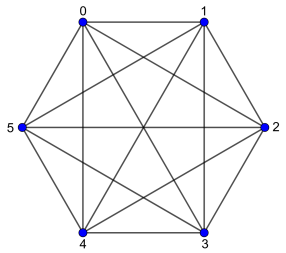


Figura 3: Representação de S_3.

Este exemplo demonstra que conceitos como paralelismo dependem intrinsecamente do sistema axiomático adotado, não sendo uma propriedade imutável. Também há espaços que não admitem retas distintas paralelas. Vejamos um caso curioso em que as retas sempre são concorrentes.

Exemplo 2.5. Consideremos o sistema de axiomas:

1. A interseção de duas retas sempre é um ponto;

2. Cada reta tem 4 pontos.

O espaço $S_4 = (X_4, \mathcal{L}_4)$ definido por $X_4 = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ e

$$\mathcal{L}_4 = \{\{0, 3, 5, 9\}, \{0, 2, 6, 7\}, \{1, 4, 5, 6\}, \{1, 3, 7, 8\}, \{2, 4, 8, 9\}\}$$

satisfaz tal sistema. Uma simples inspeção constata que não há paralelas distintas, pois a interseção de retas distintas sempre gera um ponto.

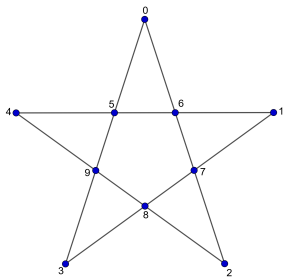


Figura 4: Representação de S_4.

3 Independência de axiomas e modelos

Em uma teoria na Matemática, uma tarefa basilar consiste em verificar a independência de certos axiomas por meio da construção de modelos. A engenhosa geometria de Lobachevsky apresenta um modelo que comprova a independência do 5^o postulado de Euclides em relação aos outros axiomas da geometria clássica. Tal façanha é um dos exemplos mais emblemáticos na história da Matemática de como a construção de um modelo pode ser extremamente demorada.

Alguns modelos simples, mas criativos, nos permitem explorar a independência de axiomas no contexto das geometrias finitas. Neste espírito, o objetivo dessa seção é analisar 3 axiomas fundamentais da geometria finita e discutir algumas de suas consequências. Elencamos tais axiomas:

A1 : Para quaisquer dois pontos distintos P e Q, existe uma única reta $r \in \mathcal{L}$ que os contém.

A2 : Se $P \in X$ e $r \in \mathcal{L}$ é uma reta tal que $P \notin r$, então existe uma única reta $s \in \mathcal{L}$ paralela a r que contém P.

A3 : Existência de um quadrângulo, isto é, existe um subconjunto de 4 pontos de X que são 3 a 3 não colineares.

Por enquanto, não vamos exigir que um espaço satisfaça simultaneamente os 3 axiomas. Pelo contrário, iniciamos a discussão com o intuito de verificar que esses 3 axiomas formam um sistema de axiomas independentes. Vamos em busca de modelos que satisfaçam exatamente 2 dos 3 axiomas.

Exemplo 3.1. Sejam $X_5 = \{0, 1, 2, 3\}$ e $\mathcal{L}_5 = \{\{0, 1, 2, 3\}\}$. O espaço $S_5 = (X_5, \mathcal{L}_5)$ (ver Figura 1) satisfaz A1 e A2 (por vacuidade), mas viola A3.



Figura 5: Exemplo de espaço que satisfaz A1 e A2, mas não A3

Exemplo 3.2. Por outro lado, o Exemplo 2.2 respeita A2 e A3 mas ignora A1.

Exemplo 3.3. Para exibirmos um espaço satisfazendo apenas A1 e A3, recorremos ao célebre plano de Fano, em homenagem ao fundador Gino Fano. Sobre os pontos em $X = \{0, 1, 2, 3, 4, 5, 6\}$, exibimos as retas de $\mathcal{L} = \{r_1, r_2, r_3, r_4, r_5, r_6, r_7\}$ em que $r_1 = \{1, 2, 4\}$, $r_2 = \{2, 3, 5\}$, $r_3 = \{3, 4, 6\}$, $r_4 = \{0, 4, 5\}$, $r_5 = \{1, 5, 6\}$, $r_6 = \{0, 1, 3\}$ e $r_7 = \{0, 2, 6\}$. O círculo inscrito descreve a reta r_7, conforme Figura 6.

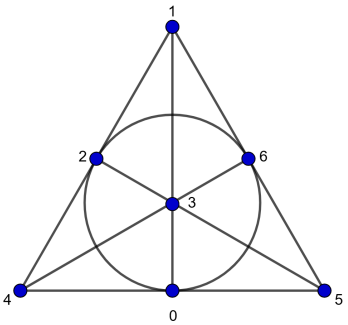


Figura 6: Plano de Fano

Por se tratar de um modelo que requer atenção especial, o quadro de incidência de cada ponto abaixo facilita a compreensão.

Ponto P	**Retas que incidem em P**
0	r_4, r_6, r_7
1	r_1, r_5, r_6
2	r_1, r_2, r_7
3	r_2, r_3, r_6
4	r_1, r_3, r_4
5	r_2, r_4, r_5
6	r_3, r_5, r_7

Tabela 1: Incidência de pontos nas retas do plano de Fano

Tal plano incorpora propriedades ligadas à dualidade: (i) há 7 pontos e 7 retas; (ii) cada reta contém 3 pontos; e (iii) cada ponto incide em 3 retas.

Afirmação 1: O plano $(X, \mathcal{L})$ satisfaz A1. De fato, observamos que quaisquer dois pontos distintos pertencem a exatamente uma reta. Por exemplo: os pontos 0 e 1 pertencem unicamente à reta r_6; os pontos 0 e 2 pertencem unicamente à reta r_7, e assim por diante. Análises semelhantes garantem que todos os outros pares satisfazem essa condição. Como são escolhidos 2 dentre os 7 pontos, há $\binom{7}{2} = 21$ pares de pontos distintos para verificarmos que estão em alguma reta r_i, com $i = 0, 1, \ldots, 6$.

Afirmação 2: o plano de Fano não satisfaz A2. Escolhemos a reta $r_7 = \{0, 2, 6\}$ e o ponto $P = 1$ fora de r_7. Um olhar atento mostra que não existe uma reta paralela a r_7 que passa por P. De fato, as únicas retas que incidem em $P = 1$ são r_1, r_5 e r_6. Como $r_1 \cap r_7 = \{2\}$, $r_5 \cap r_7 = \{6\}$ e $r_6 \cap r_7 = \{0\}$, toda reta incidente a $P = 1$ intercepta r_7. Portanto, não há reta paralela a r_7 passando por 1.

Afirmação 3: Por fim, A3 acontece. Como exemplo, os pontos em $\{0, 2, 3, 4\}$ geram um quadrângulo.

Bose [3] utilizou esta configuração para otimizar experimentos agrícolas, onde os 7 pontos representam variedades de sementes e as 7 retas representam as porções de terra, garantindo que cada par de sementes seja comparado exatamente uma vez.

A combinação dos Exemplos 3.1, 3.2 e 3.3 comprova que A1, A2 e A3 são axiomas independentes. É um ótimo momento para respondermos à pergunta feita na seção anterior a respeito da relação de paralelismo. O axioma A2, equivalente ao 5º Postulado de Euclides, torna o paralelismo em uma relação de equivalência. Quando satisfeito, o conjunto das retas de um espaço fica particionado pelas classes de equivalência formadas pela relação. Neste caso, chamamos as classes de equivalência de *classe de paralelas*. É por conta disso que o paralelismo induz uma relação de equivalência no Exemplo 2.2.

4 Planos Afins

A importância do paralelismo já havia sido explorada desde a época de Tales de Mileto no século VI a.C. (ver [5]), tornando-se uma das características mais versáteis da geometria euclidiana. Discutiremos nesta seção um modelo de espaço que tenta simular tal conceito. Conhecendo a independência e propriedades dos axiomas apresentados na seção anterior, descrevemos agora o principal objeto de estudo desse texto, os planos afins.

Definição 4.1. Um espaço $\Pi = (X, \mathcal{L})$ é um *plano afim* se satisfaz os seguintes axiomas:

A1 : Dados dois pontos distintos, existe uma única reta que passa por eles.

A2 : Se o ponto P não pertence à reta r, então existe uma única reta s paralela a r que contém P.

A3 : Existência de um quadrângulo, isto é, um subconjunto de 4 pontos de X que são 3 a 3 não colineares.

Vamos fixar algumas notações e estabelecer consequências diretas:

1. Se P e Q são pontos distintos, denotaremos a reta que incide em P e Q por $r(P, Q)$.
2. Dado P, o feixe de retas incidentes a P é $[P] = \{r : P \in r \text{ e } r \in \mathcal{L}\}$.
3. O paralelismo é uma relação de equivalência. Há ao menos 3 classes de paralelas, pois cada ponto do quadrângulo incide em pelo menos 3 retas .
4. $|X| \geq 4$ e $|\mathcal{L}| \geq 6$ devido ao quadrângulo exigido em A3;

Uma maneira de justificar esse último resultado usa combinação para contar os subconjuntos de 2 elementos do quadrângulo $\{P_1, P_2, P_3, P_4\}$ (garantidos por A3), em que cada par de pontos define exatamente uma reta (por A1). Assim, há pelo menos $\binom{4}{2} = 6$ retas.

O plano de Fano (Exemplo 3.3) não é um plano afim, pois viola o axioma A2, apesar de satisfazer os axiomas A1 e A3.

Exemplo 4.2. Sejam $X = \{0, 1, 2, 3\}$ e $\mathcal{L} = \{r_1, r_2, r_3, r_4, r_5, r_6\}$ em que

$$r_1 = \{0, 1\},\ r_2 = \{0, 2\},\ r_3 = \{0, 3\},\ r_4 = \{1, 2\},\ r_5 = \{1, 3\} \text{ e } r_6 = \{2, 3\}.$$

Ponto P	**$[P]$: retas incidentes a P**
0	r_1, r_2, r_3
1	r_1, r_4, r_5
2	r_2, r_4, r_6
3	r_3, r_5, r_6

Dados dois pontos distintos em X, por simples inspeção, há apenas uma reta de $\mathcal{L}$ que os contém. Como $r_1 // r_6$, $r_2 // r_5$ e $r_3 // r_4$, o axioma A2 acontece. A existência do quadrângulo é imediata, visto que cada reta possui apenas 2 pontos. Portanto, $\Pi = (X, \mathcal{L})$ gera um plano afim, formando as classes de paralelas: $\alpha_1 = \{r_1, r_6\}$, $\alpha_2 = \{r_2, r_5\}$ e $\alpha_3 = \{r_3, r_4\}$.

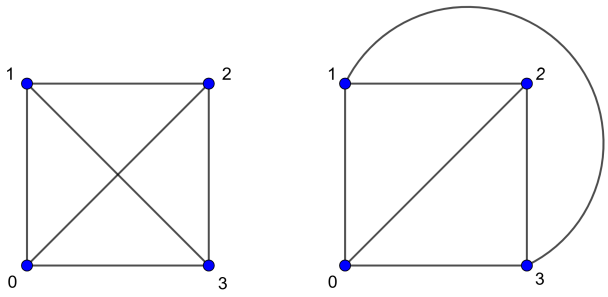


Figura 7: Representações de S.

O espaço S é o "menor"plano afim quando nos referimos a quantidade de pontos e retas.

Uma característica curiosa que causa estranheza nos planos afins é o comportamento das retas paralelas, como apresentado na figura acima, em que as representações contínuas das retas r_2 e r_5 se cruzam, quando na verdade a interseção delas é vazia.

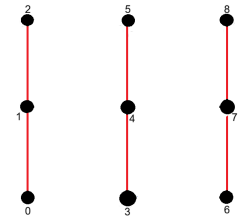
Em representações usuais no plano euclidiano, frequentemente desenhamos duas retas paralelas como se nunca se cruzassem. No entanto, em muitos modelos de planos afins, tal fenômeno pode não ocorrer, gerando uma "traição do desenho". Essa situação aparentemente paradoxal entre a intuição geométrica e a estrutura axiomática surge porque o conceito de paralelismo em um plano afim é puramente relacional: duas retas são paralelas se, e somente se, não possuem nenhum ponto em comum, independentemente de como sejam representadas graficamente.

A palavra "reta"é apenas um apelido para "bloco de elementos". Assim, mesmo que em sua representação duas retas pareçam ter interseção, pode acontecer de não compartilharem pontos em comum.

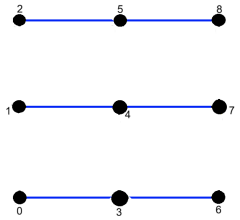
Exemplo 4.3. Vamos construir um plano afim com 9 pontos. Dado $X = \{0, 1, \ldots, 8\}$, escolhemos inicialmente uma classe α_1 de três retas paralelas, por exemplo $r_1 = \{0, 1, 2\}$, $r_2 = \{3, 4, 5\}$ e $r_3 = \{6, 7, 8\}$ (ver figura 8a). Para satisfazer A1 e A2, adicionamos as retas $r_4 = \{0, 3, 6\}$, $r_5 = \{1, 4, 7\}$ e $r_6 = \{2, 5, 8\}$, formando uma nova classe de paralelas α_2 (figura 8b). Procedendo de maneira análoga, criamos mais três retas $r_7 = \{0, 4, 8\}$, $r_8 = \{1, 5, 6\}$, $r_9 = \{2, 3, 7\}$, que formam a classe de paralelas α_3 (figura

8c). Finamente, as retas $r_{10} = \{0, 5, 7\}$, $r_{11} = \{1, 3, 8\}$, $r_{12} = \{2, 4, 6\}$ geram a última classe de paralelas α_4 (figura 8d).

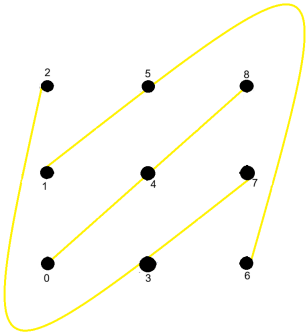
Seja $\mathcal{L} = \{r_i : 1 \leq i \leq 12\}$. Após uma inspeção cuidadosa, o espaço $\Pi = (X, \mathcal{L})$ forma um plano afim, representado na figura 9.



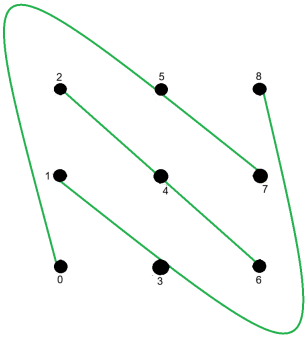
(a) Classe de paralelas α_1



(b) Classe de paralelas α_2



(c) Classe de paralelas α_3



(d) Classe de paralelas α_4

Figura 8: Classes de paralelas

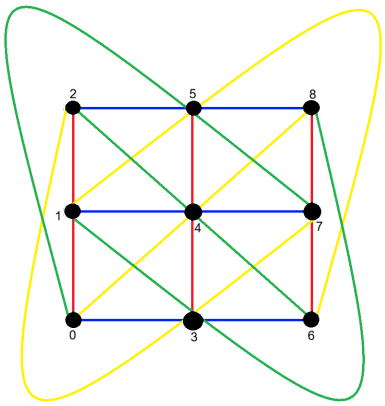


Figura 9: Representação de $\Pi = (X, \mathcal{L})$

Apesar de termos apresentado apenas dois planos afins, é possível observar certas regularidades. Em ambos os exemplos, suas retas têm a mesma quantidade de pontos, assim como as classes de paralelas. Também vemos que a quantidade de pontos, 4 e 9, são quadrados perfeitos. Essas regularidades não acontecem por acaso. De fato, um certo charme discreto fica perceptível nas propriedades abaixo.

Teorema 4.4. *Seja $\Pi = (X, \mathcal{L})$ um plano afim. Então existe $n \geq 2$ tal que:*

i) cada reta contém exatamente n pontos.

ii) para qualquer ponto P, há exatamente $n + 1$ retas que passam por P;

iii) $|X| = n^2$;

iv) $|\mathcal{L}| = n^2 + n$.

Demonstração. Esboçamos a prova aqui. Para mais detalhes, recomendamos [4, 12].
(i) Fixamos inicialmente uma reta r. Como r é um subconjunto do conjunto finito X, claramente existe $n \in \mathbb{N}$ tal que $|r| = n$. Selecionamos outra reta $s \in \mathcal{L}$. Vamos mostrar que $|r| = |s|$. Como observado anteriormente, há pelo menos 3 classes de paralelas, assim existe uma classe de paralelas α tal que $r \notin \alpha$ e $s \notin \alpha$. A ideia central da prova consiste em provar que $|r| = |\alpha| = |s|$. Para tal propósito, digamos que $\alpha = \{t_1, t_2, \ldots, t_k\}$. Seja a função $\phi : \alpha \to r$ definida por $\phi(t_i) = t_i \cap r$, $i = 1, 2, \ldots, k$.

Afirmamos que ϕ é injetora. De fato, sejam duas retas t_i e t_j em α com $i \neq j$. Como t_i e t_j são paralelas, $t_i \cap t_j = \emptyset$. Assim, $(r \cap t_i) \cap (r \cap t_j) = \emptyset$. Como $(r \cap t_i) = \{P_i\}$ e $(r \cap t_j) = \{P_j\}$, segue que $P_i \neq P_j$, ou seja, ϕ é injetora.

Resta provar a sobrejetividade. Dado $Q \in r$, se $Q \neq \phi(t_1)$, o axioma A2 garante que há uma reta t_j, $j \in \{2, \ldots, k\}$, paralela a t_1 e contendo Q. Assim $\phi(t_j) = Q$.

Logo, ϕ é bijetora, e portanto, $n = |r| = |\alpha| = k$. Um argumento análogo nos permite concluir que $|s| = |\alpha|$, e assim $|r| = |s|$. Uma análise similar comprova que $|\alpha| = n$ para qualquer classe de paralelas.

(ii) Considere $s = \{Q_1, Q_2, \ldots, Q_n\}$ uma reta de Π tal que $P \notin s$ (a existência de s decorre de A3 e A1). Cada $i = 1, 2 \ldots, n$ induz uma reta $r(P, Q_i)$. Note que $r(P, Q_i) \neq r(P, Q_j)$ quando $i \neq j$ devido a A1. Mas, por A2, existe uma reta $s^{'}$ paralela a s passando por P. Afirmamos que essas $n+1$ retas são todas as retas que incidem em P. De fato, se $t \in \mathcal{L}$ é uma reta tal que $P \in t$, então t é paralela a s ou t intercepta s. Assim, $t = s^{'}$ ou $|t \cap r(P, Q_k)| \geq 2$ para algum $k = 1, 2, \ldots, n$, caso em que $t = r(P, Q_k)$. Portanto, existem $n + 1$ retas que incidem em P, ou ainda, $|\{s \in \mathcal{L} \mid P \in s\}| = n + 1$.

(iii) Seja $\alpha = \{r_1, r_2, \ldots, r_n\}$ uma classe de retas paralelas em Π. Não é difícil ver que α é uma partição de X. O princípio aditivo da Combinatória garante que

$$|X| = \sum_{i=1}^{n} |r_i| = \sum_{i=1}^{n} n = n^2.$$

(iv) Fixamos uma reta $r = \{Q_1, Q_2, \ldots, Q_n\}$. A chave da prova consiste em perceber que os conjuntos $A = \{s \in \mathcal{L} \ ; \ s \cap r \neq \emptyset, s \neq r\}$ e $B = \{s \in \mathcal{L} \ ; \ r // s\}$ formam uma partição de $\mathcal{L}$. Logo, basta determinarmos $|A|$ e $|B|$.

Se $s \in A$, existe $i = 1, 2, \ldots, n$ tal que $s \cap r = \{Q_i\}$. Logo $s \in [Q_i] \setminus \{r\}$. Por outro lado, se $s \in \bigcup_{i=1}^{n} [Q_i] \setminus \{r\}$, obviamente $s \in A$. Daí, $|A| = |\bigcup_{i=1}^{n} [Q_i] \setminus \{r\}|$. Pelo item (ii), $|[Q_i] \setminus \{r\}| = (n + 1) - 1$, e assim $|A| = \sum_{i=1}^{n} n = n^2$.

Como B é uma classe de paralelas, o item (i) garante que $|B| = n$. Portanto, $|\mathcal{L}| = |A| + |B| = n^2 + n$.

□

O número natural n que satisfaz o teorema acima é chamado de *ordem* do plano afim. O Teorema 4.4 estabelece uma condição aritmética sobre a existência de um plano afim. É impossível encontrar um plano afim sobre 15 pontos, pois 15 não é um número quadrado, ferindo a condição (iii). Por outro lado, apenas construímos planos afins de ordem 2 e 3 nos Exemplos 2.2 e 4.3. Levantamos uma indagação natural: as condições impostas pelo Teorema 4.4 são tão restritivas a ponto de limitar drasticamente a quantidade de planos afins? O resultado garante a existência de uma vasta família de planos afins finitos, atuando como os "primos discretos"do plano afim euclidiano e motivando o título do artigo.

Teorema 4.5. *Seja p um número primo. Então existe um plano afim $\Pi = (X, \mathcal{L})$ de ordem p sobre p^2 pontos.*

Demonstração. A demonstração será dividida em quatro etapas: a construção algébrica do plano e a verificação dos três axiomas que definem um plano afim. Consulte [4, 12] para detalhes ou provas alternativas.

1. *Construção:* Quando p é um número primo, sabemos que o anel $\mathbb{Z}_p$ dos inteiros módulo p forma um corpo. Definimos o conjunto de pontos como $X = \mathbb{Z}_p \times \mathbb{Z}_p$, ou seja, pares ordenados de elementos de $\mathbb{Z}_p$. Definimos o conjunto de retas $\mathcal{L}$ através de equações lineares em $\mathbb{Z}_p$. As retas são divididas em dois tipos:

   - *Retas verticais:* Para cada $c \in \mathbb{Z}_p$, definimos $s_c = \{(c, y) : y \in \mathbb{Z}_p\}$. A família $\alpha_\infty = \{s_c : c \in \mathbb{Z}_p\}$ define a classe das retas verticais.
   - *Retas não-verticais:* Para cada $a \in \mathbb{Z}_p$ e para cada $b \in \mathbb{Z}_p$, definimos

   $$r_{a,b} = \{(x, y) \in \mathbb{Z}_p \times \mathbb{Z}_p : y = ax + b\}.$$

   Assim, para cada $a \in \mathbb{Z}_p$, $\alpha_a = \{r_{a,b} : b \in \mathbb{Z}_p\}$ forma uma classe de paralelas.

   O conjunto total de retas $\mathcal{L}$ é formado pela união de todas essas classes, ou seja,

   $$\mathcal{L} = \alpha_\infty \cup \left(\bigcup_{a \in \mathbb{Z}_p} \alpha_a \right).$$

   O total de retas é dado por $p + p \cdot p = p + p^2$. Verifiquemos agora que a estrutura $\Pi = (X, \mathcal{L})$ satisfaz os três axiomas, sendo assim um plano afim de ordem p.

2. *Verificação do Axioma A1 (Incidência): Dados dois pontos distintos $P = (x_1, y_1)$ e $Q = (x_2, y_2)$, existe uma única reta que os contém.*

   Analisamos dois casos:

   (i) Se $x_1 = x_2$: Como $P \neq Q$, devemos ter $y_1 \neq y_2$. A equação $y = ax + b$ exigiria que $y_1 = ax_1 + b$ e $y_2 = ax_1 + b$, implicando $y_1 = y_2$, o que é absurdo. Logo, a reta não pode ser do tipo $r_{a,b}$. Por outro lado, ambos satisfazem a equação $x = x_1$. Portanto, a única reta é a vertical s_{x_1}.

   (ii) Se $x_1 \neq x_2$: A reta não pode ser vertical, então procuramos $a, b \in \mathbb{Z}_p$ tais que:

   $$y_1 = ax_1 + b$$
   $$y_2 = ax_2 + b$$

Subtraindo as equações: $y_1 - y_2 = a(x_1 - x_2)$. Como p é primo e $x_1 - x_2 \neq 0$, o elemento $(x_1 - x_2)$ possui um único inverso multiplicativo em $\mathbb{Z}_p$. Logo:

$$a = (y_1 - y_2)(x_1 - x_2)^{-1}.$$

Uma vez encontrado a, substituímos na primeira equação e determinamos b unicamente por $b = y_1 - ax_1 = y_1 - (x_1 - x_2)^{-1}(y_1 - y_2)x_1$. A existência e unicidade da solução do sistema garantem a unicidade da reta $r_{a,b}$.

3. Verificação do Axioma A2 (Paralelismo): Dada uma reta l e um ponto $P = (x_0, y_0) \notin l$, existe uma única reta l' paralela a l passando por P.

Primeiramente, observemos as interseções entre os tipos de retas:
Interseção Tipo 1 com Tipo 2: Sejam s_c e $r_{a,b}$. Um ponto na interseção deve satisfazer $x = c$ e $y = ax + b$. O ponto $(c, ac + b)$ existe e é único em $\mathbb{Z}_p \times \mathbb{Z}_p$. Logo, uma reta vertical e uma não-vertical sempre são concorrentes (nunca são paralelas). Agora analisamos os casos para a reta l:

Caso i) l é do Tipo 1 ($l = s_c$): Como vimos acima, qualquer reta paralela a s_c não pode ser do Tipo 2, pois haveria interseção. Logo, a paralela deve ser do Tipo 1. A única reta do Tipo 1 que passa por $P = (x_0, y_0)$ é s_{x_0}. Como $P \notin l$, temos $x_0 \neq c$, o que implica $s_{x_0} \cap s_c = \emptyset$. Assim, $l' = s_{x_0}$ é a única paralela.

Caso ii) l é do Tipo 2 ($l = r_{a,b}$): Como $P \notin l$, temos $y_0 \neq ax_0 + b$. Procuramos l' paralela a l passando por P. Sabemos que l' não pode ser do Tipo 1 pois interceptaria l. Logo, l' deve ser do Tipo 2, digamos $r_{m,k}$. Para que $r_{m,k}$ e $r_{a,b}$ sejam paralelas (sem interseção), o sistema $mx + k = ax + b$ não deve ter solução. Isso equivale a $(m - a)x = b - k$. Se $m \neq a$, existe inverso para $(m - a)$ e haverá uma solução (interseção). Para não haver solução, é necessário que $m = a$ e $b \neq k$. Portanto, a reta procurada deve ter a forma $r_{a,k}$. Para passar por $P = (x_0, y_0)$, devemos ter $y_0 = ax_0 + k$, o que determina unicamente $k = y_0 - ax_0$. Assim, a reta r_{a,y_0-ax_0} passa por P e é paralela a l.

4. Axioma A3 (Existência de Quadrângulo): Existe uma configuração de quatro pontos, três a três não colineares.

Escolhidos os pontos $A = (0, 0)$, $B = (1, 0)$, $C = (0, 1)$ e $D = (1, 1)$, verifiquemos que nenhuma reta contém três destes pontos. Como $\{A, C\} \subset s_0$ e ambos B e D possuem sua primeira coordenada igual a 1, obrigatoriamente $\{B, D\} \cap s_0 = \emptyset$. O argumento garante que $\{A, C, B\}$ e $\{A, C, D\}$ não são colineares. De maneira análoga, $\{B, D\} \subset s_1$, enquanto $\{A, C\} \cap s_1 = \emptyset$. Assim, s_1 é a única reta contendo B e D, e como $A \notin s_1$ e $C \notin s_1$, concluímos que $\{B, D, A\}$ e $\{B, D, C\}$ não são colineares.

C tem $y = 1 \neq 0$. (Não colineares). D tem $y = 1 \neq 0$. (Não colineares). D tem $x = 1 \neq 0$. (Não colineares).

A reta que passa por B, C tem equação $y = -x + 1$ (pois passa por $(1, 0)$ e $(0, 1)$). Testando o ponto $D = (1, 1)$, temos $1 = -1 + 1$, provocando um absurdo. Logo, D não pertence à reta que passa por B e C.

Consequentemente, o conjunto $\{A, B, C, D\}$ induz um quadrângulo. Portanto, $\Pi = (X, \mathcal{L})$ gera um plano afim. □

Vamos usar o teorema anterior para construir um plano afim de ordem 3.

Exemplo 4.6. Consideremos $X = \mathbb{Z}_3 \times \mathbb{Z}_3$ o conjunto de pontos. As retas construídas pelo teorema anterior ficam:

$$s_0 = \{(0,0),(0,1),(0,2)\}; \quad s_1 = \{(1,0),(1,1),(1,2)\}; \quad s_2 = \{(2,0),(2,1),(2,2)\};$$
$$r_{0,0} = \{(0,0),(1,0),(2,0)\}; \quad r_{0,1} = \{(0,1),(1,1),(2,1)\}; \quad r_{0,2} = \{(0,2),(1,2),(2,2)\};$$
$$r_{1,0} = \{(0,0),(1,1),(2,2)\}; \quad r_{1,1} = \{(0,1),(1,2),(2,0)\}; \quad r_{1,2} = \{(0,2),(1,0),(2,1)\};$$
$$r_{2,0} = \{(0,0),(1,2),(2,1)\}; \quad r_{2,1} = \{(0,1),(1,0),(2,2)\}; \quad r_{2,2} = \{(0,2),(1,1),(2,0)\}.$$

Assim o Teorema 4.5 garante que $\Pi = (X, \mathcal{L})$ gera um plano afim de ordem 3. Curiosamente, a representação desse plano afim pode ser vista como a mesma da figura 9, basta identificar cada par ordenado (a, b) ao ponto $3a + b$.

Observação 4.7. A demonstração acima foi realizada sobre o corpo $\mathbb{Z}_p$ com p primo por simplicidade de exposição. No entanto, o resultado é válido em um contexto mais amplo. Todo o argumento se sustenta se substituirmos $\mathbb{Z}_p$ por um corpo finito (corpo de Galois) $\mathbb{F}_q$, onde $q = p^n$ denota uma potência de primo. Neste caso mais geral, a existência de inversos multiplicativos e a aritmética de corpos garantem a existência de planos afins para qualquer ordem q potência de primo.

5 Comentários Finais

Este trabalho busca difundir um "epsilon"sobre geometrias finitas, comentando brevemente a sua relevância histórica [5] e sua aplicabilidade no cenário científico atual [10]. Sob a ótica combinatória, os planos afins possuem estreita relação com estruturas importantes tais como "designs"em blocos [7, 9, 10, 12] e quadrados latinos ortogonais [1, 7, 9, 10, 12].

Além do raciocínio lógico, as geometrias finitas revelam-se instrumentos valiosos para o ensino da matemática devido ao caráter multidisciplinar, podendo ser exploradas de forma intuitiva através de jogos e materiais lúdicos [1, 6, 8, 11], o que reforça o papel dessas estruturas como pontes entre o pensamento abstrato e o aprendizado prático.

Agradecimento

Os autores agradecem ao revisor e editor pelos vários comentários que enriqueceram a versão final. Este trabalho teve o suporte do PET/Matemática-UEM e foi realizado com apoio da Fundo Nacional de Desenvolvimento da Educação (FNDE) e Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) – Código de Financiamento 001.

Data Availability

O artigo não utilizou conjuntos de dados externos.

Author Contributions

Os autores contribuíram igualmente no estudo dos tópicos, na elaboração de exemplos, na redação e revisão deste trabalho.

Referências

[1] Alegri, M.; Silva, S.B.: Sobre Sudokus e grupos. Revista Sergipana de Matemática e Educação Matemática, ReviSeM, **1** (2017), 51–63.

[2] Barbosa, J.M.: *Geometria Euclidiana Plana*. Coleção do Professor de Matemática, Editorada SBM, Rio de Janeiro, RJ, 2012.

[3] Bose, R.C.: On the construction of balanced incomplete block designs. Annals of Eugenics, **9** (1939), 353–399.

[4] Batten, L.M.: *Combinatorics of Finite Geometries*. Cambridge University Press, 1986.

[5] Boyer, C.B.; Merzbach, U.C.: *História da Matemática*. (tradução), Editora Blucher, São Paulo, SP, 2012.

[6] A.C. Ferreira, A.C.: O jogo Dobble e a introdução da geometria finita no ensino médio: como estudantes lidam com o termo primitivo "reta". Dissertação PROFMAT, Universidade de Brasília (UnB), Brasília, DF, 2024.

[7] Hughes, D.R.; Piper, F.C.: Piper, *Design theory*. Cambridge University Press, New York, 1985.

[8] Raposo, A.P.Z.: Geometrias Finitas. Dissertação, Escola de Ciências e Tecnologia, Universidade de Évora, Évora, Portugal, 2014.

[9] Simon, I.:*Configurações Combinatórias*. 13º Colóquio Brasileiro de Matemática, IMPA, Rio de Janeiro, RJ, 1981.

[10] Stinson, D.: *Combinatorial Designs: Constructions and analysis*. Springer, New York, 2004.

[11] Valeriano, M.C.: Um olhar didático sobre Geometrias finitas. Dissertação PROFMAT, Fundação Universidade Federal de Mato Grosso do Sul, Campo Grande, MS, 2024.

[12] Zucareli, W.R.: Teoria dos designs combinatórios: algumas construções clássicas. Dissertação, PMA, Universidade Estadual de Maringá (UEM), Maringá, PR, 2021.

Recebido em 14 de Fevereiro de 2026
Aceito em 08 de Outubro de 2026