UNIVERSIDADE FEDERAL DE SANTA CATARINA

CRISTIANE APARECIDA DOS SANTOS

QUADRADOS LATINOS:

Um estudo histórico-filosófico da matemática

Blumenau

2018

Cristiane Aparecida dos Santos

QUADRADOS LATINOS:
Um estudo histórico-filosófico da matemática

Trabalho de Conclusão de Curso submetido ao Curso de Licenciatura em Matemática da Universidade Federal de Santa Catarina para a obtenção do Grau de Licenciada em Matemática.

Orientador: Prof. Dr. Jorge Luiz Deolindo Silva
Coorientador: Prof. Dr. Julio Faria Corrêa

Blumenau

2018

Catalogação na fonte pela Biblioteca Universitária da Universidade Federal de Santa Catarina.

Arquivo compilado às 20:04h do dia 4 de dezembro de 2018.

Cristiane Aparecida dos Santos
Quadrados Latinos : Um estudo histórico-filosófico da matemática / Cristiane Aparecida dos Santos; Orientador, Prof. Dr. Jorge Luiz Deolindo Silva; Coorientador, Prof. Dr. Julio Faria Corrêa - Blumenau, 20:04, 4 de dezembro de 2018.
76 p.

Trabalho de Conclusão de Curso - Universidade Federal de Santa Catarina, Departamento de Matemática, Centro de Blumenau, Curso de Licenciatura em Matemática.

Inclui referências

1. Quadrados latinos. 2. Método de provas e refutações. 3. Imre Lakatos. I. Prof. Dr. Jorge Luiz Deolindo Silva II. Prof. Dr. Julio Faria Corrêa III. Curso de Licenciatura em Matemática IV. Quadrados Latinos

CDU 02:141:005.7

Cristiane Aparecida dos Santos

QUADRADOS LATINOS: Um estudo histórico-filosófico da matemática

Este Trabalho de Conclusão de Curso foi julgado adequado para obtenção do Título de Licenciada em Matemática, e aprovado em sua forma final pelo Curso de Licenciatura em Matemática do Departamento de Matemática, Centro de Blumenau da Universidade Federal de Santa Catarina.

Blumenau, 20 de novembro de 2018.

Prof. Dr. André Vanderlinde da Silva
Coordenador do Curso de Licenciatura em Matemática

Banca Examinadora:

Prof. Dr. Jorge Luiz Deolindo Silva
Orientador
Universidade Federal de Santa Catarina – UFSC

Prof. Dr. Julio Faria Corrêa
Coorientador
Universidade Federal de Santa Catarina – UFSC

Prof. Dr. André Vanderlinde da Silva
Universidade Federal de Santa Catarina– UFSC

Profª. Drª. Cíntia Rosa da Silva de Oliveira
Universidade Federal de Santa Catarina– UFSC

Dedicado à vó Dalta in memoriam.

AGRADECIMENTOS

Agradeço aos familiares e amigos pelo apoio, mesmo eu estando distante nestes últimos semestres. Aos colegas de sala pelos aprendizados e experiências na Universidade.

Agradeço aos principais envolvidos na minha formação acadêmica: os professores, os membros da banca e o Grupo de Pesquisas em Fundamentos Histórico-Filosóficos da Educação (UFSC/CNPq).

Em especial, agradeço ao meu orientador, Prof. Dr. Jorge Luiz Deolindo Silva e ao meu coorientador, Prof. Dr. Julio Faria Corrêa, pelas conversas, contribuições e debates para a finalização deste trabalho desafiador. Guardarei com grande apreço nossos seminários que se eternizarão nas páginas desta monografia.

"Nunca ande pelo caminho traçado, pois ele conduz somente até onde os outros foram. "
Grahamm Bell.

"As grandes conquistas da humanidade foram obtidas conversando, e as grandes falhas pela falta de diálogo."
Stephen Hawking

RESUMO

Os quadrados latinos ficaram famosos através dos estudos do matemático Leonhard Euler (1707-1783), que buscava uma solução para o problema dos 36 oficiais. O objetivo deste estudo foi aplicar o "método de provas e refutações" de Lakatos na teoria dos quadrados latinos, evidenciando como os conceitos, definições e resultados podem surgir pelo olhar de um estudante que não sabe o que é um quadrado latino. Este trabalho teve em seu horizonte o diálogo entre duas áreas do conhecimento: a Matemática Pura e a Educação Matemática. Construiu-se um debate histórico-filosófico para a construção e a compreensão de objetos matemáticos. Conclui-se que o método de provas e refutações pode ser usado como uma abordagem de ensino e, ainda, não se pode separar a matemática de sua história e filosofia, pois os avanços na área matemática decorrem de uma contribuição coletiva dos matemáticos ao longo do tempo.

Palavras-chaves: Quadrados latinos. Método de provas e refutações. Imre Lakatos.

ABSTRACT

Latin squares became famous through the studies of the mathematician Leonhard Euler (1707-1783), who sought a solution to the problem of the 36 officers. The purpose of this study was to apply Lakatos "method of proofs and refutations" in Latin square theory, showing how concepts, definitions and results can arise through the eyes of a student who does not know what a Latin square is. This work had on its horizon the dialogue between two areas of knowledge: Pure Mathematics and Mathematical Education. A historical-philosophical debate was built for the construction and understanding of mathematical objects. It is concluded that the method of evidence and refutations can be used as a teaching approach and, furthermore, mathematics can not be separated from its history and philosophy, since the advances in the mathematical area derive from a collective contribution of the mathematicians throughout the time.

Keywords: Latin squares. Method of proofs and refutations. Imre Lakatos.

LISTA DE FIGURAS

SUMÁRIO

1 INTRODUÇÃO

A teoria dos quadrados latinos se desenvolveu por meio da contribuição de diversos matemáticos ao longo da história. Leonhard Euler (1707-1783) foi o mais conhecido dentre eles. Sua principal contribuição foi a definição de quadrados latinos ortogonais e sua relação com a solução do problema dos 36 oficiais. O problema consiste em considerar seis regimentos, cada um com seis oficiais e com postos diferentes. A pergunta é: se podemos alinhar os 36 oficias em uma formação de seis linhas por seis colunas, de modo que cada linha e cada coluna tenha apenas um oficial de cada posto e de cada regimento?

O interessante é que Euler estudou primeiro, os quadrados mágicos. *Um* ***quadrado mágico*** *é uma matriz de ordem n na qual colocam-se os números de* 1 *até* n^2*. Em que a soma de cada linha, cada coluna e cada diagonal seja uma constante* M*, chamada de* ***constante mágica***. Um exemplo de quadrado mágico:

$$\begin{matrix} 4 & 9 & 2 \\ 3 & 5 & 7 \\ 8 & 1 & 6 \end{matrix}$$

em que a soma de todas as linhas, colunas e diagonais, resulta em $M = 15$. Após esses estudos, Euler se interessou pelos quadrados latinos.

A teoria de grupos tem fundamental importância para o estudo dos quadrados latinos neste trabalho. Já o método de provas e refutações de Lakatos, sustenta a reconstrução racional da teoria dos quadrados latinos priorizando a história e a filosofia da matemática que segundo D'Ambrosio [9], é um suporte para o entendimento dos conceitos elementares da matemática.

O objetivo deste trabalho é aplicar o método de provas e refutações na teoria dos quadrados latinos, evidenciando como os conceitos, definições e resultados podem surgir pelo olhar de um estudante que não sabe o que é um quadrado latino. O método de

Lakatos não foi utilizado de maneira idêntica ao que o autor propõe, pois não se trata de um trabalho historiográfico em sentido estrito, ou seja, não foram utilizadas fontes primárias para reconstruir a história do desenvolvimento dos quadrados latinos. O foco do trabalho é a possibilidade de pensar este método em relação ao ensino da matemática. O método de Lakatos foi utilizado para reconstruir os debates realizados nas seções de orientação desta monografia e em uma revisão bibliográfica de livros e artigos. As obras consultadas foram [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13].

No Capítulo 2, tem-se o estudo sobre Imre Lakatos e o seu método de provas e refutações, com o propósito de aproximar o leitor com os elementos da teoria utilizados no debate. Este método de Lakatos antefere a filosofia da matemática que resulta no que defende Silva [14]:

> Uma teoria filosófica tem papel articulador e coordenador que desempenha no contexto global do conhecimento e das práticas humanas, e também tem o poder de esclarecimento dos conceitos e ideias que manipula [14, p. 16].

Além disso, antefere a história da matemática como sugere Frendenthal (1981):

> A história da matemática deveria ser conhecimento integrado, mais guiado pela história que pela matemática, analisando mais os processos que os produtos apud [9, p. 6].

O método de provas e refutações é uma teoria que interliga a história e a filosofia da matemática com um objeto matemático qualquer.

No Capítulo 3, encontra-se o debate acerca da teoria dos quadrados latinos por meio do método de provas e refutações. O debate está separado em quatro aulas imaginárias intrinsecamente relacionadas com os seminários que ocorreram durante a elaboração deste trabalho. Na aula 3.1, os estudantes constroem a definição de quadrados latinos. Na aula 3.2, os estudantes discutem as relações entre quadrados latinos e quase grupos. Na aula 3.3, as relações entre quase grupos e grupos são investigadas. Na aula 3.4, debate-se os quadrados latinos ortogonais e a construção de quadrados mágicos.

No Capítulo 4, constam as duas principais teorias que embasam o trabalho do ponto de vista da matemática formal: a teoria de grupos e a teoria algébrica dos quadrados latinos. Além de que, as definições e outros resultados do debate têm como base este capítulo.

2 IMRE LAKATOS

Imre Lipschtz nasceu em 09 de novembro de 1922, em Debrecen (Húngria) tinha sua família de origem judia. Formou-se em 1944 pela Universidade de Debrecen em matemática, física e filosofia. Nos anos que passou na universidade, acontecia a Segunda Guerra Mundial, para evitar as perseguições nazistas, trocou seu sobrenome para Lakatos.

Em 1947, trabalhava como oficial sênior no Ministério da Educação Húngaro e estudava para o título de doutorado na universidade de Debrecen e na Universidade de Moscou. Lakatos tinha personalidade forte e participou de movimentos comunistas. Em 1950, foi preso acusado de *revisionismo*[1] e fora libertado em 1953, devido a morte de Stalin. Após a sua libertação, continuou a estudar em Debrecen e traduzia livros como fonte de renda. Foi o responsável por traduzir o livro de George Pólya *"How to Solve It"* para o húngaro [7].

Em 1956, com a Revolução Húngara, Lakatos fugiu do país e fixou residência na Inglaterra. Em 1961, recebeu o título de doutor em Filosofia pela Universidade de Cambridge. Lakatos lecionou na London School of Economics - de 1960 até a sua morte em 02 de fevereiro de 1974. O prêmio *"Lakatos Award"* da London School of Economics foi criado em homenagem ao papel fundamental que Lakatos teve ao escrever sobre filosofia da ciência [7].

As obras de Lakatos têm grande relevância para a filosofia da ciência e a filosofia da matemática. Entre elas, temos: "Rational reconstructions of the history of science - História da ciência e suas reconstruções racionais e outros ensaios, 1970" ; "Criticism and the growth of knowledge - A crítica e o desenvolvimento do conhecimento, 1970" ; "Proofs and refutations - Provas e refutações: a lógica do descobrimento matemático, 1978" ; "The methodology of scientific

[1] Posição dos que põem em causa as bases fundamentais de uma doutrina (particularmente do marxismo). Fonte: https://dicionario.priberam.org/revisionismo [consultado em 31-10-2018].

research programmes - A metodologia dos programas de pesquisa científica, 1977" e "Mathematics, Science and Epistemology - Matemática, Ciência e Epistemologia, 1978".

Lakatos faleceu no auge de suas produções científicas. O número pequeno de publicações refletem o lado perfeccionista deste teórico. Sua tese de doutorado: "Proofs e Refutations" fora publicada postumamente por John Worrall e Elie Zahar, em 1976. Os editores consideravam que algumas partes da obra não estavam no "nível Lakatos" de escrever. Contudo, foi preferível publicar a obra e aceitar as sugestões posteriores.

2.1 PROVAS E REFUTAÇÕES

A principal obra que fundamenta os estudos deste trabalho é a tese de doutorado de Lakatos. Publicada no Brasil como "Provas e Refutações: a lógica do descobrimento matemático", em 1978, pela editora Zahar.

A fundamentação da obra é baseada na heurística matemática de George Pólya, na filosofia de Karl Popper e na dialética de Hegel. A heurística em sua obra é o sinônimo de metodologia que é a habilidade de inventar ou fazer descobertas matemáticas. A lógica do descobrimento matemático vem da lógica situacional de Popper, nela a lógica é feita através de reconstruções racionais e teóricas que podem ser falseadas (*falsificacionismo*[2]). A dialética de Hegel valoriza o historicismo a cerca do objeto matemático é baseado em três elementos: a tese, a antítese e a síntese. [3] Na própria evolução dos fatos históricos, é possível uma melhor compreensão de resultados e mudanças de conceitos.

[2] É uma vertente filosófica da ciência defendida por Karl Popper, em que toda teoria deve ser falseada até se chegar em um resultado verídico.

[3] A dialética de Hegel, que é um processo espiral sobre o conhecimento, partindo de uma ideia base que é chamada de tese, contrariada por outra ideia, chamada de antítese e chegando a uma conclusão chamada de síntese, que passa a ser uma nova tese, e, por isso, espiral, algo que não tem fim, mas uma evolução de ideia. Fonte: https://blogdoenem.com.br/hegel-filosofia-enem/ [consultado em 01-11-2018].

Lakatos escreveu sua obra por meio de diálogos, em uma sala de aula com professor e alunos imaginários. A sua teoria se desenvolveu ao longo da obra perante as falas dos estudantes e a recíproca do professor. A parte histórica, apareceu de forma abundante nas notas de rodapé e, por algumas vezes, nas demonstrações durante o texto. O problema inicial de sua obra foi identificar alguma relação com o número de vértices, arestas e faces de um poliedro. Esta relação, encontrada pelos alunos ficou conhecida como a conjectura de Euler-Descartes (1758): $V - A + F = 2$.

O autor escreveu com grande domínio sobre o assunto, tanto na parte matemática, quanto na parte da cultura e história da matemática. Em paralelo a esses elementos, descreveu o seu método de provas e refutações, visto que a obra publicada foi baseada na sua tese de doutorado em Filosofia no ano de 1961.

As etapas do seu método seguem da seguinte forma:

(i) um problema inicial ou uma conjectura inicial;

(ii) uma prova;

(iii) crítica da prova;

(iv) melhoramentos da conjectura inicial;

(v) crítica da conjectura melhorada.

Nas etapas do método de provas e refutações, o conhecimento é construído e criticado a todo momento para a verificação da autenticidade dos resultados.

Alguns elementos são bastante característicos no método de Lakatos. A "*prova*", segundo Lakatos [12], é uma experiência mental que remonta a conjectura inicial em lemas, que por sua vez, se encaixam na validação da conjectura inicial.

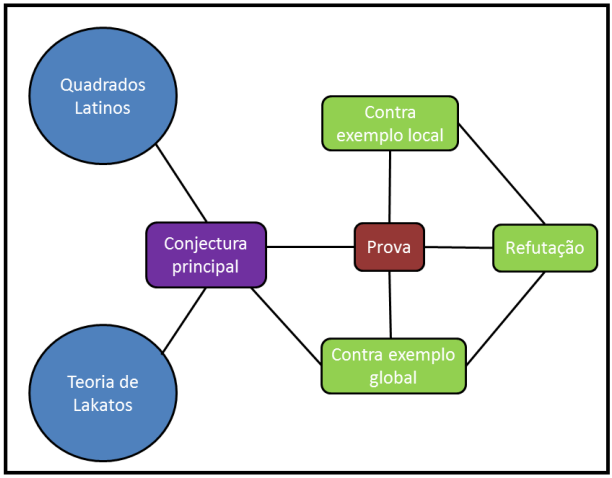
Para a verificação da veracidade da prova, precisa-se criticar. Em outras palavras, tentar refutá-la. "Crítica não significa necessariamente destruição" [12, p. 25], pois é a partir da crítica que chegamos a resultados válidos ou inválidos da conjectura inicial. Refutar uma

prova, é uma maneira de se chegar próximo da verdade e questionar os seus resultados.

Os contra exemplos são meios de se criticar uma prova ou uma conjectura. O "*contra exemplo local*", refuta um lema ou um corolário de uma prova, ou seja, existe algum argumento inválido na demonstração. O "*contra exemplo global*", refuta a conjectura inicial. Então, pode surgir o chamado "*monstro*" do método, que é um contra exemplo que refuta uma definição inicial. Caso isso acontecer deve-se fazer o "*ajuste do monstro*", deve-se corrigir o erro da definição com o intuito de melhorar os domínios dela e como consequência, refuta-se o contra exemplo. O contra exemplo usualmente usado na matemática, no método de Lakatos, é substituido pelo termo "*exceções*". Segundo ele, o termo "contra exemplo" é agressivo e pode ofender quem inventou a prova [12, p. 41].

Na Figura 2.1, tem-se um esquema dos principais elementos do método de provas e refutações utilizados neste estudo com o objeto matemático sendo os quadrados latinos.

Figura 2.1 – Esquema do método de provas e refutações.



Fonte – Elaborado pela autora (2018).

O debate do Capítulo 3, é baseado nestes elementos do método de Lakatos. Dado um problema inicial ou uma conjectura principal, os argumentos são criticados no sentido de verificação e validação dos resultados.

Tendo-se uma conjectura principal, necessita-se de uma prova que recebe constantes críticas. A tentativa de refutar-se uma prova, vem por meio de contra exemplos (*locais ou globais*). Na medida em que aparecem os contra exemplos, ficam nítidos quais passos da prova tem incoerências lógicas ou ainda, quais definições não satisfazem o domínio daquilo que se quer provar. Assim, deve-se fazer os ajustes nas definições, corolários de demonstração e até mesmo, na própria conjectura principal.

O propósito do método, é esgotar as possibilidades de possíveis contra exemplos, ajustando os conceitos e resultados sempre que possível para o argumento tornar-se um valor próximo da verdade. É através de exemplos e contra exemplos que as teorias se desenvolvem e este método enaltece a criticidade ante os resultados.

3 DEBATE HISTÓRICO-FILOSÓFICO PELO MÉTODO DE PROVAS E REFUTAÇÕES

Neste capítulo, tem-se um debate do objeto matemático quadrados latinos pelo método de provas e refutações de Lakatos. É um debate baseado na obra, *Provas e Refutações: a lógica do descobrimento matemático, 1976* do próprio autor, em que constroem-se definições e resultados com o recurso de uma sala de aula imaginária, com estudantes e um professor imaginários, a partir de um problema matemático. É histórico, pois utiliza-se de fatos históricos da matemática para validar e enriquecer os argumentos dos personagens. Contudo, diferente de Lakatos, que utilizou grande parte da história em notas de rodapé e manteve-se o mais fiel possível à história real do progresso da Conjectura de Euler-Descartes, neste trabalho, manteve-se a parte histórica dos quadrados latinos nos argumentos da professora e o que ficou fiel, foram os questionamentos decorridos dos seminários do Trabalho de Conclusão de Curso I. É filosófico, pois questiona os resultados sempre que necessário. O método salienta que a matemática progride por meio de erros e acertos com a contribuição de diversos matemáticos, em diferentes períodos da história do objeto matemático.

O debate, apesar de utilizar alguns fatos históricos a respeito dos quadrados latinos, evidencia como os conceitos, definições e resultados podem surgir pelo olhar de um estudante que não sabe o que é um quadrado latino. Na construção do debate, os elementos do método de provas e refutações de Lakatos são destacados nas notas de rodapé. Caso ocorram dúvidas sobre as propriedades utilizadas no debate, o próximo capítulo engloba a teoria de grupos e a teoria dos quadrados latinos. Assume-se no debate que os estudantes já dominam a teoria de grupos.

O debate será dividido em quatro aulas. Na primeira aula, tem-se a elaboração de uma definição de quadrados latinos por meio da observação de tabelas. Na segunda aula, tem-se a definição de quase grupos e a sua equivalência com os quadrados latinos. Na terceira aula, tem-se os quadrados latinos e seus resultados com as

propriedades de grupos. Na quarta e última aula, tem-se os quadrados latinos ortogonais, sua relação com o problema dos 36 oficiais e sua relação com quadrados mágicos.

3.1 AULA 1: DEFINIÇÃO DE QUADRADOS LATINOS

Professora: Olá caros estudantes, hoje a aula iniciará com a observação das seguintes matrizes:

$$A_1 = \begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix} \qquad B_1 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{bmatrix} \quad C_1 = \begin{bmatrix} 3 & 4 \\ 5 & 6 \end{bmatrix}$$

$$D_1 = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix} \qquad E_1 = \begin{bmatrix} ! & * \\ * & ! \end{bmatrix} \qquad F_1 = \begin{bmatrix} \alpha & \beta & \gamma \\ \gamma & \alpha & \beta \\ \beta & \gamma & \alpha \end{bmatrix}.$$

O que essas matrizes têm em comum e em que elas se diferem?

Estudante $\mathcal{L}$: As matrizes A_1, C_1, D_1 e E_1 são de ordem 2 e as matrizes B_1 e F_1 são de ordem 3.

Estudante $\mathcal{A}$: Além disso, a matriz C_1 tem todas as suas entradas distintas.

Estudante $\mathcal{T}$: Temos matrizes com números, letras e símbolos. Algumas delas obedecem certos padrões. Por exemplo, as matrizes A_1, D_1 e E_1 possuem exatamente 2 elementos distintos em suas entradas. Já a matriz C_1, possui a mesma ordem das anteriores, mas possui 4 elementos distintos em suas entradas. Já as matrizes B_1 e F_1 possuem 3 elementos distintos em suas entradas.

Professora: Correto turma! Vamos olhar agora, especificamente, para as matrizes de ordem 2 que apresentam exatamente 2 elementos distintos em suas entradas. Elas possuem algum padrão, além da sua ordem?

Estudante $\mathcal{A}$: Nas matrizes A_1 e E_1, os seus elementos trocam de posição nas linhas e nas colunas. Mas, na matriz D_1 não ocorrem

essas trocas! Nela, a primeira linha e a segunda linha são idênticas. Na primeira coluna, temos só o algarismo (zero), como na segunda coluna, temos só o algarismo (um).

Estudante $\mathcal{L}$: Então você está querendo dizer que nas matrizes A_1 e E_1, todos os seus elementos fazem permutações, tanto nas linhas, quanto nas colunas e na matriz D_1, essas permutações não ocorrem?

Professora: Exatamente estudante $\mathcal{L}$! O que você acha estudante $\mathcal{T}$?

Estudante $\mathcal{T}$: Essas permutações de elementos nas linhas e colunas acontecem de forma análoga, nas matrizes B_1 e F_1. As exceções são as matrizes C_1 e D_1 onde não ocorrem essas permutações de linhas e colunas.

Professora: Perfeito!

Estudante $\mathcal{A}$: Professora, é possível que as matrizes C_1 e D_1 tenham alguma relação com as demais matrizes?

Professora: Pensem! Vocês já encontraram semelhanças e diferenças entre elas. Sugiro que tentem elaborar uma definição para as matrizes em que ocorrem essas premutações ou uma definição para as matrizes em que não ocorrem tais permutações.

Estudante $\mathcal{L}$: Uma primeira condição é que seja uma matriz quadrada, com uma certa ordem e que tenha um conjunto bem definido.

Professora: Certo!

Estudante $\mathcal{T}$: O que você quer dizer com "conjunto bem definido"?

Estudante $\mathcal{L}$: Conjunto bem definido no sentido de que não se deva misturar letras, símbolos e números dentro do mesmo conjunto.

Estudante $\mathcal{T}$: Eu concordo que tem que ser uma matriz quadrada de uma quantidade n de elementos, mas discordo desse conjunto bem definido. Por exemplo, pegarmos o conjunto $C_0 = \{*, 3, a\}$, eu consigo montar uma matriz que satisfaz as permutações de linhas e colunas.

$$C_1 = \begin{bmatrix} * & 3 & a \\ 3 & a & * \\ a & * & 3 \end{bmatrix}$$

ou ainda, tome o conjunto $C_1'^{=}\{\alpha, *\}$, sua matriz ficaria

$$C_1' = \begin{bmatrix} \alpha & * \\ * & \alpha \end{bmatrix} .$$

Estudante $\mathcal{L}$: É verdade, mesmo o conjunto não sendo bem definido a matriz manteve as permutações das linhas e das colunas. Neste caso, trocaria "bem definido" por um conjunto finito qualquer.

Professora: Além disso, sugiro que vocês tentem enumerar os símbolos com o conjunto $X = \{0, 1, 2, \ldots, n\}$, pois discutimos que faria sentido se fosse um conjunto finito.

Estudante $\mathcal{A}$: Então, nossa definição está em uma matriz quadrada de ordem $n + 1$, com elementos do conjunto $X = \{0, 1, 2, \ldots, n\}$. Contudo, devem acontecer as permutações dos $n + 1$ elementos de X nas suas linhas e colunas.

Professora: Temos nossa primeira definição, conforme os seus argumentos.

Definição 3.1. Seja $X = \{0, 1, 2, \ldots, n\}$ um conjunto finito. Uma matriz quadrada de ordem $n+1$ tal que ocorrem permutações dos $n+1$ elementos de X nas suas linhas e nas suas colunas é um **quadrado**.

A princípio, chamei de quadrados apenas para nomear nossa definição. Mas será que ela funciona para todas as matrizes?

Estudante $\mathcal{T}$: Eu tenho um contra exemplo em que essa definição falha. Tomemos o conjunto $X = \{0, 1, 2\}$, sua matriz aplicando a Definição 3.1, é

$$X = \begin{bmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{bmatrix} \text{ ou } X' = \begin{bmatrix} 1 & 2 & 0 \\ 2 & 0 & 1 \\ 1 & 0 & 2 \end{bmatrix} \text{ e ainda temos}$$

outras possibilidades.

Estudante $\mathcal{L}$: Mas a sua matriz X' não satisfaz a Definição 3.1. Pois, a definição diz que deve acontecer permutações dos elementos do conjunto, tanto nas linhas, quanto nas colunas da matriz. Talvez, tenhamos só que explicar esta nossa restrição para não ficar nenhuma dúvida.

Estudante $\mathcal{T}$: É claro, que equívoco o meu!

Estudante $\mathcal{A}$: Concordo! Para ficar bem clara a Definição 3.1, vamos reescrevê-la assim:

Definição 3.2. Seja X um conjunto finito em que n elementos. A matriz de ordem n dos elementos de X formam permutações das linhas e das colunas da matriz, de modo que cada elemento apareça uma única vez em cada linha e em cada coluna. Essas matrizes são ditas **quadrados**.

Professora: Muito bem turma! Eu farei agora, a minha contribuição na Definição 3.2. Troquem o nome da definição de **quadrados** para a seguinte definição melhorada:

Definição 3.3. *Seja X um conjunto finito com n elementos, com $n \in \mathbb{N}$. Uma matriz quadrada de ordem n é dita ser um* ***quadrado latino*** *se todas as linhas e todas as colunas formam permutações dos n elementos de X. Isto é, cada elemento de X aparece uma única vez em cada linha e em cada coluna.*

Vamos voltar para os exemplos do início da aula. Nas matrizes abaixo, apenas C_1 e D_1 não são quadrados latinos.

$$A_1 = \begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix} \qquad B_1 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{bmatrix} \quad C_1 = \begin{bmatrix} 3 & 4 \\ 5 & 6 \end{bmatrix}$$

$$D_1 = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix} \qquad E_1 = \begin{bmatrix} ! & * \\ * & ! \end{bmatrix} \qquad F_1 = \begin{bmatrix} \alpha & \beta & \gamma \\ \gamma & \alpha & \beta \\ \beta & \gamma & \alpha \end{bmatrix}.$$

Estudante $\mathcal{T}$: Agora sim! Mas por que quadrado latino?

Professora: O nome de quadrados latinos, surgiu a partir dos estudos e notações do matemático Leonhard Euler. Ele começou os estudos no tema, com os quadrados mágicos, por volta de 1726. Em 1779, Euler enunciou os quadrados latinos para tentar resolver o problema dos 36 oficiais.

O problema consiste em considerar seis regimentos, cada um com seis oficiais e com postos diferentes. A pergunta é: se podemos alinhar os 36 oficias em uma formação de seis linhas por seis colunas, de modo que cada linha e cada coluna tenha apenas um oficial de cada posto e de cada regimento?

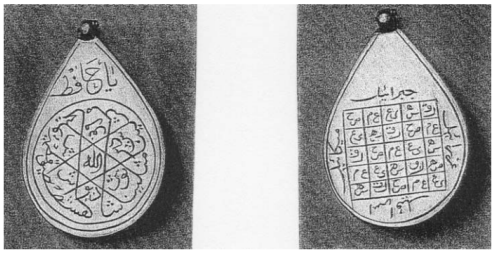
A princípio, o problema foi conjecturado sem solução. Até que em 1782, ele publicou um trabalho em que definiu quadrados latinos ortogonais e uma tentativa de solução do problema dos 36 oficiais.

Neste momento, os quadrados latinos se tornaram um objeto matemático. Euler não os definiu como quadrados latinos, o nome veio com o passar do tempo, decorrente da generalização dos símbolos das matrizes com letras gregas. Segundo Andersen [1], o matemático Joseph Sauveur já utilizava letras latinas e maiúsculas 60 anos antes de Euler. Então, provavelmente o uso de Euler pelas letras latinas descende de seus estudos em publicações de Joseph Sauveur.

Estudante $\mathcal{T}$: Então, existiram estudos em quadrados latinos anteriores aos estudos de Euler?

Professora: Sim! Os primeiros registros de quadrados latinos decorrem dos quadrados mágicos (por volta do ano 1000) em amuletos e ritos de comunidades árabes e indianas. Observem as fotos:

Figura 3.1 – Amuleto de prata de Damasco.



Fonte – Andersen [1, p. 252].

Estes amuletos apresentam formas de quadrados latinos sendo usados como forma de proteção pelos humanos. Conforme Andersen [1], quadrados latinos de entradas 2, 4, 6 e 8 foram usados em todo Oriente Islâmico por se acreditar possuírem poderes mágicos. No livro de Al-Buni, "O sol do grande conhecimento" (por volta do ano 1200) temos vários quadrados latinos como o da foto a seguir:

Figura 3.2 – Quadrado latino no livro de Al-Buni.

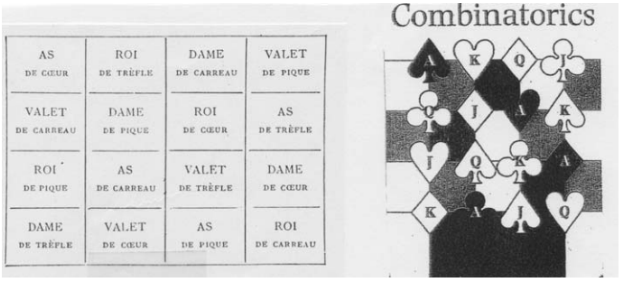
حرف الظاء للمشتري وله يوم الخميس

ظ	ث	ج	ف	خ	ش	ظ
ج	ف	خ	ش	ظ	ز	ث
خ	ش	ظ	ز	ث	ج	ف
ظ	ز	ث	ج	ف	خ	ش
ث	ج	ف	خ	ش	ظ	ز
ف	خ	ش	ظ	ز	ث	ج
ش	ظ	ز	ث	ج	ف	خ

Fonte – Andersen [1, p. 254].

Já no século XIII, Ramón Lull construiu quadrados latinos para explicar o mundo em termos combinatórios. Seguindo para o século XVIII, os quadrados latino aparecem em problemas matemáticos de natureza recreativa. Por exemplo, o enigma da carta como vemos a seguir:

Figura 3.3 – Enigma da carta.



Fonte – Andersen [1, p. 255].

Na atualidade, o Sudoko é utilizado como passatempo e possui grades de quadrados latinos em sua composição.

Figura 3.4 – Sudoko para resolução.

			8		1			
						4	3	
5								
				7		8		
						1		
	2			3				
6							7	5
		3	4					
			2			6		

Fonte – http://blogs.nature.com/news/2012/01/mathematician-claims-breakthrough-in-sudoku-mathematics.html.

Os quadrados latinos possuem aplicações em diversas áreas: teoria dos códigos, teoria dos grupos, design experimental e geometrias finitas. Quero ambientá-los com as questões em que os quadrados latinos se desenvolveram e que o seu progresso é contínuo como veremos em aulas futuras.

Estudante $\mathcal{T}$: Que interessante! Eu não imaginava que um conceito matemático tivesse em suas origens mais remotas, uma atribuição mística.

Estudante $\mathcal{A}$: Pode ser por causa da cultura daquela época. Pois, conforme Roque [13], não eram os pitágoricos que acreditavam que os números regiam o nosso mundo?

Professora: Bem lembrado Estudante $\mathcal{A}$! Se ninguém tiver mais dúvidas ou comentários finalizo a aula de hoje e proponho uma tarefa para a próxima aula: dado $X = \{0, 1, 2\}$, quantos e quais quadrados latinos podemos formar?

3.2 AULA 2: QUADRADOS LATINOS E QUASE GRUPOS

Professora: Na aula anterior, fizemos a construção da definição de um quadrado latino partindo das semelhanças e diferenças de diversas matrizes quadradas passando pelo contexto histórico do tema.

Nesta aula, vamos buscar na teoria de grupos, relações com os quadrados latinos. De acordo com Carmelo [6], os quadrados latinos podem ser construídos em termos algébricos. Vocês encontraram alguma resposta para a questão que deixei de tarefa na última aula?

Estudante $\mathcal{L}$: Sim professora! Já discutimos e chegamos à mesma conclusão. Encontramos seis quadrados latinos, pois o conjunto possui 3 elementos, logo 3! possibilidades. Veja:

$$\begin{array}{ccc} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{array} \qquad \begin{array}{ccc} 1 & 2 & 0 \\ 2 & 0 & 1 \\ 0 & 1 & 2 \end{array} \qquad \begin{array}{ccc} 2 & 0 & 1 \\ 0 & 1 & 2 \\ 1 & 2 & 0 \end{array}$$

$$\begin{array}{ccc} 0 & 2 & 1 \\ 2 & 1 & 0 \\ 1 & 0 & 2 \end{array} \quad \begin{array}{ccc} 2 & 1 & 0 \\ 1 & 0 & 2 \\ 0 & 2 & 1 \end{array} \quad \begin{array}{ccc} 1 & 0 & 2 \\ 0 & 2 & 1 \\ 2 & 1 & 0 \end{array} .$$

Professora: Perfeito! Agora, pensem: o que representa o conjunto X com uma operação $*$ dentro da teoria de grupos?

Estudante $\mathcal{T}$: Pois bem, temos que imaginar como seria o conjunto finito $X = \{0, 1, 2\}$ com uma operação $*$. Eu de imediato associo a uma estrutura binária $(X, *)$ e posso verificar se temos um grupo, correto?

Estudante $\mathcal{A}$: Sim e, ainda, mais imediato é olhar para os quadrados latinos que encontramos e compará-los com a tábua de operações de um grupo!

Professora: Vocês estão no caminho correto. Sugiro que tentem montar tábuas de operações com o conjunto X e uma operação $*$ verificando se resultam nos quadrados latinos encontrados.

Estudante $\mathcal{A}$: Eu já estava tentando fazer isso mesmo professora. Eu obtive as seguintes tábuas de operações:

$*$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$*$	0	1	2
0	1	2	0
1	2	0	1
2	0	1	2

$*$	0	1	2
0	2	0	1
1	0	1	2
2	1	2	0

$*$	0	1	2
0	0	2	1
1	2	1	0
2	1	0	2

$*$	0	1	2
0	2	1	0
1	1	0	2
2	0	2	1

$*$	0	1	2
0	1	0	2
1	0	2	1
2	2	1	0

.

Exatamente como os quadrados latinos encontrados na tarefa.

Professora: Exato! Vocês conseguem associar a esse conjunto $X = \{0, 1, 2\}$ e uma operação $*$ algum grupo clássico?

Estudante $\mathcal{A}$: Não consigo ver isso professora!

Estudante $\mathcal{L}$: Caro colega $\mathcal{A}$, perceba que o conjunto X se assemelha ao conjunto $\mathbb{Z}_m = \{\bar{0}, \bar{1}, \ldots, \overline{m-1}\}$ em que $m \in \mathbb{N}$ e $m > 1$. Mas, no caso do conjunto X citado, temos a semelhança com o $\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$

com alguma operação $*$. Pois, para todo quadrado latino gerado do conjunto $X = \{0, 1, 2\}$ com uma operação $*$, resulta em elementos de $\mathbb{Z}_3$.

No caso do primeiro quadrado latino apresentado, podemos identificar a operação de soma usual na tábua. Vejam:

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

.

Estudante $\mathcal{A}$: Agora eu consegui associar o conjunto X com o $\mathbb{Z}_3$ e uma operação $*$, mas não entendo uma coisa... Por exemplo, se eu tomar o $\mathbb{Z}_3$ com a multiplicação usual, não temos um quadrado latino. Observem:

$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{1}$

.

Estudante $\mathcal{T}$: Será que isso ocorre pela operação ser a multiplicação? Se tomarmos o conjunto $\mathbb{Z}_3$ com a soma usual, temos a seguinte tábua:

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

e esta tábua é um quadrado latino!

Pensando nas propriedades para ser grupo, o conjunto $\mathbb{Z}_3$, com as respectivas operações (soma usual e multiplicação usual) são fechados, isto é, para cada elemento operado dentro do conjunto, o resultado é um elemento que pertence ao conjunto. Na tábua da multiplicação, o elemento inverso não é satisfeito para todo elemento

de $\mathbb{Z}_3$, pois $\bar{0} \cdot \bar{0} = \bar{0}$ e $\bar{0} \neq \bar{1}$ (elemento neutro). Logo, $(\mathbb{Z}_3, \cdot)$ em que $\cdot$ é a multiplicação usual não é grupo.

Vimos em álgebra que o $(\mathbb{Z}_3, +)$ satisfaz a associatividade, elemento neutro e elemento inverso. Portanto, $(\mathbb{Z}_3, +)$ é um grupo.

Acredito que o ponto chave decorre do fato dele ser grupo. Será que toda vez que tivermos um grupo, a sua tábua satisfaz a definição de quadrados latinos? [1]

Professora: Boa pergunta! Para ajudá-los nesse debate, vou definir o que é um quase grupo e, a partir dessa definição, tentaremos encontrar uma resposta para este questionamento.

Definição 3.4. *Um **quase grupo** é um conjunto X finito com uma operação $*$, tal que para todo a, $b \in X$, existem únicos x e $y \in X$, tais que*

$$a * x = b \tag{3.1}$$

e

$$y * a = b. \tag{3.2}$$

Por exemplo, ao analizarmos as operações da tábua $(\mathbb{Z}_3, +)$, verificamos que as Equações 3.1 e 3.2 acima são satisfeitas. De fato,

$$\begin{array}{lll} \bar{0}+\bar{0}=\bar{0} & \bar{1}+\bar{0}=\bar{1} & \bar{2}+\bar{0}=\bar{2} \\ \bar{0}+\bar{1}=\bar{1} & \bar{1}+\bar{1}=\bar{2} & \bar{2}+\bar{1}=\bar{0} \\ \bar{0}+\bar{2}=\bar{2} & \bar{1}+\bar{2}=\bar{0} & \bar{2}+\bar{2}=\bar{1} \end{array} .$$

Observa-se que para $\bar{0} + \bar{1} = \bar{1}$, dados $\bar{a} = \bar{0}$ e $\bar{b} = \bar{1}$, existe um único $\bar{x} \in \mathbb{Z}_3$ tal que $\bar{a} + \bar{x} = \bar{b} \Rightarrow \bar{0} + \bar{x} = \bar{1} \Rightarrow \bar{x} = \bar{1}$.

Assim como, dados $\bar{a} = \bar{1}$ e $\bar{b} = \bar{1}$, existe um único $\bar{y} \in \mathbb{Z}_3$ tal que $\bar{y} + \bar{a} = \bar{b} \Rightarrow \bar{y} + \bar{1} = \bar{1} \Rightarrow \bar{y} = \bar{0}$. Verifica-se de maneira análoga para todos os elementos de $\mathbb{Z}_3$. Logo, $(\mathbb{Z}_3, +)$ é um quase

[1] Problema inicial do método de provas e refutações.

grupo e sua tábua de operações é

$$\begin{array}{c|ccc} + & \bar{0} & \bar{1} & \bar{2} \\ \hline \bar{0} & \bar{0} & \bar{1} & \bar{2} \\ \bar{1} & \bar{1} & \bar{2} & \bar{0} \\ \bar{2} & \bar{2} & \bar{0} & \bar{1} \end{array} .$$

Estudante $\mathcal{A}$: Espera! Deixa-me ver se entendi o exemplo. O $(\mathbb{Z}_3, +)$ é um grupo. Além disso, satisfaz a Definição 3.4 de quase grupos e sua tábua de operações é equivalente a um quadrado latino. Então, quase grupos sempre serão quadrados latinos! Ou seja, dentro da teoria de grupos, a tábua de operações de um quase grupo é equivalente à um quadrado latino. [2]

Professora: Exatamente! A Definição 3.4 de quase grupos é uma forma algébrica de descrever quadrados latinos.

Agora, temos que pensar em como mostrar que dado um grupo, a sua tábua de operações é um quadrado latino ou se existem exceções. Sugiro que vão para suas casas e pensem em uma prova para esta indagação.

3.3 AULA 3: QUASE GRUPOS E GRUPOS

Professora: Na última aula, debatemos sobre a equivalência da tábua de operações de um quase grupo e os quadrados latinos, que a partir de agora, serão citados apenas como quase grupos. Nos exemplos, percebemos que deve existir alguma relação entre a tábua de operação de determinados grupos com um quadrado latino.

Estudante $\mathcal{L}$: Sim professora! Como tínhamos visto que o $(\mathbb{Z}_3, +)$ é um grupo e sua tábua de operações equivale a um quase grupo. Falta provar:

Conjectura 1: X é grupo finito se, e somente se, sua tábua de operações é quase grupo.[3]

Porém, não consegui finalizar uma prova para este resultado.

[2] Verifique esta equivalência na Proposição 4.3 do próximo capítulo.
[3] Conjectura inicial desta aula baseado no método de provas e refutações.

Estudante $\mathcal{T}$: Eu consegui uma prova professora. Entretanto, surgiu-me uma curiosidade: por que um objeto matemático que estava a ser definido por meio de matrizes e permutações, recorreu a resultados e conceitos dentro da teoria de grupos? Eu não teria imaginado trabalhar com um quadrado latino em termos algébricos.

Professora: A sua curiosidade é bem interessante, e ao mesmo tempo, difícil de responder. Mesmo assim, tentarei construir uma reflexão sobre ela.

Segundo Malsev, a teoria de grupos surgiu de uma necessidade de obter-se um método para estudar as propriedades do mundo real, especificamente a simetria (apud Brandemberg [3, p. 32]). Ao longo do desenvolvimento da teoria de grupos, cada vez mais ela se tornara importante para a solução de problemas e, neste caso, os estudos das propriedades de simetria.

Em 1591, François Viéte iniciou a sistematização do uso de letras para representar dados em cálculos (Brandemberg [3]). Antes disso, outros matemáticos, como Diofanto, já utilizavam as letras para os cálculos, mas não de forma sistematizada.

Os quadrados latinos e os quadrados mágicos obedecem certas "simetrias". Nos primeiros registros históricos não eram utilizados números, mas símbolos. Após algum tempo, em decorrência dos estudos de Euler e sua influência, os quadrados latinos se tornaram um objeto matemático e toda a sua teoria começou a ser construída.

Até este momento, não pesquisei quais foram os primeiros matemáticos a escreverem quadrados latinos em termos algébricos, mas acredito que o "olhar inicial" para os estudos de quadrados latinos e a teoria de grupos venha da própria natureza do quadrado latino, onde iniciou com os símbolos, seguido das letras, números e até palavras.

Além disso, Brandemberg [3] cita que uma das principais entidades matemáticas do século XIX é a noção de grupo. Pois, utilizava considerável grau de abstração e generalização em suas formulações. Os matemáticos Cauchy e Galois foram os primeiros a definirem o grupo de permutações. Neste contexto, os quadrados

latinos foram definidos por meio de permutações das linhas e das colunas. Este seria o meu argumento para a associação de quadrados latinos com a teoria dos grupos.

Espero que minhas colocações façam algum sentido para sanar a sua curiosidade. Ainda, podemos pesquisar e nos aprofundar neste assunto.

Estudante $\mathcal{T}$: Fez sentido sim professora, pesquisarei em breve sobre o assunto. Mas, voltando à prova da **Conjectura 1**. Eu utilizei a lei do cancelamento à esquerda. Vejamos.

Seja $(X, *)$ um grupo. Devemos mostrar que dados quaisquer a, $b \in X$, existe uma única solução de

$$a * x = b \tag{3.3}$$

e dado a, $b \in X$, existe uma única solução de

$$x * a = b. \tag{3.4}$$

Para provar a equação (3.3), dados $a, b \in X$, temos pela lei do cancelamento à esquerda, $x = a^{-1} * b$ é solução. Para mostrar a unicidade, suponha que x' também seja solução de $a * x = b$, então

$$\begin{aligned} a * x' &= b \\ a^{-1} * (a * x') &= a^{-1} * b \\ (a^{-1} * a) * x' &= a^{-1} * b \\ e * x' &= a^{-1} * b \\ x' &= a^{-1} * b \\ x' &= x. \end{aligned}$$

Portanto, a solução da equação (3.3) é única.

Para provar a equação (3.4), dados $a, b \in X$, temos, pela lei do cancelamento à direita, $x = b * a^{-1}$ é solução. Para mostrar a unicidade, suponha que x'' também seja solução de $x'' * a = b$, segue

que

$$\begin{aligned} x'' * a &= b \\ (x'' * a) * a^{-1} &= b * a^{-1} \\ x'' * (a * a^{-1}) &= b * a^{-1} \\ x'' * e &= b * a^{-1} \\ x'' &= b * a^{-1} \\ x'' &= x. \end{aligned}$$

Portanto, a solução da equação (3.4) é única.

Note que a equação (3.3) equivale a n equação (3.1) da definição de quase grupo e a equação (3.4) equivale a equação 3.2 da definição de quase grupo, então todo grupo é um quase grupo. [4]

Entretanto, não consegui uma prova final para a recíproca.

Estudante $\mathcal{A}$: Parabéns colega pela sua prova! Eu, ao contrário de você, não consegui nenhuma prova para a conjectura, mesmo que em partes. Mas, fiz um exemplo que justifica a sua tentativa de prova. Se eu tenho $X = \{1, 2, 3\}$ com uma operação $*$ um quase grupo, então a sua tábua de operações satisfaz as propriedades de grupo. Vamos analisar o exemplo.

Considerem a seguinte tábua de operações:

$*$	1	2	3
1	1	2	3
2	2	3	1
3	3	1	2

.

A operação é fechada, pois todas as operações resultam em elementos que pertencem ao conjunto $X = \{1, 2, 3\}$. É associativa, pois

$\bar{1} * (\bar{1} * \bar{1}) = \bar{1} * \bar{1} = \bar{1}$ e $(\bar{1} * \bar{1}) * \bar{1} = \bar{1} * \bar{1} = \bar{1}$

$\bar{1} * (\bar{1} * \bar{2}) = \bar{1} * \bar{2} = \bar{2}$ e $(\bar{1} * \bar{1}) * \bar{2} = \bar{1} * \bar{2} = \bar{2}$

[4] Uma prova para conjectura inicial baseado no método de provas e refutações.

$$\bar{1} * (\bar{1} * \bar{3}) = \bar{1} * \bar{3} = \bar{3} \text{ e } (\bar{1} * \bar{1}) * \bar{3} = \bar{1} * \bar{3} = \bar{3}$$
$$\bar{1} * (\bar{2} * \bar{1}) = \bar{1} * \bar{2} = \bar{2} \text{ e } (\bar{1} * \bar{2}) * \bar{1} = \bar{2} * \bar{1} = \bar{2}$$
$$\bar{1} * (\bar{2} * \bar{2}) = \bar{1} * \bar{3} = \bar{3} \text{ e } (\bar{1} * \bar{2}) * \bar{2} = \bar{2} * \bar{2} = \bar{3}$$
$$\bar{1} * (\bar{2} * \bar{3}) = \bar{1} * \bar{1} = \bar{1} \text{ e } (\bar{1} * \bar{2}) * \bar{3} = \bar{2} * \bar{3} = \bar{1}$$
$$\bar{1} * (\bar{3} * \bar{1}) = \bar{1} * \bar{1} = \bar{1} \text{ e } (\bar{0} * \bar{0}) * \bar{0} = \bar{0} * \bar{0} = \bar{0}$$
$$\bar{1} * (\bar{3} * \bar{2}) = \bar{1} * \bar{1} = \bar{1} \text{ e } (\bar{0} * \bar{0}) * \bar{0} = \bar{0} * \bar{0} = \bar{0}$$
$$\bar{1} * (\bar{3} * \bar{3}) = \bar{1} * \bar{2} = \bar{2} \text{ e } (\bar{1} * \bar{3}) * \bar{3} = \bar{3} * \bar{3} = \bar{2}$$
$$\bar{2} * (\bar{1} * \bar{1}) = \bar{2} * \bar{1} = \bar{2} \text{ e } (\bar{2} * \bar{1}) * \bar{1} = \bar{2} * \bar{1} = \bar{2}$$
$$\bar{2} * (\bar{1} * \bar{2}) = \bar{2} * \bar{2} = \bar{3} \text{ e } (\bar{2} * \bar{1}) * \bar{2} = \bar{2} * \bar{2} = \bar{3}$$
$$\bar{2} * (\bar{1} * \bar{3}) = \bar{2} * \bar{3} = \bar{1} \text{ e } (\bar{2} * \bar{1}) * \bar{3} = \bar{2} * \bar{3} = \bar{1}$$
$$\bar{2} * (\bar{2} * \bar{1}) = \bar{1} * \bar{2} = \bar{2} \text{ e } (\bar{2} * \bar{2}) * \bar{1} = \bar{3} * \bar{1} = \bar{3}$$
$$\bar{2} * (\bar{2} * \bar{2}) = \bar{2} * \bar{3} = \bar{1} \text{ e } (\bar{2} * \bar{2}) * \bar{2} = \bar{3} * \bar{2} = \bar{1}$$
$$\bar{2} * (\bar{2} * \bar{3}) = \bar{2} * \bar{1} = \bar{2} \text{ e } (\bar{2} * \bar{2}) * \bar{3} = \bar{3} * \bar{3} = \bar{2}$$
$$\bar{2} * (\bar{3} * \bar{1}) = \bar{2} * \bar{3} = \bar{1} \text{ e } (\bar{2} * \bar{3}) * \bar{1} = \bar{1} * \bar{1} = \bar{1}$$
$$\bar{2} * (\bar{3} * \bar{2}) = \bar{2} * \bar{1} = \bar{2} \text{ e } (\bar{2} * \bar{3}) * \bar{2} = \bar{1} * \bar{2} = \bar{2}$$
$$\bar{2} * (\bar{3} * \bar{3}) = \bar{2} * \bar{2} = \bar{3} \text{ e } (\bar{2} * \bar{3}) * \bar{3} = \bar{1} * \bar{3} = \bar{3}$$
$$\bar{3} * (\bar{1} * \bar{1}) = \bar{3} * \bar{1} = \bar{3} \text{ e } (\bar{3} * \bar{1}) * \bar{1} = \bar{3} * \bar{1} = \bar{3}$$
$$\bar{3} * (\bar{1} * \bar{2}) = \bar{3} * \bar{2} = \bar{1} \text{ e } (\bar{3} * \bar{1}) * \bar{2} = \bar{3} * \bar{2} = \bar{1}$$
$$\bar{3} * (\bar{1} * \bar{3}) = \bar{3} * \bar{3} = \bar{2} \text{ e } (\bar{3} * \bar{1}) * \bar{3} = \bar{3} * \bar{3} = \bar{2}$$
$$\bar{3} * (\bar{2} * \bar{1}) = \bar{3} * \bar{2} = \bar{1} \text{ e } (\bar{3} * \bar{2}) * \bar{1} = \bar{1} * \bar{1} = \bar{1}$$
$$\bar{3} * (\bar{2} * \bar{2}) = \bar{3} * \bar{3} = \bar{2} \text{ e } (\bar{3} * \bar{2}) * \bar{2} = \bar{1} * \bar{2} = \bar{2}$$
$$\bar{3} * (\bar{2} * \bar{3}) = \bar{3} * \bar{1} = \bar{3} \text{ e } (\bar{3} * \bar{2}) * \bar{3} = \bar{1} * \bar{3} = \bar{3}$$
$$\bar{3} * (\bar{3} * \bar{1}) = \bar{3} * \bar{3} = \bar{2} \text{ e } (\bar{3} * \bar{3}) * \bar{1} = \bar{2} * \bar{1} = \bar{2}$$
$$\bar{3} * (\bar{3} * \bar{2}) = \bar{3} * \bar{1} = \bar{3} \text{ e } (\bar{3} * \bar{3}) * \bar{2} = \bar{2} * \bar{2} = \bar{3}$$
$$\bar{3} * (\bar{3} * \bar{3}) = \bar{3} * \bar{2} = \bar{1} \text{ e } (\bar{3} * \bar{3}) * \bar{3} = \bar{2} * \bar{3} = \bar{1}.$$

Possui elemento neutro, pois $1 * 1 = 1$, $2 * 1 = 2$ e $3 * 1 = 3$. Logo,

1 é o elemento neutro da tábua. Possui elemento inverso, pois

$$1 * 1 = 1 = 1 * 1 \text{ e } 2 * 3 = 1 = 3 * 2.$$

Portanto, temos que a tábua de operações desse quase grupo $(X, *)$ também satisfaz as propriedades de grupo. Além disso, ele também satisfaz a comutatividade, sendo um grupo comutativo.

Estudante $\mathcal{L}$: Vamos pensar... Será que isso vale para todo quase grupo? Como estamos trabalhando com conjuntos finitos, e no exemplo do Estudante $\mathcal{A}$, ele toma o conjunto $X = \{1, 2, 3\}$. Podemos ir analisando todas as possibilidades de permutações deste conjunto, na qual satisfazem a Definição 3.4 de quase grupos.

Como o conjunto $X = \{1, 2, 3\}$ tem 3 elementos, temos 6 possibilidades de quase grupos. Vamos considerar 6 operações neste conjunto X de maneira a gerar as seguintes tábuas de operações:

$$X_1 = \begin{array}{c|ccc} * & 1 & 2 & 3 \\ \hline 1 & 1 & 2 & 3 \\ 2 & 2 & 3 & 1 \\ 3 & 3 & 1 & 2 \end{array} \quad X_2 = \begin{array}{c|ccc} * & 1 & 2 & 3 \\ \hline 1 & 2 & 3 & 1 \\ 2 & 3 & 1 & 2 \\ 3 & 1 & 2 & 3 \end{array}$$

$$X_3 = \begin{array}{c|ccc} * & 1 & 2 & 3 \\ \hline 1 & 3 & 1 & 2 \\ 2 & 1 & 2 & 3 \\ 3 & 2 & 3 & 1 \end{array} \quad X_4 = \begin{array}{c|ccc} * & 1 & 2 & 3 \\ \hline 1 & 1 & 3 & 2 \\ 2 & 3 & 2 & 1 \\ 3 & 2 & 1 & 3 \end{array}$$

$$X_5 = \begin{array}{c|ccc} * & 1 & 2 & 3 \\ \hline 1 & 3 & 2 & 1 \\ 2 & 2 & 1 & 3 \\ 3 & 1 & 3 & 2 \end{array} \quad X_6 = \begin{array}{c|ccc} * & 1 & 2 & 3 \\ \hline 1 & 2 & 1 & 3 \\ 2 & 1 & 3 & 2 \\ 3 & 3 & 2 & 1 \end{array}.$$

Agora, vamos testar as propriedades de grupo nas tábuas.

Professora: Tomem cuidado! Cada uma dessas tábuas de operações construídas possuem uma operação diferente! (Algum tempo depois...)

Estudante $\mathcal{T}$: Caros colegas, sinto muito dizer! O X_1 feito por $\mathcal{A}$ é

verdade, mas três tábuas falharam na associatividade. Observem:

Para a associatividade em X_4, segue

$1 * (2 * 3) = 1 * 1 = 1$ e $(1 * 2) * 3 = 3 * 3 = 3$. Logo, X_4 não é grupo.

Para a associatividade em X_5, segue

$1 * (2 * 3) = 1 * 3 = 1$ e $(1 * 2) * 3 = 2 * 3 = 3$. Logo, X_5 não é grupo.

Para a associatividade em X_6, segue

$1 * (2 * 3) = 1 * 2 = 1$ e $(1 * 2) * 3 = 1 * 3 = 3$. Logo, X_6 não é grupo.

Portanto, a recíproca da **Conjectura 1** não é válida! [5]

Estudante $\mathcal{A}$: Nossa, é verdade!! Mas isso não quer dizer que devemos abandonar a prova do problema. Temos que ajustar as hipóteses e teses. O Estudante $\mathcal{T}$ provou que se temos um conjunto que satisfaz as propriedades de grupo, então a sua tábua de operações é um quase grupo, logo temos a primeira implicação. O problema está na recíproca. Significa que devemos alterar nossa conjectura. Que aliás, já temos uma prova feita.

Estudante $\mathcal{L}$: Bem pensado colega! Então, temos uma proposição demonstrada:

Proposição 3.1. *Se $(X, *)$ é um grupo finito, então a sua tábua de operações é um quase grupo.*

Professora: Muito bem, turma! Estou gostando de ver a autonomia e as análises em suas colocações. Mas, nossa aula já está terminando... Venham com estes resultados revisados que tentaremos fazer uma aplicação de quadrados latinos na próxima aula.

[5] Contra exemplo global pelo método.

3.4 AULA 4: QUADRADOS LATINOS ORTOGONAIS E QUADRADOS MÁGICOS

Professora: Nesta aula, finalizaremos nossos estudos acerca dos quadrados latinos. Vamos retomar ao problema dos 36 oficiais. Euler estudava os quadrados mágicos quando encontrou uma possível solução para o problema em questão. Ele desenvolveu vários resultados para a teoria dos quadrados latinos e conjecturou em 1782 que o problema dos 36 oficiais não tinha solução. Uma contribuição importante de Euler para o progresso da teoria algébrica dos quadrados latinos, foi a definição de quadrados latinos ortogonais. Mas antes, precisamos da seguinte definição:

Definição 3.5. *Dados dois quadrados latinos de ordem n tal que $A = (A_{i,j})$ e $B = (B_{i,j})$, definimos $A \otimes B$ como sendo a matriz quadrada de ordem n formada pelos pares $(A_{i,j}, B_{i,j})$ na linha i e coluna j, chamada de concatenação de A por B. Chamamos $A \otimes B$ de* ***contatenação*** *de A com B.*

Por exemplo, dados $A = \begin{bmatrix} 0 & 1 & 2 \\ 2 & 0 & 1 \\ 1 & 2 & 0 \end{bmatrix}$ e $B = \begin{bmatrix} 0 & 1 & 2 \\ 2 & 0 & 1 \\ 1 & 2 & 0 \end{bmatrix}$ ao concatenarmos A com B, temos

$$A \otimes B = \begin{bmatrix} (0,0) & (1,1) & (2,2) \\ (2,2) & (0,0) & (1,1) \\ (1,1) & (2,2) & (0,0) \end{bmatrix}.$$

Agora sim, podemos definir a principal contribuição de Euler na teoria algébrica do quadrados latinos.

Definição 3.6. Dois quadrados latinos de ordem n, $A = (A_{i,j})$ e $B = (B_{i,j})$, são ditos **ortogonais** $(A \perp B)$ se o par $(A_{i,j}, B_{i,j})$ ocorre apenas uma vez em $A \otimes B$.

Euler afirmou que resolver o problema dos 36 oficiais, era encontrar um par de quadrados latinos ortogonais de ordem 6. Apenas em 1901, o matemático Gaston Terry provou que Euler estava

correto. Já em 1959, os matemáticos Bose, Shrikhande e Parker [2] provaram que é possível obter quadrados latinos ortogonais de qualquer ordem, com exceção das ordens 3 e 6.

Antes de Euler, os quadrados latinos eram utilizados como forma de proteção espiritual. Em seguida, como entretenimento. Foi após Euler iniciar os seus estudos em quadrados latinos que o tema se tornou um objeto matemático. Contribuindo para aplicações na estatística, teoria de grupos, teoria de códigos e planos projetivos.

Estudante $\mathcal{A}$: Que interessante! Mas, professora, você comentou e definiu quadrados latinos ortogonais, poderia nos dar um exemplo?

Professora: Claro! Dados $A = \begin{bmatrix} 0 & 1 & 2 \\ 2 & 0 & 1 \\ 1 & 2 & 0 \end{bmatrix}$ e $B = \begin{bmatrix} 2 & 1 & 0 \\ 1 & 0 & 2 \\ 0 & 2 & 1 \end{bmatrix}$, temos

$$A \otimes B = \begin{bmatrix} (0,2) & (1,1) & (2,0) \\ (2,1) & (0,0) & (1,2) \\ (1,0) & (2,2) & (0,1) \end{bmatrix}$$

montando os pares ordenados de A com B, denotamos essa montagem de $A \otimes B$, isto é, A concatenado com B. Logo, $A \otimes B$ forma um quadrado latino ortogonal. Tudo bem?

Estudante $\mathcal{A}$: Sim, professora, achei bem intuitiva essa definição era apenas para ter certeza que compreendi o conceito.

Professora: Pois bem, quero iniciar o nosso debate de hoje com os seguintes quadrados:

$$\begin{array}{ccc} 2 & 7 & 6 \\ 9 & 5 & 1 \\ 4 & 3 & 8 \end{array} \qquad \begin{array}{ccc} 8 & 1 & 6 \\ 3 & 5 & 7 \\ 4 & 9 & 2 \end{array} .$$

O que seriam estes quadrados?

Estudante $\mathcal{A}$: Com certeza, não são quadrados latinos!

Estudante $\mathcal{L}$: Em relação aos quadros acima, eles são exemplos de quadrados mágicos. Observem que a soma de todas as linhas, colunas

e diagonais, possuem o mesmo resultado, e neste caso, é 15. É fácil a verificação disso,

$$\begin{aligned} 15 &= 9+6+4 = 4+3+8 = 2+9+4 \\ &= 2+5+8 = 7+5+3 = 6+1+8 \\ &= 4+5+6 = 2+7+6 \end{aligned}$$

e

$$\begin{aligned} 15 &= 8+1+6 = 3+5+7 = 4+9+2 \\ &= 4+5+6 = 8+3+4 = 1+5+9 \\ &= 6+7+2 = 8+5+2\ . \end{aligned}$$

Olha que nunca estudamos na graduação os quadrados mágicos. Mas, completei muitos quadrados mágicos no 6º ano do Ensino Fundamental.

Professora: Isso mesmo, completar quadrados mágicos é um ótimo passatempo para estimular o raciocínio e verificar algumas propriedades matemáticas! E vocês acham que existe alguma relação entre quadrados latinos ortogonais e quadrados mágicos?

Estudante $\mathcal{T}$: Professora, segundo o seu relato histórico, Euler estudou os quadrados mágicos antes de quadrados latinos. Logo, pensando nisso, existe alguma relação sim! Mas, qual ou quais essas relações? Acho que precisamos fazer uma definição para quadrados mágicos.

Estudante $\mathcal{A}$: Eu estava justamente pensando em uma definição. O que vocês acham dessa?

Definição 3.7. Um **quadrado mágico** é uma matriz quadrada de ordem n com todas as entradas distintas, em que a soma dos seus n elementos, tanto nas linhas, quanto nas colunas e diagonais, resultam no mesmo valor.

Estudante $\mathcal{T}$: Eu acho que faltam restrições nessa definição. Ela assim, não é suficiente!

Professora: Isso mesmo, o que acontece se eu quiser usar na matriz do meu quadrado mágico, números como: $\sqrt{3}, \pi, e, \phi, \frac{1}{3}$? Como faríamos a construção de um quadrado mágico qualquer?

Estudante $\mathcal{T}$: Para construir um quadrado mágico qualquer? Nossa, são muitas condições. Não consigo, neste momento, generalizar este quadrado mágico.

Estudante $\mathcal{L}$: Eu também não consegui generalizar, contudo, os números $\sqrt{3}, \pi, e, \phi, \frac{1}{3}$ são números com infinitas casas decimais. Além disso, são números racionais e irracionais. Conforme fossemos fazendo as somas desses números com outros elementos do quadrado mágico, os resultados seriam com infinitas casas decimais. Poderíamos fazer aproximações nos cálculos, mas isso nos induz a erros de arredondamento. Resultando que em cada arredondamento teríamos um elemento do quadrado diferente. Não podemos generalizar os elementos de quadrados mágicos para quaisquer conjuntos! Temos que nos restringir ao conjunto dos números naturais.

Estudante $\mathcal{A}$: Eu discordo colega $\mathcal{L}$! Eu consegui montar um quadrado mágico aqui com os seus elementos pertencentes ao conjuntos dos inteiros. Claro que, não consegui nenhuma generalização. Mas, podemos analisar e tirar conclusões. Eu fiz por tentativa e erro, encontrando o seguinte quadrado mágico:

$$\begin{matrix} -12 & 16 & -4 \\ 8 & 0 & -8 \\ 4 & -16 & 12 \end{matrix} .$$

Neste caso, a soma dos elementos do quadrado mágico, resulta sempre no número zero. Assim, posso definir

Definição 3.8. *Um* ***quadrado mágico*** *é uma matriz quadrada de ordem n em que todas as suas entradas são inteiros distintos, dispostos de maneira que a soma dos elementos de uma linha qualquer, de uma coluna qualquer e de uma diagonal qualquer têm sempre a mesma soma.*

Estudante $\mathcal{L}$: Agora sim, não temos mais problemas na definição. No entanto, como construímos quadrados mágicos?

Professora: Parabéns turma! Nossa definição de quadrados mágicos está bem clara. Vou lhes apresentar um método que fora publicado por Euler [10] em 1776. No método, constrói-se quadrados mágicos, a partir de quadrados latinos ortogonais.

O método de Euler: Dadas as letras latinas a, b, c e as letras gregas α, β, γ. Podemos construir os seguintes quadrados latinos:

$$Q_1 = (A_{i,j}) = \begin{bmatrix} a & b & c \\ b & c & a \\ c & a & b \end{bmatrix}$$

e

$$Q_2 = (B_{i,j}) = \begin{bmatrix} \alpha & \beta & \gamma \\ \beta & \gamma & \alpha \\ \gamma & \alpha & \beta \end{bmatrix}.$$

Temos que Q_1 não é ortogonal com Q_2, pois Q_1 concatenado com Q_2, resulta em

$$Q_1 \otimes Q_2 = ((A_{i,j}, B_{i,j})) = \begin{bmatrix} (a,\alpha) & (b,\beta) & (c,\gamma) \\ (b,\beta) & (c,\gamma) & (a,\alpha) \\ (c,\gamma) & (a,\alpha) & (b,\beta) \end{bmatrix}.$$

Logo, não satisfaz a Definição 3.5 de quadrados latinos ortogonais.

Sendo assim, devemos trocar a terceira coluna de Q_2 com a primeira coluna de Q_2, resultando em Q_3. Ao concatenarmos Q_3 com Q_1, obtemos um quadrado latino ortogonal $Q_1 \otimes Q_3$.

$$Q_3 = \begin{bmatrix} \gamma & \beta & \alpha \\ \alpha & \gamma & \beta \\ \beta & \alpha & \gamma \end{bmatrix}$$

$\Rightarrow$

$$Q_1 \otimes Q_3 = \begin{bmatrix} (a,\gamma) & (b,\beta) & (c,\alpha) \\ (b,\alpha) & (c,\gamma) & (a,\beta) \\ (c,\beta) & (a,\alpha) & (b,\gamma) \end{bmatrix}.$$

As seguintes condições devem ser satisfeitas para obtermos quadrados mágicos:

(i) $Q_1 \otimes Q_3$ deve gerar 9 pares ordenados distintos;

(ii) A sequência das letras latinas devem obedecer uma progressão aritmética de razão 3, resultando no tamanho da matriz;

(iii) $a + b = 2c$;

(iv) A sequências das letras gregas devem obedecer uma progressão geométrica de razão 1.

Da diagonal principal de Q_1, temos (a, c, b) e da diagonal secundária de Q_3, temos (α, γ, β).

Para satisfazer (i), (ii), (iii) e (iv), temos que fixar:

$$\begin{aligned} (a, c, b) &= (1, 4, 7) \\ (\alpha, \gamma, \beta) &= (3, 4, 5) \ . \end{aligned}$$

Resulta que,

$$Q_1 = (A_{i,j}) = \begin{bmatrix} 1 & 7 & 4 \\ 7 & 4 & 1 \\ 4 & 1 & 7 \end{bmatrix} \quad \text{e } Q_3 = (C_{i,j}) = \begin{bmatrix} 4 & 5 & 3 \\ 3 & 4 & 5 \\ 5 & 3 & 4 \end{bmatrix}$$

e, substituindo em $Q_1 \otimes Q_3 = ((A_{i,j}, C_{i,j}))$ tal que

$(A_{i,j}, C_{i,j}) := (A_{i,j} + C_{i,j})$ em que $+$ é a soma usual, segue que

$$\begin{bmatrix} (a+\gamma) & (b+\beta) & (c+\alpha) \\ (b+\alpha) & (c+\gamma) & (a+\beta) \\ (c+\beta) & (a+\alpha) & (b+\gamma) \end{bmatrix}$$

$\Rightarrow$

$$\begin{bmatrix} (1+4) & (7+5) & (4+3) \\ (7+3) & (4+4) & (1+5) \\ (4+5) & (1+3) & (7+4) \end{bmatrix}$$

$\Rightarrow$

$$\begin{bmatrix} 5 & 12 & 7 \\ 10 & 8 & 6 \\ 9 & 4 & 11 \end{bmatrix} .$$

Portanto, temos um quadrado mágico em que o resultado das somas é 24.

Estudante $\mathcal{L}$: Nossa, que bela aplicação de quadrados latinos ortogonais. Agora, entendo eles ficarem conhecidos como "mágicos". Na verdade, quem tem certo conhecimento matemático entende a lógica do método. Mas, pensar em todas estas condições é bem trabalhoso.

Professora: O que eu gostaria de alertá-los é que este método não foi inédito na história dos quadrados mágicos. Euler tinha certa influência na sua época, tendo muitas contribuições para a matemática. Segundo Andersen [1], o método de construção de quadrados mágicos a partir de quadrados latinos ortogonais tiveram seus primeiros registros no livro de Al-Buni - por volta do ano 1200 - que ficou conhecido como método Hindu.

O método Hindu consiste em tomarmos um quadrado latino de ordem ímpar. Dado

$$Q_1 = \begin{bmatrix} 4 & 5 & 1 & 2 & 3 \\ 5 & 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \\ 3 & 4 & 5 & 1 & 2 \end{bmatrix}$$

devemos multiplicar cada elemento da matriz pela sua respectiva ordem que neste caso é 5. Então,

$$Q_2 = \begin{bmatrix} 20 & 25 & 5 & 10 & 15 \\ 25 & 5 & 10 & 15 & 20 \\ 5 & 10 & 15 & 20 & 25 \\ 10 & 15 & 20 & 25 & 5 \\ 15 & 20 & 25 & 5 & 10 \end{bmatrix}.$$

Depois, devemos somar:

- $1^{\underline{a}}$ coluna de Q_1 com a $5^{\underline{a}}$ coluna de Q_2;
- $2^{\underline{a}}$ coluna de Q_1 com a $4^{\underline{a}}$ coluna de Q_2;

- 3ª coluna de Q_1 com a 3ª coluna de Q_2.

Obtemos,

$$Q_3 = \begin{bmatrix} 19 & 15 & 6 & 27 & 23 \\ 25 & 16 & 12 & 8 & 29 \\ 26 & 22 & 18 & 14 & 10 \\ 7 & 28 & 24 & 20 & 11 \\ 13 & 9 & 30 & 21 & 17 \end{bmatrix}.$$

Logo, Q_3 é um quadrado mágico onde o resultado das somas é 90.

Podemos ainda, subtrair o valor da ordem (5) da matriz dos elementos de Q_3, obtendo um novo quadrado mágico:

$$Q_4 = \begin{bmatrix} 14 & 10 & 1 & 22 & 18 \\ 20 & 11 & 7 & 3 & 24 \\ 21 & 17 & 13 & 9 & 5 \\ 2 & 23 & 19 & 15 & 6 \\ 8 & 4 & 25 & 16 & 12 \end{bmatrix}$$

onde as somas resultam em 65.

Euler teve grande influência no meio matemático. Talvez, seja por isso que tudo o que ele publicava era divulgado e "aceito". Os estudos de Euler e de outros matemáticos como Al-Buni, contribuíram para o desenvolvimento da teoria dos quadrados latinos, e ainda é um campo aberto e produtivo. Finalizo a aula por aqui, aguardo comentários e observações para uma próxima aula. Até!

4 TEORIA DE GRUPOS E TEORIA ALGÉBRICA DOS QUADRADOS LATINOS

Para a construção do capítulo anterior, foi imprescindível os estudos da teoria de grupos e da teoria dos quadrados latinos. Neste capítulo, veremos a matemática formal destas teorias.

4.1 GRUPOS

A teoria de grupos é importante para diversas áreas da matemática. No debate deste trabalho, os estudantes fazem o uso de diversos conceitos dessa teoria. Por exemplo, o grupo das permutações, o grupo $\mathbb{Z}_m$, tábuas de operações dos grupos e outros. Nesta seção, vamos relembrar alguns resultados.

Definição 4.1. Sejam G um conjunto não vazio e $* : G \times G \to G$ uma operação fechada sobre G. Dizemos que $(G, *)$ é um **grupo** se satisfaz as seguintes propriedades:

(i) Para todos $x, y, z \in G$, vale $x * (y * z) = (x * y) * z$;

(ii) Para todo $x \in G$, existe $e \in G$ tal que $x * e = e * x = x$. Chamamos e de **elemento neutro** de G;

(iii) Para cada elemento $x \in G$, existe $y \in G$ tal que $x*y = y*x = e$. Chamaremos o y de **elemento inverso** de x e denotaremos por x^{-1}.

Definição 4.2. Se o grupo $(G, *)$ para todo $x, y \in G$, $x * y = y * x$, dizemos que G é um **grupo abeliano** ou **comutativo**.

Exemplo 4.1.1. (a) **Grupo aditivo dos inteiros** $(\mathbb{Z}, +)$**:** O $\mathbb{Z}$ munido com a soma usual é um grupo comutativo. De fato,

(i) $\forall\ x, y, z \in \mathbb{Z}$, temos $x + (y + z) = (x + y) + z$;

(ii) $\forall\ x \in \mathbb{Z}$, existe $0 \in \mathbb{Z}$ tal que $x + 0 = 0 + x = x$;

(iii) Para cada elemento $x \in \mathbb{Z}$, existe $-x \in \mathbb{Z}$ tal que $x + (-x) = -x + x = 0$.

Além disso, dados $x, y \in \mathbb{Z}$, $x + y = y + x$.

(b) **Grupo aditivo dos racionais** $(\mathbb{Q}, +)$**, grupo aditivo dos reais** $(\mathbb{R}, +)$ **e grupo aditivo dos complexos** $(\mathbb{C}, +)$**:** $\mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$ com a soma usual são grupos comutativos.

(c) **Grupo aditivo das matrizes** $(M_{m\times n}(\mathbb{R}), +)$**:** O conjunto das matrizes de ordem $m \times n$ com entradas reais é um grupo comutativo munidos com a soma usual de matrizes.

(d) **Grupo multiplicativo dos racionais** $(\mathbb{Q}^*, \cdot)$**:** O conjunto dos números racionais excluindo o zero é um grupo comutativo com a multiplicação usual. De fato,

(i) $\forall\ x, y, z \in \mathbb{Q}^*$, temos $x \cdot (y \cdot z) = (x \cdot y) \cdot z$;

(ii) $\forall\ x \in \mathbb{Q}^*$, existe $1 \in \mathbb{Q}^*$ tal que $x \cdot 1 = 1 \cdot x = x$;

(iii) Para cada elemento $x \in \mathbb{Q}^*$, existe $\frac{1}{x} \in \mathbb{Q}^*$ tal que $x \cdot \frac{1}{x} = \frac{1}{x} \cdot x = 1$.

Além disso, dados $x, y \in \mathbb{Q}^*$, $x \cdot y = y \cdot x$.

(e) **Grupo multiplicativo dos reais** $(\mathbb{R}^*, \cdot)$ **e grupo multiplicativo dos complexos** $(\mathbb{C}^*, \cdot)$**:** O conjunto dos números reais e o conjunto dos números complexos sem o zero são grupos comutativos com a multiplicação usual.

Proposição 4.1. *Sejam $(G, *)$ um grupo e dados $a, b \in G$. Então:*

(i) O elemento neutro de $(G, *)$ é único;

(ii) O elemento inverso de $(G, *)$ é único;

(iii) Se $a * a = a$. Então, $a = e$;

(iv) $(a^{-1})^{-1} = a$;

(v) Vale a lei do cancelamento à esquerda, isto é, $a * x = a * y \Rightarrow x = y$;

(vi) Vale a lei do cancelamento à direita, isto é, $x * a = y * a \Rightarrow x = y$;

(vii) $(a * b)^{-1} = b^{-1} * a^{-1}$;

(viii) Dado x uma variável em G, então $a * x = b \Rightarrow x = a^{-1} * b$ e tem solução única.

Demonstração. (i) Suponhamos $e, e^{'} \in G$ elementos neutros de $(G, *)$. Temos que

$$e = e * e^{'} = e^{'}.$$

(ii) Dados $a, b \in G$. Suponhamos $b, b^{'}$ inversos de a. Segue que $a * b^{'} = b^{'} * a = e$, assim como $a * b = b * a = e$. Então,

$$b^{'} = e * b^{'} = (b * a) * b^{'} = b * e = b.$$

(iii) Dado $a \in G$, existe $a^{-1} \in G$ tal que $a^{-1} * a = e$.

Logo, $a^{-1} * (a * a) = a^{-1} * a = e$. Por outro lado,

$$a^{-1} * (a * a) = (a^{-1} * a) * a = e * a = a.$$

Portanto, pela associatividade, $a = e$.

(iv) Seja a^{-1} o inverso de a. Sabemos que vale a unicidade do elemento inverso. Segue que

$$a * a^{-1} = e \Rightarrow (a^{-1})^{-1} = a.$$

(v) Suponhamos $a * x = a * y$. Então,

$$\begin{aligned} x &= e * x = (a^{-1} * a) * x = a^{-1} * (a * x) = a^{-1} * (a * y) \\ &= (a^{-1} * a) * y = e * y = y. \end{aligned}$$

(vi) Suponhamos $x * a = y * a$. Então,

$$\begin{aligned} x &= x * e = x * (a * a^{-1}) = (x * a) * a^{-1} = (y * a) * a^{-1} \\ &= y * (a * a^{-1}) = y * e = x. \end{aligned}$$

(vii) Para todos $a, b \in G$, temos $(a * b) * (a * b)^{-1} = e$, como G é grupo vale a associatividade $a * (b * (a * b^{-1})) = e$.

Pela lei do cancelamento à esquerda, segue que

$$\begin{aligned} a*(b*(a*b^{-1}))=e &\Rightarrow a^{-1}*a*(b*(a*b^{-1}))=e \\ &\Rightarrow e*(b*(a*b^{-1}))=a^{-1}*e \\ &\Rightarrow b*(a*b)^{-1}=a^{-1}. \end{aligned}$$

Novamente, pela lei do cancelamento à esquerda,

$$\begin{aligned} b^{-1}*b*(a*b)^{-1}=b^{-1}*a^{-1} &\Rightarrow e*(a*b)^{-1}=b^{-1}*a^{-1} \\ &\Rightarrow (a*b)^{-1}=b^{-1}*a^{-1}. \end{aligned}$$

(viii) Pela lei do cancelamento à direita, segue que

$$\begin{aligned} a*x=b &\Rightarrow a^{-1}*(a*x)=a^{-1}*b \\ &\Rightarrow (a^{-1}*a)*x=a^{-1}*b \\ &\Rightarrow e*x=a^{-1}*b \\ &\Rightarrow x=a^{-1}*b. \end{aligned}$$

Logo, $x=a^{-1}*b$ é solução.

Para mostrar a unicidade, suponhamos que existe $x^{'}$ tal que $a*x^{'}=b$, segue que

$$\begin{aligned} a*x^{'}=b &\Rightarrow a^{-1}*(a*x^{'})=a^{-1}*b \\ &\Rightarrow (a^{-1}*a)*x^{'}=a^{-1}*b \\ &\Rightarrow e*x^{'}=a^{-1}*b \\ &\Rightarrow x^{'}=a^{-1}*b \\ &\Rightarrow x^{'}=x. \end{aligned}$$

Portanto, $a*x=b$ tem solução única em G.

■

Observação 1. Este resultado mostra que para encontrar o elemento neutro de G, devemos mostrar que $a*x=a$ para qualquer $a\in G$.

Definição 4.3. Se o conjunto G é finito, então $(G,*)$ é chamado de **grupo finito**. O número de elementos de G é chamado de **ordem** do grupo, denotado por $\circ(G)$.

Definição 4.4. A **tábua** de uma operação $*$ definida sobre um grupo finito $G = \{g_1, g_2, ..., g_n\}$ é uma tabela em que o resultado da operação $g_i * g_j$ é colocado na i-nésima linha e j-ésima coluna.

Exemplo 4.1.2. Para $G = \{g_1, g_2, g_3, g_4, g_5\}$ e uma operação qualquer $*$, temos a seguinte tábua de operações:

$*$	g_1	g_2	g_3	g_4	g_5
g_1	$g_1 * g_1$	$g_1 * g_2$	$g_1 * g_3$	$g_1 * g_4$	$g_1 * g_5$
g_2	$g_2 * g_1$	$g_2 * g_2$	$g_2 * g_3$	$g_2 * g_4$	$g_2 * g_5$
g_3	$g_3 * g_1$	$g_3 * g_2$	$g_3 * g_3$	$g_3 * g_4$	$g_3 * g_5$
g_4	$g_4 * g_1$	$g_4 * g_2$	$g_4 * g_3$	$g_4 * g_4$	$g_4 * g_5$
g_5	$g_5 * g_1$	$g_5 * g_2$	$g_5 * g_3$	$g_5 * g_4$	$g_5 * g_5$

4.1.1 Grupo de classes de restos

Vamos fazer dois exemplos de grupos finitos que usamos no capítulo anterior. Para a construção de alguns resultados da teoria dos quadrados latinos, por diversas vezes fez-se necessária a utilização do grupo de classes de restos. Nesta seção, abordaremos este grupo.

Definição 4.5. Considere o conjunto $\mathbb{Z}_m = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}$, em que $m \in \mathbb{N}$. Um elemento $\bar{x} \in \mathbb{Z}_m$, com $x \in \mathbb{Z}$, se:

(i) $x = i$, com $0 \leq i \leq m-1$;

(ii) $x < 0$ ou $x \geq m$, então $\bar{x} = \bar{r}$, em que r é o resto da divisão de x por m, isto é, $\exists\ q, r \in \mathbb{Z}$ tais que $x = mq + r$, em $0 \leq r \leq m-1$.

Exemplo 4.1.3. Considere o conjunto $\mathbb{Z}_m = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{m-1}\}$ com a operação $+$ dado por $\overline{x} + \overline{y} = \overline{x+y}$, temos que $(\mathbb{Z}_m, +)$ é um grupo comutativo. De fato,

(i) Para todos $\overline{x}$, $\overline{y}$, $\overline{z} \in \mathbb{Z}_m$, temos
$\overline{x} + (\overline{y} + \overline{z}) = \overline{x} + (\overline{y+z}) = \overline{x + (y+z)} = \overline{(x+y)+z} = (\overline{x+y}) + \overline{z} = (\overline{x} + \overline{y}) + \overline{z}$;

(ii) Para todo $\overline{x} \in \mathbb{Z}_m$, $\exists\ \overline{0} \in \mathbb{Z}_m$ tal que $\overline{x} + \overline{0} = \overline{x+0} = \overline{x} = \overline{0+x} = \overline{0} + \overline{x}$;

(iii) Para todo $\overline{x} \in \mathbb{Z}_m$, $\exists\, \overline{m-x} \in \mathbb{Z}_m$ tal que $\overline{x} + \overline{m-x} = \overline{x+(m-x)} = \overline{m} = \overline{0}$;

(iv) Para todo $\overline{x}$ e $\overline{y} \in \mathbb{Z}_m$, temos $\overline{x} + \overline{y} = \overline{x+y} = \overline{y+x} = \overline{y} + \overline{x}$.

Portanto, $(\mathbb{Z}_m, +)$ é chamado **grupo aditivo de classes de restos**.

Exemplo 4.1.4. Considere $\mathbb{Z}_m^* = \mathbb{Z}_m \backslash \{\overline{0}\}$ com a operação $\cdot$ dada por $\overline{x} \cdot \overline{y} = \overline{x \cdot y}$. Tome $\mathbb{Z}_6^*$, segue que $\overline{2} \cdot \overline{3} = \overline{6} = \overline{0}$. Mas, $\overline{0} \notin \mathbb{Z}_6^* = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$. Logo, $\mathbb{Z}_6^*$ não é grupo.

Portanto, $(\mathbb{Z}_m^*, \cdot)$ não é grupo em geral.

No entanto, o seguinte resultado é importante para a verificação de $(\mathbb{Z}_m^*, \cdot)$ ser grupo ou não.

Teorema 4.2. *$(\mathbb{Z}_m^*, \cdot)$ é um grupo se, e somente se, m é primo.*

Demonstração. Suponhamos m não primo. Então, existem inteiros x e y com $1 < x < m$ e $1 < y < m$ tais que $m = x.y$. Note $\overline{x} \neq \overline{0}$ e $\overline{y} \neq \overline{0}$, mas $\overline{x} \cdot \overline{y} = \overline{x \cdot y} = \overline{m} = \overline{0}$. Contradição, pois $\overline{0} \notin (\mathbb{Z}_m^*, \cdot)$.

Suponhamos m primo e que $\overline{a} \in \mathbb{Z}_m^*$. Então, defina

$$\begin{array}{rccc} f: & \mathbb{Z}_m^* & \to & \mathbb{Z}_m^* \\ & \overline{x} & \mapsto & \overline{a} \cdot \overline{x}\ . \end{array}$$

Logo,

$$\begin{array}{rcl} f(\overline{x}) & = & f(\overline{y}) \\ \overline{a} \cdot \overline{x} & = & \overline{a} \cdot \overline{y} \\ \overline{a} \cdot (\overline{x} - \overline{y}) & = & \overline{0} \\ \overline{a \cdot (x-y)} & = & \overline{0} \\ m & \mid & a(x-y). \end{array}$$

Como m é primo, temos que $m|a$ ou $m|x-y$. Como m não divide a, segue que $m|x-y$. Isto é, existe $k \in \mathbb{Z}^*$ tal que

$$x - y = m \cdot k \Rightarrow \overline{x - y} = \overline{m \cdot k} = \overline{0} \Rightarrow \overline{x} = \overline{y}.$$

Portanto, a função é injetora. Além disso, como $\mathbb{Z}_m^*$ é finito, a função definida é bijetora. A associatividade dos elementos de $\mathbb{Z}_m^*$ é trivial. O elemento neutro é $\bar{1}$, pois dado $\bar{a} \in \mathbb{Z}_m^*$, segue que $\bar{a} \cdot \bar{1} = \bar{1} \cdot \bar{a} = \bar{a}$. Como a função é bijetora, dado $\overline{1} \in \mathbb{Z}_m^*$, existe $\bar{x} \in \mathbb{Z}_m^*$ tal que $f(\overline{x}) = \overline{a} \cdot \overline{x} = \overline{1}$, isto é, $\overline{x}$ é o elemento inverso de $\overline{a}$. Portanto, $(\mathbb{Z}_m^*, \cdot)$ é grupo. ■

4.1.2 Grupo das permutações

Para a construção de quadrados latinos faz-se o uso de permutações de linhas ou colunas. Nesta seção vamos relembrar o grupo de permutações.

Seja E um conjunto não vazio. Considere $S(E)$ o conjunto de todas as funções bijetoras de E em E, isto é,

$$S(E) = \{f : E \to E \mid f \text{ é bijetora}\}.$$

Vamos considerar a operação composição de funções

$$\begin{array}{rccc} \circ : & S(E) \times S(E) & \to & S(E) \\ & (f, g) & \mapsto & f \circ g \end{array}$$

sobre $S(E)$.

A operação de composição é associativa. O elemento neutro da operação de composição é a identidade denotado pela função I_d. O elemento inverso de f é a função inversa f^{-1}. Então, $(S(E), \circ)$ é um grupo denominado **grupo de permutações** sobre E, pois $f \circ f^{-1} = f^{-1} \circ f = Id = f^{-1}$.

Definição 4.6. Seja $E = \{1, 2, \ldots, n\}$, $n \in \mathbb{N}$ com $n \geq 1$. $S(E)$ é denominado **grupo simétrico de grau n** denotado por S_n.

Dado $f \in S_n$ tal que $f(i) = a_i$, para todo $i \in E$, então f

pode ser denotado por

$$f = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ a_1 & a_2 & a_3 & ... & a_n \end{pmatrix}, \text{ em que } a_i \in E.$$

Os elementos de S_n são chamados de **permutação** e a ordem de S_n é $n!$.

Exemplo 4.1.5. (a) S_2 possui 2 elementos, pois

$$S_2 = \left\{ \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\}.$$

Além disso, sua tábua de operação é

$\circ$	$\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$
$\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$
$\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$

.

(b) Dados $f,\ g \in S_3$, definidas por $f = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ e $g = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$, então,

$$f \circ g = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

(c) Dados $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$ e $g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$, então

$$f \circ g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}.$$

(d) Se $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} \in S_4$, então

$$f^{-1} = \begin{pmatrix} 2 & 3 & 1 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}.$$

4.2 TEORIA ALGÉBRICA DOS QUADRADOS LATINOS

A teoria algébrica dos quadrados latinos foi desenvolvida por diversos matemáticos, mas foi Euler o principal estudioso da teoria. Nesta seção, apresentamos os conceitos de quadrados latinos e suas relações do ponto de vista da matemática formal.

4.2.1 Quadrados latinos

Definição 4.7. Seja X um conjunto finito com n elementos, com $n \in \mathbb{N}$. Um **quadrado latino** de ordem n é uma matriz $n \times n$ em que todas as linhas e todas as colunas formam permutações dos n elementos de X. Isto é, cada elemento de X aparece uma única vez em cada linha e em cada coluna.

Exemplo 4.2.1. A matriz $A = \begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix}$ é um quadrado latino. Já a matriz $B = \begin{bmatrix} 1 & 2 \\ 1 & 2 \end{bmatrix}$ não satisfaz a definição de quadrado latino, pois, as colunas da matriz não formam permutações com os elementos do conjunto $X = \{1, 2\}$.

Exemplo 4.2.2. As matrizes $D = \begin{bmatrix} a & b \\ b & a \end{bmatrix}$, $E = \begin{bmatrix} \alpha & \beta & \gamma \\ \gamma & \alpha & \beta \\ \beta & \gamma & \alpha \end{bmatrix}$ e $F = \begin{bmatrix} ! & \# \\ \# & ! \end{bmatrix}$ são exemplos de quadrados latinos com letras e símbolos.

Exemplo 4.2.3. A tábua de $\mathbb{Z}_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$ com a operação de soma usual em $\mathbb{Z}_4$, é um quadrado latino

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

.

Definição 4.8. Um **quase grupo** é um conjunto X com uma operação $*$ tal que para todos $a, b \in X$, existem únicos $x, y \in X$, tais

que as equações

$$a * x = b \tag{4.1}$$

$$y * a = b \tag{4.2}$$

têm soluções únicas.

Exemplo 4.2.4. Seja o quase grupo $(\mathbb{Z}_3, +)$, temos

$$\begin{array}{lll} \bar{0}+\bar{0}=\bar{0} & \bar{1}+\bar{0}=\bar{1} & \bar{2}+\bar{0}=\bar{2} \\ \bar{0}+\bar{1}=\bar{1} & \bar{1}+\bar{1}=\bar{2} & \bar{2}+\bar{1}=\bar{0} \\ \bar{0}+\bar{2}=\bar{2} & \bar{1}+\bar{2}=\bar{0} & \bar{2}+\bar{2}=\bar{1} \end{array} .$$

Observa-se que para $\bar{0}+\bar{1}=\bar{1}$, dados $\bar{a}=\bar{0}$ e $\bar{b}=\bar{1}$, existe um único $\bar{x} \in (\mathbb{Z}_3, +)$. De fato, $\bar{a}+\bar{x}=\bar{b} \Rightarrow \bar{0}+\bar{x}=\bar{1} \Rightarrow \bar{x}=\bar{1}$.

Assim como, dados $\bar{a}=\bar{1}$ e $\bar{b}=\bar{1}$, existe um único $\bar{y} \in (\mathbb{Z}_3, +)$. De fato, $\bar{y}+\bar{a}=\bar{b} \Rightarrow \bar{y}+\bar{1}=\bar{1} \Rightarrow \bar{y}=\bar{0}$. Verifica-se de maneira análoga para todos os elementos de $(\mathbb{Z}_3, +)$. Logo, $(\mathbb{Z}_3, +)$ é um **quase grupo**.

Exemplo 4.2.5. Tomando $X = \{1, 2, 3\}$ e uma operação $*$. Suas tábuas de operações são:

$$X_1 = \begin{array}{c|ccc} * & 1 & 2 & 3 \\ \hline 1 & 1 & 2 & 3 \\ 2 & 2 & 3 & 1 \\ 3 & 3 & 1 & 2 \end{array} \quad X_2 = \begin{array}{c|ccc} * & 1 & 2 & 3 \\ \hline 1 & 2 & 3 & 1 \\ 2 & 3 & 1 & 2 \\ 3 & 1 & 2 & 3 \end{array} \quad X_3 = \begin{array}{c|ccc} * & 1 & 2 & 3 \\ \hline 1 & 3 & 1 & 2 \\ 2 & 1 & 2 & 3 \\ 3 & 2 & 3 & 1 \end{array}$$

$$X_4 = \begin{array}{c|ccc} * & 1 & 2 & 3 \\ \hline 1 & 1 & 3 & 2 \\ 2 & 3 & 2 & 1 \\ 3 & 2 & 1 & 3 \end{array} \quad X_5 = \begin{array}{c|ccc} * & 1 & 2 & 3 \\ \hline 1 & 3 & 2 & 1 \\ 2 & 2 & 1 & 3 \\ 3 & 1 & 3 & 2 \end{array} \quad X_6 = \begin{array}{c|ccc} * & 1 & 2 & 3 \\ \hline 1 & 2 & 1 & 3 \\ 2 & 1 & 3 & 2 \\ 3 & 3 & 2 & 1 \end{array} .$$

Verificando as propriedades de grupos, temos que a associatividade falha em: X_4, X_5, X_6. Logo, temos um quase grupo que não é grupo.

Proposição 4.3. *Seja X um quase grupo finito de n elementos com uma operação $*$, então sua tábua de operações equivale a um quadrado latino.*

Demonstração. Fixando $i \in X$, defina a função $f_i : X \to X$, $f_i(j) = i * j = A_{i,j}$, em que $A_{i,j}$ é a i-ésima linha da tábua de operações do quase grupo que denotamos por A. Resulta da definição de quase grupos que para todos $a, b \in X$, existe um único $j \in X$ tal que $a * j = b$. Logo, f_i é uma bijeção, e portanto, uma permutação. Isto é, toda linha da tábua é uma permutação dos n elementos de X.

Analogamente, se fixarmos $j \in X$, defina a função permutação $f_j : X \to X$, $f_j(i) = j * i = A_{j,i}$, onde $A_{j,i}$ é a j-ésima coluna da tábua de operações do quase grupo que denotamos por A. Resulta da definição de quase grupos que para todo $a, b \in X$, existe um único $i \in X$ tal que $i * a = b$. Logo, f_j é uma bijeção, e portanto, uma permutação. Isto é, toda coluna da tábua é uma permutação dos n elementos de X.

■

Exemplo 4.2.6. Seja o quase grupo $(\mathbb{Z}_3, +)$, temos que sua tábua de operações é um quadrado latino

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

.

Observação 1. A partir de agora, por abuso de linguagem faremos o uso da equivalência entre quase grupos finitos e quadrados latinos. Isto é, a tábua de operações de um quase grupo é equivalente a tabela de um quadrado latino.

De acordo com Carmelo [6], os quadrados latinos foram definidos tanto em termos combinatórios quanto de forma algébrica - quase grupos - o seguinte resultado nos garante que a tábua de operações de um grupo finito é um quadrado latino.

Proposição 4.4. *Todo grupo é um quase grupo.*

Demonstração. Seja $(X, *)$ um grupo. Devemos mostrar que dado a, $b \in X$, existe uma única solução de

$$a * x = b \tag{4.3}$$

e dado $a, b \in X$, existe uma única solução de

$$x * a = b \ . \tag{4.4}$$

Para provar a equação (4.3), dados $a, b \in X$, temos pela lei do cancelamento à esquerda $x = a^{-1} * b$ é solução. Para mostrar a unicidade, suponha x' solução de $a * x = b$, segue que

$$\begin{aligned} a * x' &= b \\ a^{-1} * (a * x') &= a^{-1} * b \\ (a^{-1} * a) * x' &= a^{-1} * b \\ e * x' &= a^{-1} * b \\ x' &= a^{-1} * b \\ x' &= x \ . \end{aligned}$$

Portanto, a solução da equação (4.3) é única.

Para provar a equação (4.4), dados $a, b \in X$, temos pela lei do cancelamento à direita $x = b * a^{-1}$. Assim, x é solução de (4.4). Para mostrar a unicidade, suponha x'' solução de $x * a = b$, segue que

$$\begin{aligned} x'' * a &= b \\ (x'' * a) * a^{-1} &= b * a^{-1} \\ x'' * (a * a^{-1}) &= b * a^{-1} \\ x'' * e &= b * a^{-1} \\ x'' &= b * a^{-1} \\ x'' &= x \ . \end{aligned}$$

Portanto, a solução da equação (4.4) é única.

Note que a equação (4.3) equivale a equação (4.1) da definição de quase grupo e a equação (4.4) equivale a equação (4.2) da definição de quase grupo, então todo grupo é um quase grupo. ■

Observação 2. A recíproca da Proposição 4.4 é falsa, pois dado

$A = \begin{bmatrix} 1 & 0 & 2 \\ 0 & 2 & 1 \\ 2 & 1 & 0 \end{bmatrix}$. A matriz A falha na associatividade dos elementos, pois $(1 * 0) * 2 = 0 * 2 = 2$ e $1 * (0 * 2) = 1 * 2 = 1$.

Com este resultado, conseguimos garantir sempre a existência de quadrados latinos.

Proposição 4.5. *Dado $n \geq 2$ com $n \in \mathbb{N}$, sempre existe um quadrado latino de ordem n.*

Demonstração. Seja $(\mathbb{Z}_n, +)$ o grupo com a soma usual. Portanto, $(\mathbb{Z}_n, +)$ é um quase grupo. A tábua de operações desse grupo

$+$	0	1	2	$\cdots$	$n-1$
0	0	1	2	$\cdots$	$n-1$
1	1	2	3	$\cdots$	0
2	2	3	4	$\cdots$	1
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
$n-1$	$n-1$	0	1	$\cdots$	$n-2$

é um quadrado latino, em que cada linha tem n elementos distintos e o mesmo acontece para as colunas da tábua. ■

Exemplo 4.2.7. No conjunto do $\mathbb{Z}_m^*$, com a multiplicação usual, sempre que m é primo, temos um grupo. Portanto, podemos obter um quadrado latino de ordem $m - 1$.

Podemos construir quadrados latinos utilizando permutação de linhas e colunas. Defina a permutação Π em $\{0, 1, 2, \ldots, n-1\}$ representada por $\Pi = \begin{pmatrix} 0 & 1 & i & n-1 \\ \pi(0) & \pi(1) & \pi(i) & \pi(n-1) \end{pmatrix}$.

Existem $n!$ possibilidades de permutações em $\{0, 1, 2, \ldots, n-1\}$.

Definição 4.9. Seja α uma permutação de $X = \{0, 1, 2, \ldots, n-1\}$. Dado $A = (A_{i,j})$ uma matriz $n \times n$, defina A^α uma matriz tal que $A^\alpha_{i,j} = A_{i,\alpha(j)}$. Seja β uma permutação de $X = \{0, 1, 2, \ldots, n-1\}$. Dado A uma matriz $n \times n$, defina A^β uma matriz tal que $A^\beta_{i,j} = A_{\beta(i),j}$.

Para a construção de quadrados latinos a partir de permutações de Π, devemos fixar que a matriz A seja um quadrado latino. Então, A^α e A^β também serão quadrados latinos.

Exemplo 4.2.8. Seja $A = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{bmatrix}$ um quadrado latino. Considere $\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ uma permutação. Temos que

$$A = \begin{bmatrix} A_{1,1} & A_{1,2} & A_{1,3} \\ A_{2,1} & A_{2,2} & A_{2,3} \\ A_{3,1} & A_{3,2} & A_{3,3} \end{bmatrix}.$$

Aplicando a permutação α em A, segue que

$$A^\alpha = \begin{bmatrix} A_{1,\alpha(1)} & A_{1,\alpha(2)} & A_{1,\alpha(3)} \\ A_{2,\alpha(1)} & A_{2,\alpha(2)} & A_{2,\alpha(3)} \\ A_{3,\alpha(1)} & A_{3,\alpha(2)} & A_{3,\alpha(3)} \end{bmatrix}$$

$$= \begin{bmatrix} A_{1,3} & A_{1,2} & A_{1,1} \\ A_{2,3} & A_{2,2} & A_{2,1} \\ A_{3,3} & A_{3,2} & A_{3,1} \end{bmatrix}$$

$$= \begin{bmatrix} 3 & 2 & 1 \\ 1 & 3 & 2 \\ 2 & 1 & 3 \end{bmatrix}.$$

4.2.2 Quadrados latinos ortogonais e mutuamente ortogonais

Definição 4.10. Dados dois quadrados latinos de ordem n, $A = (A_{i,j})$ com $1 \leq i \leq n$, $1 \leq j \leq n$ e $B = (B_{i,j})$, definimos $A \otimes B$ como sendo a matriz quadrada de ordem n formada pelos pares $(A_{i,j}, B_{i,j})$ na linha i e coluna j. Chamamos a matriz $A \otimes B$ de **concatenação** de A com B.

Exemplo 4.2.9. Dados $A = \begin{bmatrix} 0 & 1 & 2 \\ 2 & 0 & 1 \\ 1 & 2 & 0 \end{bmatrix}$ e $B = \begin{bmatrix} 0 & 1 & 2 \\ 2 & 0 & 1 \\ 1 & 2 & 0 \end{bmatrix}$, ao

concatenarmos A com B, temos $A \otimes B = \begin{bmatrix} (0,0) & (1,1) & (2,2) \\ (2,2) & (0,0) & (1,1) \\ (1,1) & (2,2) & (0,0) \end{bmatrix}$.

Definição 4.11. Dois quadrados latinos de ordem n, $A = (A_{i,j})$ e $B = (B_{i,j})$, são ditos **ortogonais** ($A \perp B$) se o par $(A_{i,j}, B_{i,j})$ ocorre apenas uma vez em cada entrada de $A \otimes B$.

Exemplo 4.2.10. (a) Dados $A = \begin{bmatrix} 0 & 1 & 2 \\ 2 & 0 & 1 \\ 1 & 2 & 0 \end{bmatrix}$ e

$B = \begin{bmatrix} 1 & 2 & 0 \\ 2 & 0 & 1 \\ 0 & 1 & 2 \end{bmatrix}$, ao concatenarmos A com B, temos

$$A \otimes B = \begin{bmatrix} (0,1) & (1,2) & (2,0) \\ (2,2) & (0,0) & (1,1) \\ (1,0) & (2,1) & (0,2) \end{bmatrix}.$$

Como as entradas da matriz $A \otimes B$ são todas distintas, os quadrados latinos A e B são ortogonais.

(b) O Exemplo 4.2.9 é um caso de concatenação que garante que A e B não são quadrados latinos ortogonais.

Definição 4.12. Um conjunto $\{X_1, X_2, ..., X_r\}$ de quadrados latinos de ordem n é chamado **conjunto de quadrados latinos mutuamente ortogonais**, se dois a dois os quadrados latinos no conjunto forem ortogonais. Denotamos esse conjunto por r-MOLS(n).

Exemplo 4.2.11. (a) Para $X = \{0, 1, 2, 3\}$, segue que

$$X_1 = \begin{bmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \end{bmatrix} \quad X_2 = \begin{bmatrix} 0 & 2 & 3 & 1 \\ 3 & 1 & 0 & 2 \\ 1 & 3 & 2 & 0 \\ 2 & 0 & 1 & 3 \end{bmatrix}$$

$$X_3 = \begin{bmatrix} 0 & 3 & 1 & 2 \\ 2 & 1 & 3 & 0 \\ 3 & 0 & 2 & 1 \\ 1 & 2 & 0 & 3 \end{bmatrix} \text{ são quadrados latinos.}$$

Concatenando X_1, X_2 e X_3 dois a dois, segue que

$$X_1 \otimes X_2 = \begin{bmatrix} (0,0) & (1,2) & (2,3) & (3,1) \\ (1,3) & (0,1) & (3,0) & (2,2) \\ (2,1) & (3,3) & (0,2) & (1,0) \\ (3,2) & (2,0) & (1,1) & (0,3) \end{bmatrix}$$

$$X_2 \otimes X_3 = \begin{bmatrix} (0,0) & (2,3) & (3,1) & (1,2) \\ (3,2) & (1,1) & (0,3) & (2,0) \\ (1,3) & (3,0) & (2,2) & (0,1) \\ (2,1) & (0,2) & (1,0) & (3,3) \end{bmatrix}$$

$$X_3 \otimes X_1 = \begin{bmatrix} (0,0) & (3,1) & (1,2) & (2,3) \\ (2,1) & (1,0) & (3,3) & (0,2) \\ (3,2) & (0,3) & (2,0) & (1,1) \\ (1,3) & (2,2) & (0,1) & (3,0) \end{bmatrix}.$$

Logo, $\{X_1, X_2, X_3\}$ forma um conjunto de quadrados latinos mutuamente ortogonais de ordem 4. Isto é, 3-MOLS(4) = $\{X_1, X_2, X_3\}$.

Exemplo 4.2.12. Vamos construir um quadrado mágico a partir de um quadrado latino ortogonal.

*Um **quadrado mágico** é uma matriz quadrada de ordem $n \times n$ com $n \in \mathbb{Z}$, dispostos de maneira que a soma dos elementos de uma linha qualquer, de uma coluna qualquer e de uma diagonal qualquer têm sempre a mesma soma.*

Utilizando o método de Euler [10]:

$$\text{Dados } A = \begin{bmatrix} a & b & c \\ b & c & a \\ c & a & b \end{bmatrix} \text{ e } B = \begin{bmatrix} \alpha & \beta & \gamma \\ \beta & \gamma & \alpha \\ \gamma & \alpha & \beta \end{bmatrix}.$$

Concatenando A com B, segue que A não é quadrado latino ortogonal com B, pois

$$A \otimes B = \begin{bmatrix} (a,\alpha) & (b,\beta) & (c,\gamma) \\ (b,\beta) & (c,\gamma) & (a,\alpha) \\ (c,\gamma) & (a,\alpha) & (b,\beta) \end{bmatrix}.$$

Sendo assim, devemos trocar a terceira coluna de B com a primeira coluna de B, resultando em C um quadrado latino. Ao concatenarmos C com A, obtemos que A é ortogonal a C, pois

$$C = \begin{bmatrix} \gamma & \beta & \alpha \\ \alpha & \gamma & \beta \\ \beta & \alpha & \gamma \end{bmatrix} \Rightarrow A \otimes C = \begin{bmatrix} (a,\gamma) & (b,\beta) & (c,\alpha) \\ (b,\alpha) & (c,\gamma) & (a,\beta) \\ (c,\beta) & (a,\alpha) & (b,\gamma) \end{bmatrix}.$$

As seguintes condições devem ser satisfeitas para obtermos quadrados mágicos:

(i) $A \otimes C$ deve gerar 9 pares ordenados distintos;

(ii) As sequências das letras latinas devem obedecer uma progressão aritmética de razão 3, resultando no tamanho da matriz;

(iii) $a + b = 2c$;

(iv) As sequências das letras gregas devem obedecer uma progressão geométrica de razão 1.

Da diagonal principal de A, temos (a, c, b) e da diagonal secundária de C, temos (α, γ, β).

Para satisfazer (i), (ii), (iii) e (iv), temos que fixar:

$$\begin{aligned} (a, c, b) &= (1, 4, 7) \\ (\alpha, \gamma, \beta) &= (3, 4, 5). \end{aligned}$$

Resulta que

$$A = (A_{i,j}) = \begin{bmatrix} 1 & 7 & 4 \\ 7 & 4 & 1 \\ 4 & 1 & 7 \end{bmatrix} \text{ e } C = C_{i,j} = \begin{bmatrix} 4 & 5 & 3 \\ 3 & 4 & 5 \\ 5 & 3 & 4 \end{bmatrix}.$$

Substituindo em $A \otimes C$ tal que $(A_{i,j}, B_{i,j}) = (A_{i,j} + C_{i,j})$ em que $+$ é a soma usual, segue que

$$\begin{bmatrix} (a+\gamma) & (b+\beta) & (c+\alpha) \\ (b+\alpha) & (c+\gamma) & (a+\beta) \\ (c+\beta) & (a+\alpha) & (b+\gamma) \end{bmatrix}$$

$\Rightarrow$

$$\begin{bmatrix} (1+4) & (7+5) & (4+3) \\ (7+3) & (4+4) & (1+5) \\ (4+5) & (1+3) & (7+4) \end{bmatrix}$$

$\Rightarrow$

$$\begin{bmatrix} 5 & 12 & 7 \\ 10 & 8 & 6 \\ 9 & 4 & 11 \end{bmatrix}.$$

Portanto, temos um quadrado mágico com o resultado das somas resultam em 24.

5 CONSIDERAÇÕES FINAIS

No decorrer do desenvolvimento deste trabalho foi possível o estudo da teoria dos quadrados latinos, do método de provas e refutações de Lakatos e da consonância do objeto matemático com a história e a filosofia da matemática. Este trabalho teve em seu horizonte o diálogo entre duas áreas de conhecimento: a Matemática Pura e a Educação Matemática.

Conclui-se neste trabalho que uma definição matemática é tão importante quanto os seus resultados. A definição trás a essência do objeto matemático, sendo a partir dela que todos os resultados matemáticos são verificados e validados. Um problema inicial refutado não resulta em um fracasso matemático, e sim, atesta que este conhecimento progride por meio de provas e refutações.

Além disso, a partir da definição de quadrados latinos, foi possível a reconstrução de resultados importantes como a equivalência de quadrados latinos e quase grupos, a validação da Proposição 4.4, assim como a conceituação de quadrados latinos ortogonais e sua aplicação na construção de quadrados mágicos.

A matemática formal foi importante para o desenvolvimento do debate, pois por meio do conhecimento dela, a professora pode ministrar as aulas e orientar seus estudantes com o conhecimento científico. No entanto, o debate reforça a ideia de que a matemática avança por meio de erros e acertos de vários matemáticos ao longo do tempo. Na qual a matemática, tanto na área da Matemática Pura, quanto na Educação Matemática, segundo Silva [14] é um produto humano que muda com o tempo, conforme as culturas, problemas práticos e teóricos da sociedade em que a produz.

O método de Lakatos prioriza a história e a filosofia da matemática. De acordo com D'Ambrosio [9],

> História e filosofia da matemática não se separam e para entender a História da Matemática devemos refletir sobre a filosofia da matemática e a natureza do conhecimento matemático [9, p. 3].

Com isso, conclui-se que a história da matemática está ligada com a construção do conhecimento matemático e a filosofia da matemática com a compreensão do conhecimento matemático.

Conforme abordado no trabalho, o método de Lakatos estimula a criatividade e a autonomia dos envolvidos. Podendo vir a ser um auxílio em um grande desafio da educação matemática, como indica D'Ambrosio [9], que é harmonizar processos e produtos inegavelmente necessários para atuações plenas na sociedade. E ainda, este método pode ser usado como uma abordagem de ensino como sugerem Karakus e Bütün [11] e como exemplificado no debate.

Enfim, não pode-se esquecer do valor científico que cada área tem em seu campo do conhecimento. Mais ainda, não pode-se separar a matemática de sua história e sua filosofia, visto que a filosofia é um meio para a compreensão de conceitos que existem na matemática formal e ainda, a história nos mostra que a matemática se desenvolve por uma contribuição coletiva dos matemáticos.

> A filosofia da matemática sem a história da matemática é vazia, e esta sem aquela é cega (paráfrase de Kant - o entendimento sem a sensibilidade é vazio, a sensibilidade sem o entendimento é cega)- Imre Lakatos [14, p. 21].

REFERÊNCIAS

[1] Lars Dovling Andersen. "Latin square". Em: *Combinatorics: ancient and modern*. Ed. por John J. Watkins e Robin. Wilson. Reino Unido: Oxford University Press, 2013. Cap. 2, pp. 251–283.

[2] Raj Chandra Bose, Sharadchandra S Shrikhande e Ernest T Parker. "Further results on the construction of mutually orthogonal Latin squares and the falsity of Euler's conjecture". Em: *Canad. J. Math* 12 (1960), pp. 189–203.

[3] João Cláudio Brandemberg. "Uma análise histórico-epistemológica do conceito de grupo". Em: *São Paulo: Livraria da Física* (2010).

[4] Richard H Bruck. "Some results in the theory of quasigroups". Em: *Transactions of the American Mathematical Society* 55 (1944), pp. 19–52.

[5] Peter J Cameron. *Combinatorics: topics, techniques, algorithms*. Cambridge University Press, 1994.

[6] Emerson Luiz do Monte Carmelo. *Configurações combinatórias*. Notas de Aula, 2016, p. 30.

[7] Robert S Cohen, Paul K Feyerabend e Marx W Wartofsky. *Essays in memory of Imre Lakatos*. Vol. 39. Springer Science & Business Media, 2012.

[8] Ubiratan D'AMBROSIO. "Reflexões sobre história, filosofia e matemática". Em: *Bolema: boletim de educação matemática, Rio Claro* 2 (1992), pp. 42–60.

[9] Ubiratan D'Ambrosio. "Priorizar história e filosofia da matemática na educação". Em: *Tópicos Educacionais-ISSN: 2448-0215* 18.1-2 (2011).

[10] L. Euler. "On magic squares". Em: *ArXiv Mathematics e-prints* (ago. de 2004). eprint: math/0408230.

[11] Fatih Karakus e Mesut Bütün. "Examining the method of proofs and refutations in pre-service teachers education". Em: *Bo-*

lema: Boletim de Educação Matemática 27.45 (2013), pp. 215–232.

[12] Imre Lakatos. *A lógica do descobrimento matemático: provas e refutações*. Zahar, 1978.

[13] Tatiana Roque. *História da matemática: uma visão crítica, desfazendo mitos e lendas*. Zahar, 2012.

[14] Jairo José da Silva. *Filosofias da matemática*. Unesp, 2007.