UNIVERSIDADE ESTADUAL DE MARINGÁ
DEPARTAMENTO DE MATEMÁTICA
PROGRAMA PROFISSIONAL DE MESTRADO
EM REDE NACIONAL - PROFMAT

NELIDY MOTIZUKI

SUDOKU E TEORIA DE GRUPOS

Maringá

2019

NELIDY MOTIZUKI

SUDOKU E TEORIA DE GRUPOS

Trabalho de Conclusão de Curso elaborado como parte dos requisitos para a obtenção de grau de mestre do Programa Profissional em Matemática em Rede Nacional - PROFMAT

Universidade Estadual de Maringá

Departamento de Matemática

Programa Profissional de Matemática em Rede Nacional - PROFMAT

Orientadora: Prof[a]. Dr. Marcela Duarte Ferrari

Maringá

2019

Dados Internacionais de Catalogação-na-Publicação (CIP)
(Biblioteca Central - UEM, Maringá - PR, Brasil)

Motizuki, Nelidy

M918s Sudoku e teoria de grupos / Nelidy Motizuki. -- Maringá, PR, 2019.
107 f.: il. color., figs., tabs.

Orientadora: Profa. Dra. Marcela Duarte Ferrari.
Dissertação (Mestrado Profissional) - Universidade Estadual de Maringá, Centro de Ciências Exatas, Departamento de Matemática, Programa de Pós-Graduação em Matemática (PROFMAT) - Mestrado Profissional, 2019.

1. Sudoku. 2. Teoria de Grupos. 3. Quadrados Latinos. 4. Construções Lineares de Keedwell. I. Ferrari, Marcela Duarte, orient. II. Universidade Estadual de Maringá. Centro de Ciências Exatas. Departamento de Matemática. Programa de Pós-Graduação em Matemática (PROFMAT) - Mestrado Profissional. III. Título.

CDD 23.ed. 512.2

Ademir Henrique dos Santos - CRB-9/1065

NÉLIDY MOTIZUKI

SUDOKU E TEORIA DE GRUPOS

Dissertação apresentada ao Programa de Mestrado Profissional em Matemática em Rede Nacional do Departamento de Matemática, Centro de Ciências Exatas da Universidade Estadual de Maringá, como parte dos requisitos necessários para a obtenção do título de Mestre em Matemática tendo a Comissão Julgadora composta pelos membros:

COMISSÃO JULGADORA:

Profa. Dra. Marcela Duarte Ferrari
DMA/Universidade Estadual de Maringá (Orientadora)

Prof. Dr. Laerte Bemm
DMA/Universidade Estadual de Maringá

Prof. Dr. Thiago Henrique de Freitas
Universidade Tecnológica Federal do Paraná - Guarapuava

Aprovada em: 30 de agosto de 2019.
Local de defesa: Auditório do DMA, Bloco F67, campus da Universidade Estadual de Maringá.

Dedico este trabalho aos meus amados pais Akemi C. M. Motizuki (in memoriam) e Kenjiro Motizuki.

Agradecimentos

Agradeço minha orientadora Marcela pelo incentivo, paciência e compreensão durante a realização deste trabalho, além de todo conhecimento compartilhado. Sou grata pela dedicação e carinho de minha família, ao meu pai Kenjiro por seu amor incondicional, à minha mãe Akemi por me ensinar à viver com respeito e ao meu irmão Helder pelo apoio durante a minha trajetória de vida e acadêmica. Agradeço à instituição e aos professores do mestrado pela sabedoria e experiência divida conosco.

Não poderia deixar de agradecer às minhas amigas Renata e Elaine que me encorajaram a entrar no mestrado, também sou grata às amigas que conheci durante os estudos Aline, Bruna, Sandra e Simone, pelos bons momentos. Manifesto minha gratidão a todos que contribuíram na minha vida acadêmica e pessoal. Por fim, agradeço à Deus pela força e por me mostrar a beleza de viver.

"Precisamos dar um sentido humano às nossas construções. E, quando o amor ao dinheiro,ao sucesso nos estiver deixando cegos, saibamos fazer pausas para olhar os lírios do campo e as aves do céu.
(Érico Veríssimo)

Resumo

O sudoku é um quebra-cabeça bidimensional que se resume tipicamente na colocação lógica dos algarismos de 1 a 9. Assim, não demorou para que alguns matemáticos iniciarem as suas pesquisas procurando por padrões no sudoku. Este trabalho explora a relação entre o sudoku e a álgebra com o objetivo de verificar se é possível construí-lo por meio da teoria de grupos e quadrados latinos com o intuito de utilizar essa construção como uma atividade diferenciada em sala de aula. Para tanto, realizamos uma pesquisa bibliográfica explorando artigos referentes ao assunto. Verificamos que é possível construir o sudoku utilizando classes laterais e as construções lineares de Keedwell. A partir desses resultados foi possível elaborar uma sugestão de atividade para aplicar em sala.

Palavras-chave: Sudoku. Teoria de Grupos. Quadrados Latinos. Construções Lineares de Keedwell.

Abstract

Sudoku is a two-dimensional puzzle that typically work with logical placement of the numerals from 1 to 9. Therefore, it didn't take long for some mathematicians started their searching for patterns in sudoku. This project explores the relationship between sudoku and algebra in order to verify if is possible to construct the puzzle with Group Theory and Latin Squares in order to use this construction as a different activity in the classroom. Thus, a bibliographic research was made by exploring articles related to the subject. We concluded that it is possible to construct the sudoku using Cosets and also using Linear Keedwell Contruction. From these results it was possible to elaborate an activity to apply in class.

Keywords: Sudoku. Group Theory. Latin Square. Linear Keedwell Contruction.

Lista de ilustrações

Sumário

INTRODUÇÃO

O sudoku é um quebra-cabeça que se tornou febre nos anos 80, apesar do nome ser de origem japonesa o jogo foi inventado nos Estados Unidos por Howard Garns, um arquiteto e admirador de quebra-cabeças. (DELAHAYE, 2006) A origem do sudoku está relacionada aos quadrados latinos, os quais surgiram a partir da tentativa da solução de um problema proposto por Euler. Tal problema é conhecido como o problema dos 36 oficiais, o qual o matemático tenta encontrar uma tabela 6×6, a qual deve distribuir 36 oficiais em 6 regimentos distintos com 6 patentes distintas de maneira que cada regimento tenha exatamente um oficial de uma das 6 patentes. (ALEGRI; SILVA, 2017)

Não demorou muito para o jogo despertar o interesse de pesquisas relacionadas a área das ciências exatas. A respeito dos estudos matemáticos relacionados ao sudoku temos a teoria de grupos como uma das principais ferramentas, o qual estuda as estruturas algébricas denominadas de grupos que são fundamentais para a álgebra abstrata e servirão como base para o estudo dos quadrados latinos, oferecendo assim suporte para nossos estudos a respeito do sudoku. (JUSSIEN, 2007)

Associando a álgebra com o sudoku procuramos um meio de construir o quebra-cabeça utilizando a teoria de grupos e os quadrados latinos. Portanto, realizamos uma pesquisa bibliográfica para reunir informações e teorias que poderíamos utilizar para a construção. Primeiramente efetuamos um estudo algébrico e utilizamos o livro de Introdução à álgebra (GONÇALVES, 2003), exploramos também artigos científicos que relacionam a estrutura algébrica com o jogo. Agora, para a produção da atividade nos baseamos nos conteúdos estruturantes das Diretrizes Curriculares da Educação Básica: Matemática do Paraná (PARANÁ, 2008) e nos Parâmetros Curriculares Nacionais (BRASIL, 1998).

Verificamos então a possibilidade de uma aplicação da álgebra para a elaboração do sudoku, a qual nos permitirá a construção de uma atividade para ser aplicada em sala de aula. O principal objetivo era verificar a possibilidade de utilizar a teoria de grupos e relacioná-la ao sudoku, posteriormente surgiu a ideia de elaborar uma atividade dos resultados obtidos com a pesquisa. Deste modo, trazendo uma atividade diferenciada e mais atrativa para os alunos.

O trabalho está dividido em 4 capítulos, o primeiro é referente as regras do jogo e a história do sudoku. O segundo capítulo é um estudo sobre os quadrados latinos, uma vez que esse assunto servirá de base teórica para construção do sudoku. Para compreender melhor os quadrados latinos há no apêndice a teoria necessária sobre teoria de grupos. Já no capítulo 3 temos a aplicação da álgebra para construir o jogo e por fim no último capítulo há uma sugestão de atividade utilizando as construções do capítulo 3.

Capítulo 1

O JOGO: SUDOKU

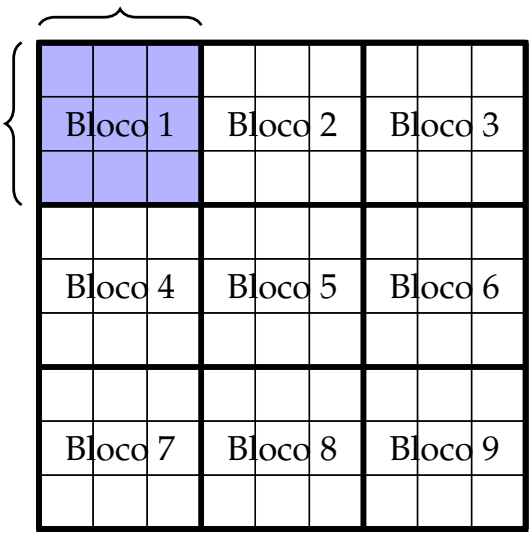
Neste capítulo conheceremos as regras do sudoku e como podemos solucionar o quebra-cabeça. Para isso utilizaremos informações contidas no artigo *The science behind Sudoku* (A ciência do Sudoku) da revista *Scientific American*(DELAHAYE, 2006) e também usaremos as informações dos livros *A to Z Sudoku* (JUSSIEN, 2007) e *Taking Sudoku seriously: The math behind the world's most popular pencil puzzle* (ROSENHOUSE; TAALMAN, 2011) para comentar um pouco sobre a história do jogo, falaremos de sua origem e de como ele foi criado.

Figura 1 – Exemplo de um jogo de sudoku.

			1					3
		6	3	7			4	8
				5		2		9
	7	9					1	5
6			7		5			2
5	3					7	6	
4		1		3				
8	6			2	4	5		
3					8			

O jogo tradicional é jogado em uma malha de 9 linhas e 9 colunas na qual é dividida em 9 sub-malhas as quais denominaremos de blocos, isto é, cada bloco possui 3 linhas e 3 colunas, ilustrados na Figura 2.

Figura 2 – Blocos do sudoku



Cada quebra-cabeça válido possui uma única solução e apesar de ser completado com números poderia ser completado com qualquer conjunto de nove símbolos diferentes, veja (DELAHAYE, 2006). O jogo já se inicia com alguns quadrados preenchidos com números de 1 a 9, como na Figura 1, os quais são chamados de pistas.

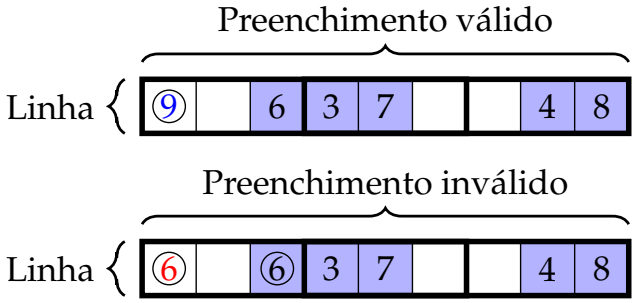
O objetivo no sudoku é preencher a malha 9×9 de maneira que cada linha, coluna e bloco contenha os algarismos de 1 a 9 uma única vez, ou seja, não pode haver a repetição de um mesmo algarismo numa mesma linha, ou numa mesma coluna, ou em um mesmo bloco do quebra-cabeça, veja (ROSENHOUSE; TAALMAN, 2011). Na Figura 3 temos a solução do sudoku da Figura 1. Note que não há a repetição de algarismos em cada linha, coluna e bloco.

Figura 3 – Solução da Figura 1

7	8	2	1	4	9	6	5	3
9	5	6	3	7	2	1	4	8
1	4	3	8	5	6	2	7	9
2	7	9	4	6	3	8	1	5
6	1	4	7	8	5	3	9	2
5	3	8	2	9	1	7	6	4
4	2	1	5	3	7	9	8	6
8	6	7	9	2	4	5	3	1
3	9	5	6	1	8	4	2	7

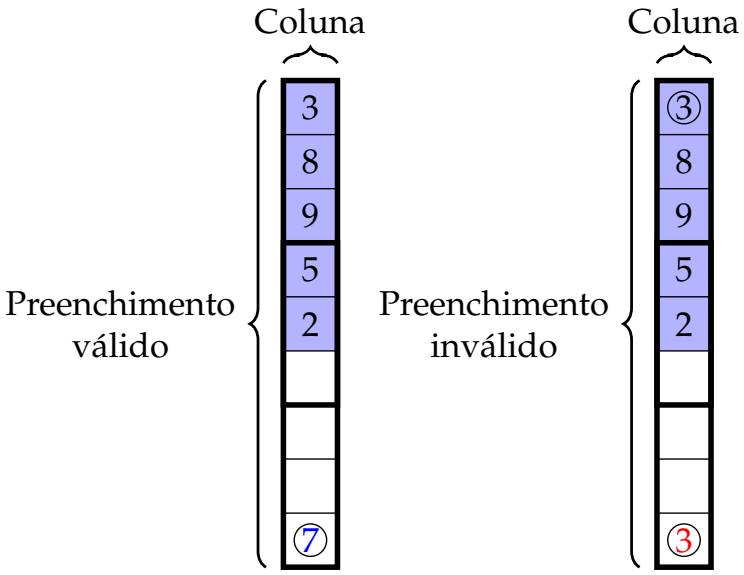
Isto é, cada algarismo aparece uma vez em cada linha, uma única vez em cada coluna e uma única vez em cada bloco.

Figura 4 – Linhas do sudoku.



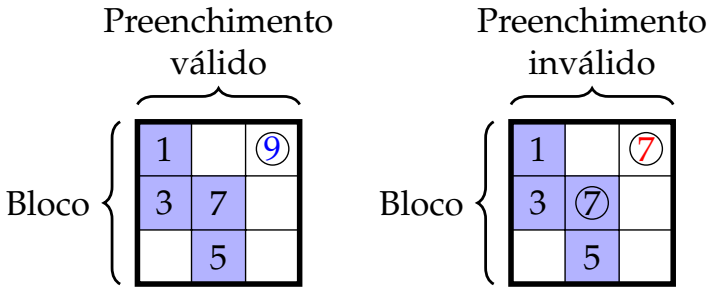
Para cada coluna temos que cada algarismo de 1 a 9 aparece uma única vez.

Figura 5 – Colunas do sudoku.



A mesma situação ocorre para os blocos do sudoku.

Figura 6 – Blocos do sudoku.



1.1 As regras do jogo

Podemos resumir as regras do sudoku da seguinte forma:

1. Devemos preencher cada bloco (sub-malha 3×3) com os algarismos de 1 a 9;
2. Em cada linha da malha aparecem algarismos de 1 a 9 uma única vez;
3. Em cada coluna da malha aparecem algarismos de 1 a 9 uma única vez.

Existem muitas estratégias para resolver sudokus manualmente, mas com duas abordagens práticas um jogador pode obter um bom ponto de partida para preencher o seu quebra-cabeça. Primeiro devemos observar como as linhas, colunas ou blocos estão preenchidos e eliminar as opções de algarismos que são impossíveis de ocuparem certas casas. Com isso o jogador pode reduzir consideravelmente as possibilidades de preenchimento de certos espaços e às vezes identificando lugares em que apenas um algarismo pode ocupar uma determinada casa.

Posteriormente, o jogador deve procurar casas vazias em que um determinado algarismo se encaixa em determinada linha, coluna ou bloco. Por exemplo, podemos localizar os únicos lugares em que o algarismo 1 caberia na linha 3. Por vezes, essa busca leva ao jogador a estabelecer uma única maneira de preencher uma casa. Essa estratégia pode ajudar, mostrando que o algarismo 1 se encaixa em dois ou três espaços. (DELAHAYE, 2006)

No exemplo a seguir podemos notar que o algarismo 1 só pode ocorrer na terceira linha e na sétima coluna, visto que, dada as restrições nos dois primeiros blocos (blocos 1 e 2) conforme a Figura 7, isto é, o número 1 já existe nesses blocos. Temos que esse número só pode ocorrer no bloco 3 na terceira linha, uma vez que o 1 já ocupa a 1ª linha do sudoku.

Figura 7 – Exemplo de estratégia de jogo.

			1					4
1	2	4				3	6	7
			3			①	2	5
4		2	7	1				3
	1		9	4				
			6		2	4	7	1
8		1						9
2		3		9		5		
	8	5	8			7	4	

Para discutirmos melhor sobre o sudoku na próxima seção definiremos um sudoku completo como sendo a malha 9×9 preenchida com os números iniciais, os quais chamaremos de pistas, juntamente com a sua solução, veja a Figura 3, e vamos definir um sudoku inicial como a malha 9×9 do sudoku preenchida somente com as pistas, veja a Figura 1.

1.2 A história do jogo

A palavra sudoku é uma abreviação de uma expressão japonesa "suji wa dokushin ni kagiru", a qual significa que cada dígito deve ser único. A origem do jogo está ligada com os quadrados latinos. Um quadrado latino de ordem n é basicamente uma matriz $n \times n$ preenchida com n símbolos de maneira que um mesmo símbolo não se repete na mesma coluna ou na mesma linha, veja a Definição 2.1.3. Esses quadrados foram objetos de estudos de Leonhard Euler (1707 – 1783). (JUSSIEN, 2007)

Figura 8 – Quadrado latino de ordem 9.

1	2	3	4	5	6	7	8	9
2	3	4	5	6	7	8	9	1
3	4	5	6	7	8	9	1	2
4	5	6	7	8	9	1	2	3
5	6	7	8	9	1	2	3	4
6	7	8	9	1	2	3	4	5
7	8	9	1	2	3	4	5	6
8	9	1	2	3	4	5	6	7
9	1	2	3	4	5	6	7	8

O primeiro sudoku que se assemelha ao quadrado latino de ordem 9 surgiu em uma edição da revista Dell Pencil Puzzles and World Games no ano de 1979. O jogo foi criado por um arquiteto americano aposentado chamado Howard Garns. Esse quebra-cabeça foi lançado nessa revista com o nome de Number Place (lugar dos números). Alguns anos mais tarde a editora japonesa Nikoli introduziu o jogo no Japão com o nome de sudoku. Curiosamente os japoneses conhecem mais o quebra-cabeça pelo nome em inglês "number place"e os americanos pelo nome japonês "sudoku". (DELAHAYE, 2006)

A popularização do sudoku inicialmente se deve à Wayne Gould que passou mais de cinco anos escrevendo um programa de computador que gerasse esses jogos. Wayne também influenciou a publicação do sudoku na revista The Times. Já, no ano de 1989 a companhia de software LOADSTAR publicou o DigiHunt, o primeiro software capaz de

produzir sudokus. Posteriormente, em meados de julho de 2005 o quebra-cabeça chega até a França. (JUSSIEN, 2007)

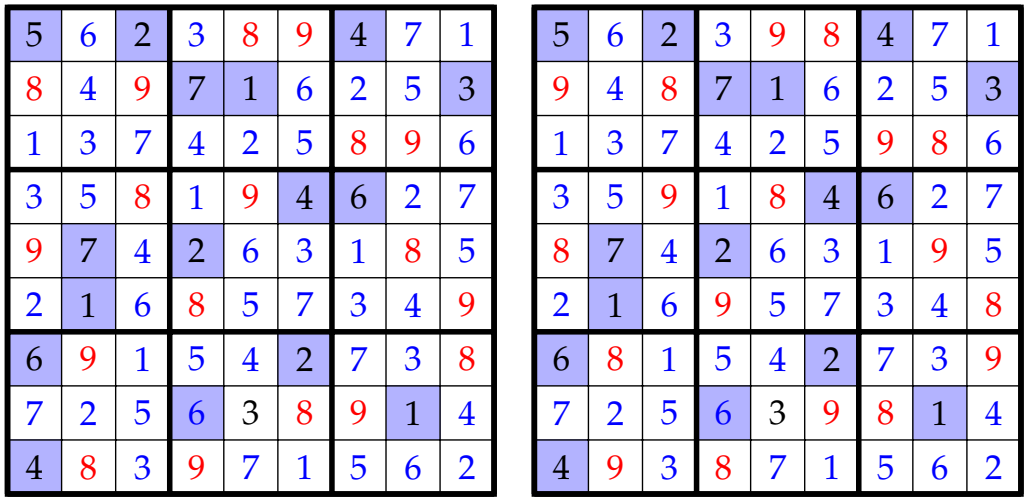
Deste modo, muitos jornais em vários países passaram a publicar o jogo. Tornando ele tão popular que lançaram revistas e livros inteiros direcionados a esse tipo de entretenimento. Não demorou muito para que o sudoku despertasse a atenção de matemáticos para investigar quantos jogos distintos podem existir. Observaram que a resposta deveria ser menor que o número de quadrados latinos distintos de ordem 9. Existem somente 12 quadrados latinos de ordem 3, 576 de ordem 4, mas existem 5.524.751.496.156.892.842.531.225.600 de ordem 9. Estimaram a quantidade de sudokus completos distintos com o uso da lógica matemática e computadores, mas isso não foi tarefa fácil, esse número é 6.670.903.752.021.072.936.960. O resultado foi obtido por Bertram Felgenhauer da Universidade Tecnológica da Alemanha e Frazer Jarvis da Universidade de Sheffield, Inglaterra. (DELAHAYE, 2006)

O campo de pesquisa que relaciona a matemática com o sudoku é muito interessante. Sendo que a teoria combinatória e a teoria de grupos são fundamentais para o estudo desse tema e alguns softwares específicos são utilizados para o auxílio desses estudos. (JUSSIEN, 2007) Note que um sudoku inicial cuja solução é única pode dar origem a outros sudokus iniciais. Tal quebra-cabeça possui interesse para os matemáticos se for mínimo, ou seja, se a remoção de uma pista implicar que a solução do sudoku não é mais única. Calcular o número de sudokus iniciais que são mínimos é atualmente um desafio.

Outro desafio que ainda não possui solução é responder qual deve ser o menor número de pistas de um sudoku inicial para que a sua solução seja única. Estudos indicam que a resposta é de 17 pistas, mas esse resultado ainda não foi provado. O matemático Gordon Royle da Universidade do Oeste da Austrália conseguiu determinar mais de 38 mil exemplos de sudokus iniciais que satisfazem esse critério. Outro matemático da Universidade Nacional da Irlanda, Gary McGuire, lidera estudos na busca de um sudoku inicial com 16 pistas, o qual aparentemente não existe, pois, ainda não conseguiram identificar um sudoku inicial com tais propriedades.

Em contrapartida, Royre com outros pesquisadores conseguiram determinar um sudoku inicial de 16 pistas com apenas duas soluções, o que não significa que um sudoku válido, isto é, um sudoku inicial que possua uma única solução, com 16 pistas não exista. O pesquisador afirma que se fosse possível analisar um sudoku inicial por segundo a pesquisa demoraria em torno de 173 anos e mesmo que conseguisse dividir a pesquisa entre 10 mil computadores a pesquisa iria demorar cerca de um ano. O pesquisador afirma que é necessário a implementação de algoritmos melhores para tornar a pesquisa possível.

Figura 9 – Exemplo de sudoku com 16 pista e duas soluções



Fonte: Adaptação da Figura 1 de (MARTINS; PICADO, 2012).

Atualmente os sudokus são gerados na sua maioria por softwares de computador, um algoritmo que resolve um quebra-cabeça desse tipo pode gerar outros sudokus iniciais. Há também outros softwares, que conseguem verificar se um sudoku possui mais de uma solução e caso haja mais de uma solução se acrescentam mais pistas quanto forem necessárias para que a solução desse sudoku seja única. (DELAHAYE, 2006) A complexidade para resolver um sudoku por meio de um algoritmo é considerado um problema de NP-completo [1]. Podemos pensar que a dificuldade de solucionar um quebra-cabeça sudoku está intimamente ligada ao número de pistas iniciais, mas isso não é verdade. Pois, existem vários sudokus de nível fácil com apenas 17 pistas, enquanto existe sudokus iniciais com mais de trinta pistas difíceis de solucionar. (JUSSIEN, 2007)

A solução computacional mais comum para resolver um jogo é o backtracking, o qual é um algoritmo que utiliza tentativa e erro para solucionar o quebra-cabeça. Durante o processo esse algoritmo pode retornar a um estado anterior ao qual já foi analisado caso necessário. (DELAHAYE, 2006) Descreveremos um exemplo desse tipo de programa e para isso relacionaremos cada casa do sudoku com os números de 1 a 81 como segue na Figura 10.

[1] A classe dos problemas NP são do tipo que podem ser verificados em tempo polinomial, já a classe NP-completo são problemas NP cuja resolução de um deles puder ser efetuada em tempo polinomial então problema NP-completo terá uma solução nesse tempo, o qual é o tempo de execução que é limitado superiormente por uma expressão polinomial.

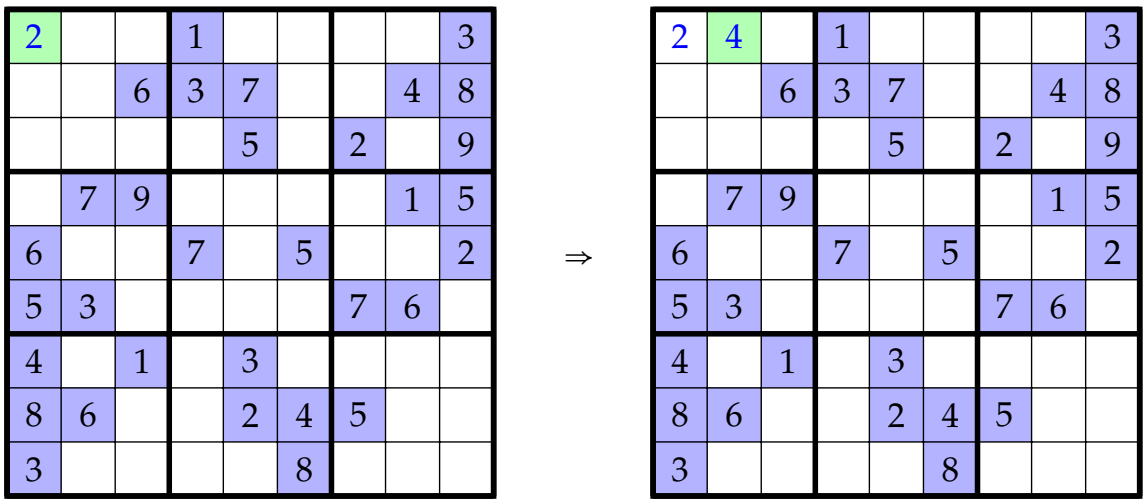
Figura 10 – Enumeração das casas do sudoku.

1	2	3	4	5	6	7	8	9
10	11	12	13	14	15	16	17	18
19	20	21	22	23	24	25	26	27
28	29	30	31	32	33	34	35	36
37	38	39	40	41	42	43	44	45
46	47	48	49	50	51	52	53	54
55	56	57	58	59	60	61	62	63
64	65	66	67	68	69	70	71	72
73	74	75	76	77	78	79	80	81

O software começa percorrer as casas do sudoku de maneira crescente conforme a Figura 10 e identifica a primeira casa vazia, após isso ele vai testar os algarismos de 1 a 9 nessa casa, caso ele não encontre algum conflito com a linha, ou seja, caso não exista a repetição do número testado na linha, não encontre conflito na coluna ou no bloco ele insere o número testado. Após esse procedimento o algoritmo identifica a próxima casa vazia e faz o mesmo processo, não havendo conflito. Caso contrário o algoritmo retorna à última casa preenchida soma uma unidade ao algarismo e verifica a possibilidade dessa casa ser preenchida com esse número, senão ele soma mais uma unidade e tenta o mesmo procedimento novamente. Observando que durante o avanço das casas o algoritmo pode retornar mais de uma casa, se necessário. (DELAHAYE, 2006)

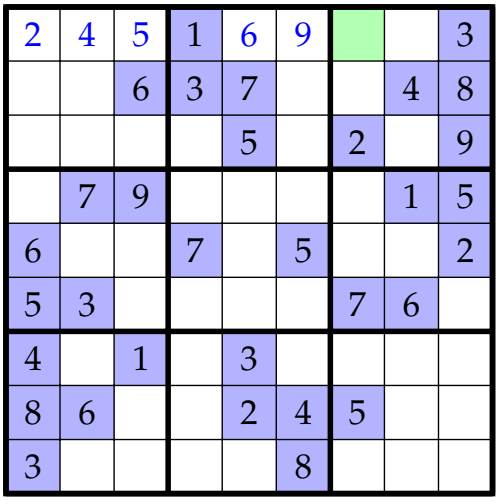
Assim, se usarmos o programa para resolver o sudoku da Figura 1. Ele identificaria a casa 1 como a primeira casa vazia, tentaria inserir o algarismo 1, mas isso daria conflito com a linha. Tentaria inserir o algarismo 2 e como não há conflito ele insere esse algarismo nessa casa. Depois ele identificaria a casa 2 como vazia e tentaria colocar o algarismo 1 nessa casa, mas daria conflito com a linha, tentaria o algarismo 2, mas obteria outro conflito com a linha, tentaria o algarismo 3, mas há um conflito com a coluna e por fim o algoritmo insere o algarismo 4,conforme a Figura 11.

Figura 11 – Inicio da solução da Figura 1 por backtracking.



Realizando esse procedimento, até a casa 6 teríamos o resultado da Figura 12 e na casa 7 o algoritmo não poderia colocar nenhum algarismo de 1 a 9, pois teria algum conflito, assim retornando à casa anterior. Mas, como a soma é maior que 9, ele apaga o algarismo dessa casa e retorna mais uma casa para a casa 5 e soma 1 unidade ao algarismo já existente e verifica se não há conflito, caso haja ele soma mais uma unidade ao número existente e vai realizando esse método recursivamente até terminar o quebra-cabeça.

Figura 12 – Exemplo da solução da Figura 1 por backtracking.



Capítulo 2

QUADRADOS LATINOS

No jogo sudoku é possível relacionar a sua malha 9×9 com a álgebra abstrata, especificamente com a teoria de grupos. Desta maneira, poderemos compreender alguns aspectos dessa teoria, descrita no apêndice, com o objetivo de utilizá-la na construção desse quebra-cabeça e compreender melhor o Capítulo 2.

Assim, nesse capítulo estudaremos sobre os quadrados latinos, os quais antecederam o sudoku e que nos fornecerão pistas de como construir esse quebra-cabeça. Por conseguinte, utilizaremos o artigo Sobre sudoku e grupos (ALEGRI; SILVA, 2017), o qual nos fornecerá suporte teórico para entender como poderemos elaborar esse jogo.

2.1 Definição e exemplos

Primeiramente, vamos definir o que é um quadrado linha para depois definir o quadrado latino.

Definição 2.1.1 (Quadrado Linha)**.** Um quadrado linha de ordem n, $n \geq 1$, é uma matriz quadrada de ordem n cujas entradas de cada linha da matriz correspondem a imagem de uma permutação de S_n. (Veja a Definição A.2.7).

Exemplo 2.1.2. Considere o seguinte quadrado linha P de ordem 9.

$$P = \left[\begin{array}{|ccc|ccc|ccc|} \hline 1&2&3&4&5&6&7&8&9\\ 3&2&1&9&8&6&7&5&4\\ 9&8&7&5&1&2&6&3&4\\ \hline 1&4&2&8&7&6&3&5&9\\ 6&9&5&1&3&2&4&7&8\\ 7&9&3&1&5&6&4&8&2\\ \hline 5&1&3&2&4&6&9&8&7\\ 4&5&6&9&8&1&2&7&3\\ 2&5&7&4&3&9&1&6&8\\ \hline \end{array}\right]$$

Note que não temos a repetição de algarismos nas linhas, mas os algarismos podem se repetir em uma mesma coluna.

Além disso, cada linha da matriz P é a imagem de uma permutação de S_9.

Denotando os elementos de S_9 por f_i, para $i = 1,2,3,4,5,6,7,8,9$, temos:

$$f_i = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ a_{i1} & a_{i2} & a_{i3} & a_{i4} & a_{i5} & a_{i6} & a_{i7} & a_{i8} & a_{i9} \end{pmatrix}$$

e, para $i = 1,2,3,4,5,6,7,8,9$, temos

$$\begin{aligned} f_i : \{1,2,3,4,5,6,7,8,9\} &\longrightarrow \{1,2,3,4,5,6,7,8,9\} \\ j &\longmapsto f_i(j) = a_{ij}. \end{aligned}$$

No exemplo anterior, Exemplo 2.1.2, segue que

$$f_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \end{pmatrix}, \quad f_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 2 & 1 & 9 & 8 & 6 & 7 & 5 & 4 \end{pmatrix},$$

$$f_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 8 & 7 & 5 & 1 & 2 & 6 & 3 & 4 \end{pmatrix}, \quad f_4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 4 & 2 & 8 & 7 & 6 & 3 & 5 & 9 \end{pmatrix},$$

$$f_5 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 9 & 5 & 1 & 3 & 2 & 4 & 7 & 8 \end{pmatrix}, \quad f_6 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 9 & 3 & 1 & 5 & 6 & 4 & 8 & 2 \end{pmatrix},$$

$$f_7 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 1 & 3 & 2 & 4 & 6 & 9 & 8 & 7 \end{pmatrix}, \quad f_8 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 5 & 6 & 9 & 8 & 1 & 2 & 7 & 3 \end{pmatrix}$$

$$\text{e} \quad f_9 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 5 & 7 & 4 & 3 & 9 & 1 & 6 & 8 \end{pmatrix}.$$

Portanto, podemos denotar o quadrado linha P por

$$P = \begin{pmatrix} f_1 \\ f_2 \\ f_3 \\ f_4 \\ f_5 \\ f_6 \\ f_7 \\ f_8 \\ f_9 \end{pmatrix},$$

isto é,

1	2	3	4	5	6	7	8	9	$\longrightarrow f_1$
3	2	1	9	8	6	7	5	4	$\longrightarrow f_2$
9	8	7	5	1	2	6	3	4	$\longrightarrow f_3$
1	4	2	8	7	6	3	5	9	$\longrightarrow f_4$
6	9	5	1	3	2	4	7	8	$\longrightarrow f_5$
7	9	3	1	5	6	4	8	2	$\longrightarrow f_6$
5	1	3	2	4	6	9	8	7	$\longrightarrow f_7$
4	5	6	9	8	1	2	7	3	$\longrightarrow f_8$
2	5	7	4	3	9	1	6	8	$\longrightarrow f_9$

.

Portanto, podemos denotar o quadrado linha P por

$$P = \begin{pmatrix} f_1 \\ f_2 \\ \vdots \\ f_n \end{pmatrix} = (f_1,\ f_2,\ \ldots\ ,\ f_n),$$

ou seja,

$$\begin{array}{|c|c|c|c|l}
\hline
a_{11} & a_{12} & \cdots & a_{1n} & \longrightarrow f_1 \\
\hline
a_{21} & a_{22} & \cdots & a_{2n} & \longrightarrow f_2 \\
\hline
\vdots & \vdots & \ddots & \vdots & \vdots \\
\hline
a_{n1} & a_{n2} & \cdots & a_{nn} & \longrightarrow f_n \\
\hline
\end{array}$$

onde $f_i \in S_n$, para $i = 1, \ldots, n$, de forma que:

$$f_i = \begin{pmatrix} 1 & 2 & \cdots & n \\ a_{i1} & a_{i2} & \cdots & a_{1n} \end{pmatrix} \text{ e } f_i(j) = a_{ij},\ j = 1, 2, \ldots, n.$$

Entretanto, um quadrado linha pode não representar um resultado de um jogo de sudoku, já que sua configuração permite que se obtenha elementos iguais na mesma coluna, isto é, pode existir um quadrado linha $P = (f_1,\ f_2,\ \ldots\ ,\ f_n)$ tal que $f_i(j) = a_{ij} = a_{lj} = f_l(j)$, por exemplo,

1	2	4	5	6	7	8	9	3
2	5	4	3	7	9	6	1	8
3	7	8	1	5	4	2	6	9
1	7	9	3	4	5	8	2	6
4	2	3	7	1	5	6	8	9
6	3	2	1	4	8	7	5	9
4	2	1	5	3	6	7	8	9
8	6	3	1	2	4	5	7	9
3	9	1	6	5	8	2	4	7

o que não satisfaz as regras do jogo sudoku, pois, temos que garantir que não existam elementos repetidos na linha, na coluna e no bloco. Assim, devemos introduzir um novo conceito para representar o resultado de um jogo de sudoku.

Definição 2.1.3 (Quadrado Latino)**.** Um quadrado latino de ordem n, $n \geq 1$ é um quadrado linha de ordem n, cujas entradas são distintas de maneira que seus elementos não se repitam na mesma linha ou na mesma coluna.

Isto é, seja $L = (a_{ij})$ um quadrado latino de ordem n, então temos

$$a_{il} \neq a_{ik} \text{ e } a_{ij} \neq a_{rj} \ \forall \ i, l, k, j \in \{1, 2, \ldots, n\}.$$

a_{11}	a_{12}	$\cdots$	a_{1n}
a_{21}	a_{22}	$\cdots$	a_{2n}
$\vdots$	$\vdots$	$\ddots$	$\vdots$
a_{n1}	a_{n2}	$\cdots$	a_{nn}

Exemplo 2.1.4. Exibimos a seguir um exemplo de quadrado latino de ordem 9.

Figura 13 – Exemplo de um quadrado latino de ordem 9.

2	1	3	4	6	5	7	8	9
1	3	4	6	5	7	8	9	2
3	4	6	5	7	8	9	2	1
4	6	5	7	8	9	2	1	3
6	5	7	8	9	2	1	3	4
5	7	8	9	2	1	3	4	6
7	8	9	2	1	3	4	6	5
8	9	2	1	3	4	6	5	7
9	2	1	3	4	6	5	7	8

Observação 2.1.5. Note que todo quadrado latino é um quadrado linha, mas nem todo quadrado linha é um quadrado latino.

Considere os quadrados a seguir, o quadrado da esquerda é um quadrado latino $L = (a_{ij})$ de ordem 9 e o quadrado da direita é um quadrado linha, $P = (b_{ij})$ de ordem 9.

Perceba que o quadrado da direita não é um quadrado latino de ordem 9, pois, existem algarismos que se repetem na coluna, por exemplo, $a_{52} = 5 = a_{53}$.

2	1	3	4	6	5	7	8	9
1	3	4	6	5	7	8	9	2
3	4	6	5	7	8	9	2	1
7	8	9	2	1	3	4	6	5
8	9	2	1	3	4	6	5	7
9	2	1	3	4	6	5	7	8
4	6	5	7	8	9	2	1	3
6	5	7	8	9	2	1	3	4
5	7	8	9	2	1	3	4	6

1	2	3	4	5	6	7	8	9
3	2	1	9	8	6	7	5	4
9	8	7	5	1	2	6	3	4
5	1	3	2	4	6	9	8	7
4	5	6	9	8	1	2	7	3
2	5	7	4	3	9	1	6	8
1	4	2	8	7	6	3	5	9
6	9	5	1	3	2	4	7	8
7	9	3	1	5	6	4	8	2

Definição 2.1.6 (Tabela de Cayley)**.** A tabela de Cayley é uma tábua de operações de um grupo finito. (Veja a Definição A.2.23).

Atente-se que na construção da Tabela de Cayley de um jogo de sudoku não podemos ter repetições de elementos nem nas linhas e, nem nas colunas.

Exemplo 2.1.7 (Grupo de Klein)**.** Mostraremos a tabela do grupo conhecido como grupo de Klein, o qual possui 4 elementos.

Representaremos o elemento neutro por e, e, os outros elementos por a_2, a_3 e a_4. Definimos a operação $*$ desse grupo como:

(i) $a_2 * a_2 = a_3 * a_3 = a_4 * a_4 = e$;

(ii) $a_2 * a_3 = a_3 * a_2 = a_4$;

(iii) $a_2 * a_4 = a_4 * a_2 = a_3$;

(iv) $a_3 * a_4 = a_4 * a_3 = a_2$.

Assim, para o grupo $G = \{e,\ a_2,\ a_3,\ a_4\}$ com a operação definida acima temos a tabela de Cayley dada por:

$*$	e	a_2	a_3	a_4
e	e	a_2	a_3	a_4
a_2	a_2	e	a_4	a_3
a_3	a_3	a_4	e	a_2
a_4	a_4	a_3	a_2	e

.

Proposição 2.1.8 (Existência de Quadrados Latinos)**.** Para qualquer natural $n > 1$, existe um quadrado latino de ordem n.

Demonstração. Para os inteiros $1,\ 2, \ldots,\ n$, vamos construir um quadrado latino L, da seguinte forma, na primeira linha da matriz de L, inserimos os elementos em ordem crescente, ou seja, para $i = 1$,

$$a_{1j} = j = \big(1 + j\big) - 1,$$

para todo $j = 1, 2, \ldots, n$.

Na segunda linha tomamos a ordem dos elementos da primeira linha e transladamos os elementos uma posição para esquerda e colocamos o primeiro elemento na última coluna, isto é, para $i = 2$,

$$\begin{cases} a_{2n} = a_{11} = a_{1((2+n-1)-n)}, \\ \\ a_{2j} = a_{1(j+1)} = j + 1 = \big(2 + j\big) - 1 = \big(i + j\big) - 1, \end{cases}$$

para todo $j = 1, 2, \ldots, n - 1$.

Para a terceira linha tomamos a ordem dos elementos da segunda linha e fazemos o mesmo procedimento que fizemos para a segunda linha, assim

$$\begin{cases} a_{3n} = a_{12} = a_{1((3+n-1)-n)}, \\ \\ a_{3(n-1)} = a_{11} = a_{1((3+(n-1)-1)-n)}, \\ \\ a_{3j} = a_{2(j+1)} = a_{1(j+2)}, \end{cases}$$

para todo $j = 1, 2, \ldots, n - 2$.

Fazendo esse processo até a n-ésima linha, conseguimos o quadrado latino:

$$a_{ij} = \begin{cases} j, & \text{se} \quad i = 1 \\ \\ a_{1(j+i-1)}, & \text{se} \quad i > 1 \text{ e } j + i - 1 < n \\ a_{1(j+i-1-n)}, & \text{se} \quad i > 1 \text{ e } j + i - 1 \geq n \end{cases}$$

Isto é,

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

.

■

Note que, pela construção anterior não há algarismos repetidos nas linhas, pois, os elementos de 1 a n são distintos e as linhas são preenchidas com n elementos.

Também, não temos algarismos repetidos nas colunas, caso contrário pelo modo de construção deveríamos ter ao menos 2 algarismos repetidos em uma mesma linha, o que não ocorre.

Observação 2.1.9. Note que os quadrados latinos são bem parecidos com as tabelas de Cayley de grupos, isto é, toda tabela de Cayley é um quadrado latino, conforme o Corolário 2.2.6. Mas, não podemos afirmar que todo quadrado latino é uma tabela de Cayley como poderemos observar no Exemplo 2.2.12 na próxima seção.

2.2 Grupos e quadrados latinos

Nesta seção temos como objetivo demonstrar que toda tábua de operação de um grupo finito é sempre um quadrado latino, mas a recíproca não é verdadeira, ou seja, toda tabela de Cayley é um quadrado latino.

Exemplo 2.2.1. Dadas as duas tabelas a seguir.

$*$	1	2	3	4
1	1	4	3	2
2	2	3	4	1
3	3	1	2	4
4	4	2	1	3

$*$	1	2	3	4
1	1	2	3	4
2	2	1	4	3
3	3	4	1	2
4	4	3	2	1

Observe que a tabela da direita representa a tábua de operação do grupo de Klein, (veja o Exemplo 2.1.7) o qual elemento neutro está representado pelo algarismo 1 e os

elementos $a_2,\ a_3,\ a_4$ por $2, 3, 4$, respectivamente. Por outro lado, a tabela da esquerda não representa a tabela de um grupo, pois, a operação não é associativa. De fato, temos $(3 * 1) * 2 = 3 * 2 = 1$, mas $3 * (1 * 2) = 3 * 4 = 4$.

Previamente à demonstração de que toda tabela de Cayley é um quadrado latino, vamos definir uma estrutura algébrica mais simples que o grupo, (veja a Definição A.1.3 item (iii)), chamada de quasigrupo.

Definição 2.2.2 (Quasigrupo)**.** Seja um conjunto Q munido de uma operação binária $*$ se para todo elemento $a, b \in Q$, as equações $a * x = b$ e $y * a = b$ são unicamente solúveis para x e y em Q, ou seja, se $a * x_1 = b$ e $a * x_2 = b$ temos $x_1 = x_2$ e se $a * y_1 = b$ e $a * y_2 = b$ temos $y_1 = y_2$, então a estrutura algébrica $(Q, *)$ é um quasigrupo.

Observação 2.2.3. Devido a lei de cancelamento todo grupo é um quasigrupo.

Proposição 2.2.4 (A Tábua de operações e os Quadrados Latinos)**.** Dada a tábua de operação de um quasigrupo finito $(G, *)$ obtemos um quadrado latino de ordem n.

Demonstração. Considere sem perda de generalidade um quasigrupo com $G = \{1, 2, \ldots, n\}$, cuja a tábua de operação é dada por:

$*$	1	2	$\cdots$	n
1	$1 * 1$	$1 * 2$	$\cdots$	$1 * n$
2	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
n	$\cdots$	$\cdots$	$\cdots$	$n * n$

.

Suponha por absurdo, que a tábua de operação não seja um quadrado latino. Logo, existe algum elemento que se repete na linha ou algum elemento que se repete na coluna. Se há algum elemento repetido na mesma linha, suponha na linha 1, então teríamos $1 * x_1 = b$ e $1 * x_2 = b$, tais que $x_1 \neq x_2$ com $x_1, x_2, b \in G$, o que contradiz o fato de G ser um quasigrupo. Analogamente, se supormos que existam elementos repetidos na mesma coluna, teríamos que a equação $y * a = b$ não teria solução única para y, com $y, a, b \in G$. ■

Proposição 2.2.5. Se $(Q, *)$ possui uma estrutura algébrica de quasigrupo associativa então $(Q, *)$ é um grupo.

Demonstração. Primeiramente, como por hipótese a estrutura é associativa basta mostrar que a estrutura algébrica possui elemento neutro e que para todo elemento pertencente à G existe o inverso. Vamos mostrar que existe o elemento neutro e, único. Assim, pela definição de quasigrupo existem $e_1, e_2, x \in Q$, tais que $x * e_1 = x$ e $e_2 * x = x$. Então, temos que

$$x * e_1 * e_1 = x * e_1 = x.$$

Como, a equação $x * (e_1 * e_1) = x * e_1$ possui uma única solução temos $e_1 * e_1 = e_1$. Agora, se $a \in Q$ de maneira que $e_1 * a = x$, então

$$e_2 * e_1 * a = e_2 * x = x = e_1 * a.$$

Portanto, como a equação $(e_2 * e_1) * a = e_1 * a$ possui uma única solução temos que $e_2 * e_1 = e_1$, e ainda como $e_1 * e_1 = e_1$ obtemos $e_2 * e_1 = e_1 * e_1$ e pela definição de quasigrupo conseguimos $e_2 = e_1$. Então, tomando $e = e_1$ temos que para qualquer $y \in Q$, $e * y = e * e * y$, implicando $y = e * y$. Da mesma maneira, obtemos $y = y * e$. Dado que x e y são arbitrários então e é o elemento neutro de $(Q, *)$.

Agora mostraremos que para todo $x \in Q$ existe um único inverso. Pela definição de quasigrupo e pela existência do elemento neutro existem únicos $a, b \in Q$, tais que $x * a = e$ e $b * x = e$. Assim,

$$a = e * a = (b * x) * a = b * (x * a) = b * e = b.$$

Logo, tomando $x^{-1} = a = b$ temos o desejado. ∎

Colorário 2.2.6. A tábua de operação de um grupo finito de ordem n é um quadrado latino de ordem n.

Demonstração. De fato, uma vez que a tábua de operação de um quasigrupo é um quadrado latino e todo grupo é um quasigrupo. ∎

Observação 2.2.7. Consequentemente, como a tabela de Cayley é a tábua de operação de um grupo finito, (ver 2.1.6) temos pelo Corolário 2.2.6 que toda tabela de Cayley é um quadrado latino.

Observação 2.2.8. Para o próximo exemplo utilizaremos o grupo $(\mathbb{Z}_n, +)$. (Veja o Exemplo A.2.25). Adotaremos também a notação da Observação A.2.22.

Exemplo 2.2.9. Seja o seguinte quadrado latino em que seus elementos pertencem à $\mathbb{Z}_4$ com a operação adição,

$+$	1	2	3	4
1	2	3	4	1
2	3	4	1	2
3	4	1	2	3
4	1	2	3	4

tomando duas linhas quaisquer e as considerando como as imagens de uma permutação de S_4 o resultado da composição dessas linhas será uma das linhas do quadrado. Assim, compondo a 1^a com a 2^a linha, obtemos a 3^a linha:

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

Logo, se $f_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ e $f_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$, temos $f_1 \circ f_2(x) = f_{1+2}(x)$. Note que, a terceira linha pode ser obtida, calculando $(1+2)+x = 1+(2+x)$, $\forall x \in \mathbb{Z}_4$, equivalentemente se $f_1 \circ f_2(x) = f_{1+2}(x)$, onde $f_g(x) = g + x$.

Mostraremos com o próximo teorema que se a composição de duas linhas do quadrado latino resultarem em uma linha desse quadrado, então o quadrado é uma tabela de Cayley de um grupo.

Teorema 2.2.10 (Caracterização dos Quadrados Latinos)**.** Um quadrado latino é a tabela de um grupo se, e somente se, a composição de quaisquer duas linhas é uma linha do quadrado.

Demonstração. Seja L um quadrado latino de maneira que o mesmo representa a tábua de operação de grupo $(X, *)$, em que $X = \{1, 2, \ldots, n\}$ com a operação binária $*$ explicitada nesse quadrado.

Considere o elemento neutro de X dado por 1 e a aplicação definida por:

$$\begin{aligned} f : X &\to S_n \\ g \mapsto f_g : X &\to X \\ x &\mapsto f_g(x) = g * x. \end{aligned}$$

De maneira que $f_g \in S_n$, onde $f_g(x) = g * x, \forall x \in X$.

Perceba que f está bem definida, pois, se $g = h$, temos $g * x = h * x$, então $f_g(x) = f_h(x), \forall x \in X$.

Vamos mostrar que o quasigrupo $(X, *)$ é associativo (ou seja, que $(X, *)$ é um grupo) se, e somente se, $f(X)$ é subgrupo de S_n.

Assim, seja $(X, *)$ um quasigrupo associativo, então

$$f_g \circ f_h(x) = f_g(f_h(x)) = f_g(h * x) = g * (h * x) = (g * h) * x = f_{g*h}(x), \forall x \in X,$$

e logo $f_g \circ f_h = f_{g*h}$.

Portanto, $f(X)$ é subgrupo de S_n, pois $f_1(x) = 1 * x$ é o elemento neutro de $f(X)$, uma vez que

$$f_g \circ f_1(x) = g * (1 * x) = g * x = f_g \quad \text{e} \quad f_1 \circ f_g(x) = 1 * (g * x), \ \forall g \in X.$$

E ainda, para $\forall g \in X$ temos $g^{-1} \in X$, pois

$$f_g \circ f_g^{-1} = g * g^{-1} * x = 1 * x = f_1 = g^{-1} * g * x = f_g^{-1}(x) \circ f_g.$$

Reciprocamente, seja $f(X)$ um subgrupo de S_n. Logo, $f_a \circ f_b = f_c$ para algum c em X.

Considere $f_a \circ f_b(1)$ e $f_c(1)$, então $f_a(b * 1) = f_a(b) = a * b = f_c(1) = c * 1$, logo $a * b = c$.

Portanto, $(a * b) * c = f_{a*b} = f_{a*b}(c) = f_a \circ f_b(c) = f_a(b * c) = a * (b * c)$, para quaisquer a, b e $c \in X$.

Note que $(f(X), \circ)$ é de fato um subgrupo de S_n, pois a composição de quaisquer duas permutações $f(X)$ está ainda em $f(X)$, uma vez que o elemento neutro $f_1 \in f(X)$ e o oposto de f_g^{-1} de f_g pertence à $f(X)$, $\forall g \in X$.

Então, nos resta mostrar que $f_a \circ f_b = f_c$, ou seja, vamos mostrar que a composição de duas linhas é uma linha do quadrado latino L. De fato, sejam as linhas

$$L_a = (f_a(1), f_a(2), \ldots, f_a(n)) \quad \text{e} \quad L_b = (f_b(1), f_b(2), \ldots, f_b(n))$$

a composição delas é dada por:

$$L_a \circ L_b = (f_a(1), f_a(2), \ldots, f_a(n)) \circ L_b = (f_b(1), f_b(2), \ldots, f_b(n))$$

Portanto, $L_a \circ L_b$ é uma linha de L se $L_a \circ L_b = (f_c(1), f_c(2), \ldots, f_c(n))$ e isso ocorre se, e somente se, $f_a \circ f_b = f_c$. ■

Observação 2.2.11. O Teorema 2.2.10 é conhecido como Método de Siu e para mostrar que um quadrado latino não é uma tabela de Cayley basta mostrar que existem pelo menos duas linhas do quadrado que quando compostas não geram uma outra como mostramos no Exemplo 2.2.12 a seguir.

Exemplo 2.2.12. Considere o seguinte quadrado latino.

1	2	3	4	6	5	7	8	9
4	5	6	7	8	9	1	2	3
7	8	9	1	2	3	4	5	6
2	7	1	3	6	4	8	9	5
8	3	5	2	9	1	6	4	7
9	6	4	5	7	8	2	3	1
3	1	2	6	4	5	9	7	8
5	9	7	8	1	2	3	6	4
6	4	8	9	3	7	5	1	2

Compondo a sexta linha com a segunda linha é possível notar que o resultado não é outra linha do quadrado, portanto, o quadrado latino não é uma tabela de Cayley.

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

2.3 MOLS

Definição 2.3.1 (Operação $\odot$)**.** Sejam dois quadrados latinos de ordem n dados por $L_1 = (a_{ij})$ e $L_2 = (bij)$ definimos $L_1 \odot L_2$ como a matriz $c_{ij} = (a_{ij}, b_{ij})$ de ordem n com entradas em $\mathbb{Z} \times \mathbb{Z}$.

Exemplo 2.3.2. Dados os seguintes quadrados latinos de ordem 4.

$$L_1 = \begin{array}{|c|c|c|c|}\hline 2&1&3&4\\\hline 4&3&2&1\\\hline 1&2&4&3\\\hline 3&4&1&2\\\hline\end{array} \qquad L_2 = \begin{array}{|c|c|c|c|}\hline 4&2&3&1\\\hline 3&1&2&4\\\hline 1&3&4&2\\\hline 2&4&1&3\\\hline\end{array}$$

Temos que, $L_1 \odot L_2$ é dado por:

$$L_1 \odot L_2 = \begin{bmatrix} (2,4) & (1,2) & (3,3) & (4,1) \\ (4,3) & (3,1) & (2,2) & (1,4) \\ (1,1) & (2,3) & (4,4) & (3,2) \\ (3,1) & (4,4) & (1,1) & (2,3) \end{bmatrix}.$$

Definição 2.3.3 (Quadrados Ortogonais)**.** Sejam dois quadrados latinos de ordem n, $L_1 = (a_{ij})$ e $L_2 = (b_{ij})$, dizemos que esses quadrados são ortogonais se o par (a_{ij}, b_{ij}) ocorre apenas uma vez em $L_1 \odot L_2$, ou seja, $(a_{ij}, b_{ij}) \neq (a_{lk}, b_{lk})$ $\forall i, j, l, k$. Escrevemos $L_1 \perp L_2$.

Exemplo 2.3.4. Sejam os seguintes quadrados latinos de ordem 4.

$$L_1 = \begin{array}{|c|c|c|c|}\hline 1&4&2&3\\\hline 3&2&4&1\\\hline 4&1&3&2\\\hline 2&3&1&4\\\hline\end{array} \qquad L_2 = \begin{array}{|c|c|c|c|}\hline 1&3&4&2\\\hline 4&2&1&3\\\hline 2&4&3&1\\\hline 3&1&2&4\\\hline\end{array}$$

Assim,

$$L_1 \odot L_2 = \begin{bmatrix} (1,1) & (4,3) & (2,4) & (3,2) \\ (3,4) & (2,2) & (4,1) & (1,3) \\ (4,2) & (1,4) & (3,3) & (2,1) \\ (2,3) & (3,1) & (1,2) & (4,4) \end{bmatrix}.$$

Logo, os quadrados latinos L_1 e L_2 são ortogonais, ou seja, $L_1 \perp L_2$.

Exemplo 2.3.5. Agora, se tomarmos os seguintes quadrados latinos de ordem 4.

$$M_1 = \begin{array}{|c|c|c|c|}\hline 1&4&2&3\\\hline 3&2&4&1\\\hline 4&1&3&2\\\hline 2&3&1&4\\\hline\end{array} \qquad M_2 = \begin{array}{|c|c|c|c|}\hline 1&3&4&2\\\hline 4&1&2&3\\\hline 3&2&1&4\\\hline 2&4&3&1\\\hline\end{array}$$

Observe que

$$M_1 \odot M_2 = \begin{bmatrix} (1,1) & (4,3) & (2,4) & (3,2) \\ (3,4) & (2,1) & (4,2) & (1,3) \\ (4,3) & (1,2) & (3,1) & (2,4) \\ (2,2) & (3,4) & (1,3) & (4,1) \end{bmatrix}.$$

e assim os quadrados latinos M_1 e M_2 não são ortogonais, pois o par $(1,3)$ se repete em $M_1 \odot M_2$.

Definição 2.3.6 (MOLS)**.** Dado um conjunto $M = \{L_1, L_1, \ldots, L_k\}$ de quadrados latinos de ordem n. Dizemos que esse conjunto é mutualmente ortogonal se para cada $i \neq j$, o quadrado latino L_i é ortogonal ao quadrado latino L_j, com $1 \leq i, j \leq k$.

Vamos denotar o conjunto M por MOLS, que em inglês significa *Mutually Ortogonal Latin Squares*.

Exemplo 2.3.7. Podemos verificar no conjunto a seguir os quadrados latinos formam um conjunto mutualmente ortogonal.

$$\begin{array}{|c|c|c|c|}\hline 1&2&4&3\\\hline 2&1&3&4\\\hline 4&3&1&2\\\hline 3&4&2&1\\\hline\end{array} \qquad \begin{array}{|c|c|c|c|}\hline 1&2&4&3\\\hline 4&3&1&2\\\hline 3&4&2&1\\\hline 2&1&3&4\\\hline\end{array} \qquad \begin{array}{|c|c|c|c|}\hline 1&2&4&3\\\hline 3&4&2&1\\\hline 2&1&3&4\\\hline 4&3&1&2\\\hline\end{array}$$

Proposição 2.3.8 (Ortogonalidade de MOLS)**.** Para um conjunto k de MOLS, uma permutação dos símbolos não afeta a ortogonalidade.

Demonstração. Sejam dois quadrados latinos de ordem n dados pelas matrizes $L = [l_{ij}]_{n\times n}$ e $L' = [l'_{ij}]_{n\times n}$, com $l_{ij}, l'_{ij} \in I_n = \{1, 2, \ldots, n\}$ de maneira que L e L' são mutualmente ortogonais, ou seja, para a matriz $L \odot L' = [(l_{ij}, l'_{ij})]$ podemos associar cada elemento da matriz ao par ordenado $(l_{ij}, l'_{ij}) \in I_n \times I_n$, em que (l_{ij}, l'_{ij}) aparece uma única vez entre os n^2 pares (l_{ij}, l'_{ij}), $1 \leq i, j \leq n$. Assim, se $l_{ij} = l_{xy}$ e $l'_{ij} = l'_{xy}$ então $i = x$ e $j = y$.

Representamos uma bijeção entre os elementos da mesma posição das matrizes L e L' na matriz $L \odot L'$, da seguinte maneira:

$$\begin{aligned} I_n \times I_n &\to I_n \times I_n \\ (i,j) &\mapsto (l_{ij}, l'_{ij}) \end{aligned}$$

Lembrando que $(l_{ij}, l'_{ij}) \in I_n \times I_n$ aparece uma única vez entre os n^2 pares de $I_n \times I_n$. Definimos as permutações σ e σ' em I_n, para L e L', respectivamente. Queremos mostrar que L^σ e $L'^{\sigma'}$ ainda são ortogonais.

Suponha por absurdo que $L \perp L'$ mas $L^\sigma \not\perp L'^{\sigma'}$, então existe um par $(i,j) \neq (x,y)$ tal que $l^\sigma_{ij} = l^\sigma_{xy}$ e $l'^{\sigma'}_{ij} = l'^{\sigma'}_{xy} \Rightarrow (l^\sigma_{ij}, l'^{\sigma'}_{ij}) = (l^\sigma_{xy}, l'^{\sigma'}_{xy})$, mas como σ e σ' são bijetivas temos σ^{-1} e σ'^{-1}. Assim, $(l^{\sigma\circ\sigma^{-1}}_{ij}, l'^{\sigma'\circ\sigma'^{-1}}_{ij}) = (l^{\sigma\circ\sigma^{-1}}_{x} y, l'^{\sigma'\circ\sigma'^{-1}}_{xy}) \Rightarrow (l_{ij}, l'_{ij}) = (l_{xy}, l'_{xy})$ com $(i,j) \neq (x,y)$, fato esse que não pode ocorrer pois $L \perp L'$. ∎

Exemplo 2.3.9. Sejam os quadrados latinos do exemplo 2.3.4 dados em seguida.

$$T_1 = \begin{array}{|c|c|c|c|} \hline 1 & 4 & 2 & 3 \\ \hline 3 & 2 & 4 & 1 \\ \hline 4 & 1 & 3 & 2 \\ \hline 2 & 3 & 1 & 4 \\ \hline \end{array} \qquad T_2 = \begin{array}{|c|c|c|c|} \hline 1 & 3 & 4 & 2 \\ \hline 4 & 2 & 1 & 3 \\ \hline 2 & 4 & 3 & 1 \\ \hline 3 & 1 & 2 & 4 \\ \hline \end{array}$$

Note que, $T_1 \perp T_2$ aplicando a permutação $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}$ ao quadrado T_1 e aplicando a permutação $\sigma' = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}$ em T_2 obtemos os quadrados T_1^σ e $T_2^{\sigma'}$.

$$T_1^\sigma = \begin{array}{|c|c|c|c|} \hline 1 & 2 & 3 & 4 \\ \hline 4 & 3 & 2 & 1 \\ \hline 2 & 1 & 4 & 3 \\ \hline 3 & 4 & 1 & 2 \\ \hline \end{array} \qquad T_2^{\sigma'} = \begin{array}{|c|c|c|c|} \hline 1 & 2 & 3 & 4 \\ \hline 3 & 4 & 1 & 2 \\ \hline 4 & 3 & 2 & 1 \\ \hline 2 & 1 & 4 & 3 \\ \hline \end{array}$$

Portanto,

$$T_1{}^{\sigma} \odot T_2{}^{\sigma'} = \begin{bmatrix} (1,1) & (2,2) & (3,3) & (4,4) \\ (4,3) & (3,4) & (2,1) & (1,2) \\ (2,4) & (1,3) & (4,2) & (3,1) \\ (3,2) & (4,1) & (1,4) & (2,3) \end{bmatrix}.$$

Logo, $T_1{}^{\sigma} \perp T_2{}^{\sigma'}$.

Definição 2.3.10. Definimos $N(n)$ a maior quantidade possível de quadrados latinos dentro de um conjunto, tal que esse conjunto é formado por MOLS de ordem n.

Proposição 2.3.11 (Limitante para $N(n)$)**.** Para cada $n \geq 2$, $N(n) \leq n-1$.

Demonstração. Dado um conjunto $M = \{L_1, L_2, \ldots, L_k\}$ de quadrados latinos mutualmente ortogonais. Tomamos dois quadrados desse conjunto, digamos L_1 e L_2. Pela Proposição 2.3.8 podemos efetuar permutações em L_1 e L_2 sem afetar a sua ortogonalidade, então fazemos isso de maneira que a primeira linha de cada quadrado é dada por $(1, 2, \ldots, n)$, então:

$$L_1 = \begin{array}{|c|c|c|c|} \hline 1 & 2 & \cdots & n \\ \hline a & - & \cdots & - \\ \hline \vdots & \vdots & \ddots & \vdots \\ \hline - & - & \cdots & - \\ \hline \end{array} \qquad L_2 = \begin{array}{|c|c|c|c|} \hline 1 & 2 & \cdots & n \\ \hline b & - & \cdots & - \\ \hline \vdots & \vdots & \ddots & \vdots \\ \hline - & - & \cdots & - \\ \hline \end{array}$$

Note que, os símbolos a e b não podem assumir o valor 1, pois, L_1 e L_2 são quadrados latinos. Também, não podemos ter $a = b$, uma vez que os pares (i, i) com $i \in I_n = \{1, 2, \ldots, n\}$ já ocupam a primeira linha de $L_1 \odot L_2$. Assim, há no máximo $n-1$ símbolos para escolher no lugar de a e como não há dois quadrados latinos ortogonais com o mesmo símbolo na mesma posição de a temos que $N(n) \leq n-1, \ \forall n \geq 2$.

■

2.4 Relação de grupos e MOLS

Definição 2.4.1 (Conjunto dos Quadrados Linha, RL_n)**.** Denominamos o conjunto RL_n como o conjunto de todos os quadrados linha (veja Definição 2.1.1 de ordem n.

Definição 2.4.2. Definimos a operação $\circ : RL_n \times RL_n \to RL_n$, tal que dados dois quadrados linha A e B temos $A \circ B = (h_1, \ldots, h_n)$, de maneira que $A = (f_1, \ldots, f_n)$, $B = (g_1, \ldots, g_n)$ e $h_i = f_i(g_i(x))$, para $x \in \{1, 2, \ldots, n\}$.

Exemplo 2.4.3. Sejam os quadrados linhas A e B abaixo:

$$A = \begin{array}{|c|c|c|c|}\hline 1&2&3&4\\\hline 2&3&4&1\\\hline 3&4&1&2\\\hline 4&1&2&3\\\hline\end{array} \qquad B = \begin{array}{|c|c|c|c|}\hline 2&4&3&1\\\hline 1&2&4&3\\\hline 4&3&1&2\\\hline 3&1&2&4\\\hline\end{array}$$

Assim, se $A = (f_1, f_2, f_3, f_4)$ e $B = (g_1, g_2, g_3, g_4)$ temos:

$$f_1 = \begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}, \quad f_2 = \begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}, \quad f_3 = \begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix} \text{ e } f_4 = \begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix};$$

$$g_1 = \begin{pmatrix}1&2&3&4\\2&4&3&1\end{pmatrix}, \quad g_2 = \begin{pmatrix}1&2&3&4\\1&2&4&3\end{pmatrix}, \quad g_3 = \begin{pmatrix}1&2&3&4\\4&3&1&2\end{pmatrix} \text{ e } g_4 = \begin{pmatrix}1&2&3&4\\3&1&2&4\end{pmatrix}.$$

Para calcular $A \circ B$ fazemos:

$$f_1 \circ g_1 = \begin{pmatrix}1&2&3&4\\2&4&3&1\end{pmatrix}, \quad f_2 \circ g_2 = \begin{pmatrix}1&2&3&4\\2&3&1&4\end{pmatrix},$$
$$f_3 \circ g_3 = \begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix} \text{ e } f_4 \circ g_4 = \begin{pmatrix}1&2&3&4\\2&4&1&3\end{pmatrix}.$$

Logo, obtemos o seguinte quadrado linha:

$$A \circ B = \begin{array}{|c|c|c|c|}\hline 2&4&3&1\\\hline 2&3&1&4\\\hline 2&1&3&4\\\hline 2&4&1&3\\\hline\end{array}$$

Teorema 2.4.4. $(RL_n, \circ)$ é um grupo de ordem $(n!)^n$.

Demonstração. Sejam os quadrados linha $A = (f_1, f_2, \ldots, f_n)$, $B = (g_1, g_2, \ldots, g_n)$ e $C = (h_1, h_2, \ldots, h_n) \in (RL_n, \circ)$. Primeiramente vamos mostrar que $(RL_n, \circ)$ é grupo. De fato,

(i) $(RL_n, \circ)$ é associativa, uma vez que

$$\begin{aligned}(A \circ B \circ C) &= A \circ (g_1 \circ h_1, g_2 \circ h_2, \ldots, g_n \circ h_n) \\ &= (f_1 \circ (g_1 \circ h_1), f_2 \circ (g_2 \circ h_2), \ldots, f_n \circ (g_n \circ h_n)) \\ &= ((f_1 \circ g_1) \circ h_1, (f_2 \circ g_2) \circ h_2, \ldots, (f_n \circ g_n) \circ h_n) \\ &= (A \circ B) \circ C.\end{aligned}$$

(ii) Existe o elemento neutro $E \in RL_n$, basta tomar $E = (e, e, \ldots, e)$ de maneira que e é a permutação identidade. Assim, $A \circ E = (f_1 \circ e, f_2 \circ e, \ldots, f_n \circ e) = (f_1, f_2, \ldots, f_n) = A$ e $E \circ A = (e \circ f_1, e \circ f_2, \ldots, e \circ f_n) = A$ para todo $A \in RL_n$.

(iii) Para qualquer que seja $A \in RL_n$ existe $A^{-1} \in RL_n$ tal que $A \circ A^{-1} = A^{-1} \circ A = E$, para isso tomamos $A^{-1} = (f_1^{-1}, f_2^{-1}, \ldots, f_n^{-1})$.

Portanto, de (i), (ii) e (iii) $(RLn, \circ)$ é um grupo. Para calcular o número de elementos de RL_n utilizamos o princípio multiplicativo, pois, para cada entrada de f_i, $i \in \{1, 2, \ldots, n\}$ de $A = (f_1, f_2, \ldots, f_n)$ temos $n!$ possibilidades e como A possui n entradas temos que a quantidade é dada por $\underbrace{n! \cdot n! \cdot \ldots \cdot n!}_{n \text{ parcelas}} = (n!)^n$ ∎

Proposição 2.4.5. Sejam $R \in RL_n$ e $E = (e, \ldots, e)$, assim E e R são ortogonais se, e somente se, R é um quadrado latino.

Demonstração. Seja $R \perp E$, com $R \in RL_n$ então como cada linha de R é a imagem de uma permutação de S_n, não há a repetição de algarismos nas linhas. Assim, basta mostrar que não há a repetição de algum algarismo nas colunas de R. Vamos fixar a coluna j do quadrado linha R e mostraremos que $a_{ij} \neq a_{kj}$ sempre que $i \neq k$. Suponha o quadrado $R \odot E$, dessa forma temos a entrada (a_{ij}, j) localizada na linha i e coluna j e a entrada (a_{kj}, j) localizada na linha k e coluna j. Veja,

$$R \odot E = \begin{bmatrix} - & \cdots & \cdots & - \\ \vdots & (a_{ij}, j) & \cdots & - \\ \vdots & (a_{kj}, j) & \ddots & \vdots \\ - & \cdots & \cdots & - \end{bmatrix}.$$

Dado que $R \perp E$, então temos que um par de $R \odot E$ é $(i, j) \neq (k, j)$, assim $(a_{ij}, j) \neq (a_{kj}, j)$ e $a_{ij} \neq a_{kj}$.

Reciprocamente, se R é um quadrado latino com um elemento de R da forma a_{ij}. Para mostrar que $R \perp E$ basta mostrar que não há pares repetidos na mesma coluna. Note que, o elemento (a_{ij}, j) de $R \odot E$ só pode ocorrer uma única vez, dado que R é um quadrado latino. Logo, temos que R é ortogonal a E. ■

Observação 2.4.6. Denotaremos a composição de quadrados $A \circ B$ por AB.

Teorema 2.4.7. Seja $\{A_1, A_2, \ldots, A_n\}$ um conjunto de quadrados linha mutualmente ortogonais. Para qualquer quadrado linha X, o conjunto $\{XA_1, XA_2, \ldots, XA_n\}$ é composto de quadrados linha mutualmente ortogonais.

Demonstração. Sejam $A, B \in \{A_1, A_2, \ldots, A_n\}$ vamos mostrar que $XA \perp XB$. Assim, suponha por absurdo que o par (u, v) ocorre na linha m e coluna p e também na linha n e coluna q em $XA \odot XB$. Observe:

$$XA \odot XB = \begin{bmatrix} - & \cdots & \cdots & - \\ \vdots & \vdots & (u,v) & - \\ \vdots & (u,v) & \vdots & \vdots \\ - & \cdots & \cdots & - \end{bmatrix}.$$

Agora, seja $x(m,p)$ elemento de X localizado na linha m e coluna p, então

$$u = (x(m,p),p) = (x(n,q),q) \text{ e } v = (x(m,p),p) = (x(n,q),q),$$

assim temos que o par $(x(n,q),q), b(x(n,q),q) = (x(m,p),p), b(x(m,p),p)$ o que contradiz o fato de A e B serem ortogonais. Logo, XA e XB são ortogonais. ■

Proposição 2.4.8. Sejam A e B dois quadrados linha. Os quadrados A e B são ortogonais se, e somente se, existe um quadrado latino L tal que $AL = B$.

Demonstração. Sejam A e B quadrados ortogonais e considere $L = A^{-1}B$, temos que L é quadrado linha pelo Teorema 2.4.4. Note que, $L = A^{-1}B$ e $A^{-1}A = E$ são ortogonais pelo Teorema 2.4.7 e pela Proposição 2.4.5 obtemos que L é um quadrado latino. E mais, $AL = AA^{-1}B = EB = B$. Reciprocamente, se L é um quadrado latino de maneira que $AL = B$, pela Proposição 2.4.5 temos que L é ortogonal a E. Portanto, pelo Teorema 2.4.7 temos que $AL = B$ e $AE = A$ são ortogonais, ou seja, $B \perp A$.

■

Colorário 2.4.9. Seja A um quadrado latino e m o menor inteiro positivo tal que A^m não é latino, assim $\{A, A^2, \ldots, A^{m-1}\} = B$ é um conjunto ortogonal de quadrados latinos.

Demonstração. Dados A^j e $A^k \in B$ com $j < k$ temos que $A^j A^{k-j} = A^k$ onde $A^{k-j} \in B$ é um quadrado latino. Assim o resultado segue de 2.4.8. ■

Exemplo 2.4.10. Seja o seguinte quadrado latino L.

$$L = \begin{array}{|c|c|c|}\hline 1 & 2 & 3 \\ \hline 2 & 3 & 1 \\ \hline 3 & 1 & 2 \\ \hline \end{array}$$

Note que, $L \circ L = L^2$, representada posteriormente.

$$\begin{array}{|c|c|c|}\hline 1 & 2 & 3 \\ \hline 2 & 3 & 1 \\ \hline 3 & 1 & 2 \\ \hline \end{array} \circ \begin{array}{|c|c|c|}\hline 1 & 3 & 2 \\ \hline 2 & 3 & 1 \\ \hline 3 & 1 & 2 \\ \hline \end{array} = \begin{array}{|c|c|c|}\hline 1 & 3 & 2 \\ \hline 3 & 1 & 2 \\ \hline 2 & 3 & 1 \\ \hline \end{array}$$

Temos que, $L^2 \circ L = L^3$, caracterizado a seguir.

$$\begin{array}{|c|c|c|}\hline 1 & 2 & 3 \\ \hline 3 & 2 & 1 \\ \hline 2 & 3 & 1 \\ \hline \end{array} \circ \begin{array}{|c|c|c|}\hline 1 & 2 & 3 \\ \hline 2 & 3 & 1 \\ \hline 3 & 1 & 2 \\ \hline \end{array} = \begin{array}{|c|c|c|}\hline 1 & 2 & 3 \\ \hline 1 & 2 & 3 \\ \hline 1 & 2 & 3 \\ \hline \end{array}$$

Portanto, o conjunto $\{L, L_2\}$ é ortogonal. De fato,

$$L \odot L_2 = \begin{bmatrix} (1,1) & (2,2) & (3,3) \\ (2,3) & (3,1) & (1,2) \\ (3,2) & (1,3) & (1,1) \end{bmatrix}.$$

Capítulo 3

APLICAÇÕES

Estudaremos neste capítulo duas formas de construir o sudoku completo, ou seja, o sudoku já preenchido com a sua solução. A Construção 1 é baseada nos estudos do artigo *Cosets and Cayley-Table* (CARMICHAEL; SCHLOEMAN; WARD, 2010), a qual utiliza o conjunto $\mathbb{Z}_9$ e as suas classes laterais. Já para a Construção 2 é fundamentada no artigo *Constructions os complet sets of orthogonal diagonal Sudoku squares* (KEEDWELL, 2010), e sua demonstração é restrita a casos específicos de sudoku 9×9, pois, para o caso genérico necessita a compreenção de corpos de Galois.

3.1 Construção 1 do sudoku completo

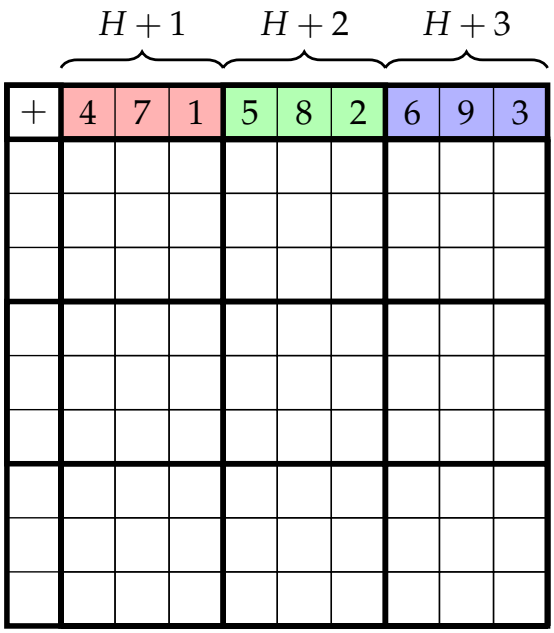
Exemplo 3.1.1. Para construir o sudoku completo tome o grupo $(\mathbb{Z}_9, +)$ de maneira que

$$\mathbb{Z}_9 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}, \overline{8}\}.$$

Denotaremos a classe do $\overline{0}$ por 9 e as classes $\overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}, \overline{8}$ por 1,2,3,4,5,6,7 e 8, respectivamente. Tomamos o subgrupo $H = \{3, 6, 9\}$ e calculamos as suas classes laterais dadas por:

$$H + 1 = \{4, 7, 1\}, \quad H + 2 = \{5, 8, 2\} \quad \text{e} \quad H + 3 = \{6, 9, 3\}.$$

Na tábua de operação de $(\mathbb{Z}_9, +)$ dispomos esses conjuntos da seguinte forma:



A partir das classes laterais $H + 1 = \{4, 7, 1\}$, $H + 2 = \{5, 8, 2\}$ e $H + 3 = \{6, 9, 3\}$ montaremos os conjuntos formados pelos representantes de cada classe lateral, dados por L_1, L_2 e L_3. Assim, para construir L_1 tomamos o primeiro elemento de cada conjunto das classes laterais,

$$\{4, 7, 1\}; \quad \{5, 8, 2\}; \quad \{6, 9, 3\};$$

$$L_1 = \{4, 5, 6\}.$$

Para construir o conjunto L_2 selecionamos o segundo elemento de cada classe lateral,

$$\{4, 7, 1\}; \quad \{5, 8, 2\}; \quad \{6, 9, 3\};$$

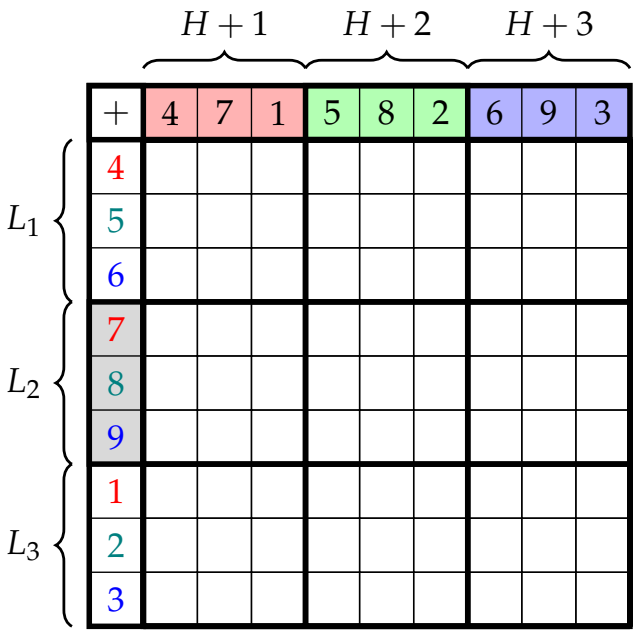
$$L_2 = \{7, 8, 9\}.$$

Por fim, com os restantes dos elementos de cada conjunto construímos o conjunto L_3,

$$\{4, 7, 1\}; \quad \{5, 8, 2\}; \quad \{6, 9, 3\};$$

$$L_3 = \{1, 2, 3\}.$$

Agora, organizamos os conjuntos L_1, L_2 e L_3 da seguinte maneira.



Por último, fazemos a soma em $\mathbb{Z}_9$ completando a tábua de operação.

+	4	7	1	5	8	2	6	9	3
4	8	2	5	9	3	6	1	4	7
5	9	3	6	1	4	7	2	5	8
6	1	4	7	2	5	8	3	6	9
7	2	5	8	3	6	9	4	7	1
8	3	6	9	4	7	1	5	8	2
9	4	7	1	5	8	2	6	9	3
1	5	8	2	6	9	3	7	1	4
2	6	9	3	7	1	4	8	2	5
3	7	1	4	8	2	5	9	3	6

Note, que não temos a repetição dos algarismos nas linhas, nas colunas e nem nos blocos. Assim, obtemos um sudoku completo com a soma em $\mathbb{Z}_9$.

Generalizaremos essa construção por meio da Proposição 3.1.2, dada a seguir.

Proposição 3.1.2 (Construção 1)**.** Seja G um grupo finito e H um subgrupo de G com ordem k índice n (o índice é o número de classes laterais de H em G), assim $|G| = nk$. Sejam $Hg_1, Hg_2, \ldots, Hg_n$ as classes laterais [1] distintas à direita de H em G, com $H = \{h_1, h_2, \ldots, h_k\}$. Assim, arranjando a tabela de Cayley de G e rotulando as colunas pelos elementos de $Hg_1, Hg_2, \ldots, Hg_n$ e rotulando as linhas pelos elementos do conjunto $T_1, T_2, \ldots, T_k$, em que $T_i = \{h_i g_1, h_i g_2, \ldots, h_i g_n\}$ nos fornece uma tabela de sudoku completo de G com blocos de dimensão $n \times k$ se, e somente se, $T_1, T_2, \ldots, T_k$ particionam G em conjuntos completos [2] dos representantes distintos das classes laterais à esquerda de H em G.

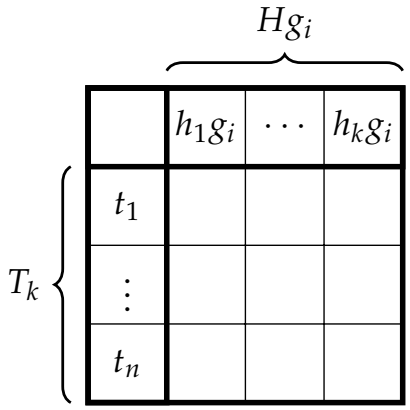
Demonstração. Utilizando as classes laterais a construção da tabela é dada da seguinte maneira.

		Hg_1			...			Hg_n		
		h_1g_1	$\cdots$	h_kg_1	$\cdots$	$\cdots$	$\cdots$	h_1g_n	$\cdots$	h_kg_n
T_1	h_1g_1									
	$\vdots$									
	h_1g_n									
$\vdots$	$\vdots$									
	$\vdots$									
	$\vdots$									
T_k	h_kg_1									
	$\vdots$									
	h_kg_n									

Seja um bloco qualquer indexado por $T_h = \{t_1, t_2, \ldots, t_n\}$, de maneira que $t_i = h_i g_j$, e, Hg_i é dado pela seguinte tabela.

[1] Note que, para o grupo $(\mathbb{Z}_n, +)$ as classes laterais à direita e à esquerda são iguais uma vez que $(\mathbb{Z}_n, +)$ é abeliano.

[2] Chamamos de um elemento de uma classe lateral à direita (à esquerda) de representante da classe. Um conjunto de todos od de representantes de todas as classes laterais à direita (à esquerda) de um grupo é chamado de conjunto completo de representantes das classes laterais à direita (à esquerda) de um grupo.



Queremos mostrar que se $T_1, T_2, \ldots, T_k$ particionam G em conjuntos completos dos representantes distintos das classes laterais à esquerda de H em G então a tabela é um sudoku. Assim, como na tabela de Cayley do grupo G não há elementos repetidos nem nas colunas ou nas linhas, então T_h é um conjunto com elementos distintos de representantes de todas as classes laterais. Desse modo, basta mostrar que todos os elementos de G aparecem em um bloco arbitrário. Então, seja o bloco B arbitrário, como na tabela anterior, indexado por T_h e Hg_i. Os elementos do bloco B são dados por:

$$B = \{t_1Hg_i \cup t_2Hg_i \cup \cdots \cup t_nHg_i\}.$$

Como $H = \{h_1, h_2, \ldots, h_k\}$, temos que:

$$\begin{aligned} Hg_i &= h_1g_i \cup h_2g_i \cup \cdots \cup h_kg_i \\ &= (h_1 \cup h_2 \cup \cdots \cup h_k)g_i. \end{aligned}$$

Então, a união dos elementos do bloco B são dados por:

$$\begin{aligned} B &= t_1Hg_i \cup t_2Hg_i \cup \cdots \cup t_nHg_i \\ &= (t_1H \cup t_2H \cup \cdots \cup t_nH)g_i \\ &= Gg_i \\ &= G. \end{aligned}$$

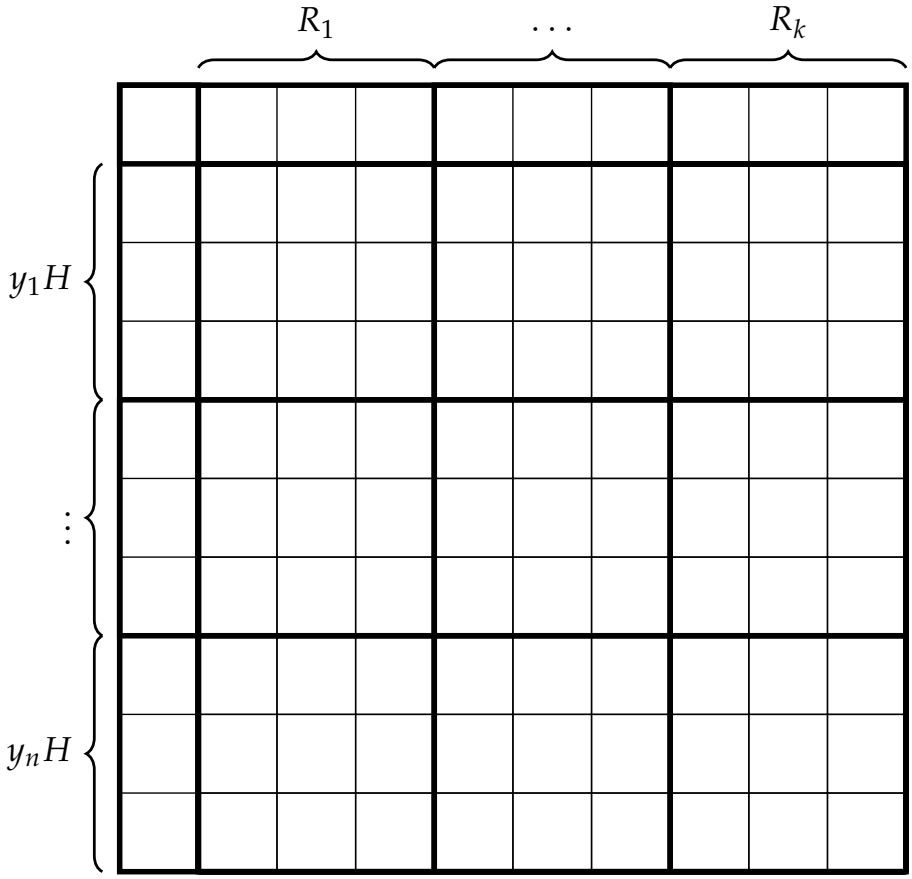
Logo, todos os elementos do bloco aparecem uma única vez, pois a quantidade de elementos no bloco é $n \times k$ e $|G| = nk$.

Agora, se cada elemento de G aparece em um bloco B, então

$$\begin{aligned} G &= Gg_i^{-1} \\ &= Bg_i^{-1} \\ &= t_1Hg_ig_i^{-1} \cup t_2Hg_ig_i^{-1} \cup \cdots \cup t_nHg_ig_i^{-1} \\ &= t_1H \cup t_2H \cup \cdots \cup t_nH. \end{aligned}$$

Como há n classes laterias de ordem k e $|G| = nk$, então devemos ter n classes laterais distintas na união. ∎

Observação 3.1.3. Se $y_1H, y_2H, \ldots, y_nH$ são classes laterais à esquerda de H em G então montando a tábua de operação com as linhas indexadas por $y_1H, y_2H, \ldots, y_nH$ e as colunas em $R_1, R_2, \ldots, R_k$ obtemos um sudoku completo com blocos de dimensão $k \times n$ se, e somente se, $R_1, R_2, \ldots, R_k$ particionam G em conjuntos completos de representantes de classes laterais à direita de H em G. Assim, podemos montar a tabela da seguinte maneira.



A demonstração é análoga à demonstração da Proposição 3.1.2.

Podemos fazer uma outra construção derivada da Construção 1 estendendo uma tabela de Cayley como no exemplo a seguir.

Exemplo 3.1.4. Utilizaremos o grupo $(\mathbb{Z}_8, +)$, de maneira que $\mathbb{Z}_8 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}\}$, onde denotaremos $\overline{0}$ por 8 e denotaremos as classes $\overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}$ por 1, 2, 3, 4, 5, 6 e 7, respectivamente. Aplicaremos a Construção 1 para o subgrupo cíclico $\langle 2 \rangle = \{0, 2, 4, 6\}$ e depois estenderemos essa construção.

Primeiramente, tomamos $\langle 4 \rangle = \{0, 4\}$ um subgrupo de $\langle 2 \rangle = \{0, 2, 4, 6\}$. Note que, tanto as classes laterais à direita e à esquerda de $\langle 4 \rangle$ são iguais. Dadas por $\langle 4 \rangle + 0 = \{0, 4\}$ e $\langle 4 \rangle + 2 = \{2, 6\}$, tais conjuntos particionam $\langle 2 \rangle = \{0, 2, 4, 6\}$. Assim, podemos aplicar a Construção 1 para o subgrupo $\langle 2 \rangle = \{0, 2, 4, 6\}$ em $\mathbb{Z}_8$. De maneira que $L_1 = \{0, 2\}$ e $L_2 = \{4, 6\}$, então:

		$\langle 4\rangle + 0$	$\langle 4\rangle + 2$		
	$+$	0	4	2	6
L_1	0	0	4	2	6
	2	2	6	4	0
L_2	4	4	0	6	2
	6	6	2	0	4

Agora, para extender a tabela anterior construiremos as classes laterais de $\langle 2\rangle$. Assim, $0 + \langle 2\rangle = \{0, 2, 4, 6\}$ e $1 + \langle 2\rangle = \{1, 3, 5, 7\}$ e tomando o conjunto $C = \{0, 1\}$ com os representantes de cada classe lateral construímos os seguintes conjuntos

$$0 + L_1 = 0 + \{0, 2\} = \{0, 2\}; \quad 1 + L_1 = 1 + \{0, 2\} = \{1, 3\};$$

$$0 + L_2 = 0 + \{4, 6\} = \{4, 6\}; \quad 1 + L_2 = 1 + \{4, 6\} = \{5, 7\},$$

para indexar as linhas. Para indexar as colunas construímos os conjuntos

$$(\langle 4\rangle + 0) + 0 = \{0, 4\} + 0 = \{0, 4\}; \quad (\langle 4\rangle + 0) + 1 = \{0, 4\} + 0 = \{1, 5\};$$

$$(\langle 4\rangle + 2) + 0 = \{2, 6\} + 0 = \{2, 6\}; \quad (\langle 4\rangle + 2) + 1 = \{2, 6\} + 1 = \{3, 7\}.$$

Então, vamos estender a construção da tabela anterior utilizando todos os elementos de $\mathbb{Z}_8$ com a soma da seguinte maneira:

		$\{0,4\}+0$		$\{0,4\}+1$		$\{2,6\}+0$		$\{2,6\}+1$	
	$+$	0	4	1	5	2	6	3	7
$0 + L_1$	0	0	4	1	5	2	6	3	7
	2	2	6	3	7	4	0	5	1
$1 + L_1$	1	1	5	2	6	3	7	4	0
	3	3	7	4	8	5	1	6	2
$0 + L_2$	4	4	0	5	1	6	2	7	3
	6	6	2	7	3	0	4	1	5
$1 + L_2$	5	5	1	6	2	7	3	0	4
	7	7	3	0	4	1	5	2	6

Logo, obtemos uma tabela de Cayley que é também um sudoku completo.

Proposição 3.1.5 (Extensão da Construção 1)**.** Seja G um grupo finito de ordem $tk \times n$ e A um subgrupo de G de ordem nk. Sejam $C_1, C_2, \ldots, C_k$ conjuntos que particionam A e $R_1, R_2, \ldots, R_n$ conjuntos que também particionam A de maneira que a tabela seguinte é a tabela de Cayley de A que forma um sudoku completo.

$*$	C_1	C_2	$\cdots$	C_k
R_1				
R_2				
$\cdots$				
R_n				

Sejam $\{l_1, l_2, \ldots, l_t\}$ e $\{r_1, r_2, \ldots, r_t\}$ conjuntos completos das classes lateral à esquerda e à direita, respetivamente de A em G, então arranjando a tabela de Cayley de G com as colunas indexadas pelos elementos dos conjuntos $C_i r_j$, $i = 1, 2, \ldots, k$, $j = 1, 2, \ldots, t$ e as linhas do bloco, indexadas por $l_j R_b$, com $j = 1, 2, \ldots, t$ e $b = 1, 2, \ldots, n$ (conforme a tabela dada posteriormente), temos que

$*$	C_1r_1	C_2r_1	$\cdots$	C_kr_1	C_1r_2	$\cdots$	C_kr_2	$\cdots$	C_1r_t	$\cdots$	C_kr_1
l_1R_1											
l_2R_1											
$\vdots$											
l_tR_1											
l_1R_2											
$\vdots$											
l_tR_2											
$\vdots$											
l_1R_n											
$\vdots$											
l_tR_n											

essa tabela é uma tabela de Cayley de G que é um sudoku completo com os blocos com dimensão $tk \times n$.

Demonstração. Para mostrar que essa extensão nos fornece um sudoku completo basta mostrar que em um bloco qualquer aparecem todos os elementos de G, uma vez que a tabela é uma tabela de Cayley. Assim, seja um bloco B qualquer dado a seguir.

	$C_i r_j$
$l_1 R_b$	
$\vdots$	
$l_t R_b$	

Note que, os elementos do bloco B, são dados da seguinte forma:

$$B = l_1 R_b C_i r_j \cup l_2 R_b C_i r_j \cup \cdots \cup l_t R_b C_i r_j.$$

Como a tabela do subgrupo A é uma tabela de Cayley que forma um sudoku completo, então $R_b C_i = A$. Logo,

$$\begin{aligned} & B = l_1 R_b C_i r_j \cup l_2 R_b C_i r_j \cup \cdots \cup l_t R_b C_i r_j \\ \Rightarrow\ & B = l_1 A r_j \cup l_2 A r_j \cup \cdots \cup l_t A r_j \\ \Rightarrow\ & B = (l_1 A \cup l_2 A \cup \cdots \cup l_t A) r_j \\ \Rightarrow\ & B = G r_j \\ \Rightarrow\ & B = G. \end{aligned}$$

E dado que no bloco temos $nk \times n$ elementos, pois, C_i possui n elementos e R_b possui k elementos de modo que possuímos t conjuntos $l_m R_b$, $m = 1, \ldots, t$, então pelo princípio multiplicativo temos nk elementos nas colunas e n elementos nas linhas gerando um bloco de dimensão $tk \times n$. Portanto, cada elemento de G aparece uma única vez no bloco, uma vez que a ordem de $|G| = tk \times n$. ∎

3.2 Construção 2 do sudoku completo

Para a Construção 2 primeiramente criaremos um bloco do sudoku e a partir dele desenvolveremos o sudoku completo. Assim, utilizaremos um bloco de dimensão $p \times p$ de maneira que esse p seja primo. Então, para construir um sudoku completo 9×9 utilizaremos $p = 3$. Definiremos que dado um bloco inicial X com p^2 símbolos, a operação $X\alpha$ é a permutação cíclica das linhas do bloco X de maneira que a segunda linha se torne a primeira linha, a terceira linha se torne a segunda linha e que a primeira linha se torne a última linha do bloco.

Exemplo 3.2.1. Seja o bloco X de dimensão 3×3, apresentado a seguir, dado pelos símbolos de 1 a 9, então temos que $X\alpha$ é dado pelo quadrado abaixo.

$$X = \begin{array}{|c|c|c|}\hline 1 & 2 & 4 \\ \hline 3 & 7 & 8 \\ \hline 9 & 5 & 6 \\ \hline \end{array} \qquad X\alpha = \begin{array}{|c|c|c|}\hline 3 & 7 & 8 \\ \hline 9 & 5 & 3 \\ \hline 1 & 2 & 4 \\ \hline \end{array}$$

Definiremos também a operação $X\beta$ de maneira que permutamos as colunas de forma cíclica da direita para a esquerda, de modo que a segunda coluna se torne a primeira coluna, a terceira coluna se torne a segunda coluna e a primeira coluna vire a última coluna do bloco.

Exemplo 3.2.2. Vamos realizar a operação $X\beta$ referente ao bloco X do Exemplo 3.2.1.

$$X = \begin{array}{|c|c|c|}\hline 1 & 2 & 4 \\ \hline 3 & 7 & 8 \\ \hline 9 & 5 & 6 \\ \hline \end{array} \qquad X\beta = \begin{array}{|c|c|c|}\hline 2 & 4 & 1 \\ \hline 7 & 8 & 3 \\ \hline 5 & 6 & 9 \\ \hline \end{array}$$

Além disso, podemos combinar as operações ou ainda realizar a mesma operação mais de uma vez, calculando $X\alpha\beta$ ou $X\alpha^2$.

Exemplo 3.2.3. Utilizando o bloco X do Exemplo 3.2.1 podemos calcular $X\alpha\beta$ e $X\alpha^2$, dados em seguida.

$$X = \begin{array}{|c|c|c|}\hline 1 & 2 & 4 \\ \hline 3 & 7 & 8 \\ \hline 9 & 5 & 6 \\ \hline \end{array} \qquad X\alpha\beta = \begin{array}{|c|c|c|}\hline 7 & 8 & 3 \\ \hline 5 & 3 & 9 \\ \hline 2 & 4 & 1 \\ \hline \end{array}$$

$$X = \begin{array}{|c|c|c|}\hline 1 & 2 & 4 \\ \hline 3 & 7 & 8 \\ \hline 9 & 5 & 6 \\ \hline \end{array} \qquad X\alpha^2 = \begin{array}{|c|c|c|}\hline 9 & 5 & 3 \\ \hline 3 & 7 & 8 \\ \hline 1 & 2 & 4 \\ \hline \end{array}$$

Exemplo 3.2.4. Construiremos agora um sudoku completo baseado na construção linear de Kedweell, a qual exploraremos no decorrer dessa seção. Desenvolveremos um sudoku 9×9 de maneira que seus blocos tenham dimensão 3×3. Primeiramente, montamos um bloco Y dispondo os elementos de 1 a 9 aleatoriamente, como no bloco a seguir.

$$Y = \begin{array}{|c|c|c|}\hline 1 & 2 & 3 \\ \hline 4 & 8 & 9 \\ \hline 7 & 6 & 5 \\ \hline \end{array}$$

Uma maneira de construir um sudoku pelo todo método de construção linear de Keedweell é dada pela matriz abaixo, a qual dispõe os blocos do sudoku da seguinte forma.

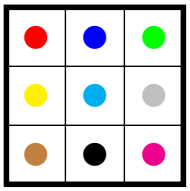
Y	$Y\alpha$	$Y\alpha^2$
$Y\alpha\beta$	$Y\alpha^2\beta$	$Y\beta$
$Y\alpha^2\beta^2$	$Y\beta^2$	$Y\alpha\beta^2$

Logo, com a matriz anterior e o bloco Y obtemos o seguinte sudoku completo.

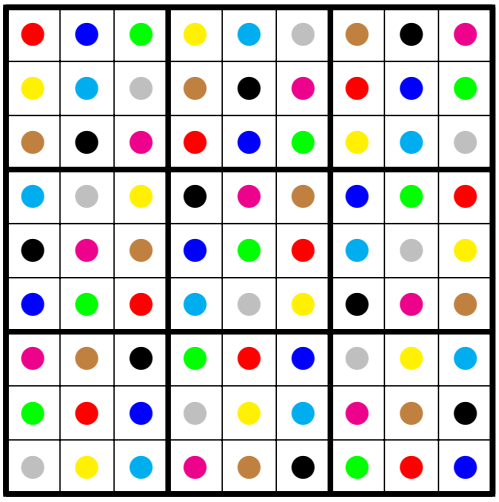
1	2	3	4	8	9	7	6	5
4	8	9	7	6	5	1	2	3
7	6	5	1	2	3	4	8	9
8	9	4	6	5	7	2	3	1
6	5	7	2	3	1	8	9	4
2	3	1	8	9	4	6	5	7
5	7	6	3	1	2	9	4	8
3	1	2	9	4	8	5	7	6
9	4	8	5	7	6	3	1	2

Note que, para qualquer configuração do bloco Y temos que o método de construção de Keedwell nos dá um sudoku completo. Esse fato será demonstrado pela Proposição 3.2.6.

Exemplo 3.2.5. Tomando o bloco Y com a seguinte configuração.

$Y =$ 

Podemos fazer a mesma construção anterior não importando o símbolo que utilizamos para construir o bloco Y.



Para construir sudokus completos utilizando a construção linear de Keedwell para $p = 3$, ou seja, um sudoku de ordem 9 temos 6 formas de construir. Dadas pelas seguintes matrizes.

Y	$Y\alpha$	$Y\alpha^2$
$Y\alpha\beta$	$Y\alpha^2\beta$	$Y\beta$
$Y\alpha^2\beta^2$	$Y\beta^2$	$Y\alpha\beta^2$

Y	$Y\alpha\beta^2$	$Y\alpha^2\beta$
$Y\alpha^2\beta^2$	$Y\beta$	$Y\alpha$
$Y\alpha\beta$	$Y\alpha^2$	$Y\beta^2$

Y	$Y\alpha^2\beta$	$Y\alpha\beta^2$
$Y\beta^2$	$Y\alpha^2$	$Y\alpha\beta$
$Y\beta$	$Y\alpha^2\beta^2$	$Y\alpha$

Y	$Y\alpha^2$	$Y\alpha$
$Y\alpha\beta^2$	$Y\beta^2$	$Y\alpha^2\beta^2$
$Y\alpha^2\beta$	$Y\alpha\beta$	$Y\beta$

Y	$Y\alpha^2\beta^2$	$Y\alpha\beta$
$Y\alpha^2\beta$	$Y\alpha$	$Y\beta^2$
$Y\alpha\beta^2$	$Y\beta$	$Y\alpha^2$

Y	$Y\alpha\beta$	$Y\alpha^2\beta^2$
$Y\beta$	$Y\alpha\beta^2$	$Y\alpha^2$
$Y\beta^2$	$Y\alpha$	$Y\alpha^2\beta$

Proposição 3.2.6. Os seis tipos de construção linear de Keedweel com $p = 3$ geram sudokus completos de ordem 9.

Demonstração. Note que, como as operações α e β de permutação de linhas e colunas são cíclicas, temos que em cada bloco aparecem os 9 símbolos sem repetição. Assim, basta mostrar que não existem símbolos repetidos na mesma coluna e na mesma linha. Para que não existam símbolos repetidos na mesma linha devemos ter as potências de α variando de 0 à 2 em uma mesma linha de uma das tabelas anteriores, ou seja, para as três linhas devem aparecer α^0, α^1 e α^2. De fato, seja um símbolo x dado em uma determinada linha do sudoku. Suponha por absurdo que esse elemento se repita em uma das linhas, então devemos ter dois blocos na mesma linha em uma das 6 matrizes das construções lineares de Keedwell de maneira que α tenham a mesma potência módulo 3, o que contradiz as 6 maneiras de construção dessas matrizes para $p = 3$.

Da mesma forma não existem símbolos repetidos na mesma coluna, pois, temos potências distintas de β em uma mesma coluna de cada uma das 6 tabelas para a construção linear de Keedweel. Consequentemente, como aparecem todas as potências α^0, α^1 e α^2 em cada linha na construção de Keedweel e aparecem todas as potências β^0, β^1 e β^2 em cada coluna, não há a repetição de um mesmo símbolo em cada linha do sudoku e também não há a repetição de símbolos na coluna. ■

Utilizaremos a notação LK quando nos referirmos à construção linear de Keedwell.

Proposição 3.2.7. Os seis tipos de construção LK com $p = 3$ formam um conjunto mutualmente ortogonal.

Demonstração. Sejam duas construções LK quaisquer A e B com $p = 3$ e sem perda de generalidade tome essas construções LK formadas com os símbolos de 1 a 9. Note que, pela Definição 2.4.8 para que $A = (a_{ij})$ e $B = (b_{ij})$ sejam ortogonais devemos ter todos os pares (a_{ij}, b_{ij}) distintos em $A \odot B$, ou seja, como $p = 3$ devemos ter todos os pares ordenados de $\{1,2,3,4,5,6,7,8,9\} \times \{1,2,3,4,5,6,7,8,9\}$ aparecendo uma única vez. Suponha por absurdo que nas construções A e B exista um par $(a_{mn}, b_{mn}) = (a_{lk}, b_{lk})$ de maneira que a posição $(m,n) \neq (l,k)$. Assim, como em cada bloco temos os elementos de 1 a 9 aparecendo uma única vez devemos ter os elementos de (m,n) e (l,k) ocupando blocos distintos. Então, sejam os blocos das construções LK dispostos da seguinte maneira.

Bloco 01	Bloco 02	Bloco 03
Bloco 04	Bloco 05	Bloco 06
Bloco 07	Bloco 08	Bloco 09

Assim, suponha sem perda de generalidade que a posição (m,n) pertença ao bloco 01 então a posição (l,k) deve pertencer à um bloco distinto ao bloco 01. Logo, (a_{mn}, b_{mn})

e (a_{lk}, b_{lk}) estão em blocos distintos em $A \odot B$. Mas, por hipótese $(a_{mn}, b_{mn}) = (a_{lk}, b_{lk})$ e como as construções LK originam-se de permutações cíclicas de linhas e colunas devemos ter a_{mn} e a_{lk} decorrentes da mesma permutação, ou seja, suponhamos que $a_{mn} \in Y\alpha\beta$, então $a_l k \in Y\alpha\beta$. A mesma situação ocorre para b_{mn} e b_{lk}, assim caso $b_{mn} \in Y\beta$ então $b_{lk} \in Y\beta$. Portanto, teríamos A e B com dois blocos de mesma localização e com a mesma permutação como segue no exemplo abaixo.

$A =$

	$Y\beta$	
$Y\alpha\beta$		

$B =$

	$Y\beta$	
$Y\alpha\beta$		

O que seria um absurdo, uma vez que nas construções LK com $p = 3$ não existem duas construções com essa configuração. ■

De forma análoga, podemos afirmar para o caso $p = 2$ que as construções LK abaixo geram um sudoku 4×4 funciona de modo semelhante ao sudoku 9×9, mas possui apenas algarismos de 1 a 4.

Y	$Y\alpha$
$Y\alpha\beta$	$Y\alpha$

Y	$Y\alpha\beta$
$Y\beta$	$Y\alpha$

Exemplo 3.2.8. A seguir temos um conjunto de MOLS dado pela construção LK com $p = 3$.

1	2	3	4	5	6	7	8	9
4	5	6	7	8	9	1	2	3
7	8	9	1	2	3	4	5	6
5	6	4	8	9	7	2	3	1
8	9	7	2	3	1	5	6	4
2	3	1	5	6	4	8	9	7
9	7	8	3	1	2	6	4	5
3	1	2	6	4	5	9	7	8
6	4	5	9	7	8	3	1	2

1	2	3	6	4	5	8	9	7
4	5	6	9	7	8	2	3	1
7	8	9	3	1	2	5	6	4
9	7	8	2	3	1	4	5	6
3	1	2	5	6	4	7	8	9
6	4	5	8	9	7	1	2	3
5	6	4	7	8	9	3	1	2
8	9	7	1	2	3	6	4	5
2	3	1	4	5	6	9	7	8

1	2	3	8	9	7	6	4	5
4	5	6	2	3	1	9	7	8
7	8	9	5	6	4	3	1	2
3	1	2	7	8	9	5	6	4
6	4	5	1	2	3	8	9	7
9	7	8	4	5	6	2	3	1
2	3	1	9	7	8	4	5	6
5	6	4	3	1	2	7	8	9
8	9	7	6	4	5	1	2	3

1	2	3	7	8	9	4	5	6
4	5	6	1	2	3	7	8	9
7	8	9	4	5	6	1	2	3
6	4	5	3	1	2	9	7	8
9	7	8	6	4	5	3	1	2
3	1	2	9	7	8	6	4	5
8	9	7	5	6	4	2	3	1
2	3	1	8	9	7	5	6	4
5	6	4	2	3	1	8	9	7

1	2	3	9	7	8	5	6	4
4	5	6	3	1	2	8	9	7
7	8	9	6	4	5	2	3	1
8	9	7	4	5	6	3	1	2
2	3	1	7	8	9	6	4	5
5	6	4	1	2	3	9	7	8
6	4	5	2	3	1	7	8	9
9	7	8	5	6	4	1	2	3
3	1	2	8	9	7	4	5	6

1	2	3	5	6	4	9	7	8
4	5	6	8	9	7	3	1	2
7	8	9	2	3	1	6	4	5
2	3	1	6	4	5	7	8	9
5	6	4	9	7	8	1	2	3
8	9	7	3	1	2	4	5	6
3	1	2	4	5	6	8	9	7
6	4	5	7	8	9	2	3	1
9	7	8	1	2	3	5	6	4

Capítulo 4

BENEFÍCIOS DO SUDOKU NA APRENDIZAGEM

Por fim, neste capítulo apresentaremos uma sugestão de atividade em sala de aula fundamentada nas construções 1 e 2 do sudoku completo do capítulo anterior. Tomamos como alicerce os Parâmetros Curriculares Nacionais de Matemática e as Diretrizes Curriculares da Educação Básica: Matemática entre outros artigos com o intuito de mostrar a relevância de uma atividade mais atrativa e significativa para o aluno. Nessa atividade será desenvolvido um material manipulativo de forma que o estudante seja capaz de resolver o quebra-cabeça de maneira mais ágil, permitindo uma resolução mais ativa e evitando o tempo gasto caso o aluno investigasse a resolução do sudoku utilizando lápis e papel.

4.1 Fundamentação teórica

Conforme as Diretrizes Curriculares da Educação Básica do Paraná (PARANÁ, 2008) os conteúdos das disciplinas devem ser cultivados de maneira contextualizada e sempre questionando a rigidez da apresentação tradicional e atemporal dos conhecimentos. Dessa forma, a escola deve promover a prática fundamentada em diversas metodologias. Assim, de acordo com os Parâmetros Curriculares Nacionais da Matemática (BRASIL, 2006), a disciplina deve contribuir na formação do cidadão ao desenvolver metodologias que motivem a construção de estratégias que estimulem a iniciativa e a criatividade, as quais fomentem a comprovação e resultados de problemas e enfatizem tanto o trabalho coletivo como a autonomia resultante da capacidade do discente enfrentar desafios.

Portanto, o jogo é uma forma interessante para propor um problema matemático, uma vez que há uma apresentação mais atrativa para o conteúdo a ser trabalhado e beneficiando a criatividade na busca de estratégias para resolvê-lo. Esse objeto de aprendizagem também incentiva o planejamento de ações e possibilita uma atitude positiva diante dos erros, pois, podem ser corrigidas de modo natural no decorrer da atividade. (BRASIL, 2006)

De acordo com as orientações curriculares para o ensino médio do Ministério da Educação (MEC):

> Os jogos e brincadeiras são elementos muito valiosos no processo de apropriação do conhecimento. Permitem o desenvolvimento de competências no âmbito da comunicação, das relações interpessoais, da liderança e do trabalho em equipe, utilizando a relação entre cooperação e competição em um contexto formativo. O jogo oferece o estímulo e o ambiente propícios que favorecem o desenvolvimento espontâneo e criativo dos alunos e permite ao professor ampliar seu conhecimento de técnicas ativas de ensino, desenvolver capacidades pessoais e profissionais para estimular nos alunos a capacidade de comunicação e expressão, mostrando-lhes uma nova maneira, lúdica, prazerosa e participativa de relacionar-se com o conteúdo escolar, levando a uma maior apropriação dos conhecimentos envolvidos. (BRASIL, 2006, p.28)

Segundo os Parâmetros Curriculares Nacionais (BRASIL, 1998) os jogos possibilitam ao professor analisar e avaliar as estratégias utilizadas pelos alunos, a capacidade do discente compreender as regras e de se comunicar durante a realização da atividade. Existe também a possibilidade observar o autocontrole e o respeito com os demais. Assim, desenvolvendo não só a parte cognitiva, mas também incentivando a competência emocional, social e moral.

O uso desse recurso não se restringe a trabalhar com jogos prontos, mas possibilitar a criação do mesmo por parte dos alunos. Esse encaminhamento reproduz um sentimento de pertencimento, no qual cada etapa deve ser discutida delimitando o papel de cada indivíduo no procedimento. (BRASIL, 2006)

> Os jogos podem contribuir para um trabalho de formação de atitudes – enfrentar desafios, lançar-se à busca de soluções, desenvolvimento da crítica, da intuição, da criação de estratégias e da possibilidade de alterá-las quando o resultado não é satisfatório – necessárias para aprendizagem da Matemática. (BRASIL, 1998, p.47)

A utilização desse método na aprendizagem matemática busca um ensino diferente do processo baseado em decorar regras e conteúdos sem a reflexão mais a aprofundada em um conteúdo específico ou a aplicação desses conhecimentos de maneira não significativa. Assim, os jogos são uma ferramenta que não apenas diverte quem joga, mas auxilia no estudo proporcionando um desafio. Todavia, é necessária atenção para o mau uso dos jogos com uma escolha aleatória e sem finalidade específica. (MENEZES; MUZATTI, 2016)

O jogo e outros materiais possuem um papel importante no ensino e aprendizagem, mas é necessário incorporar o uso desses materiais às situações que exercitem a análise e a reflexão de problemas. Assim, além de ser um mecanismo sociocultural de maneira que a matemática está relacionada, a atividade do jogo é natural ao desenvolvimento do indivíduo porque vai contra a ideia de obrigação, apesar de exigir o cumprimento de regras. (BRASIL, 2006)

Segundo o artigo *A aplicação do jogo Sudoku no ensino médio como ferramenta para auxiliar o discente a pensar e refletir*, o jogo lógico possibilita o aumento cognitivo na resolução de cálculos. Elevando também o ânimo dos discentes a questionarem e investigarem problemas tanto em sala de aula como no âmbito social. (OLIVEIRA, 2014) O jogo permite ao jogador desenvolver seus raciocínios e estratégias de maneira adequada, pois, o sudoku é baseado na disposição lógica dos algarismos. Com esse recurso é possível ir contra a metodologia de ensino que se resume a um modelo de aulas expositivas. (MENEZES; MUZATTI, 2016)

> O jogo Sudoku tornou visível a elevação do cognitivo na resolução dos cálculos que foram propostos, tornando assim os alunos mais aptos e capazes para resolução de problemas lógicos que precisam de mais atenção e concentração, a busca que nós professores temos para que nossos alunos tenham mais ânimo em nossas aulas, e para que sejam mais investigativos questionadores e que haja um fio de interesse e prazer no que estão estudando, acontece quando usamos os jogos. (OLIVEIRA, 2014, p.14)

4.2 Sugestão de atividade

O encaminhamento pedagógico matemático deve contribuir nas habilidades do estudante constatar regularidades, indagar conjecturas, interpretar e descrever fenômenos matemáticos em outras áreas do saber. Portanto, baseado nas Diretrizes Curriculares do Ensino Básico do Paraná a atividade de sudoku que abordaremos é fundamentada no conteúdo estruturante de números e álgebra mais especificamente em conjuntos numéricos e operações, matrizes e sistemas lineares. (PARANÁ, 2008)

Desenvolveremos uma atividade com o jogo sudoku utilizando material manipulativo, com o intuito de que os alunos consigam jogar e elaborar o seu próprio quebra-cabeça. O objetivo dessa atividade em sala de aula é de que o aluno interprete as matrizes e compreenda as suas operações, reconheça e resolva equações algébricas e identifique e resolva o problema.

Dividiremos a atividade em duas aulas de cinquenta minutos de maneira que na primeira aula será apresentado o jogo e suas regras e também será construído o material manipulativo. Na segunda aula o professor poderá utilizar tanto a Construção 1 do sudoku completo ou a Construção 2 para construir o sudoku e consequentemente o quebra-cabeça.

4.2.1 Aula 1

Primeiramente vamos comentar um pouco sobre a história do sudoku e suas regras. Posteriormente, será disponibilizado um quebra-cabeça para que os alunos, com o professor, resolvam em sala de aula. Após essa resolução será apresentado o material manipulativo para os alunos construírem.

Plano de Aula: Construção 1 - Parte I						
Dados de Identificação						
Disciplina:	Matemática	**Data:**	$XX/XX/2019$	**Nível:**	Ensino Médio	**Duração:** 50 minutos
Conteúdo Estruturante:	Números e Álgebra					
Conteúdo Específico:	Sistemas Lineares e Matrizes					
Objetivos						
Objetivos Geral:	· Conhecer e resolver um quebra-cabeça sudoku; · Identificar uma matriz; · Reconhecer as posições dos elementos de uma matriz.					
Objetivos Específico:	· Comparar os elementos de um sudoku com os elementos de uma matriz; · Investigar por meio do raciocínio lógico a resolução do sudoku.					
Desenvolvimento do tema:	Descrição da abordagem teórica e prática do tema se encontra na subseção 4.2.1.1.					
Recursos didáticos:	· Régua; · Tesoura; · 2 papéis (ou cartolinas) com cores distintas; · 1 papel cartão (ou papel que possua os dois lados com cores distintas); · Pincel atômico (ou canetinha).					
Avaliação:	Compreenção e participação na resolução do sudoku, assim como a confecção do material manipulativo.					
Bibliografia:	DELAHAYE, J.-P. The science behind sudoku.Scientific American, Nature PublishingGroup, v. 294, n. 6, p. 80–87, 2006. CARMICHAEL, J.; SCHLOEMAN, K.; WARD, M. B. Cosets and cayley-sudoku tables. Mathematics Magazine, Taylor and Francis, v. 83, n. 2, p. 130 – 139, 2010.					

4.2.1.1 Desenvolvimento da Aula 1

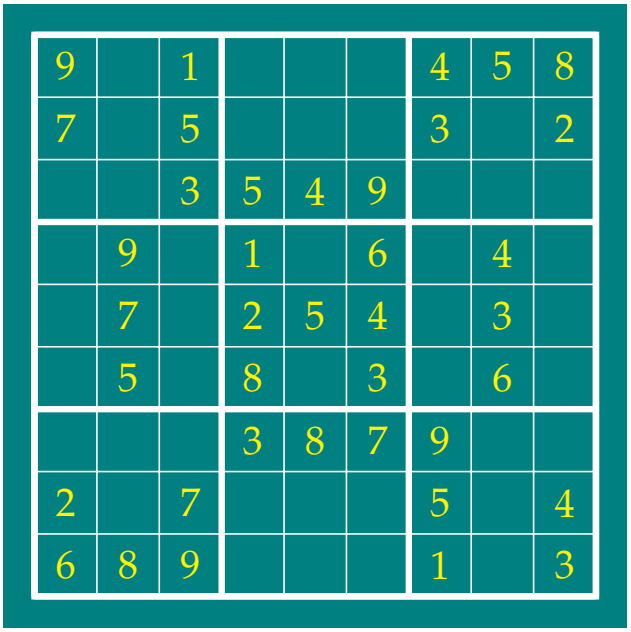
1ª Etapa: Conhecendo o jogo.

Nessa etapa será apresentado as regras do sudoku mais tradicional 9×9 já citada no Capítulo 1. Caso o professor deseje trazer alguns fatos curiosos sobre o sudoku é possível pedir a leitura prévia do artigo A Ciência do Sudoku [1].

2ª Etapa: Jogando.

Para que os alunos se habituem às regras do sudoku apresentaremos um jogo que pode ser retirado do site <http://www.sudoku.name/index-pt.php> e solicitaremos a sua resolução para a turma. Para esse procedimento o professor desenhará o sudoku na lousa e escreverá as pistas com giz colorido para diferenciar dos outros números que serão preenchidos e marcará uma borda mais grossa nos blocos 3×3 e mostrará o sudoku como uma aos alunos indicando cada elemento da malha como um elemento a_{ij} da matriz.

Figura 14 – Modelo do sudoku na lousa



Posteriormente, o professor solicita para os alunos tentarem resolver o sudoku proposto falando os números e indicando sua posição como elemento de uma matriz, o estudante pode falar número 3 na linha 2 e coluna 4, por exemplo. Após o preenchimento do sudoku o professor pode conferir com os alunos se a solução está correta. Lembrando que o gabarito do jogo se encontra disponível no mesmo site em que o jogo foi retirado.

[1] O artigo A Ciência do Sudoku se encontra na revista Scientific American Brasil disponível em: <http://sciam.uol.com.br/a-ciencia-do-sudoku/>. Acessado em 30 de junho de 2019.

Figura 15 – Modelo da resolução do sudoku na lousa

9	6	1	7	3	2	4	5	8
7	4	5	6	1	8	3	9	2
8	2	3	5	4	9	6	1	7
3	9	8	1	7	6	2	4	5
1	7	6	2	5	4	8	3	9
4	5	2	8	9	3	7	6	1
5	1	4	3	8	7	9	2	6
2	3	7	9	6	1	5	8	4
6	8	9	4	2	5	1	7	3

3ª Etapa: Montagem do material manipulativo.

Propomos a construção do jogo sudoku por meio de um material manipulativo que o professor confeccionará com seus estudantes utilizando o material descrito no início da atividade baseada na Construção 1 descrita no Capítulo 3. Para otimizar o tempo pode-se dividir a classe em grupos de no máximo 4 alunos para elaborar esse material.

(1º Passo) No papel cartão ou em um papel que possua a frente e o verso de cores distintas construa uma quadrado de $18cm \times 18cm$ e divida esse mesmo quadrado em 9 colunas e 9 linhas com um lápis, ou uma caneta e marque números de 1 a 9 em cada linha do quadrado e depois no verso marque números de 9 a 1, de maneira que o mesmo número fique escrito na frente e no verso do papel como na figura a seguir.

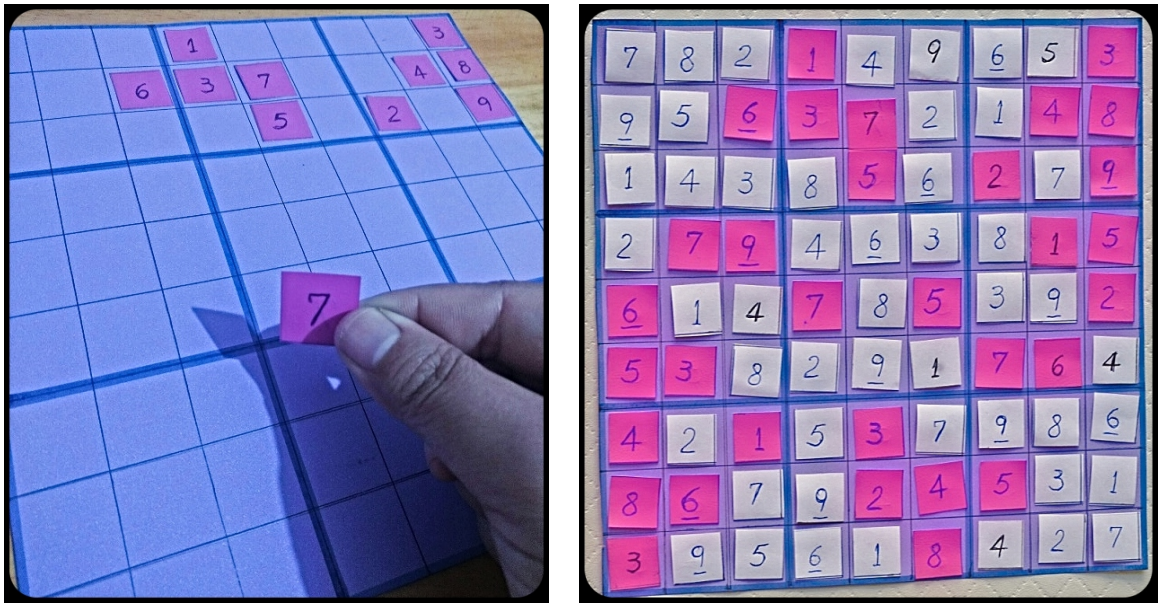
Figura 16 – Frente e verso do papel

1	2	3	4	5	6	7	8	9
1	2	3	4	5	6	7	8	9
1	2	3	4	5	6	7	8	9
1	2	3	4	5	6	7	8	9
1	2	3	4	5	6	7	8	9
1	2	3	4	5	6	7	8	9
1	2	3	4	5	6	7	8	9
1	2	3	4	5	6	7	8	9
1	2	3	4	5	6	7	8	9

1	2	3	4	5	6	7	8	9
1	2	3	4	5	6	7	8	9
1	2	3	4	5	6	7	8	9
1	2	3	4	5	6	7	8	9
1	2	3	4	5	6	7	8	9
1	2	3	4	5	6	7	8	9
1	2	3	4	5	6	7	8	9
1	2	3	4	5	6	7	8	9
1	2	3	4	5	6	7	8	9

Depois recortamos cada quadrado menor $2cm \times 2cm$. Cada quadrado será uma peça do nosso quebra-cabeça. O lado colorido representará os números fixos do sudoku e o verso branco (ou de outra cor) serão as peças que preencherão o quebra-cabeça.

Figura 17 – Peças do sudoku



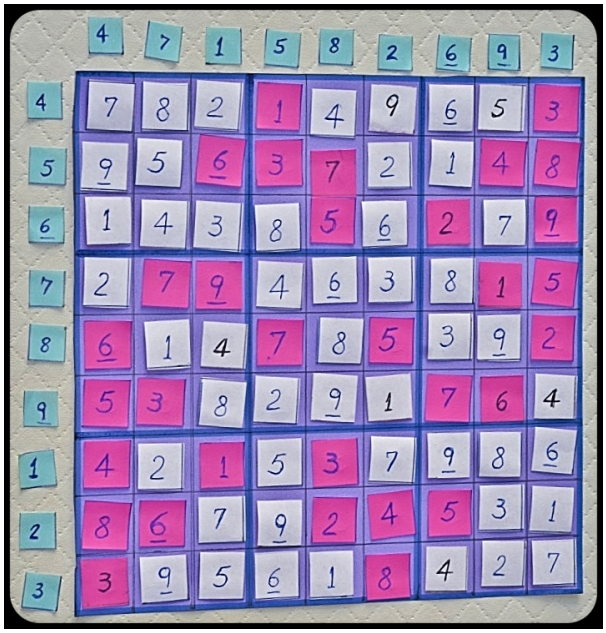
(2º Passo) Escolhemos um dos papéis coloridos e fazemos mais 18 peças, as quais servirão de guia para efetuarmos as operações elementares para montar o sudoku. Para isso, faça mais 18 quadrados $1,5cm \times 1,5cm$ e marque números de 1 a 9, de forma que temos um par de peças com o mesmo algarismo conforme a ilustração abaixo.

Figura 18 – Peças auxiliares

1	2	3	4	5	6	7	8	9
1	2	3	4	5	6	7	8	9

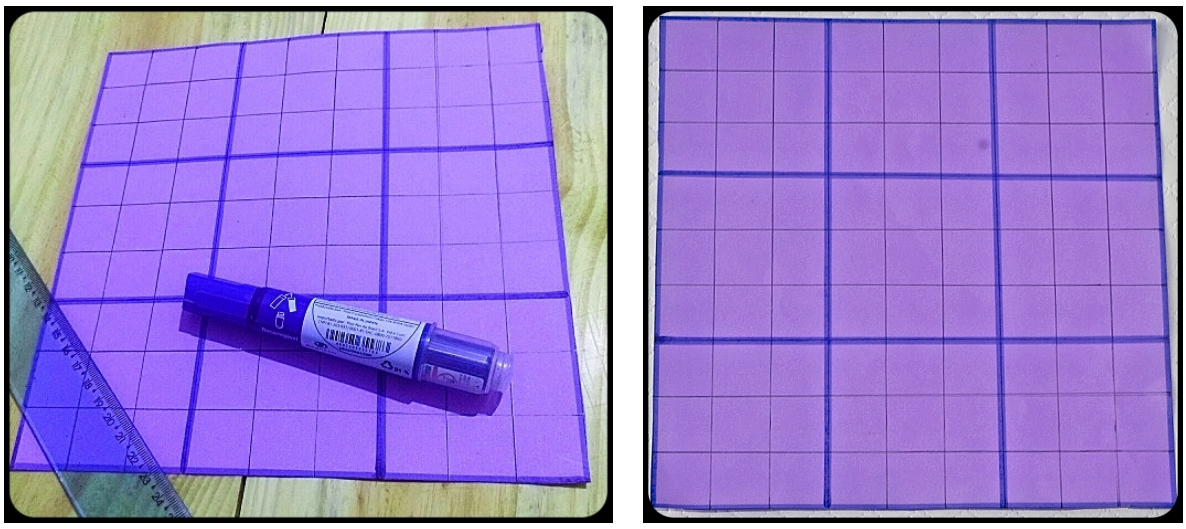
Recorte os quadrados para obter mais 18 peças, as quais vão auxiliar na Construção 1. Agora, para a Construção 2 essas peças não são necessárias.

Figura 19 – Exemplo do sudoku com peças auxiliares



(3º Passo) Para montar o tabuleiro onde as peças serão inseridas pegue o papel ou cartolina com uma cor distinta da utilizada anteriormente e do papel cartão. Nesse papel faça um quadrado de $22,5cm \times 22,5cm$ e divida esse quadrado em uma malha com 9 linhas e 9 colunas, de forma que os quadrados menores tenham a dimensão de $2,5cm \times 2,5cm$. Com o pincel atômico ou canetinha marque as linhas da grade para destacar os blocos do sudoku como na foto a seguir.

Figura 20 – Tabuleiro do sudoku



Observação 4.2.1. Após a construção do material manipulativo o professor pode optar em realizar a Aula Construção 1 - Parte II ou a Aula Construção 2 - Parte II.

4.2.2 Aula 2 Construção 1

Na segunda aula vamos utilizar a Construção 1 do sudoku completo do Capítulo 3 para que cada grupo de alunos consiga montar o seu quebra-cabeça, utilizando a soma dos números inteiros e o resto da divisão por 9 por meio de equações. Posteriormente solicitaremos que cada grupo retirem peças aleatoriamente do sudoku deixando no mínimo 40 peças e cada grupo trocará de material permitindo a resolução desses sudokus por parte de cada grupo.

Plano de Aula: Construção 1 - Parte II						
Dados de Identificação						
Disciplina:		**Data:**	$XX/XX/2019$	**Nível:**	Ensino Médio	**Duração:** 50 minutos
Conteúdo Estruturante:	Números e Álgebra					
Conteúdo Específico:	Sistemas Lineares e Matrizes					
Objetivos						
Objetivos Geral:	· Elaborar a construção do sudoku. · Identificar e manipular elementos de uma matriz. · Resolver equações lineares.					
Objetivos Específico:	· Interpertrar conceitos da adição, subtração, multiplicação, divisão de números inteiros e suas propriedades; · Operar elementos de matrizes;					
Desenvolvimento do tema:	Descrição da abordagem teórica e prática do tema se encontra na subseção 4.2.2.1					
Recursos didáticos:	· Material manipulativo construído na subseção 4.2.1.1.					
Avaliação:	Participar na construção do sudoku por meio de resolução de sistemas lineres e relatar conjecturas e experiências para a construção do sudoku de uma forma diferente.					
Bibliografia:	DELAHAYE, J.-P. The science behind sudoku.Scientific American, Nature PublishingGroup, v. 294, n. 6, p. 80–87, 2006. CARMICHAEL, J.; SCHLOEMAN, K.; WARD, M. B. Cosets and cayley-sudoku tables. Mathematics Magazine, Taylor and Francis, v. 83, n. 2, p. 130 – 139, 2010.					

4.2.2.1 Desenvolvimento da Aula 2 de Construção 1

Nesta aula dividiremos a sala em grupos de no máximo 4 alunos para que cada grupo construa o seu quebra-cabeça. As seguintes etapas mostram como os alunos podem montar um sudoku.

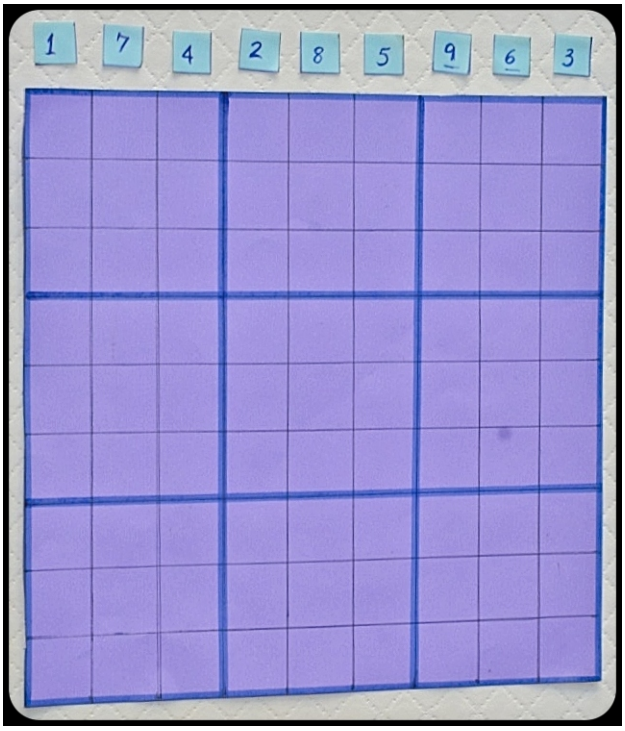
4ª Etapa: Construindo o quebra-cabeça.

Para construir [2] o sudoku vamos utilizar os conjuntos:

$$H+1=\{1,7,4\}; \quad H+2=\{2,8,5\}; \quad H+3=\{9,6,3\}.$$

Solicitamos para os alunos que disponham esses conjuntos acima da primeira linha do tabuleiro, a qual denominaremos de linha 0 da matriz, de maneira que os elementos de um mesmo conjunto fique delimitado pelo mesmo bloco, ou seja, os elementos de um mesmo conjunto podem mudar de posição desde que fiquem em cima de um mesmo bloco utilizando as peças coloridas que possuem as numerações de 1 a 9, mas não possuem a numeração no verso. Segue um exemplo.

Figura 21 – Exemplo com as peças auxiliares



Assim, podemos relacionar cada elemento de um conjunto $H+k$ com cada elemento de um conjunto de posições de elementos na matriz dado por $\{a_{0l}, a_{0l+1}, a_{0l+2}\}$, com $k,l=1,2,3$. Pedimos agora aos alunos para montar mais 3 conjuntos e para isso o grupo de alunos devem escolher um elemento de cada conjunto anterior. Assim, para montar o

[2] Retome o Exemplo 3.1.1 onde $H=3,6,9$.

conjunto L_1 é tomado um elemento de cada conjunto $H+1$, $H+2$ e $H+3$. Os estudantes podem formar, por exemplo, o seguinte conjunto:

$$H+1=\{\not{1},7,\not{4}\};\quad H+2=\{\not{2},\not{8},5\};\quad H+3=\{\not{9},6,\not{3}\};$$

$$L_1=\{7,5,6\}.$$

Para compor o segundo conjunto L_2 requisitamos aos grupos que escolham um elemento de cada conjunto $H+1$, $H+2$ e $H+3$ de maneira que os elementos sejam distintos de L_1. Seguindo o exemplo é possível escolher:

$$H+1=\{1,\not{7},\not{4}\}\quad H+2=\{\not{2},8,\not{5}\}\quad H+3=\{\not{9},\not{6},3\}$$

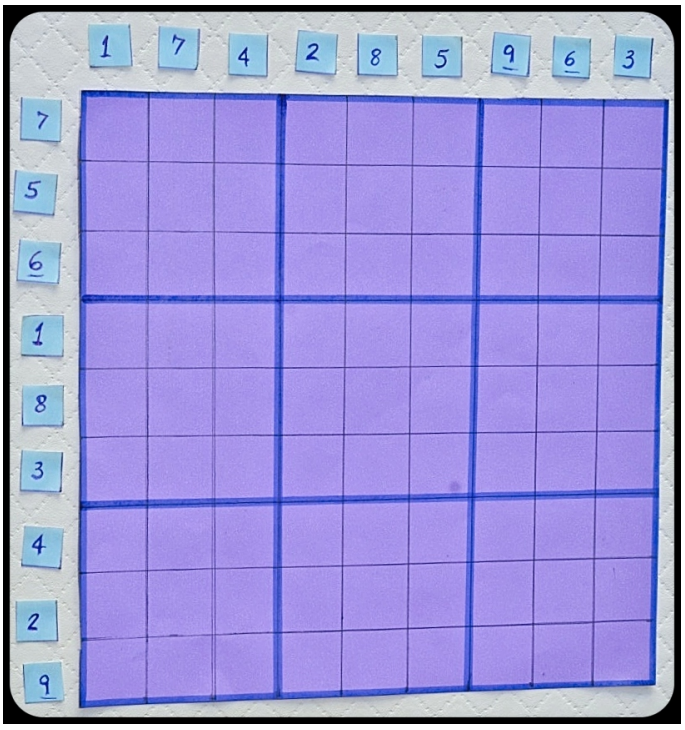
$$L_3=\{1,8,3\}$$

Por fim, o último conjunto é dado pelos elementos que sobram de $H+1$, $H+2$ e $H+3$ que são distintos dos elementos de L_1 e L_2. Assim, seguindo nosso exemplo, temos:

$$L_3=\{4,2,9\}$$

Os alunos devem dispor os conjuntos L_1, L_2 e L_3 na coluna à esquerda da primeira coluna, a qual será denominada de coluna 0, e os elementos de cada conjunto delimitados por cada bloco, por exemplo:

Figura 22 – Exemplo II com as peças auxiliares



Relacionando cada elemento de um conjunto L_m com cada elemento de um conjunto de posições de elementos na matriz dado por $\{a_{n0}, a_{(n+1)0}, a_{(n+2)0}\}$, com $m,n=1,2,3$.

Posteriormente, será explicado como será preenchido as outras posições da matriz para gerar um sudoku completo. Baseado na Construção 1 do sudoku completo o professor pode citar alguns exemplos de como será efetuada a soma dos elementos do sudoku. De acordo com a Figura 22, temos:

$$a_{13} = 7 + 4 = 13 = 9 \cdot 1 + 4;$$

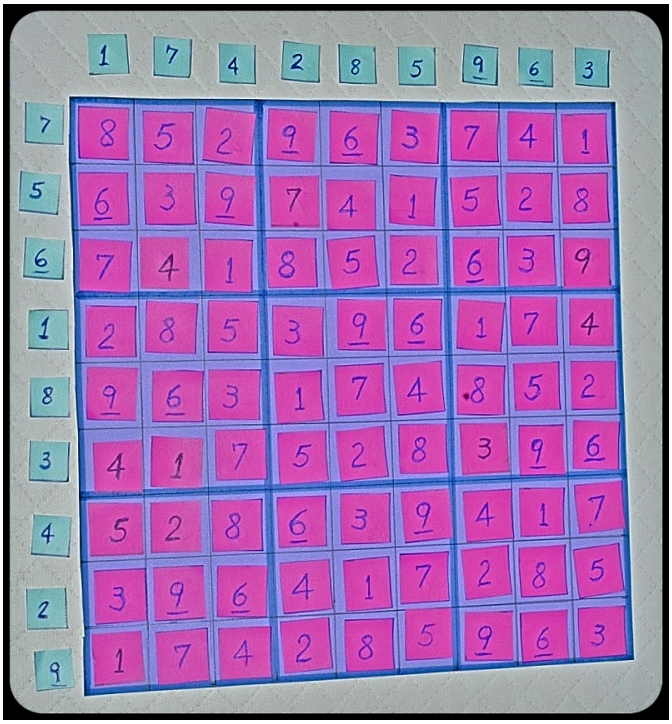
$$a_{26} = 5 + 5 = 10 = 9 \cdot 1 + 1.$$

Com alguns exemplos como esses e comparando o material manipulativo a uma matriz, a turma juntamente com o professor pode chegar na seguinte fórmula do termo geral da matriz que representa o sudoku:

$$a_{0j} + a_{i0} = 9 \cdot q_{ij} + a_{ij},$$

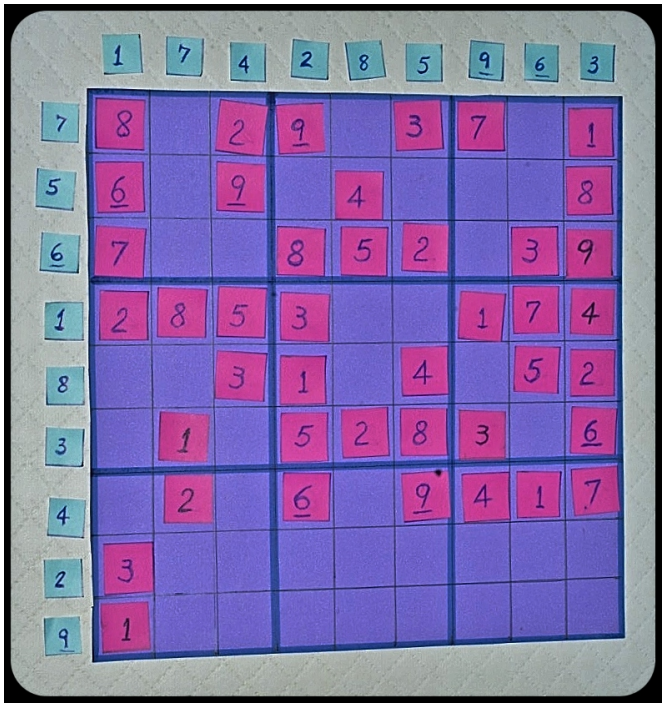
de maneira que $q_{ij} \in \mathbb{Z}$ e $0 \leq a_{ij} < 9$. Assim, é possível para os grupos construírem agora o sudoku completo por meio da operação elementar da soma e do cálculo do resto da divisão por 9, para cada elemento de a_{ij} do tabuleiro.

Figura 23 – Exemplo do sudoku completo



O professor solicitará que cada grupo preencha o tabuleiro com os resultados obtidos utilizando o material manipulativo com as peças de forma que fiquem somente com a parte mais colorida voltada para cima.

Figura 24 – Exemplo do quebra-cabeça



O docente deve solicitar ao grupo de alunos que retirem algumas peças deixando no mínimo 35 peças ou mais, caso os estudantes tenham curiosidade é possível verificar se o sudoku possui uma única resposta no site <https://sudokuspoiler.azurewebsites.net/>. Em todo caso o quebra-cabeça montado possui ao menos uma solução, o que será necessário para a próxima etapa.

5ª Etapa: Resolvendo o sudoku criado.

Na 5ª etapa pedimos para as equipes trocarem de material manipulativo para que outro aluno ou outra equipe tente resolver o quebra-cabeça. Tomando o cuidado de não fornecer as peças da coluna e nem da linha 0, para que a outra equipe tente resolver o sudoku da outra equipe de uma forma mais recreativa sem realizar as equações.

6ª Etapa: Investigando a construção.

Questionar aos estudantes se temos algum padrão específico para que a construção do sudoku seja possível, como o realizado na etapa 4. A resposta para essa pergunta se encontra no Capítulo 3, mas infelizmente não poderemos partilhar a demonstração com os alunos, pois exige um pouco de conhecimento de grupos e classes laterais. Mas, é possível partilhar que podemos alterar a ordem dos elementos dos conjuntos que ainda é possível construir um sudoku completo. E ainda, é possível permutar os conjuntos desde que todos os elementos do conjunto sejam delimitados por um único bloco.

7ª Etapa: Finalização.

Para finalizar a atividade o professor pode pedir um relatório das conclusões das

investigações dos alunos e realizar uma discussão dos resultados obtidos em sala.

4.2.3 Aula 2 Construção 2

Uma outra opção para a segunda parte da aula seria utilizar a Construção 2 do sudoku completo do Capítulo 3, nessa construção os alunos devem permutar as linhas e colunas dos blocos utilizando o material manipulativo para que cada grupo de alunos consiga montar o seu quebra-cabeça. Solicitaremos que cada grupo retirem peças aleatóriamente do sudoku deixando no mínimo 40 peças para trocarem entre os grupos os sudokus deixando a resolução para o outro grupo.

Plano de Aula: Construção 2 - Parte II						
Dados de Identificação						
Disciplina:	**Data:**	$XX/XX/2019$	**Nível:**	Ensino Médio	**Duração:**	50 minutos
Conteúdo Estruturante:	Números e Álgebra					
Conteúdo Específico:	Sistemas Lineares e Matrizes					
Objetivos						
Objetivos Geral:	· Elaborar a construção do sudoku. · Identificar e manipular elementos de uma matriz.					
Objetivos Específico:	· Interpertrar conceitos da adição, subtração, multiplicação, divisão de números inteiros e suas propriedades; · Permutar elementos de matrizes;					
Desenvolvimento do tema:	Descrição da abordagem teórica e prática do tema se encontra na subseção 4.2.3.1					
Recursos didáticos:	· Material manipulativo construído na subseção 4.2.1.1.					
Avaliação:	Participar na construção do sudoku por meio de permutação de elementos na matriz e relatar conjecturas e experiências para a construção do sudoku.					
Bibliografia:	DELAHAYE, J.-P. The science behind sudoku.Scientific American, Nature PublishingGroup, v. 294, n. 6, p. 80–87, 2006. KEEDWELL, A. D. Constructions of complete sets of orthogonal diagonal sudoku squares. Australasian J. Combinatorics, v. 47, p. 227–238, 2010.					

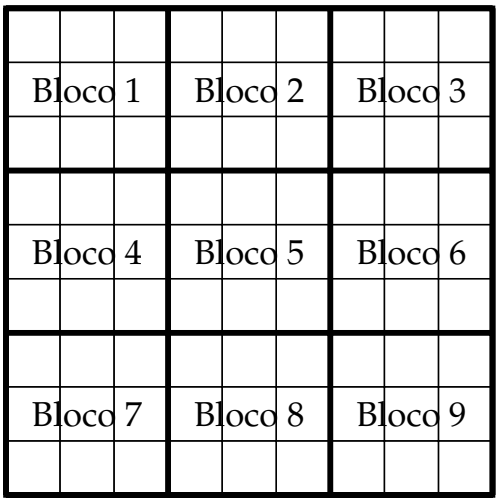
4.2.3.1 Desenvolvimento da Aula 2 de Construção 2.

Dividiremos a sala em grupos de no máximo 4 alunos, analogamente à segunda parte da aula para a Construção 1, para que cada grupo construa o seu quebra-cabeça. Nas próximas etapas mostram como os alunos podem montar um sudoku.

4ª Etapa: Construindo o quebra-cabeça.

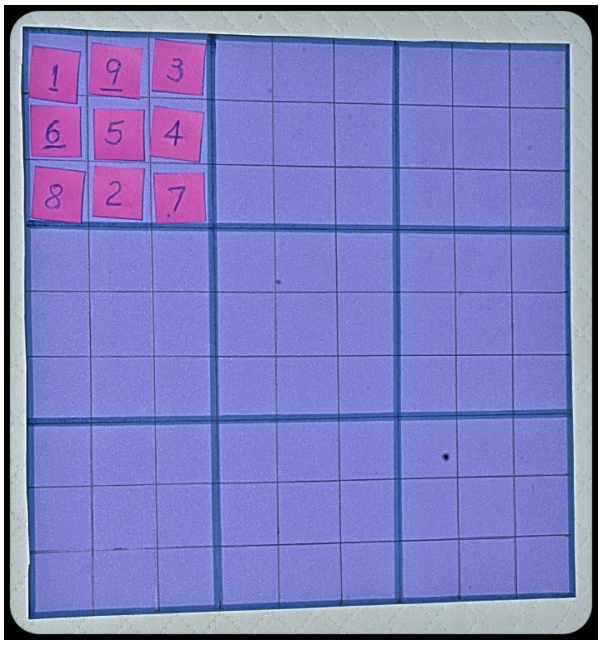
Primeiramente, o professor irá numerar os blocos como na figura seguinte.

Figura 25 – Blocos do sudoku



Depois solicitará para que os grupos preencham o bloco 1 com algarismos de 1 a 9 aleatoriamente utilizando as peças do material manipulativo.

Figura 26 – Exemplo de preenchimento do Bloco 1



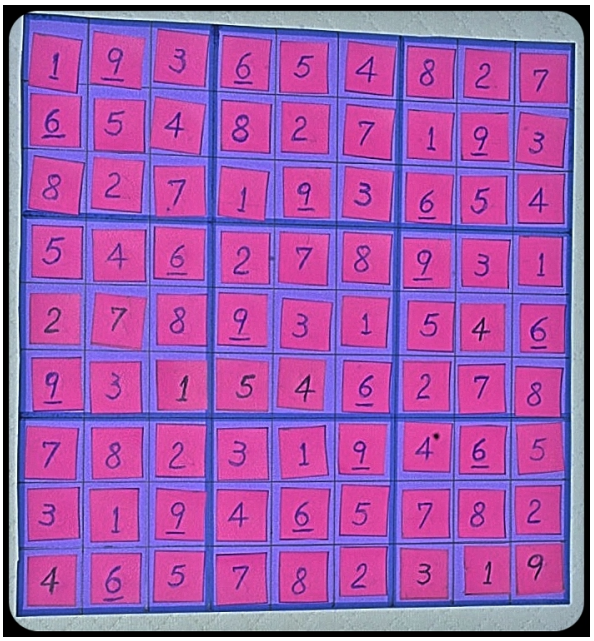
Para construir o sudoku o professor mostrará para os grupos realizarão as permutações das linhas e das colunas. De acordo, com o Exemplo 3.2.2 e o Exemplo 3.2.3.

Em seguida, o docente pede aos alunos para construírem o sudoku de acordo com a seguinte tabela [3]:

Y	$Y\alpha$	$Y\alpha^2$
$Y\alpha\beta$	$Y\alpha^2\beta$	$Y\beta$
$Y\alpha^2\beta^2$	$Y\beta^2$	$Y\alpha\beta^2$

Cada grupo deve construir um sudoku com o material manipulativo de modo que o tabuleiro fique preenchido com as peças voltadas com a face colorida para cima de acordo com as operações dadas na tabela anterior.

Figura 27 – Exemplo da Construção 2 do sudoku

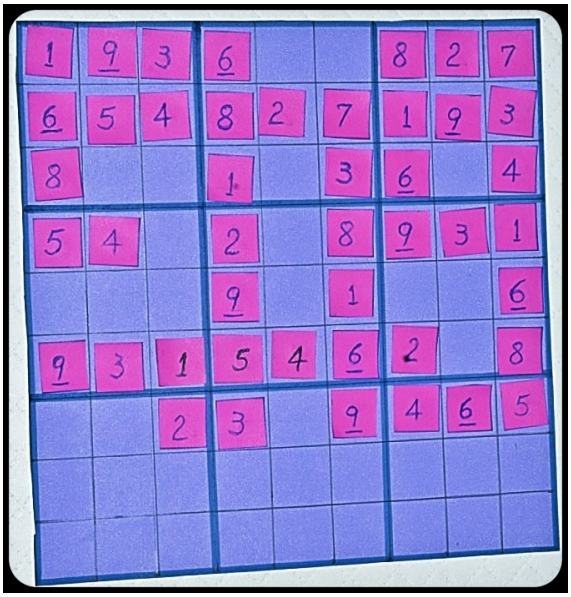


5ª Etapa: Resolvendo o sudoku criado.

Nessa etapa o professor pedirá para que os alunos retirem algumas peças aleatoriamente de maneira que restem no mínimo 40 peças no tabuleiro. Posteriormente solicitamos para as equipes trocarem de material manipulativo para que outro aluno ou outra equipe tente resolver o quebra-cabeça.

[3] O professor pode escolher uma dentre as 6 tabelas da página 44.

Figura 28 – Exemplo do sudoku dado pela Construção 2



6ª Etapa: Investigando a construção.

O professor pode questionar se existe outro padrão de construção semelhante para que a construção do sudoku seja possível, como o realizado na etapa 4. A resposta para essa pergunta se encontra no capítulo 3, com as 6 tabelas das construções lineares de Keedwell para $p = 3$, o professor pode compartilhar essa informação, mas não será possível realizar a demonstração para os alunos, pois exige um pouco de lógica matemática, como a demonstração por absurdo. Mas, é possível partilhar as outras tabelas para que os estudantes consigam construir outros tipos de sudoku.

7ª Etapa: Finalização.

Para finalizar a atividade o docente poderá pedir um relatório das conclusões das investigações dos alunos da 6ª etapa e realizaremos uma discussão dos resultados obtidos em sala.

CONCLUSÃO

Este trabalho permitiu analisarmos a relação existente entre a álgebra e o jogo sudoku. Para isso se fez necessário conhecer a Teoria de Grupos e suas propriedades, estudamos os subgrupos e classes laterais, as quais serviram de base para a Construção 1 do sudoku completo. Ainda relacionada à Teoria de Grupos vimos que podemos relacionar um grupo finito a um subgrupo de S_n, o que nos permite relacionar um grupo com o quebra-cabeça. A teoria trabalhada no apêndice permitiu uma melhor compreensão dos quadrados latinos descritos no Capítulo 2, uma vez que esses quadrados antecedem o sudoku. Vimos que é possível representar a estrutura algébrica de grupo finito por meio de um quadrado latino e que toda tábua de operação de um grupo finito resulta em um quadrado latino, mas nem todo quadrado latino é a tábua de operação de um grupo.

No Capítulo 3 foi possível entendermos duas construções do sudoku completo por meio da Teoria de Grupos e dos quadrados latinos, analisamos essas construções com exemplos e exploramos também a demonstração de cada uma, expondo como a matemática está relacionada com o nosso cotidiano. Consequentemente, foi possível elaborar uma atividade explorando as construções estudadas nesse capítulo. Já no Capítulo 4 segue a elaboração de uma atividade em sala de aula, a qual foi dividida em duas aulas de 50 minutos de maneira que a segunda aula pode ser trabalhada com uma das construções do sudoku.

Propomos também a construção de um material manipulativo para tornar a aula mais atrativa e dinâmica para os alunos, uma vez que o uso de recursos e materiais são importantes na exploração de problemas segundo os Parâmetros Curriculares Nacionais (BRASIL, 1998). Portanto, desejamos que esse trabalho auxilie professores e acadêmicos a entender um pouco mais de álgebra de maneira mais agradável e cativante. Ressaltando o conhecimento matemático fora do ambiente escolar de uma maneira diferenciada. Explorando um pouco da matemática contida no jogo sudoku e aproveitando os resultados para aplicar diretamente em sala.

Referências

ALEGRI, M.; SILVA, S. B. Sobre sudokus e grupos. *Revista Sergipana de Matemática e Educação Matemática*, v. 2, n. 1, p. 51–63, 2017.

BRASIL. *Parâmetros curriculares nacionais: Matemática*. Brasília: Ministério da Educação, Secretaria da Educação Fundamental, 1998.

BRASIL. *Orientações curriculares para o ensino médio: Ciências da natureza, matemática e suas tecnologias*. 1. ed. Brasília: Ministério da Educação, Secretaria da Educação Básica, 2006. v. 2.

CARMICHAEL, J.; SCHLOEMAN, K.; WARD, M. B. Cosets and cayley-sudoku tables. *Mathematics Magazine*, Taylor & Francis, v. 83, n. 2, p. 130–139, 2010.

DELAHAYE, J.-P. The science behind sudoku. *Scientific American*, Nature Publishing Group, v. 294, n. 6, p. 80–87, 2006.

GONÇALVES, A. *Introdução à álgebra*. 5. ed. Rio de Janeiro: Impa, 2003.

JUSSIEN, N. *A to Z of Sudoku*. ISTE, 2007.

KEEDWELL, A. D. Constructions of complete sets of orthogonal diagonal sudoku squares. *Australasian J. Combinatorics*, v. 47, p. 227–238, 2010.

MARTINS, P. M.; PICADO, J. Existe um sudoku com 16 pistas? *Boletim da Sociedade Portuguesa de Matemática*, n. 66, 2012.

MENEZES, A. L. J. de; MUZATTI, L. A. F. Jogos no ensino da matemática. *Revista Interface Tecnológica*, v. 13, n. 1, p. 53–67, 2016.

OLIVEIRA, R. G. d. A aplicação do jogo sudoku no ensino médio como ferramenta para auxiliar o discente a pensar e refletir. in: Paraná. secretaria de estado da educação. superintendência de educação. os desafios da escola pública paranaense na perspectiva do professor pde. 2014.

PARANÁ. *Diretrizes Curriculares da Educação Básica: Matemática*. Curitiba: SEED, 2008.

ROSENHOUSE, J.; TAALMAN, L. *Taking sudoku seriously: The math behind the world's most popular pencil puzzle*. OUP USA, 2011.

SILVA, H. B. da; COSTA, E. T. Estruturas de grupos finitos. *Revista Eletrônica de Matemática*, n. 2, 2010.

Apêndices

APÊNDICE A

TEORIA DE GRUPOS

A.1 Definições

No apêndice estudaremos um pouco sobre a teoria de grupos e trabalharemos desde a definição das estruturas algébricas básicas às classes laterais. Porexemplo, veremos vários resultados e o Teorema da Representação de grupos para melhor compreender os capítulos desenvolvidos no trabalho. Tais estudos foram realizados por meio da pesquisa no livro, Introdução à álgebra (GONÇALVES, 2003), os quais são trabalhados por meio de definições, demonstrações de resultados e exemplos.

Definição A.1.1 (Operação Binária)**.** Seja A um conjunto não vazio. Uma operação binária sobre A é uma função $* : A \times A \to A$, denotada por $*(x, y) = x * y$, isto é,

$$\begin{aligned} * : A \times A &\to A \\ (x, y) &\mapsto x * y. \end{aligned}$$

Observação A.1.2. Como para todo $(x, y) \in A \times A$ temos $x * y \in A$, dizemos que a operação $*$ é fechada em A.

Definição A.1.3 (Estrutura Algébrica)**.** Considere A um conjunto não vazio e seja $*$ uma operação em A. Denominamos a estrutura algébrica $(A, *)$ de:

(i) **Semigrupo** se a operação $*$ é associativa, ou seja,

$$\forall x, y, z \in A, \text{temos } (x * y) * z = x * (y * z);$$

(ii) **Monoide** se a operação $*$ é associativa e possui um elemento neutro $e \in A$, ou seja,

$$\forall x \in A,\ \exists\, e \in A \text{ tal que } x * e = e * x = x;$$

(iii) **Grupo** se $(A, *)$ é um monoide e cada elemento $x \in A$ tenha inverso com relação à operação $*$, isto é, temos que,

$$\forall x \in A,\ \exists\, x' \in A \text{ tal que } x * x' = x' * x = e.$$

Se $(A, *)$ é um grupo que satisfaz a condição de que para cada par $x, y \in A$ temos $x * y = y * x$, dizemos que essa estrutura é um grupo abeliano.[1]

Exemplo A.1.4. (i) A estrutura algébrica $(\mathbb{N}, +)$ é um monoide comutativo.

$$x + y = y + x$$

Note que, $(\mathbb{N}, +)$ não é grupo, uma vez que todo número natural $x \geq 1$ não possui inverso aditivo em $\mathbb{N}$.

(ii) A estrutura algébrica $(\mathbb{Z}, +)$ é um grupo abeliano.

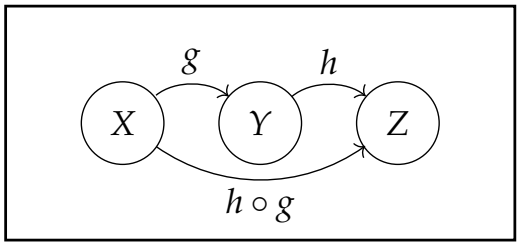
(iii) As estruturas $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ e $(\mathbb{C}, +)$ com a operação usual de adição também são grupos.

Exemplo A.1.5 (Monoide das transformações de um conjunto A)**.** Seja A um conjunto não vazio. Chamaremos de transformação de A uma função $f : A \to A$ e de $M(A)$ o conjunto de todas as transformações de A. Dada $\circ$ a operação de composição de funções e com as funções $g : X \to Y$ e $h : Y \to Z$, definimos:

$$\begin{aligned} h \circ g : X &\to Z \\ x &\mapsto (h \circ g)(x) = h(g(x)), \end{aligned}$$

podemos ainda representar o comportamento da função $h \circ g$ pelo diagrama a seguir.

Figura 29 – Composição de funções.



Observe que o conjunto $M(A)$ é fechado para a operação de composição de funções. De fato, sejam duas funções $i, j \in M(A)$ então $i : A \to A$ e $j : A \to A$, logo $j \circ i : A \to A \in M(A)$.

Verificaremos que $(M(A).\circ)$ **é um monoide não comutativo** quando o conjunto A contém ao menos dois elementos distintos.

[1] Esse grupo recebe o nome de *grupo abeliano* devido ao matemático norueguês Niels Henrik Abel (1802-1829). (SILVA; COSTA, 2010)

(i) $\circ$ é associativa.

Com efeito, sejam $f, g, h \in M(A)$,

$$f : A \to A,\ g : A \to A \text{ e } h : A \to A$$

temos

$$((h \circ g) \circ f)(x) = (h \circ g)((f(x)) = h(g(f(x))) \tag{A.1}$$

e

$$(h \circ (g \circ f))(x) = h(g \circ f)(x) = h(g(f(x))) \tag{A.2}$$

$\forall x \in X$, portanto, das equações (A.1) e (A.2) temos o desejado,

$$(h \circ g) \circ f = h \circ (g \circ f).$$

(ii) $\circ$ possui elemento neutro.

Seja a função identidade definida em A da seguinte forma:

$$\begin{aligned} I_A : A &\to A \\ x &\mapsto I_A(x) = x. \end{aligned}$$

Assim, I_A é elemento neutro de $(M(A), \circ)$. De fato, para cada função $f \in M(A)$, temos

$$(I_A \circ f)(x) = I_A(f(x)) = f(x) \tag{A.3}$$

e

$$(f \circ I_A)(x) = f(I_A(x)) = f(x), \tag{A.4}$$

$\forall x \in A$ então de (A.3) e (A.4), obtemos

$$I_A \circ f = f \circ I_A = f.$$

Logo, $(M(A), \circ)$ é um monoide. Agora, vamos mostrar que esse monoide não é comutativo.

Assuma dois elementos a e b distintos do conjunto A, e suponha as transformações constantes $f : A \to A$ e $g : A \to A$, dadas por

$$f(x) = a \text{ e } g(x) = b,\ \forall x \in A.$$

Assim, para cada elemento $x \in A$ temos

$$(f \circ g)(x) = f(g(x)) = f(b) = a \tag{A.5}$$

e

$$(g \circ f)(x) = g(f(x)) = g(a) = b. \tag{A.6}$$

Portanto, de (A.5) e (A.6) segue que

$$f \circ g \neq g \circ f.$$

Assim, a operação $\circ$ não é comutativa em $M(A)$.

Proposição A.1.6. Uma transformação $f \in M(A)$ é invertível se, e somente se, f é bijetora.

Demonstração. Seja $f \in M(A)$ uma transformação invertível. Logo, existe uma função $g \in M(A)$ de maneira que

$$f \circ g = g \circ f = I_A.$$

Queremos mostrar que f é injetora e sobrejetora, ou seja, bijetora.

(i) f é injetora.
De fato, sejam $x_1, x_2 \in A$ no domínio e suponhamos que $f(x_1) = f(x_2)$. Vamos mostrar que $x_1 = x_2$, então

$$x_1 = I_A(x_1) = (g \circ f)(x_1) = g(f(x_1)) = g(f(x_2)) = (g \circ f)(x_2) = I_A(x_2) = x_2.$$

Portanto, f é injetora.

(ii) f é sobrejetora.
Pois, para cada elemento $y_0 \in A$ no contradomínio temos

$$y_0 = I_A(y_0) = (f \circ g)(y_0) = f(g(y_0)) = f(x_0)$$

com $g(y_0) = x_0$.
Assim, para cada $y_0 \in A$ no contradomínio existe $x_0 \in A$ no domínio tal que $f(x_0) = y_0$, então f é sobrejetora.

Reciprocamente, seja f uma função bijetora do conjunto $M(A)$. Seja a transformação $g \in M(A)$ uma candidata a função inversa de f que definiremos da seguinte maneira.

Como f é sobrejetora para cada elemento $a \in A$ no contradomínio de f, existe $b \in A$ no domínio de f tal que $f(b) = a$. E ainda, como f é injetora, então o elemento b é único, ou seja, se $b' \in A$ e $f(b') = a$ então $f(b) = f(b') \Rightarrow b = b'$.

Vamos definir a função g no ponto a como $g(a) = b$. Agora, definida a função g, para cada elemento $a \in A$ do contradomínio de g e cada $b \in A$ no domínio de g, temos a seguinte equivalência $f(a) = b$ e $g(b) = a$, isto é, $f(a) = b \Leftrightarrow g(b) = a$.

Mostraremos que $f \circ g = g \circ f = I_A$. Sejam $f(x) = \alpha$ e $g(x) = \beta$ para cada $x \in A$, assim $g(\alpha) = x$ e $f(\beta) = x$. Portanto,

$$(f \circ g)(x) = f(g(x)) = f(\beta) = x = I_A \tag{A.7}$$

e

$$(g \circ f)(x) = g(f(x)) = g(\alpha) = x = I_A. \tag{A.8}$$

Logo, $(f \circ g)(x) = (g \circ f)(x) = A$. ■

A.2 Propriedades

Proposição A.2.1. Seja $(G, *)$ um grupo então existe um único elemento neutro $e \in G$ da operação $*$ em G.

Demonstração. Suponha e_1 e e_2 dois elementos neutros da operação $*$, ou seja, $x * e_1 = e_1 * x = x$ e $y * e_2 = e_2 * y = y$, $\forall x, y \in G$. Note que,

$$e_1 = e_1 * e_2 = e_2.$$

Logo, $e_1 = e_2$, ou seja, o elemento neutro é único. ■

Proposição A.2.2. Para qualquer $x \in G$, existe um único elemento $y \in G$, elemento inverso de x relativamente à operação $*$ do grupo $(G, *)$.

Demonstração. Fixado $a \in G$. Suponha que existam dois elementos a_1 e a_2 inversos ao elemento a, ou seja, $a * a_1 = a_1 * a = e$ e $a * a_2 = a_2 * a = e$. Então,

$$a_1 = a_1 * e = a_1 * (a * a_2) = (a_1 * a) * a_2 = e * a_2 = a_2.$$

Portanto, o elemento inverso é único, uma vez que $a_1 = a_2$. ■

Observação A.2.3. Dessa forma, dado $x \in G$, escreveremos x^{-1} para inverso multiplicativo e $-x$ para o inverso aditivo.

Proposição A.2.4. Para x e $y \in G$ de maneira que x' e y' sejam seus respectivos inversos, temos que o inverso de $x * y$ é $y' * x'$ dado $(G, *)$.

Demonstração. Por hipótese, temos

$$x * x' = x' * x = e \text{ e } y * y' = y' * y = e.$$

Queremos mostrar que $(y' * x') * (x * y) = (x * y) * (y' * x') = e$. De fato,

$$\begin{aligned}
&(y' * x') * (x * y) = y' * (x' * x) * y \\
\Rightarrow\ &(y' * x') * (x * y) = y' * e * y \\
\Rightarrow\ &(y' * x') * (x * y) = y' * y \\
\Rightarrow\ &(y' * x') * (x * y) = e
\end{aligned}$$

e

$$\begin{aligned}
&(x * y) * (y' * x') = x * (y * y') * x' \\
\Rightarrow\ &(x * y) * (y' * x') = x * e * x' \\
\Rightarrow\ &(x * y) * (y' * x') = x * x' \\
\Rightarrow\ &(x * y) * (y' * x') = e.
\end{aligned}$$

■

Proposição A.2.5. Seja um grupo $(G, *)$ e $x \in G$ então $(x^{-1})^{-1} = x$.

Demonstração. Considere e o elemento neutro de $(G, *)$, assim $x = x * e = x * x^{-1} * (x^{-1})^{-1}$. ■

Definição A.2.6. Um grupo $(G, *)$ é dito finito se o conjunto G é finito, neste caso a ordem do grupo G é dada pelo número de elementos de G, a qual denotaremos por $|G|$. Caso G seja um conjunto infinito dizemos que $(G, *)$ é um grupo infinito e que $|G| = \infty$.

Definição A.2.7 (Grupo das permutações)**.** Dado o conjunto $S \neq \varnothing$ e $G = \{f : S \to S : f \text{ bijetora}\}$. Seja $*$ a operação composição de funções, ou seja,

$$\begin{aligned}
* : G \times G &\to G \\
(g, f) &\mapsto g \circ f
\end{aligned}$$

então temos que $(G, *)$ é um grupo, conhecido como grupo das permutações, sendo a identidade dada por,

$$\begin{aligned}
I_S : S &\to S \\
x &\mapsto x.
\end{aligned}$$

Note que,$(G, *)$ é de fato um grupo, pois $*$ é associativa e possui elemento neutro pelos itens (i), (ii) do Exemplo A.1.5 e pela Proposição A.1.6 todo elemento de G possui inverso em relação à operação $*$.

Caso $S = \{1, 2, \ldots, n\}$ denotamos esse grupo das permutações por S_n, e ainda, o número de elementos de $S_n = n!$, pois, $n!$ é justamente o número de maneira que podemos permutar n objetos.

Exemplo A.2.8. O grupo S_n, em que $n \geq 3$ não é grupo abeliano.

De fato, dadas as funções $f, g \in S_n$ definidas por $f : \{1, 2, 3, \ldots, n\} \to \{1, 2, 3, \ldots, n\}$ tal que $f(1) = 2$, $f(2) = 1$, $f(x) = x \ \forall x, \ 3 \leq x \leq n$ e $g : \{1, 2, 3, \ldots, n\} \to \{1, 2, 3, \ldots, n\}$ tal que $g(1) = 3$, $g(2) = 2$, $g(3) = 1$, $g(x) = x \ \forall x, \ 4 \leq x \leq n$. Temos,

$$(g \circ f)(1) = g(f(1)) = g(2) = 2$$

e

$$(f \circ g)(1) = f(g(1)) = f(3) = 3.$$

Logo, $g \circ f \neq f \circ g$.

Notação: Seja f um elemento de S_n, denotaremos esse elemento por:

$$f = \begin{pmatrix} 1 & 2 & 3 & \ldots & \text{n} \\ \text{f(1)} & \text{f(2)} & \text{f(3)} & \ldots & \text{f(n)} \end{pmatrix}.$$

Exemplo A.2.9. Os elementos de S_3 são:

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}; \qquad f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = f_1^{-1};$$

$$f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = f_2^{-1}; \qquad f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = f_3^{-1};$$

$$f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = f_5^{-1}; \qquad f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = f_4^{-1}.$$

Observe que, para operar dois elementos em S_3 compomos os elementos da seguinte forma:

$$f_1 \circ f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = f_4.$$

Note que, para o elemento 1 temos $1 \leftrightarrow 1$ por f_2 e depois $1 \leftrightarrow 2$ por f_1. Para o elemento 2, temos que $2 \leftrightarrow 3$ por f_2 e $3 \leftrightarrow 3$ por f_1. Por fim, $3 \leftrightarrow 2$ por f_2 e $2 \leftrightarrow 1$ por f_1.

Agora, vamos estudar a aritmética dos restos e as classes de equivalência, pois, esses assuntos serão necessários para a análise da tabela do sudoku.

Para entendermos o grupo $(\mathbb{Z}_n, +)$, vamos trabalhar com a aritmética dos restos. Para isto primeiramente recordemos a divisão euclidiana.

Teorema A.2.10 (Princípio da boa ordem)**.** O conjunto dos números naturais é bem-ordenado, isto é, todo subconjunto $S \neq \varnothing$ de números naturais possui um elemento mínimo.

Demonstração. Vamos, tomar um subconjunto $C \subset \mathbb{N}$ que não possui elemento mínimo, então vamos mostrar que C deve ser o conjunto vazio. Considerando o conjunto $S = \{m \in \mathbb{N}; \forall n \in \mathbb{N},\ n < m \Rightarrow n \notin C\}$, note que $S = \mathbb{N} - C$. Por indução vamos mostrar que $S = \mathbb{N}$, note que $1 \in S$, uma vez que para cada $n \in \mathbb{N}$, $n < 1$ é falso. Vamos supor que $k \in S$, então se n é menor que o sucessor de k temos que $n < k$ ou $n = k$. Mas, para $n < k$ temos que $n \notin C$ e se $n = k \Rightarrow n \notin C$, pois, $n \in S$. Assim, para ambos os casos $n \notin C$. Portanto, todo sucessor de k pertence ao conjunto S. Logo, $S = \mathbb{N}$. ∎

Teorema A.2.11. Sejam a e $b \in \mathbb{Z}$, em que $a \neq 0$. Existem únicos números q e r inteiros tais que,

$$b = a \cdot q + r, \text{ com } 0 \leq r < |a|.$$

Demonstração. Vamos provar a existência de q e r tais que $b = a \cdot q + r$ e $0 \leq r < |a|$. Primeiramente, considere o conjunto $X = \{b - ay; y \in \mathbb{Z}\} \cap (\mathbb{N} \cup 0)$. Como $a \neq 0$ então existe $n \in \mathbb{Z}$ tal que $n \cdot (-a) > -b \Rightarrow n \cdot (-a) + b > 0 \Rightarrow b - na > 0$ e portanto, $X \neq \varnothing$. Note, que o conjunto é limitado inferiormente por 0 então existe um menor elemento do conjunto X, pelo Princípio da boa ordem.

Suponha r o menor elemento desse conjunto tal que $r = -baq$, e pela definição de X temos $r \geq 0$. Agora, vamos mostrar que $r < |a|$. Então, suponha por absurdo que $r \geq |a|$. Assim, existe $x \in \mathbb{N} \cup \{0\}$ de maneira que $r = |a| + x$ e portanto, $0 \leq x < r$, pois, temos $r > x$. Ainda de $r = |a| + x$ temos $r = a + x \Rightarrow b - aq = a + x \Rightarrow b - (q+1)a = x$ ou $r = -a + x \Rightarrow b - aq = -a + x \Rightarrow b - (q-1)a = x$, ou seja, $x \in X$ e $0 \leq x < r$. Isto é um absurdo, pois r é o menor elemento em X.

Para provar a unicidade suponha que existam q, q_1, r e r' tais que,

$$a = bq + r, \qquad 0 \leq r < b; \tag{A.9}$$

$$a = bq_1 + r_1, \qquad 0 \leq r_1 < b. \tag{A.10}$$

Subtraindo as equações (2.9) e (2.10), temos $r - r_1 = b(q_1 - q)$. Note que, como $0 \leq r < b$ e $0 \leq r_1 < b$ então $0 \leq r - r_1 < b \Rightarrow 0 \leq b(q_1 - q) < b$. Mas, $b > 0$ então $0 \leq q - q_1 < 1$ isso ocorre se, e somente se, $q - q_1 = 0$, uma vez que q e q_1 são inteiros. Assim, $q = q_1$ e $r = r_1$.

∎

Definição A.2.12. Com $n \in \mathbb{N}$, dois números a e $b \in \mathbb{Z}$ são congruentes módulo n se, e somente se, n divide $b - a$. E denotamos por,

$$a \equiv b \bmod n.$$

Podemos dizer também que se a é congruente a b módulo n se os restos da sua divisão euclidiana por n são iguais.

Exemplo A.2.13. Temos que $7 \equiv 10 \bmod 3$, pois, 3 divide $10 - 7 = 3$, podemos pensar também que os restos da divisão euclidiana de 7 e 10 por 3 são iguais a 1, portanto, 7 é congruente a 10 módulo $n = 3$.

Decorre da definição de congruência, módulo $n \in \mathbb{Z}$ fixado, é uma relação de equivalência, ou seja, ela é reflexiva, simétrica e transitiva.

Proposição A.2.14. Seja $n \in \mathbb{N}$. Para todos $a, b, c \in \mathbb{Z}$, temos que:

(i) $a \equiv a \bmod n$ (reflexiva);

(ii) se $a \equiv b \bmod n$ então $b \equiv a \bmod n$ (simétrica);

(iii) se $a \equiv b \bmod n$ e $b \equiv c \bmod n$ então $a \equiv c \bmod n$ (transitiva).

Demonstração. Para o item (i), temos que n divide $a - a = 0$ logo $a \equiv a \bmod n$. Agora, para demonstrar o item (ii) temos que se $a \equiv b \bmod n$ então n divide $b - a$, assim n também divide $a - b$. Para o item (iii) temos que $a \equiv b \bmod n$ e $b \equiv c \bmod n$ então n divide $b - a$ e n divide $b - c$. Portanto, n divide $(b - a) + (c - b) = c - a$ e assim n divide $c - a$ então $a \equiv c \bmod n$. ∎

Definição A.2.15. Definimos classe de equivalência de r em relação a $x \bmod n$, denotada por $\overline{r}$, com $n \in \mathbb{Z}$, como:

$$\overline{r} = \{x \in \mathbb{Z}; x \bmod n\},$$

ou ainda,

$$\overline{r} = \{kn + r : k \in \mathbb{Z}, 0 \leq r < n\}.$$

Definição A.2.16. Definimos o conjunto $\mathbb{Z}_n$, como:

$$\mathbb{Z}_n = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}.$$

Proposição A.2.17. Se $n \in \mathbb{N} \cup \{0\}$ então $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}$ é um conjunto contendo exatamente n classes de equivalência.

Demonstração. Primeiro vamos mostrar que se $0 \leq x < y < n$ então $\overline{x} \neq \overline{y}$, com $x, y, n \in \mathbb{Z}$. Temos que, $\overline{y} = \overline{x} \Leftrightarrow x \equiv y \bmod n \Leftrightarrow 0 < y - x = kn$ para algum $k \in \mathbb{Z}$. Mas, como $a \leq x < y < y < n$ então $y - x$ não pode ser múltiplo de n, isto é, $\overline{x} \neq \overline{y}$. Portanto, $\{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}$ é um conjunto contendo exatamente n elementos.

Agora, vamos mostrar que $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}$. Então, basta mostrar que se $\overline{x} \in \mathbb{Z}_n$ temos que $\overline{x} \in \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}$. Escolhemos $k \in \mathbb{Z}$ suficientemente grande de maneira que $x' = x + kn$ seja não negativo. Deste modo, x' é congruente a x módulo n, ou seja, $x' \equiv x \bmod n$ então $\overline{x'} = \overline{x}$. Assim, é suficiente mostrar que $x' \in \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}$, com $x' \geq 0$.

Pelo teorema (A.2.11) temos que $\exists q,\ r \in \mathbb{Z}$ tais que $x' = qn + r$, em que $0 \leq r < n$. Assim, $x' - r = qn$, ou seja, $x' \equiv r \mod n$. Logo, $\overline{x} = \overline{x'} = \overline{r}$. ∎

Proposição A.2.18. Seja $n \in \mathbb{N}$. Se $x \equiv x' \mod n$ e $y \equiv y' \mod n$. Então,

(i) $x + y \equiv x' + y' (\mod n)$;

(ii) $x \cdot y \equiv x' \cdot y' (\mod n)$.

Demonstração. Por hipótese, $x - x' = kn$ e $y - y' = sn$ com $k, s \in \mathbb{Z}$, então

$$\begin{aligned}(x + y) - (x' + y') &= (x - x') + (y - y') \\ &= kn + sn \\ &= (k + s)n,\end{aligned}$$

e assim, $x + y \equiv x' + y' (\mod n)$ e isso demonstra o item (i). Para mostrar o item (ii), fazemos

$$\begin{aligned}(x \cdot y) &= (kn + x')(sn + y') \\ &= (ksn)n + (ky')n + (x's)n + x' \cdot y',\end{aligned}$$

daí,

$$\begin{aligned}(x \cdot y) - x' \cdot y' &= (ksn)n + (ky')n + (x's)n + x' \cdot y' - x' \cdot y' \\ &= (ksn)n + (ky')n + (x's)n,\end{aligned}$$

logo $x \cdot y \equiv x' \cdot y' (\mod n)$. ∎

Colorário A.2.19. Seja $n \in \mathbb{N}$. Se $\overline{x} = \overline{x'}$ e $\overline{y} = \overline{y'}$, então:

(i) $\overline{x + y} = \overline{x' + y'}$;

(ii) $\overline{x \cdot y} = \overline{x' \cdot y'}$.

Definição A.2.20. Pelo Colorário (A.2.19) as regras:

$$\overline{x} + \overline{y} = \overline{x + y} \qquad \text{e} \qquad \overline{x} \cdot \overline{y} = \overline{x \cdot y},$$

definem as operações de adição e multiplicação no conjunto $\mathbb{Z}_n$, respectivamente por:

$$\begin{aligned}+ : \mathbb{Z}_n \times \mathbb{Z}_n &\to \mathbb{Z} \\ (\overline{x}, \overline{y}) &\mapsto \overline{x + y} = \overline{x} + \overline{y}\end{aligned} \qquad \text{e} \qquad \begin{aligned}\cdot : \mathbb{Z}_n \times \mathbb{Z}_n &\to \mathbb{Z} \\ (\overline{x}, \overline{y}) &\mapsto \overline{x \cdot y} = \overline{x} \cdot \overline{y}\end{aligned}$$

Exemplo A.2.21. Dado $\mathbb{Z}_9 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}, \overline{8}\}$, temos que $\overline{2} + \overline{9} = \overline{2+9} = \overline{11} = \overline{2}$, pois o reto da divisão de 11 por 9 é 2 e $\overline{3} \cdot \overline{4} = \overline{3 \cdot 4} = \overline{12} = \overline{3}$, uma vez que o resto da divisão de 12 por 9 é 3.

Observação A.2.22. Para facilitar a visualização nos exemplos seguintes denotaremos as classes de equivalência, em $\mathbb{Z}_n$, $\overline{a}$ por a e para a classe $\overline{0}$ por n.

Definição A.2.23 (Tábua de Operação)**.** Seja $G = \{a_1, a_2, \ldots, a_n\}$, com $n \geq 1$ um conjunto com n elementos e $*$ uma operação sobre G definida pela seguinte aplicação $f : G \times G \to G$ que associa cada par ordenado (a_i, a_j) ao elemento $f(a_i, a_j) = a_i * a_j = a_{ij}$. Assim, podemos representar os elementos a_{ij} em uma tabela, a qual denominamos de tábua de operação, da seguinte maneira,

$*$	a_1	a_2	$\cdots$	a_n
a_1	$a_1 * a_1$	$a_1 * a_2$	$\cdots$	$a_1 * a_n$
a_2	$a_2 * a_1$	$a_2 * a_2$	$\cdots$	$a_2 * a_n$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
a_n	$a_n * a_1$	$a_n * a_2$	$\cdots$	$a_n * a_n$

.

Exemplo A.2.24. Abaixo, seguem as tábuas de operação de adição e multiplicação em $\mathbb{Z}_9$, de maneira que as classes de equivalência $\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}$ e $\overline{8}$ serão denotadas por $9, 1, 2, 3, 4, 5, 6, 7$ e 8, respectivamente.

Figura 30 – Tábuas de adição e multiplicação em $\mathbb{Z}_9$

+	1	2	3	4	5	6	7	8	9
1	2	3	4	5	6	7	8	9	1
2	3	4	5	6	7	8	9	1	2
3	4	5	6	7	8	9	1	2	3
4	5	6	7	8	9	1	2	3	4
5	6	7	8	9	1	2	3	4	5
6	7	8	9	1	2	3	4	5	6
7	8	9	1	2	3	4	5	6	7
8	9	1	2	3	4	5	6	7	8
9	1	2	3	4	5	6	7	8	9

·	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9
2	2	4	6	8	1	3	5	7	9
3	3	6	9	3	6	9	3	6	9
4	4	8	3	7	2	6	1	5	9
5	5	1	6	2	7	3	8	4	9
6	6	3	9	6	3	9	6	3	9
7	7	5	3	1	8	6	4	2	9
8	8	7	6	5	4	3	2	1	9
9	9	9	9	9	9	9	9	9	9

Exemplo A.2.25. $(\mathbb{Z}_n, +)$ é um grupo abeliano.

Demonstração. Para mostrar que $(\mathbb{Z}_n, +)$ é um grupo abeliano, vamos mostrar os itens a seguir.

(i) Para todo $\overline{x}$, $\overline{y}$, $\overline{z} \in (\mathbb{Z}_n, +)$, temos

$$\begin{aligned}\overline{x} + (\overline{y} + \overline{z}) &= \overline{x} + (\overline{y+z}) \\ &= \overline{x + (y+z)} \\ &= \overline{(x+y) + z} \\ &= (\overline{x+y}) + \overline{z} \\ &= (\overline{x} + \overline{y}) + \overline{z}.\end{aligned}$$

(ii) Tomando $\overline{0}$, temos que para todo $\overline{x} \in \mathbb{Z}_n$, $\overline{x} + \overline{0} = \overline{x+0} = \overline{x}$.

(iii) Seja $\overline{n-x} \in \mathbb{Z}_n$ então para todo $\overline{x}$ temos $\overline{x} + \overline{n-x} = \overline{x + (n-x)} = \overline{n} = \overline{0}$.

(iv) Note que, $\forall\ \overline{x},\ \overline{y} \in \mathbb{Z}_n$ temos $\overline{x} + \overline{y} = \overline{x+y} = \overline{y+x} = \overline{y} + \overline{x}$.

Logo, $(\mathbb{Z}, +)$ é um grupo abeliano. ∎

Definição A.2.26. Seja $(G, \cdot)$ um grupo e $x \in G$. Se $n \in \mathbb{Z}$ vamos definir x^n da seguinte maneira:

$$x^n = \begin{cases} e & \text{se } n = 0 \\ x^{n-1} \cdot x & \text{se } n > 0 \\ (x^{-n})^{-1} & \text{se } n < 0 \end{cases}.$$

Proposição A.2.27. Se $m, n \in \mathbb{Z}$ temos:

(i) $x^m \cdot x^n = x^{m+n}$;

(ii) $(x^m)^n = x^{mn}$.

Demonstração. Vamos demonstrar o item (i) por indução em n, assim fixamos x e m arbitrariamente. Então, por definição temos:

$$x^m \cdot x^1 = x^m \cdot x = x^{m+1}.$$

Agora, supondo que $x^m \cdot x^n = x^{m+n}$ obtemos:

$$x^m \cdot x^{n+1} = x^m \cdot (x^n \cdot x) = (x^m \cdot x^n) \cdot x = x^{m+n} \cdot x = x^{m+n+1}.$$

Para o item (ii) utilizaremos também a indução sobre n, fixando x e m, temos:

$$(x^m)^1 = x^m = x^{m \cdot 1}.$$

Suponha que $(x^m)^n = x^{mn}$, então

$$(x^m)^{n+1} = (x^m)^n \cdot x^m = x^{mn} \cdot x^m = x^{mn+m} = x^{m(n+1)}.$$

■

Exemplo A.2.28 (Grupo Cíclico)**.** Se denotarmos $\langle x \rangle = \{x^m : m \in \mathbb{Z}\} \subset G$, em que G é um grupo, então como $x^0 = e$, $(x^m)^{-1} = x^{-m}$ e $x^m \cdot (x^n \cdot x^q) = x^{m(nq)} = x^{(mn)q} = (x^m \cdot x^n) \cdot x^q$ segue que $\langle x \rangle$ é um grupo. E ainda, o grupo $\langle x \rangle$ é chamado de grupo cíclico gerado pelo elemento $x \in G$.

Exemplo A.2.29. $\langle 3 \rangle \in (\mathbb{Z}_9, +)$ é um grupo cíclico dado por $\{\overline{3}, \overline{6}, \overline{0}\}$.

A.3 Subgrupos e classes laterais

Definição A.3.1 (Subgrupo)**.** Sejam G um grupo e H um subconjunto não vazio de G. Dizemos que H é um subgrupo de G se H for ele próprio um grupo com a mesma operação de G.

Notação: $H \leq G$.

Para simplificar as notações e as operações de um grupo, denotaremos um grupo $(G, *)$ como grupo G e a operação $a * b$ denotaremos por ab.

Proposição A.3.2. Seja G um grupo H um subconjunto não vazio de G. As condições a seguir são equivalentes:

(i) H é um subgrupo de G.

(ii) (a) $e \in H$

(b) $\forall a, b \in H$ tem-se $ab \in H$

(c) $\forall a \in H$ tem-se $a^{-1} \in H$.

(iii) $\forall a \in H$ tem-se $a^{-1} \in H$.

Demonstração. (i) $\Rightarrow$ (ii) Segue imediatamente da definição de subgrupo, da unicidade do elemento neutro e e da unicidade do elemento a^{-1} inverso de a. Temos que (ii) $\Rightarrow$ (i), então mostraremos que H é grupo. Pelos itens (a) e (c) H possui elemento neutro e inverso, basta então mostrar que a operação de H é associativa. De fato, pela condição (b) H é fechado para a operação de G e como a operação em G é associativa a operação em H também é associativa.

Para mostrar que (ii) $\Rightarrow$ (iii), note que pelo item (a) $e \in H$ então $H \neq \varnothing$ e pelo item (c) se $b \in H \Rightarrow b^{-1} \in H$. Portanto, se $a, b \in H$, temos por (b) que $ab^{-1} \in H$. Agora,

temos que (iii) $\Rightarrow$ (ii), pois, se $H \neq \varnothing \Rightarrow \exists a \in H$. Assim, $e = aa^{-1} \in H$. Mas, se $a \in H$ segue que $a^{-1} = ea^{-1} \in H$, e finalmente se $a, b \in H$ tem-se $a, b^{-1} \in H$ e daí $ab = a(b^{-1})^{-1} \in H$, pela Proposição A.2.5. ■

Exemplo A.3.3. Seja G um grupo e $x \in G$. Então, o $\langle x \rangle = H$ é um subgrupo de G. De fato, ver Exemplo A.2.28.

Exemplo A.3.4. Sejam $H_1, \ldots, H_n$ subgrupos de um grupo G. Então, $H = H_1 \cap \cdots \cap H_n$ é um subgrupo de G.

Demonstração. Temos que $e \in H$, pois, $e \in H_i, \forall i \in \{1, 2, \ldots, n\}$, então $H \neq \varnothing$. E ainda, se $a, b \in H \Rightarrow a, b^{-1} \in H_i, \forall i \in \{1, 2, \ldots, n\}$, então $ab^{-1} \in H$ e pela Proposição A.3.2 item (iii) H é um subgrupo de G. ■

Exemplo A.3.5. Sejam $H_1 \subseteq H_2 \subseteq \cdots \subseteq H_n \subseteq H_{n+1} \subseteq \ldots$ subgrupos de um grupo G. Então, $H = \bigcup_{i=1}^{\infty} H_i$ é um subgrupo de G.

Demonstração. Note que, $e \in H$, pois, $e \in H_i \subset H$ então $H \neq \varnothing$. Além disso, se $a, b \in H \Rightarrow a \in H_r, b \in H_s$ onde $r, s \in \{1, 2, \ldots, n, \ldots\}$. Assumimos $r \leq s$, sem perda de generalidade, então $a, b \in H_s$, uma vez que, $H_r \subseteq H_s$. Portanto, $ab^{-1} \in H_s \subset H \Rightarrow ab^{-1} \in H$ e assim pela proposição A.3.2 item (iii) H é subgrupo de G. ■

Proposição A.3.6. Seja G um grupo e H um subgrupo de G. Temos que, $x, y \in G$, $x \equiv y \ (mod\ H) \Leftrightarrow xy^{-1} \in H$ define uma relação de equivalência no conjunto G.

Demonstração. A relação é reflexiva, pois, $x \equiv x \ (mod\ H), \forall x \in G$, uma vez que $xx^{-1} = e \in H$. Temos que essa relação também é transitiva, ou seja, $x \equiv y \ (mod\ H) \Rightarrow y \equiv x \ (mod\ H)$. Pois, se $xy^{-1} \in H$ então $yx^{-1} = (xy^{-1})^{-1} \in H$. Por, fim a relação é transitiva, isto é, se $x \equiv y \ (mod\ H)$ e $y \equiv z \ (mod\ H) \Rightarrow x \equiv z \ (mod\ H)$. De fato, temos $xy^{-1} \in H$ e $yz^{-1} \in H \Rightarrow (xy^{-1})(yz^{-1}) = xz^{-1} \in H$. Logo, $x, y \in G$, $x \equiv y \ (mod\ H) \Leftrightarrow xy^{-1} \in H$ define uma relação de equivalência no conjunto G. ■

Definição A.3.7 (Classe Lateral)**.** Sejam G um grupo e H um subgrupo de G. Para cada elemento $a \in G$, define-se a classe lateral à direita de H, determinada por a por:

$$Ha = \{ha : h \in H\}.$$

Analogamente, definimos

$$aH = \{ah : h \in H\}$$

como sendo a classe lateral à esquerda de H, determinada por a.

Observação A.3.8. Se G é um grupo abeliano, então $Ha = aH, \forall a \in G$. Mas, se G não for abeliano podemos ter $Ha \neq aH$, para certos elementos a do grupo G.

Exemplo A.3.9. Seja o grupo $(\mathbb{Z}_9, +)$ e seja o subgrupo $H = \{\overline{3}, \overline{6}, \overline{9}\} = \langle\overline{3}\rangle$. As classes laterais à direita de $\mathbb{Z}_9$ são dadas por:

$$H + \overline{1} = \{\overline{4}, \overline{7}, \overline{1}\}; \qquad H + \overline{4} = \{\overline{7}, \overline{1}, \overline{4}\}; \qquad H + \overline{7} = \{\overline{1}, \overline{4}, \overline{7}\};$$

$$H + \overline{2} = \{\overline{5}, \overline{8}, \overline{2}\}; \qquad H + \overline{5} = \{\overline{8}, \overline{2}, \overline{5}\}; \qquad H + \overline{8} = \{\overline{2}, \overline{5}, \overline{8}\};$$

$$H + \overline{3} = \{\overline{6}, \overline{9}, \overline{3}\}; \qquad H + \overline{6} = \{\overline{9}, \overline{3}, \overline{6}\}; \qquad H + \overline{9} = \{\overline{3}, \overline{6}, \overline{9}\}.$$

Note que,

$$H + \overline{0} = H + \overline{3} = H + \overline{6};$$
$$H + \overline{1} = H + \overline{4} = H + \overline{7};$$
$$H + \overline{2} = H + \overline{5} = H + \overline{8}.$$

Assim, temos somente três classes laterais distintas.

Observação A.3.10. Seja G um grupo e H um subgrupo de G, vamos denotar G/H o conjunto das classes laterais à direita de H. Assim, no exemplo anterior temos $G/H = \{H + \overline{1}, H + \overline{2}, H + \overline{3}\}$. Note ainda que, $H + \overline{1} \cup H + \overline{2} \cup H + \overline{3} = G$.

Teorema A.3.11. Seja um grupo G e um subgrupo H de G. Então:

(i) $\forall a, b \in G$, temos
$$Ha = Hb \Leftrightarrow ab^{-1} \in H.$$

(ii) $\forall a, b \in G$, se $b \in H$ então $Hb = Ha$.

(iii) Duas classes laterais direitas de H são iguais ou disjuntas, ou seja,
$$\forall a, b \in G, Ha = Hb \text{ ou } Ha \cap Hb = \varnothing.$$

Note que, $Ha = H \Leftrightarrow a \in H$.

(iv) Se H é finito, então, para cada $a \in G$, o número de elementos de Ha é igual ao número de elementos de H, ou seja, $|Ha| = |H|, \forall a \in G$.

(v) A reunião de todas as classes laterais direitas de H distintas é igual a G, isto é,
$$\bigcup_{a \in G} Ha = G.$$

Demonstração. (i) Note que, $a \in Ha$, pois, sendo e o elemento neutro de G temos $a = e * a \in Ha$. Seja $Ha = Hb$ então $a \in Ha$ e $a \in Hb$, ou seja, $a = hb$ para algum $h \in H$. Assim,$a = hb \Rightarrow ab^{-1} = hbb^{-1} \Rightarrow ab^{-1} = h \in H$. Reciprocamente, seja $ab^{-1} \in H$ vamos mostrar que $Ha \subset Hb$ e depois mostraremos que $Hb \subset Ha$.

Assim, mostraremos que $Ha \subset Hb$. Seja $x \in Ha$, então $x = ha$ para algum $h \in H$. Como H é um grupo, temos

$$x = ha = (ha)e = (ha)(b^{-1}b) = (h(ab^{-1}))b,$$

e como $h(ab^{-1}) \in H$, temos que $x \in Hb$.

Agora, para mostrar que $Hb \subset Ha$ observe como H é um subgrupo temos $ab^{-1} \in H$ e também $(ab^{-1})^{-1} = ba^{-1} \in H$. Tomando $x \in Hb$, temos $x = hb$ para algum $h \in H$ e assim

$$x = hb = (hb)e = (hb)(a^{-1}a) = (h(ba^{-1}))a,$$

já que $h(ba^{-1}) \in H$ temos $x \in Ha$.

(ii) Tome $b \in Ha$, assim $b = ha$ para algum $h \in H$ então $h = ba^{-1}$ o que implica que $ba^{-1} \in H$. Logo, pelo item (i) temos $Ha = Hb$.

(iii) Vamos mostrar que Ha e Hb são iguais ou disjuntas. Suponhamos, que Ha e Hb não são disjuntas. Assim, existe $x \in G$ tal que $x \in Ha \cap Hb$. Logo, $x = ha = h'b$, para certos $h, h' \in H$. Daí, como $ha = h'b \Rightarrow h^{-1}ha = h^{-1}h'b \Rightarrow ea = h^{-1}h'b \Rightarrow a = h^{-1}h'b$. Portanto, $ab^{-1} = (h^{-1}h'b)b^{-1} = h^{-1}h'$ e temos que $ab^{-1} \in H$. Logo, pelo item (i) $Ha = Hb$.

(iv) Para mostrar que o número de elementos de Ha é igual ao número de elementos de H vamos tomar a aplicação $f : H \to Ha$, definida por $f(h) = ha, \forall h \in H$ e mostraremos que f é bijetora. A função f é sobrejetora, pois, cada elemento de Ha é dado por ha para algum $h \in H$, ou seja, $ha = f(h)$ para algum $h \in H$. Note que f é injetora, uma vez que se $f(h_1) = f(h_2) \Rightarrow h_1a = h_2a \Rightarrow h_1aa^{-1} = h_2aa^{-1} \Rightarrow h_1 = h_2$. Portanto, como f é bijetora temos que $|H| = |Ha|$.

(v) Para demonstrar que $\bigcup_{a \in G} Ha = G$ vamos mostrar que $\bigcup_{a \in G} Ha \subset G$ e que $\bigcup_{a \in G} Ha \supset G$. Note que, $aH \subset G$, para cada $a \in G$, assim $\bigcup_{a \in G} Ha \subset G$. Em contrapartida, temos que para cada elemento $a \in G$, temos $a \in Ha$, assim $a \in \bigcup_{a \in G} Ha$. Logo, $\bigcup_{a \in G} Ha \subset G$, e portanto $\bigcup_{a \in G} Ha = G$. Podemos mostrar analogamente que a união de todas as classes laterais à esquerda módulo H também é igual a G.

■

Proposição A.3.12. Seja G um grupo e H um subgrupo de G. Considere o conjunto $G/H = \{Ha; a \in G\}$ e a operação em G/H dada por:

$$\begin{aligned} \star : G/H \times G/H &\to G/H \\ (Ha_1, Ha_2) &\mapsto Ha_1 \star Ha_2 = Ha_1a_2. \end{aligned}$$

Então, G/H munido da operação $\star$ é um grupo.

Demonstração. Para mostrar que o conjunto G/H munido da operação $\star$ é um grupo, vamos mostrar que a operação é associativa, possui elemento neutro e para todo $Ha \in G/H$ temos o seu inverso.

(i) A operação é associativa, uma vez que para $Ha_1, Ha_2, Ha_3 \in G/H$ temos,

$$\begin{aligned}(Ha_1 \star Ha_2) \star Ha_3 &= H(a_1a_2) \star Ha_3 \\ &= H(a_1a_2)a_3 \\ &= Ha_1(a_2a_3) \\ &= Ha_1 \star (Ha_2a_3) \\ &= Ha_1 \star (Ha_2 \star Ha_3).\end{aligned}$$

(ii) Seja $H = He$, então para cada classe lateral $Ha \in G/H$ temos,

$$Ha \star He = Hae = Ha = Hea = He \star Ha.$$

Assim, H é a identidade do grupo.

(iii) Para cada elemento $Ha \in G/H$, existe Ha^{-1} tal que,

$$Ha \star Ha^{-1} = Haa^{-1} = H = Ha^{-1}a = Ha^{-1} \star Ha.$$

■

Definição A.3.13 (Grupo Quociente)**.** O grupo G/H munido da operação $\star$ é chamado de grupo quociente.

Teorema A.3.14. (Teorema de Lagrange) Se G é um grupo finito e H é um subgrupo de G, então $|H|$ é um divisor de $|G|$, ou seja, a ordem de H é um divisor da ordem de G.

Demonstração. Sendo G um grupo finito temos que G/H é finito. Digamos que, $|G/H| = n$ e $G/H = \{Hx_1, Hx_2, \ldots, Hx_n\}$. Assim, $G = \{Hx_1 \cup Hx_2 \cup \cdots \cup Hx_n\}$ o que implica que $|G| = |Hx_1| + |Hx_2| + \cdots + |Hx_n|$. Note que, $|Hx_i| = |H| \forall i,\ 1 \leq i \leq n$, pelo item (iv) do Teorema A.3.11. Assim, temos $|G| = |Hx_1| + |Hx_2| + \cdots + |Hx_n| = n|H|$ e logo $\dfrac{|G|}{|H|} = n$ demonstrando o teorema. ■

A.4 Subgrupo Normal e Homomorfismo

Definição A.4.1. Seja G um grupo e seja H um subgrupo de G denotado por $H \leq G$. Se $g \in G$ definimos a função ψ_g (conjugação pelo elemento $g \in G$) por

$$\begin{aligned}\psi_g : G &\to G \\ x &\mapsto \psi_g(x) = x^g = g^{-1}xg.\end{aligned}$$

Observe que $\psi_g(H) = \{\psi_g(h) : h \in H\} = \{h^g = g^{-1}hg : h \in H\}$ e denotaremos por H^g ou $g^{-1}Hg$.

Definição A.4.2. Um subgrupo $H \leq G$ é denominado normal (ou invariante) em G se $\psi_g(H) = H^g \subseteq H, \forall g \in G$.

Notação: $H \trianglelefteq G$.

Observação A.4.3. Note que, $H^g \subseteq H, \forall g \in G \Rightarrow H^g = H, \forall g \in G$. De fato, pois, $\forall h \in H$ tenho $g^{-1}hg \in H^g \Rightarrow H \subseteq H^g$ e como por hipótese $H^g \subseteq H$, temos $H^g = H$.

Proposição A.4.4. Sejam N_1 e N_2 subgrupos normais de G, então $N_1 \cap N_2 \trianglelefteq G$.

Demonstração. Seja $x \in N_1 \cap N_2$ e $g \in G$, se $x \in N_1 \cap N_2 \Rightarrow x \in N_1$ e $x \in N_2$. Pela definição de grupo normal, temos $x^g \in N_1^g = N_1$ e $x^g \in N_2^g = N_2 \Rightarrow x^g \in (N_1 \cap N_2) = (N_1 \cap N_2)^g, \forall g \in G$. Logo, $N_1 \cap N_2 \trianglelefteq G$. ∎

Definição A.4.5. Sejam os grupos $(G, *)$ e $(G', \circledast)$ denotados respectivamente por G e G' e $\psi : G \to G'$ uma função de G em G'. Dizemos que ψ é um homomorfismo se

$$\psi(x * y) = \psi(x) \circledast \psi(y), \ \forall x, y \in G,$$

ou ainda,

$$\psi(xy) = \psi(x)\psi(y), \ \forall x, y \in G.$$

Definição A.4.6. Um isomorfismo de grupos é um homomorfismo bijetivo, ou seja, se $\psi : G \to G'$ é um isomorfismo então vale $\psi(xy) = \psi(x)\psi(y), \ \forall x, y \in G$ e ψ é bijetora, e nesse caso dizemos que G é isomorfo a G' e denotamos $G \simeq G'$.

Proposição A.4.7. Seja S um conjunto finito com n elementos, então o grupo das permutações de S dado por $\mathcal{P}(S)$ é isomorfo a S_n.

Demonstração. Sejam $S = \{x_1, x_2, \ldots, x_n\}$ e a função

$$\begin{aligned} \rho : S &\to \{1, 2, \ldots, n\} \\ x_i &\mapsto \rho(x_i) = i. \end{aligned}$$

Note que, ρ é uma bijeção, pois, se $\rho(x_i) = \rho(x_j) \Rightarrow i = j \Rightarrow x_i = x_j$ e como a quantidade de elementos de S é igual aos elementos de $\{1, 2, \ldots, n\}$ temos que ρ é sobrejetora.

Agora, definimos a função $F : \mathcal{P}(S) \to S_n$ por $F(f) = \rho \circ f \circ \rho', \forall f \in \mathcal{P}(S)$, em que $\circ$ é a operação de composição de funções. Vamos mostrar que F é um isomorfismo, assim temos

$$\begin{aligned} F(f \circ g) &= \rho \circ (f \circ g) \circ \rho^{-1} \\ &= \rho \circ f \circ \rho^{-1} \circ \rho \circ g \circ \rho^{-1} \\ &= F(f) \circ F(g). \end{aligned}$$

Logo, F é um homomorfismo de grupos.

Temos que, se $f, g \in \mathcal{P}(S)$ suponha $F(f) = F(g) \Rightarrow \rho \circ f \circ \rho^{-1} = \rho \circ g \circ \rho^{-1} \Rightarrow \rho \circ f \circ \rho^{-1} \circ \rho = \rho \circ g \circ \rho^{-1} \circ \rho \Rightarrow \rho \circ f = \rho \circ g \Rightarrow \rho^{-1} \circ \rho \circ f = \rho^{-1} \circ \rho \circ g \Rightarrow f = g$, portanto, F é injetiva.

Se $\sigma \in S_n$, então $\rho^{-1} \circ \sigma \circ \rho \in \mathcal{P}(S)$ e $F(\rho^{-1} \circ \sigma \circ \rho) = \rho \circ \rho^{-1} \circ \sigma \circ \rho \circ \rho^{-1} = \sigma$ e assim F é sobrejetora. ■

Proposição A.4.8. Seja G um grupo e $N \trianglelefteq G$. Então, para todo $x, y \in G$, $\overline{x}\ \overline{y} = \overline{xy}$ define uma operação no conjunto das classes G/N e mais ainda G/N é um grupo com essa operação.

Demonstração. Para mostrar que $\overline{x}\ \overline{y} = \overline{xy}$ é uma operação em G/N vamos mostrar que essa operação independe da escolha dos representantes das classes. Assim, sejam $\overline{x} = \overline{a}$ e $\overline{y} = \overline{b}$ queremos mostrar que $\overline{x}\ \overline{y} = \overline{a}\ \overline{b}$, isto é, $\overline{xy} = \overline{ab}$.

Então, basta mostrarmos que $Nxy = Nab$, ou seja, que $(xy)(ab)^{-1} \in N$. Mas, note que $xy(ab)^{-1} = xyb^{-1}a^{-1}$ e que por hipótese $\overline{x} = \overline{a}$ e $\overline{y} = \overline{b}$ então $xa^{-1} \in N$ e $yb^{-1} \in N$.

Logo, se $n_1 = xa^{-1} \in N$ e $n_2 = yb^{-1} \in N$ então,

$$\begin{aligned}(xy)(ab)^{-1} &= xyb^{-1}a^{-1} \\ &= x(n_2)a^{-1} \\ &= (n_1a)(n_2)a^{-1} \\ &= n_1(an_2a^{-1}).\end{aligned}$$

Assim, como $n_1 \in N$ e $an_2a^{-1} \in N^{a^{-1}} = N$ temos que $(xy)(ab)^{-1} \in N$ e portanto a operação independe da escolha dos representantes. Vamos mostrar agora que G/N é um grupo. Então,

(i) o elemento identidade de G/N é $\overline{e} = Ne = N$, pois $\overline{e}\ \overline{x} = \overline{ex} = \overline{x} = \overline{xe} = \overline{x}\ \overline{e}, \forall \overline{x} \in G/N$.

(ii) $\overline{x}\ (\overline{y}\ \overline{z}) = \overline{x}\ \overline{(yz)} = \overline{x(yz)} = \overline{(xy)z} = \overline{(xy)}\ \overline{z} = (\overline{x}\ \overline{y})\ \overline{z}$, então é válida a associatividade $\forall\ \overline{x}, \overline{y}, \overline{z} \in G/N$.

(iii) se $\overline{x} \in G/N$ então $\overline{x^{-1}}\ \overline{x} = \overline{x}\ \overline{x^{-1}} = \overline{xx^{-1}} = \overline{e}$, assim existe elemento inverso $\forall \overline{x} \in G/N$.

Portanto, $\overline{G} = G/N$ é um grupo munido da operação $\overline{x}\ \overline{y} = xy, \forall\ \overline{x}, \overline{y} \in \overline{G}$. ■

Teorema A.4.9 (1º Teorema do homomorfismo)**.** Sejam G e G' grupos com identidades e e e' respectivamente e $\psi : G \to G'$ um homomorfismo. Então:

(i) $Im(\psi) = \psi(G) = \{\psi(g) : g \in G\}$ é um subgrupo de G'. (chamado de imagem do homomorfismo)

(ii) $N(\psi) = \{g \in G : \psi(g) = e'\}$ é um subgrupo normal de G. (chamado de núcleo do homomorfismo) e ainda,

$$\psi \text{ é injetiva} \Leftrightarrow N(\psi) = \{e\}$$

(iii) $G/N(\psi) \simeq Im(\psi)$.

Demonstração. (i) Para $Im(\psi)$ ser um subgrupo de G' basta mostrar que $Im(\psi) \neq \varnothing$ e que tomando dois elementos de $Im(\psi)$, sejam eles $\psi(g_1)$ e $\psi(g_2) \Rightarrow \psi(g_1)\psi(g_2) \in Im(\psi)$. De fato, $e' = \psi(e) \in Im(\psi)$ pois $ee = e \Rightarrow \psi(e)\psi(e) = \psi(e) \Rightarrow \psi(e)\psi(e)\psi(e)^{-1} = \psi(e)\psi(e)^{-1} \Rightarrow \psi(e) = e'$, assim $Im(\psi) \neq \varnothing$.

Agora, tomando $\psi(g_1), \psi(g_2) \in Im(\psi) \Rightarrow \psi(g_1)\psi(g_2)^{-1} = \psi(g_1 g_2^{-1}) \in Im(\psi), \forall g \in G$, uma vez que $\psi(g)\psi(g)^{-1} = e' = \psi(e) = \psi(gg^{-1}), \forall g \in G$.
(ii) Vamos mostrar que $N(\psi)$ é subgrupo de G. Assim,

(a) $e \in N(\psi)$, visto que $\psi(e) = e'$.

(b) $g_1,\ g_2 \in N(\psi) \Rightarrow g_1 g_2 \in N(\psi)$. De fato, $g_1,\ g_2 \in N(\psi) \Rightarrow \psi(g_1 g_2) = \psi(g_1)\psi(g_2) = e'e' = e' \Rightarrow g_1 g_2 \in N(\psi)$.

(c) $g \in N(\psi) \Rightarrow g^{-1} \in N(\psi)$. Pois, $g \in N(\psi) \Rightarrow \psi(g^{-1}) = \psi(g)^{-1} = e'^{-1} = e' \Rightarrow g^{-1} \in N(\psi)$. Portanto, $N(\psi)$ é um subgrupo de G.

Vamos mostrar que $N(\psi) \trianglelefteq G$. De fato, se $n \in N(\psi)$ e $g \in G$ temos,

$$\psi(g^{-1}ng) = \psi(g)^{-1}\psi(n)\psi(g) = \psi(g)^{-1}e'\psi(g) = e',$$

assim $g^{-1}ng \in N(\psi), \forall n \in N(\psi), \forall g \in G$ e logo $N(\psi.) \trianglelefteq G$.

Agora, basta mostrar que ψ é injetiva $\Leftrightarrow N(\psi) = \{e\}$. Assim, se $x, y \in G$, temos $\psi(x) = \psi(y) \Leftrightarrow \psi(x)\psi(y)^{-1} = \psi(y)\psi(y)^{-1} \Leftrightarrow \psi(x)\psi(y)^{-1} = e' \Leftrightarrow \psi(xy^{-1}) = e' \Leftrightarrow xy^{-1}$, assim segue se ψ é injetora temos $\psi(x) = \psi(y) \Rightarrow x = y \Rightarrow xx^{-1} \in N(\psi), \forall x \in G \Rightarrow N(\psi) = e$. Agora, se $N(\psi) = e$ suponha $\psi(x) = \psi(y) \Rightarrow xy^{-1} \in N(\psi) \Rightarrow xy^{-1} = e \Rightarrow xy^{-1}y = ey \Rightarrow x = y$, então ψ é injetiva.

(iii) Mostraremos que $G/N(\psi) \simeq Im(\psi)$. Seja $\overline{G} = G/N(\psi)$ e $N = N(\psi) \trianglelefteq G$ e definimos

$$\begin{aligned} \overline{\psi} : \overline{G} &\to Im(\psi) \\ \overline{g} &\mapsto \psi(g). \end{aligned}$$

Note que, a função $\overline{\psi}$ está bem definida uma vez que,

$$\begin{aligned} \overline{g} = \overline{h} \Rightarrow g, h \in N(\psi) &\Rightarrow gh^{-1} \in N(\psi) \Rightarrow \psi(gh^{-1}) = e' \\ &\Rightarrow \psi(g)\psi(h)^{-1}\psi(h) = e'\psi(h) \\ &\Rightarrow \psi(g) = \psi(h). \end{aligned}$$

Temos que, $Im(\overline{\psi}) = Im(\psi)$ por construção e assim $\overline{\psi}$ é sobrejetora.
$\overline{\psi}$ é um homomorfismo, pois, se $\overline{x}, \overline{y} \in \overline{G} = G/N(\psi)$ temos pela Proposição A.4.8,

$$\overline{\psi}(\overline{x}\ \overline{y}) = \overline{\psi}(\overline{xy}) = \psi(xy) = \psi(x)\psi(y) = \overline{\psi}(\overline{x})\overline{\psi}(\overline{y}).$$

Mais ainda, $\overline{\psi}$ é injetiva. De fato,

$$\overline{\psi}(\overline{x}) = e' \Leftrightarrow \psi(x) = e' \Leftrightarrow \overline{x} = \overline{e}$$

Logo, $N(\overline{\psi}) = \{\overline{e}\}$ e pelo item (ii) temos que $\overline{\psi}$ é injetiva. Portanto, $\overline{\psi}$ é um isomorfismo de $\overline{G}$ sobre $Im(\psi)$ e assim $\overline{G} = G/N(\psi) \trianglelefteq Im(\psi)$.

■

A.5 Teorema da Representação de Grupos

Definição A.5.1. Sejam G um grupo e H um subgrupo de G tal que $|G/H| = n$. Dizemos que o índice de H em G é igual a n e indicamos por $[G : H]$.

Teorema A.5.2 (Teorema de Representação)**.** Seja G um grupo e H um subgrupo de G índice n, ou seja, $|G/N| = n$. Então, $\exists\ N \subseteq H$, tal que $N \trianglelefteq G$ e mais G/N é isomorfo a um subgrupo de S_n.

Demonstração. Seja $S = G/H = \{Hx_1, Hx_2, \ldots, Hx_n\}$ e $\mathcal{P}(S)$ o grupo de permutações do conjunto S. Definimos a função ψ como

$$\begin{array}{lll} \psi : G \to \mathcal{P} & \text{, onde} & \omega(g) : S \to S \\ g \mapsto \omega(g) & & Hx_i \mapsto Hx_i g^{-1}. \end{array}$$

A função ψ está bem definida, uma vez que para cada $g \in G$ o elemento g está relacionado a uma única função $\omega(g)$, e mais se $g \in G$, temos $\omega(g)(Hx_i) = \omega(g)(Hxj) \Leftrightarrow Hx_i g^{-1} = Hx_j g^{-1} \Leftrightarrow Hx_i = Hx_j$ então $\omega(g)$ é injetora e $|S| = n$, assim $\omega(g) \in P(S), \forall g \in G$.

Vamos mostrar que ψ é um homomorfismo. De fato, temos que

$$\begin{aligned} \psi(gh)(Hx_i) &= Hx_i(gh)^{-1} \\ &= Hx_i h^{-1} g^{-1} \\ &= \psi(g)(Hx_i h^{-1}) \\ &= \psi(g)(\psi(h)(Hx_i)) \\ &= (\psi(g) \circ \psi(h))(Hx_i) \\ &= \psi(g)\psi(h)(Hx_i), \end{aligned}$$

$\forall g, h \in G$ e $\forall Hx_i \in S$. Assim, como ψ é um homomorfismo então podemos calcular o seu núcleo, dado por

$$N(\psi) = \{g \in G : \omega(g) = I_S\} = \{g \in G : Hx_i g^{-1} = Hx_i, \forall i = \{1, 2, \ldots, n\}\}.$$

Então,

$$\begin{aligned} g \in N(\psi) &\Leftrightarrow Hx_i g^{-1} = hx_i, \forall i = \{1, 2, \ldots, n\} \\ &\Leftrightarrow Hx_i = Hx_i g, \forall i = \{1, 2, \ldots, n\} \\ &\Leftrightarrow H = H(x_i g x_i^{-1}), \forall i = \{1, 2, \ldots, n\} \\ &\Leftrightarrow x_i g x_i^{-1} \in H, \forall i = \{1, 2, \ldots, n\} \\ &\Leftrightarrow g \in x_i^{-1} H x_i = H^{x_i}, \forall i = \{1, 2, \ldots, n\}. \end{aligned}$$

Assim, $g \in N(\psi) \Leftrightarrow g \in H^{x_1}$ e como $G = \{Hx_1 \cup Hx_2 \cup \cdots \cup Hx_n\}$ (união disjunta) e $H^{hx_1} = H^{x_i}, \forall h \in H$ temos que:

$$g \in N(\psi) \Leftrightarrow g \in H, \qquad \forall x \in G \Leftrightarrow \bigcap_{x \in G} g \in H^x.$$

Logo, $N(\psi) = \bigcap_{x \in G} g \in H^x$ e pela Proposição A.4.4 se $N = \bigcap_{x \in G} g \in H^x$ então $N \trianglelefteq G$, pois, $N = N(\psi)$, e ainda $N \subseteq H^e = H$.

Agora, vamos mostrar que N é o maior subgrupo normal de G. De fato, se $L \trianglelefteq G$ e $L \subseteq H$ temos que $L^x = L \subseteq H^x, \forall x \in G$ e portanto $L \subseteq \bigcap_{x \in G} g \in H^x = N$. Então, $N = \bigcap_{x \in G} g \in H^x$ é o maior subgrupo de G contido em H. Por fim, pelo Teorema A.4.9 conhecido como 1º Teorema do homomorfismo temos $G/N \simeq Im(\psi) = \{\omega(g) : g \in G\}$ e como $\mathcal{P} \simeq S_n$ pela Proposição A.4.7 temos que G/N é isomorfo a um subgrupo de S_n. ■

Colorário A.5.3 (Teorema de Cayley)**.** Seja G um grupo de ordem $|G| = n$ então G é isomorfo a um subgrupo do S_n.

Exemplo A.5.4. O grupo $(\mathbb{Z}_9, +)$ é isomorfo ao subgrupo de S_9 (subgrupo das permutações do conjunto $\{1, 2, 3, 4, 5, 6, 7, 8, 9\}$).

Índice