



Universidade do Estado do Rio de Janeiro

Centro de Tecnologia e Ciência

Instituto de Matemática e Estatística

Silvia Fernanda Gomes de Araujo

**Jogos lineares finitos como motivação para o estudo de matrizes e sistemas
lineares**

Rio de Janeiro

2016

Silvia Fernanda Gomes de Araujo

Jogos lineares finitos como motivação para o estudo de matrizes e sistemas lineares



- Dissertação apresentada, como requisito parcial para obtenção do título de Mestre, ao Programa de Pós-graduação de Mestrado Profissional em Matemática em Rede Nacional (PROFMAT), da Universidade do Estado do Rio de Janeiro.

Orientador: Prof. Dr. Roberto Alfonso Olivares Jara

Rio de Janeiro

2016

CATALOGAÇÃO NA FONTE
UERJ / REDE SIRIUS / BIBLIOTECA CTC-A

A663 Araujo, Silvia Fernanda Gomes de.
Jogos lineares finitos como motivação para o estudo de matrizes e sistemas lineares / Silvia Fernanda Gomes de Araujo – 2016.
75f. : il.

Orientador: Roberto Alfonso Olivares Jara.
Dissertação (Mestrado Profissional em Matemática em Rede Nacional - PROFMAT) - Universidade do Estado do Rio de Janeiro, Instituto de Matemática e Estatística.

1. Matemática - Estudo e ensino - Teses. 2. Matemática (Ensino médio) - Teses. 3. Matrizes - Teses. 4. Equações lineares - Teses.. I. Jara, Roberto Alfonso Olivares. II. Universidade do Estado do Rio de Janeiro. Instituto de Matemática e Estatística. III. Título.

CDU 51:37.012

Rosalina Barros *CRB/7 - 4204* - Responsável pela elaboração da ficha catalográfica.

Autorizo para fins acadêmicos e científicos, a reprodução total ou parcial desta dissertação, desde que citada a fonte.

Assinatura

Data

Silvia Fernanda Gomes de Araujo

Jogos lineares finitos como motivação para o estudo de matrizes e sistemas lineares

Dissertação apresentada, como requisito parcial para obtenção do título de Mestre, ao Programa de Pós-graduação de Mestrado Profissional em Matemática em Rede Nacional (PROFMAT), da Universidade do Estado do Rio de Janeiro.

Aprovada em 31 de agosto de 2016.

Banca Examinadora

Prof. Dr. Roberto Alfonso de Olivares Jara (Orientador)
Instituto de Matemática e Estatística - UERJ

Prof.^a Dra. Cláudia Ferreira Reis Concordido
Instituto de Matemática e Estatística - UERJ

Prof. Dr. Albetã Costa Mafra
Universidade Federal do Rio de Janeiro

Rio de Janeiro

2016

DEDICATÓRIA

À minha avó Isabel, minha boa e doce, meu coração...

AGRADECIMENTOS

Agradeço, primeiramente, a Deus, por colocar em meus caminhos todos aqueles que de algum modo puderam ajudar-me a chegar até aqui. Por permitir-me acordar a cada dia e encontrar forças. Por acalmar-me nos momentos de maior aflição, embalando e ninando, como a um bebê.

À minha família, especialmente meu filho Alexandre, pelo apoio incondicional em todas as horas, minha mãe Marilene e tia Marly, exemplos como guerreiras, e meus irmãos, cúmplices em todos os projetos.

Ao meu professor e orientador Roberto Alfonso Olivares Jara, pela dedicação, sabedoria e paciência com que contribuiu para a construção deste trabalho.

A todos os professores do PROFMAT do polo UERJ, pela seriedade profissional com que atuam no curso de mestrado, permitindo o enriquecimento da minha formação.

Aos meus colegas de turma Ricardo José Chamon Alves, Leandro Borges Salgado Teixeira, Darlan de Azevedo Gomes, Everaldo Quinelato e, especialmente, Márcio Pereira Barbosa, por todo o apoio e horas de estudo.

A todos os demais amigos, que aguentaram minhas mudanças de humor e ausências.

À CAPES, pelo apoio financeiro, que ajudou a concluir o curso.

Eu vou para onde quer que você vá
Bem lá em cima ou lá em baixo
Eu vou para onde quer que você vá

Alex Band / Aaron Kamin

RESUMO

ARAÚJO, Silvia Fernanda Gomes de. *Jogos lineares finitos como motivação para o estudo de matrizes e sistemas lineares*. 2016. 75 f. Dissertação (Mestrado Profissional em Matemática em Rede Nacional / PROFMAT) – Instituto de Matemática e Estatística, Universidade do Estado do Rio de Janeiro, Rio de Janeiro, 2016.

Este trabalho de conclusão de curso apresenta uma abordagem para o ensino de Matrizes e Sistemas Lineares no Ensino Médio. Com a intenção de diversificar a forma como esses conteúdos são apresentados, o método utilizado foi o estudo e resolução de Jogos Lineares Finitos. Direcionado a professores e graduandos em Matemática, espera-se que este trabalho forneça mais uma ferramenta útil para atrair a atenção dos alunos, e facilitar a prática docente referente ao tema. Para isto, no desenvolvimento e no final do trabalho, são apresentadas atividades utilizando aritmética modular e a possibilidade do uso de material concreto em sala de aula. Outro cuidado foi com a escolha da linguagem matemática utilizada, a fim de que essa possa ser adaptada sem maiores dificuldades pelos professores, para a apresentação do tema aos alunos.

Palavras-chave: Jogos lineares finitos. Aritmética modular. Matrizes. Sistemas Lineares.

ABSTRACT

ARAÚJO, Silvia Fernanda Gomes de. *Linear finite games as motivation for the study of matrices and systems of linear equations*. 2016. 75f. Dissertação (Mestrado Profissional em Matemática em Rede Nacional – PROFMAT) – Instituto de Matemática e Estatística, Universidade do Estado do Rio de Janeiro, Rio de Janeiro, 2016.

This final paper provides an approach for the teaching of Matrices and Systems of Linear Equations in High School. In order to diversify how the contents are provided, the method used was the study and solving of linear finite games. Constructed to teachers and undergraduate in Mathematics, this study is expected to be an useful tool to attract students and facilitate the practical teaching for the theme. For such, the development and the final part of this study brings activities which deals with modular arithmetic and the possibility of using concret material in class. Another point was the choice of the mathematics language used, so that this can be adapted without difficulty by teachers, for presenting the topic to the students.

Keywords: Linear finite games. Modular arithmetic. Matrices. Systems of linear Equations.

LISTA DE FIGURAS

Figura 1 – Sistema de Lâmpadas.....	37
Figura 2 – Sistema de Lâmpadas com lâmpadas C e E acesas.....	38
Figura 3 – Sistema de Lâmpadas com lâmpadas C e D acesas.....	38
Figura 4 – Sistema de Lâmpadas com lâmpada B acesa.....	39
Figura 5 – Cartas com letras pretas.....	52
Figura 6 – Cartas com letras brancas.....	52
Figura 7 – Cartas com configurações.....	52
Figura 8 – Disposição das cartas após escolha da configuração.....	53
Figura 9 – Sistema de lâmpadas azuis.....	54
Figura 10 – O quebra-cabeça.....	58
Figura 11 – Mudanças de estado para o quebra-cabeças dos nove quadrados.....	59
Figura 12 – O quebra-cabeça dos nove quadrados com três estados.....	68

SUMÁRIO

	INTRODUÇÃO	11
1	PRINCIPAIS ASPECTOS HISTÓRICOS	13
1.1	A Origem dos Sistemas de Equações Lineares	13
1.2	O Surgimento das Matrizes	14
1.3	A Teoria dos Números	15
1.4	A Teoria dos Anéis	16
1.5	Espaços Vetoriais	17
2	ÁLGEBRA LINEAR E ARITMÉTICA MODULAR	18
2.1	Anel e Corpo	18
2.2	Aritmética Modular	20
2.3	Matrizes	23
2.4	Sistemas de Equações Lineares	29
2.5	Espaços Vetoriais	32
2.6	Transformações Lineares	35
3	JOGOS LINEARES FINITOS	37
3.1	Sistema de Lâmpadas	37
3.2	Generalização do Sistema de Lâmpadas	47
4	ATIVIDADES	50
4.1	Atividade 1 – Jogo de Cartas	50
4.2	Atividade 2	53
4.3	Atividade 3	56
4.4	Atividade 4	58
4.5	Atividade 5	67
	CONCLUSÃO	73
	REFERÊNCIAS	75

INTRODUÇÃO

A escolha do tema surgiu da necessidade cada vez maior de, em sala de aula, atrair o interesse dos alunos para o estudo da Matemática. Através da prática docente em escola pública estadual, foi possível observar que os alunos fazem uso frequente de aparelhos tecnológicos, especialmente os celulares. E mais: não escondem sua preferência por aulas com o uso de computadores. Aliado a isto, o uso da tecnologia faz-se extremamente necessário em sala de aula, tanto para dinamizar a apresentação dos conteúdos, quanto para motivar o aluno à aprendizagem. Em contrapartida, o material que as salas de aula dispõem não atendem às necessidades dos professores e alunos, ou pela quantidade insuficiente, ou pelos problemas que apresentam.

A fim de explorar o interesse dos alunos pelos processos computacionais, sem envolver formação específica para tal, e ainda com o desafio do uso do computador não ser imprescindível, a escolha do trabalho voltou-se para a aplicação de conteúdos relativos às Matrizes e Sistemas Lineares. Essa escolha levou aos Jogos Lineares Finitos, conceito introduzido por David Poole (1955-) em seu livro *Linear algebra: a modern introduction*, de 2004, traduzido para o português sob o título *Álgebra Linear*. Segundo Poole (2014, p.104, grifo e negritos do autor),

Há muitas situações nas quais devemos considerar um sistema físico que tem apenas um número finito de *estados*. Às vezes esses estados podem ser alterados por meio da aplicação de certos processos, cada um dos quais produzindo uma quantidade finita de efeitos. Por exemplo, uma lâmpada pode estar acesa ou apagada, e um interruptor pode mudar o estado da lâmpada de acesa para apagada e vice-versa. Sistemas digitais que surgem em ciência da computação muitas vezes são desse tipo.[...] Problemas que envolvem esse tipo de situação são chamados **jogos lineares finitos**.

Assim, este trabalho é dirigido a professores e graduandos em Matemática. O objetivo é propor atividades para auxílio do estudo de Matrizes e Sistemas Lineares, utilizando exemplos de jogos lineares finitos. Embora a abordagem dada ao estudo de alguns desses jogos não necessite de computador, espera-se que sua aplicação em sala de aula seja bem-sucedida.

O primeiro capítulo deste trabalho apresenta uma breve visão do surgimento e evolução dos conteúdos de Álgebra Linear e Aritmética que serviram de base teórica para o desenvolvimento do tema.

O segundo capítulo disserta sobre os principais conhecimentos matemáticos necessários à compreensão dos Jogos Lineares Finitos a serem estudados. Esses conceitos teóricos utilizados abordam a Aritmética Modular e partes importantes da Álgebra Linear. Neste

capítulo, a resolução de Sistemas Lineares é feita com uma abordagem diferente da que se costuma fazer no Ensino Médio.

O terceiro capítulo consiste na descrição e estudo de um jogo linear finito. Nele é verificado o desenvolvimento necessário para a solução do jogo, através de processos matemáticos. É também abordada uma solução geral para o jogo em questão.

O quarto capítulo propõe atividades pedagógicas que possam ser aplicadas em sala de aula. As soluções destas atividades também se encontram neste capítulo.

1 PRINCIPAIS ASPECTOS HISTÓRICOS

1.1 A Origem dos Sistemas de Equações Lineares

Autores como Bertolini (2016), Boyer (1996) e Poole (2014) foram referências bibliográficas para esta seção.

Na matemática ocidental antiga há poucos registros de sistemas de equações lineares. Entretanto, no Oriente, o tema recebeu maior atenção. Datada do início do primeiro século da era cristã, a obra chinesa conhecida como *Nove Capítulos Sobre os Procedimentos Matemáticos* (ou somente *Nove Capítulos*) é considerada como a de maior destaque na história da matemática chinesa. Pela importância da obra na matemática oriental, ela é frequentemente comparada aos *Elementos* de Euclides¹. Com o nome original de *Jiuzhang Suanshu*², a obra é de autoria desconhecida e a hipótese mais aceitável é de que ela foi elaborada por diversos autores, concentrando o conhecimento matemático mais relevante da época.

A obra apresenta 246 problemas de aritmética e geometria, e o capítulo 8, intitulado *Fangsheng*, é destinado à resolução de sistemas lineares. Com o auxílio de pequenas barras de bambu sobre um tabuleiro, os chineses representavam os sistemas lineares por meio de seus coeficientes, utilizando números, inclusive negativos, dispostos em linhas e colunas, algo semelhante às matrizes. Através da manipulação das barras, descobriram o método de resolução de sistemas por eliminação, semelhante ao método da decomposição de Gauss, apresentado somente no século XIX. Porém os chineses só consideravam sistemas lineares com o mesmo número de equações e variáveis. Além disso, não há registro de como o algoritmo chinês funcionava, e qual o motivo desses sistemas levarem a uma única solução.

Em 1809, o alemão Carl Friedrich Gauss (1777-1855), na obra intitulada *Theoria Motus*, apresentou uma técnica de resolução de equações lineares, hoje conhecida como *método de eliminação de Gauss*, ou *eliminação Gaussiana*. Em 1888, o professor de Geodésia alemão Wilhelm Jordan (1842-1899) publicou uma alteração no método de Gauss, que passou a ser conhecido como *método de Gauss-Jordan*, muito utilizado na resolução dos sistemas lineares. Ainda se deve a Gauss a introdução na matemática de um processo iterativo² para resolver

¹Euclides de Alexandria (por volta de 325 a.C. – 265 a.C.) foi um dos mais proeminentes matemáticos da Antiguidade, conhecido pelo seu tratado matemático - Os Elementos.

² Processo que se repete várias vezes para se chegar a um resultado.

sistemas lineares de grande dimensão, que precede o método conhecido como *método de Gauss-Seidel*.

No estudo de sistemas lineares, vale ressaltar a contribuição dada pelos trabalhos de Joseph Louis Lagrange (1736-1813), Pierre Simon Laplace (1749-1827) e Charles Jacobi (1804-1851). Jacobi efetuou vários trabalhos sobre sistemas lineares, baseados nos estudos de Gauss sobre mínimos quadrados. Os trabalhos de Jacobi influenciaram seu aluno Ludwig Seidel (1821-1896). Os dois matemáticos resolveram vários problemas usando métodos iterativos que foram batizados com seus nomes.

1.2 O Surgimento das Matrizes

Para elaborar esta seção, buscou-se suporte teórico em Hefez (2012), Iezzi (2004) e Poole (2004).

O matemático inglês Arthur Cayley (1821-1895) foi um dos primeiros a estudar as matrizes. Em 1855, Cayley publicou uma matéria sobre teoria das transformações lineares. O resultado já aparecera antes, em 1801, na obra de Gauss, intitulada *Disquisitiones Arithmeticae*. Esta obra é um tratado em latim sobre a Teoria dos Números, grande paixão de Gauss.

Inicialmente as matrizes eram utilizadas quase que unicamente na resolução de sistemas lineares e apenas há pouco mais de 150 anos foi reconhecida sua importância.

Em 1790, Lagrange faz o primeiro uso implícito da noção de matrizes. Acredita-se que o primeiro a dar um nome às matrizes foi Augustin-Louis Cauchy (1789-1857), chamando-as de “tabelas”. O nome “matriz” surgiu com James Joseph Sylvester (1814-1897), em 1850, embora ele as visse apenas como mero ingrediente dos determinantes. Somente com Cayley as matrizes começaram a suplantarem os determinantes em importância.

Cayley divulgou o nome “matriz” e passou a demonstrar sua aplicação. Em seu artigo de 1855, Cayley introduziu as matrizes para simplificar a notação de uma transformação linear. Assim, em lugar de

$$\begin{cases} x' = ax + by \\ y' = cx + dy \end{cases} \quad \text{escreveu} \quad (x', y') = \begin{bmatrix} a & b \\ c & d \end{bmatrix} (x, y).$$

A definição do produto de matrizes surgiu-lhe observando o efeito de duas transformações sucessivas. Isto levou à ideia de inversa de uma matriz. Apenas três anos

depois, Cayley introduz o conceito de adição de matrizes e de multiplicação de matrizes por escalar, salientando as propriedades algébricas dessas operações.

As aplicações das matrizes são inúmeras, principalmente no campo computacional. Sua importância é tão grande, que foi a elas que o físico teórico alemão Werner Karl Heisenberg (1901-1976) recorreu quando criou a Mecânica Quântica, trabalho pelo qual recebeu o Prêmio Nobel de Física de 1932.

1.3 A Teoria dos Números

Serviram como referências bibliográficas para a elaboração desta seção os autores Boyer (2016), Coutinho (2009) e Poole (2004).

O interesse pelo estudo dos números inteiros data desde as civilizações mais antigas. Porém é na Grécia que se verifica a teoria dos números tal qual é entendida na atualidade. A teoria dos números é originada da *aritmética* dos gregos, que tratava do estudo das propriedades fundamentais dos inteiros. Domínio de matemáticos e filósofos, os problemas abordados pelos gregos antigos são discutidos em detalhes nos famosos *Elementos*, de Euclides. Entre os treze livros, os que tratavam da teoria dos números eram os de número VII, VIII e IX. Embora a teoria dos números tenha sido estudada por vários matemáticos gregos, seguidos por árabes, indianos e europeus, esta ficou esquecida aproximadamente do século IV ao século XVII.

Entre 1621 e 1636, o francês Pierre de Fermat (1601-1665), matemático amador (magistrado por profissão), adquire o texto original em grego da Aritmética de Diofanto (viveu no século III, sem precisão de seu nascimento e morte). Como não havia revista dedicada à matemática na época, Fermat inicia correspondência através de cartas com outros matemáticos. O mais famoso entre esses foi o frade francês Marin Mersenne (1588-1648). Foi através dessas correspondências que a obra de Fermat chegou aos dias atuais. Depois de sua morte, seu filho coletou e publicou seus resultados. Infelizmente sua obra nesse assunto não chegou a interessar os contemporâneos. Fermat deixou contribuições importantes também em outros ramos da matemática, como ao cálculo diferencial e integral, à geometria e à teoria de probabilidades, por exemplo.

O sucessor de Fermat no estudo da teoria dos números foi o matemático suíço Leonhard Euler (1707-1783), nascido quarenta e dois anos após a morte de Fermat. Somente em 1730 Euler interessa-se pela obra de Fermat. Através de seus estudos, Euler popularizou a teoria dos

números como Fermat não o havia feito. Mas a sistematização da teoria dos números só teve início com as *Disquisitiones arithmeticae* de Gauss, de 1801, obra que é a principal responsável pela notação utilizada na álgebra das congruências. O enfoque atual da teoria dos números teve origem na obra de Gauss. Por sua vasta contribuição à teoria dos números, geometria diferencial, análise e física, Gauss ficou conhecido como o ‘príncipe dos matemáticos’. Assim, a maior parte dos estudos atuais em teoria dos números são originadas ou da Grécia Antiga, ou de um dos matemáticos Fermat, Euler e Gauss.

1.4 A Teoria dos Anéis

Para dissertar sobre a Teoria dos Anéis, buscou-se suporte teórico em Brandemberg (2016), Domingues (2014) e Iezzi (2004).

Em 1872, o matemático alemão Julius Wilhelm Richard Dedekind (1831-1916) publicou a obra *Stetigkeit und Irrationale Zahlen* (Continuidade e Números Irracionais). Maior obra de Dedekind, nela é feita a definição de números irracionais pelos cortes de Dedekind. O estudo dos números algébricos foi iniciado por Dedekind quando este editava obras do matemático Johann Peter Gustav Lejeune Dirichlet. Esse estudo permitiu-lhe adicionar suplementos à sua maior obra, introduzindo a noção de *ideal*. O termo anel foi sugerido posteriormente em 1897, pelo matemático David Hilbert (1862-1943).

A primeira definição axiomática dos anéis foi dada por Adolf Fraenkel (1891-1965), em um ensaio matemático em 1914. Mas as melhores contribuições para o avanço da teoria abstrata da estrutura algébrica de Anel foram feitas pela alemã Amalie Emmy Noether (1882-1935).

Em 1921, Noether criou a primeira fundamentação axiomática da teoria dos anéis comutativos, em seu trabalho *Ideal Theory in Rings*, que se transformou em uma ferramenta poderosa, com aplicações em diversas áreas da matemática. Nele, Noether usou de forma elegante a condição de cadeia ascendente em anéis, mais tarde denominados *Anéis Noetherianos*, em sua homenagem. Este trabalho é considerado a maior contribuição de Noether para a matemática. Em 1927, em seu artigo *Abstract Study of Ideal Theory in Algebraic Number - and Function - fields*, Noether fez uma caracterização para um anel abstrato, generalizando o que Dedekind fizera anteriormente para o anel de números algébricos. Tais anéis são chamados atualmente de *Domínios de Dedekind*.

A influência de Noether foi além de seus próprios estudos. Entre seus alunos mais talentosos, o holandês Bartel Leendert van der Waerden (1903-1996) publica, baseado nas aulas de Noether, o clássico *Álgebra Moderna* (1930). Considerada revolucionária, essa obra difundiu pelo mundo a álgebra moderna ou abstrata, cuja ideia central é a de estrutura algébrica.

1.5 Espaços Vetoriais

Autores como Hefez (2012) e Poole (2004) foram referências bibliográficas para a elaboração desta seção.

A Álgebra Linear é, em resumo, a parte da Matemática que estuda os espaços vetoriais e certas funções entre eles, chamadas de transformações lineares. Embora muitos conteúdos básicos da Álgebra Linear datem da antiguidade, o tema começou a ter sua forma atual em meados do século XIX.

Em 1844, o matemático alemão Hermann Grassmann (1809-1877) introduziu a ideia de espaço vetorial, apesar de não o chamar assim. Seu trabalho era de difícil compreensão e não recebeu a devida atenção.

A primeira definição abstrata para um espaço vetorial foi dada pelo matemático italiano Giuseppe Peano (1858-1932), em seu livro *Calcolo Geometrico*, de 1888. Baseado nos estudos de Grassmann, Peano tornou claro seus conceitos e descreveu os axiomas para um espaço vetorial como hoje é conhecido.

O trabalho de Peano também introduziu conceitos sobre conjuntos. As notações \cup , \cap , \in para “união”, “intersecção” e “é um elemento de”, respectivamente, são as mais usadas, apesar de não terem sido aceitas de imediato pelos matemáticos.

O estudo de Peano sobre os espaços vetoriais também obteve pouca importância por muitos anos. Seu estudo obteve aceitação somente em 1918, quando Hermann Weyl (1885-1955) o repetiu em seu livro *Space, Time, Matter*, uma introdução à teoria da relatividade de Einstein.

Outras aplicações de Álgebra Linear fora da Matemática encontram-se em mecânica quântica, na Física, e na teoria de análise de regressão, na Estatística.

2 ÁLGEBRA LINEAR E ARITMÉTICA MODULAR

O desenvolvimento dos Jogos Lineares Finitos requer conceitos estudados em Álgebra Linear e Aritmética Modular. Para melhor compreensão do tema, a seguir serão apresentados os principais conceitos matemáticos necessários a esse estudo.

2.1 Anel e Corpo

Definição 2.1.1: Um *anel* $(A, +, \cdot)$ é um conjunto A não vazio onde estão definidas duas operações, chamadas de *adição* e *multiplicação* em A , denotadas por $+$ e \cdot

$$\begin{array}{ll} + : A \times A \rightarrow A & \text{e} & \cdot : A \times A \rightarrow A \\ (a, b) \mapsto a + b & & (a, b) \mapsto a \cdot b \end{array}$$

de tal modo que $(A, +, \cdot)$ deve satisfazer as 6 propriedades seguintes para quaisquer que sejam os valores $a, b, c \in A$:

- A1) $a + b = b + a$ (comutatividade da adição)
- A2) $(a + b) + c = a + (b + c)$ (associatividade da adição)
- A3) Existe $0 \in A$ tal que $a + 0 = 0 + a = a$ (existência do elemento neutro para a adição)
- A4) Para todo $x \in A$, existe um único $y \in A$, denotado por $y = -x$, tal que $x + y = y + x = 0$ (existência de inverso aditivo)
- A5) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ (associatividade do produto)
- A6) $a \cdot (b + c) = a \cdot b + a \cdot c$;
 $(a + b) \cdot c = a \cdot c + b \cdot c$ (distributividade à esquerda e à direita)

Definição 2.1.2: Um *anel com identidade 1* é um anel $(A, +, \cdot)$ que satisfaz a propriedade:

- A7) Existe $1 \in A, 0 \neq 1$, tal que $x \cdot 1 = 1 \cdot x = x$, para todo $x \in A$.

Definição 2.1.3: Um *anel comutativo* é um anel $(A, +, \cdot)$ que satisfaz a propriedade:

- A8) Para todo $x, y \in A, x \cdot y = y \cdot x$

Definição 2.1.4: Um *anel comutativo com identidade* é um anel $(A, +, \cdot)$ que satisfaz simultaneamente as propriedades A7 e A8.

Exemplo 2.1.5: São anéis comutativos com identidade os conjuntos \mathbb{Z} , \mathbb{Q} , \mathbb{R} , \mathbb{C} , quando considerados com suas operações de adição e multiplicação usuais.

Definição 2.1.6: Um *anel sem divisores de zero* é um anel $(A, +, \cdot)$ que satisfaz a propriedade: A9) Para todos $x, y \in A$, se $x \cdot y = 0$ então $x = 0$ ou $y = 0$.

Os anéis que não verificam esta propriedade são chamados de anéis com divisores de zero.

Definição 2.1.7: Um *domínio de integridade ou simplesmente domínio* é um anel $(A, +, \cdot)$ comutativo, com identidade e sem divisores de zero. Isto equivale a dizer que um *domínio* é um conjunto A que satisfaz as nove propriedades descritas anteriormente.

Os conjuntos \mathbb{Z} , \mathbb{Q} , \mathbb{R} , \mathbb{C} , quando considerados com suas operações usuais de adição e multiplicação são exemplos de domínios. Nas seções seguintes serão definidas duas famílias de anéis que possuem divisores de zero, e portanto não serão domínios (conjuntos de matrizes quadradas de uma determinada ordem e conjuntos de classes residuais módulo algum número inteiro positivo).

Definição 2.1.8: Um *corpo* é um anel comutativo com identidade $(A, +, \cdot)$ que satisfaz a propriedade:

A10) Para todo $x \in A$, $x \neq 0$, existe $y \in A$ tal que $x \cdot y = y \cdot x = 1$.

O elemento y na propriedade A10 acima é unicamente determinado e chamado o inverso (multiplicativo) de x e é denotado por x^{-1} . Além disso, como os elementos não nulos de um corpo possuem inverso, diz-se que eles são invertíveis.

Proposição 2.1.9: Todo corpo é um domínio de integridade.

Demonstração: De fato, suponha que x e y sejam elementos de um corpo K tais que $x \cdot y = 0$. Então, se $x = 0$, tem-se a afirmação. Se x é diferente de zero, existe x^{-1} em K e, portanto, multiplicando por x^{-1} na igualdade $x \cdot y = 0$ obtém-se:

$$\begin{aligned}x^{-1}(x \cdot y) &= x^{-1} \cdot 0 \\(x^{-1} x) y &= 0 \\1 \cdot y &= 0 \\y &= 0\end{aligned}$$

Logo, K é um domínio.

Por outro lado, a recíproca vale no caso finito, isto é,

Proposição 2.1.10: Todo domínio de integridade finito é um corpo.

Demonstração: Veja Lidl (1994, p.12, Teorema 1.31).

Mas, se o domínio não é finito, não necessariamente será um corpo. Para ilustrar isto, considere o domínio \mathbb{Z} dos números inteiros. Como os únicos invertíveis em \mathbb{Z} são 1 e -1, ele não é um corpo.

Exemplo 2.1.11: São corpos os conjuntos \mathbb{Q} , \mathbb{R} , \mathbb{C} (em relação às suas operações usuais de adição e multiplicação).

2.2 Aritmética Modular

Definição 2.2.1: Dados a , b e m inteiros quaisquer, com $m > 1$, diz-se que a é congruente a b módulo m , e escreve-se

$$a \equiv b \pmod{m}$$

se $a - b$ é múltiplo inteiro de m . Isto equivale a dizer que $m \mid a - b$ (lê-se: m divide a menos b).

Exemplo 2.2.2:

- a) $27 \equiv 5 \pmod{2}$, pois $2 \mid 27 - 5$, isto é, $2 \mid 22$.
- b) $38 \equiv 0 \pmod{19}$, pois $38 - 0 = 38$ é múltiplo de 19.
- c) $17 \equiv -7 \pmod{6}$, pois $17 - (-7) = 24$ é múltiplo de 6.

Proposição 2.2.3: Seja m inteiro positivo. Para todos a, b, c inteiros, tem-se que:

- (i) $a \equiv a \pmod{m}$,
- (ii) se $a \equiv b \pmod{m}$, então $b \equiv a \pmod{m}$,
- (iii) se $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m}$, então $a \equiv c \pmod{m}$.

Estas propriedades decorrem imediatamente da definição de congruência. Como elas correspondem respectivamente às propriedades de reflexão, simetria e transitividade, conclui-se que a congruência é uma *relação de equivalência*.

Definição 2.2.4: Seja dado um inteiro $m > 1$. O conjunto de números inteiros

$$\bar{a} = \{x \in \mathbb{Z}; x \equiv a \pmod{m}\}$$

é chamado de classe residual módulo m do elemento a de \mathbb{Z} .

Como a relação de congruência é uma relação de equivalência, as classes residuais módulo m levam à seguinte partição de \mathbb{Z} :

$$\begin{aligned} \bar{0} &= \{x \in \mathbb{Z}; x \equiv 0 \pmod{m}\} \\ \bar{1} &= \{x \in \mathbb{Z}; x \equiv 1 \pmod{m}\} \\ &\vdots \\ \overline{m-1} &= \{x \in \mathbb{Z}; x \equiv m-1 \pmod{m}\}. \end{aligned}$$

Seguem até $\overline{m-1}$, pois claramente começam a repetir-se. Isto é, $\bar{m} = \bar{0}$, $\overline{m+1} = \bar{1}$, ...

O conjunto de todas as classes residuais módulo m será representado por \mathbb{Z}_m . Portanto,

$$\mathbb{Z}_m = \{\bar{0}, \bar{1}, \dots, \overline{m-1}\}.$$

Exemplo 2.2.5: Se $m = 2$, então $\mathbb{Z}_2 = \{\bar{0}, \bar{1}\}$, onde

$$\bar{0} = \{x \in \mathbb{Z}; x \equiv 0 \pmod{2}\} = \{x \in \mathbb{Z}; x \text{ é par}\} \text{ e}$$

$$\bar{1} = \{x \in \mathbb{Z}; x \equiv 1 \pmod{2}\} = \{x \in \mathbb{Z}; x \text{ é ímpar}\}.$$

Exemplo 2.2.6: Se $m = 3$, então $\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$, onde

$$\bar{0} = \{3t; t \in \mathbb{Z}\}, \bar{1} = \{3t + 1; t \in \mathbb{Z}\} \text{ e } \bar{2} = \{3t + 2; t \in \mathbb{Z}\}.$$

Uma característica importante das classes residuais é que transformam a congruência $a \equiv b \pmod{m}$ na igualdade $\bar{a} = \bar{b}$ em \mathbb{Z}_m .

Outra característica é que em \mathbb{Z}_m pode-se definir as seguintes operações:

Adição: $\bar{a} + \bar{b} = \overline{a + b}$

Multiplicação: $\bar{a} \cdot \bar{b} = \overline{a \cdot b}$

Observação: De agora em diante, e quando não houver confusão, será denotada a classe residual \bar{a} apenas por a , e o conjunto de todas as classes residuais módulo m , apenas por $\mathbb{Z}_m = \{0, 1, 2, \dots, m - 1\}$.

Exemplo 2.2.7: As operações de adição e multiplicação no conjunto $\mathbb{Z}_2 = \{0, 1\}$ são dadas do seguinte modo:

$$\begin{array}{c|cc} + & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 0 \end{array} \qquad \begin{array}{c|cc} \cdot & 0 & 1 \\ \hline 0 & 0 & 0 \\ 1 & 0 & 1 \end{array}$$

Exemplo 2.2.8: As operações de adição e multiplicação no conjunto $\mathbb{Z}_3 = \{0, 1, 2\}$ são dadas do seguinte modo:

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

Teorema 2.2.9: Considere o conjunto $(\mathbb{Z}_m, +, \cdot)$ de todas as classes residuais módulo m , com as operações $+$ e \cdot de adição e multiplicação como definidas acima.

(a) Se m é qualquer inteiro maior do que um e não primo, então $(\mathbb{Z}_m, +, \cdot)$ é um anel comutativo e com divisores de zero.

(b) Se m é um número primo, por exemplo, $m = p$, então $(\mathbb{Z}_m, +, \cdot)$ é um corpo.

Demonstração: Veja Lidl (1994, p.14, Teorema 1.38).

2.3 Matrizes

Definição 2.3.1: Dados m e n inteiros não nulos, e um corpo K , uma *matriz em K de ordem m por n* , ou apenas uma matriz em K , m por n (escreve-se $m \times n$), é toda tabela A (ou $A_{m \times n}$) formada por elementos de K , distribuídos por m linhas e n colunas. Cada elemento de K é chamado de *entrada* da matriz, denotado como a_{ij} e situado no cruzamento da i -ésima linha com a j -ésima coluna. Assim,

$$A = A_{m \times n} = [a_{ij}]_{m \times n} = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}, \text{ com } a_{ij} \in K.$$

Observação: Na maioria das vezes, o corpo K utilizado é o corpo \mathbb{R} dos números reais.

Algumas Matrizes Especiais

Dependendo do valor de m e n , uma matriz $m \times n$ recebe um nome especial:

Definição 2.3.2: *Matriz linha* é toda matriz do tipo $1 \times n$, ou seja, é qualquer matriz que tem uma única linha.

Definição 2.3.3: *Matriz coluna* é toda matriz do tipo $m \times 1$, ou seja, é qualquer matriz que tem uma única coluna.

Definição 2.3.4: *Matriz quadrada de ordem n* é toda matriz do tipo $n \times n$.

Definição 2.3.5: Se $A = [a_{ij}]$ é uma matriz quadrada de ordem n , as entradas a_{ii} , com $1 \leq i \leq n$, formam a *diagonal principal* de A .

Definição 2.3.6: Uma *matriz diagonal de ordem n* é toda matriz quadrada de ordem n em que as entradas que não pertencem à diagonal principal são iguais a zero. Isto é:

$A = [a_{ij}]_{n \times n}$ é matriz diagonal se, e somente se, $a_{ij} = 0$ para cada $1 \leq i, j \leq n$, tais que $i \neq j$:

$$\begin{bmatrix} a_{11} & 0 & \cdots & 0 \\ 0 & a_{22} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a_{nn} \end{bmatrix}$$

Definição 2.3.7: A matriz diagonal de ordem n cujas entradas da diagonal principal são iguais ao número 1, é chamada de *matriz identidade de ordem n* e representa-se usualmente por I_n . Em algumas situações representa-se I_n apenas por I .

$$I_n = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix}_{n \times n}$$

Definição 2.3.8: Uma *matriz triangular superior de ordem n* é uma matriz quadrada de ordem n em que todas as entradas abaixo da diagonal principal são iguais a zero:

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ 0 & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a_{nn} \end{bmatrix}$$

Logo, uma matriz quadrada $A = [a_{ij}]$ de ordem n é triangular superior se $a_{ij} = 0$ sempre que $i > j$.

Definição 2.3.9 Uma *matriz triangular inferior de ordem n* é uma matriz quadrada de ordem n em que todas as entradas acima da diagonal principal são iguais a zero:

$$\begin{bmatrix} a_{11} & 0 & \cdots & 0 \\ a_{21} & a_{22} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix}.$$

Logo, uma matriz quadrada $A = [a_{ij}]$ de ordem n é triangular inferior se $a_{ij} = 0$ sempre que $i < j$.

Definição 2.3.10: *Matriz nula* é qualquer matriz $m \times n$ cujas entradas são todas iguais a zero. Costuma-se denotar por $0_{m \times n}$. Por exemplo,

$$0_{3 \times 2} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

Às vezes é necessário saber quando duas matrizes são iguais.

Definição 2.3.11: Diz-se que *duas matrizes* $A = [a_{ij}]_{m \times n}$ e $B = [b_{ij}]_{p \times q}$ *são iguais*, escrevendo $A = B$, quando $m = p$, e $n = q$, $a_{ij} = b_{ij}$, para todo $1 \leq i \leq m$ e para todo $1 \leq j \leq n$. Isto é, duas matrizes são iguais se, e somente se, tem a mesma ordem e as mesmas entradas nas posições correspondentes.

Operações com Matrizes

A seguir serão apresentadas as operações nas matrizes que serão utilizadas ao longo deste trabalho.

Definição 2.3.12: *Adição*

A *adição* de duas matrizes $A = [a_{ij}]$ e $B = [b_{ij}]$, da mesma ordem $m \times n$, é dada por uma matriz $C = [c_{ij}]$, também de ordem $m \times n$, obtida por

$$c_{ij} = a_{ij} + b_{ij}, \text{ para todo } i \text{ e para todo } j.$$

Definição 2.3.13: *Multiplicação de uma Matriz por um Escalar*

Dada uma matriz $A = [a_{ij}]_{m \times n}$, define-se o *produto de A pelo número real k*, como

$$kA = [ka_{ij}]_{m \times n}$$

Observação: O produto escalar $(-1)A = [-a_{ij}]$ costuma-se escrever simplesmente como $-A$, onde $-A$ é a *matriz oposta de A*. Além disso, o produto escalar permite definir a subtração de matrizes.

$$A - B = A + (-B)$$

Definição 2.3.14: *Multiplicação de matrizes*

Sejam $A = [a_{ik}]_{m \times n}$ e $B = [b_{kj}]_{n \times p}$ duas matrizes. Define-se o *produto de A por B*, denotado por AB , como a matriz $C = [c_{ij}]_{m \times p}$ tal que

$$c_{ij} = a_{i1} \cdot b_{1j} + a_{i2} \cdot b_{2j} + \dots + a_{in} \cdot b_{nj} = \sum_{k=1}^n a_{ik} b_{kj}$$

para todo $1 \leq i \leq m$ e para todo $1 \leq j \leq p$.

Definição 2.3.15: Uma matriz A chama-se *invertível* quando é quadrada e existe uma matriz A^{-1} , chamada a *inversa de A*, tal que $A^{-1} \cdot A = A \cdot A^{-1} = I$.

Considerando as operações de adição e de multiplicação de matrizes anteriores, tem-se o seguinte resultado:

Teorema 2.3.16: Se $M_n(K)$ representa o conjunto de todas as matrizes quadradas de ordem n , com entradas no corpo K , então $(M_n(K), +, \cdot)$ é um anel não comutativo com identidade.

Demonstração: Veja Dummit (2004, p. 235)

Observação: O anel $M_n(K)$ possui divisores de zero, pois, por exemplo, se $n = 2$, $K = \mathbb{R}$ e se A e B são as seguintes matrizes:

$$A = \begin{bmatrix} 1 & 2 \\ 2 & 4 \end{bmatrix} \text{ e } B = \begin{bmatrix} -6 & 2 \\ 3 & -1 \end{bmatrix}, \text{ então } A \neq \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, B \neq \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \text{ e } A \cdot B = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

Forma Escalonada de Uma Matriz

Definição 2.3.17: Uma matriz está na *forma escalonada por linhas* quando satisfaz às seguintes propriedades:

- i) Toda linha nula está abaixo de todas as linhas não nulas;
- ii) O primeiro elemento não nulo, chamado de *líder*, de cada uma de suas linhas não nulas está à esquerda do líder de cada uma das linhas subsequentes.

Para se obter uma *matriz escalonada*, é utilizado o método do *escalamento*, através de operações elementares, descrito a seguir:

Seja A uma matriz $m \times n$. Chama-se de L_i a i -ésima linha de A , para todo $1 \leq i \leq m$. As *operações elementares sobre as linhas da matriz A* definem-se da seguinte forma:

- (i) Permutação das linhas L_i e L_j , indicada por $L_i \leftrightarrow L_j$;
- (ii) Multiplicação de uma linha L_i por um escalar c não nulo, indicada por $L_i \rightarrow cL_i$;
- (iii) Substituição de uma linha L_i pela sua soma com um múltiplo c de L_j , indicada por $L_i \rightarrow L_i + cL_j$.

Para escalonar uma matriz, trabalha-se coluna por coluna, da esquerda para a direita e de cima para baixo. O elemento líder em uma coluna é usado para criar zeros sob ele. O elemento líder nesse processo é chamado de *pivô* e essa parte do processo é chamada de *pivoteamento*.

Definição 2.3.18: Sejam as matrizes A e B de mesma ordem. A matriz A é dita ser *equivalente por linhas* ou *linha-equivalente* à matriz B , se B pode ser obtida de A por um número finito de aplicações sucessivas de operações elementares sobre linhas.

Exemplo 2.3.19:

As matrizes $A = \begin{bmatrix} 3 & 2 \\ -1 & 0 \\ 2 & 1 \end{bmatrix}$ e $B = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{bmatrix}$ são equivalentes por linhas, pois

$$\begin{bmatrix} 3 & 2 \\ -1 & 0 \\ 2 & 1 \end{bmatrix} \xrightarrow{L_1 \leftrightarrow L_2} \underbrace{\begin{bmatrix} -1 & 0 \\ 3 & 2 \\ 2 & 1 \end{bmatrix}}_C \xrightarrow{\substack{L_2 \rightarrow L_2 + 3L_1 \\ L_3 \rightarrow L_3 + 2L_1}} \underbrace{\begin{bmatrix} -1 & 0 \\ 0 & 2 \\ 0 & 1 \end{bmatrix}}_D \xrightarrow{\substack{L_1 \rightarrow -1L_1 \\ L_2 \rightarrow L_2 - 2L_3}} \underbrace{\begin{bmatrix} 1 & 0 \\ 0 & 0 \\ 0 & 1 \end{bmatrix}}_E \xrightarrow{L_2 \leftrightarrow L_3} \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{bmatrix}$$

Observação: Como as operações elementares são todas reversíveis, a relação ser linha equivalentes é uma relação de equivalência. Segue que as matrizes A , B , C , D e E do exemplo acima são todas duas a duas linha equivalentes.

Teorema 2.3.20: Toda matriz de ordem $m \times n$ é linha equivalente a uma matriz na forma escalonada por linhas.

Demonstração: Veja Kolman (2006, p.60, Teorema 1.5)

Da observação acima e do Teorema 2.3.20, vem imediatamente o seguinte resultado:

Corolário 2.3.21: As matrizes A e B são linha equivalentes se, e somente se, puderem ser reduzidas à mesma forma escalonada por linhas.

Definição 2.3.22: Uma matriz $m \times n$ está na *forma escalonada reduzida por linhas* se for nula ou:

- i) está na forma escalonada por linhas e,
- ii) acima e abaixo de cada pivô (que são iguais a 1), todos os elementos são iguais a zero.

Exemplo 2.3.23: A matriz abaixo está na forma escalonada reduzida por linhas:

$$\begin{bmatrix} 1 & 2 & 0 & 0 & -3 & 1 \\ 0 & 0 & 1 & 0 & 4 & -1 \\ 0 & 0 & 0 & 1 & 3 & -2 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Teorema 2.3.24: Toda matriz é linha equivalente a uma única matriz na forma escalonada reduzida por linhas.

Demonstração: Veja Kolman (2006, p.63, Teorema 1.6).

2.4 Sistemas de Equações Lineares

Definição 2.4.1: Um *sistema com m equações lineares e n incógnitas* é um sistema do tipo

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = b_2 \\ \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = b_m \end{cases}$$

onde, para $1 \leq i \leq m$ e $1 \leq j \leq n$, cada x_j é variável e os números a_{ij} (coeficientes) e b_i (termos independentes) são elementos de um corpo K dado. Cada equação do sistema é chamada de *equação linear*.

Um sistema linear tem como *conjunto solução* toda sequência ou n-upla ordenada (c_1, c_2, \dots, c_n) de elementos em K que satisfazem a cada equação do sistema. Isto é,

$$a_{i1}c_1 + a_{i2}c_2 + \cdots + a_{in}c_n = b_i, 1 \leq i \leq m$$

Os *sistemas lineares homogêneos* são aqueles cujos termos independentes são todos nulos. Todo sistema homogêneo admite como uma de suas soluções a sequência nula, isto é, (c_1, c_2, \dots, c_n) , $c_j = 0$, para todo $1 \leq j \leq n$, chamada de *solução trivial*. Se existir outra solução qualquer, é chamada de *solução não trivial do sistema*.

Com relação ao número de soluções, a *classificação de um sistema linear* é dada por uma das seguintes situações:

(i) *Possível*: quando seu conjunto solução é não vazio, isto é, existe pelo menos uma solução.

Dentre os sistemas possíveis, há dois tipos distintos: *determinado*, quando existe apenas uma solução, ou *indeterminado*, quando existe mais de uma solução;

(ii) *Impossível*: quando seu conjunto solução é vazio.

Resolução de Sistemas Lineares

Os sistemas lineares são perfeitamente representados pela equação matricial

$$AX = B$$

de modo que

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}, \quad X = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} \quad \text{e} \quad B = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{bmatrix},$$

onde A é a *matriz dos coeficientes*, X é a *matriz das incógnitas* e B é a *matriz dos termos independentes*.

Assim, o sistema pode ser representado como a *matriz ampliada* (ou matriz completa) do sistema, que consiste da matriz A (matriz incompleta) acrescida da coluna relativa aos termos independentes, denotada por:

$$(A|B) = \left[\begin{array}{cccc|c} a_{11} & a_{12} & \cdots & a_{1n} & b_1 \\ a_{21} & a_{22} & \cdots & a_{2n} & b_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} & b_m \end{array} \right]$$

Definição 2.4.2: Dois sistemas de equações lineares são ditos *sistemas equivalentes* quando suas matrizes ampliadas forem linha equivalentes.

O seguinte resultado é uma consequência direta do corolário 2.3.21;

Proposição 2.4.3: Dois sistemas de equações lineares equivalentes *possuem o mesmo conjunto solução*.

Definição 2.4.4: O *posto* de uma matriz A , denotado por p_A , é o número de linhas não nulas de qualquer uma de suas formas escalonadas por linhas.

Teorema 2.4.5 (Teorema do Posto): Considere um sistema linear com m equações e n incógnitas, representado pela equação matricial $AX = B$. Sejam p_{AB} o posto da matriz ampliada do sistema e p_A o posto da matriz dos coeficientes do sistema. Então:

- (i) o sistema é possível se, e somente se, $p_{AB} = p_A$.
- (ii) o sistema é possível e determinado se $p_{AB} = p_A = n$.
- (iii) o sistema é possível e indeterminado se $p_{AB} = p_A < n$. Neste caso, $n - p_A$ é o número de *variáveis livres* do sistema, isto é, variáveis que podem assumir qualquer valor em K .

Demonstração: Veja Hefez (2012, p.49, Teorema 2.2.6).

Prosseguindo com a resolução do sistema, escalona-se a matriz ampliada $(A|B)$, até obter sua forma escalonada reduzida por linhas, *ignorando todas as linhas nulas*, denotada por $(R|S)$. Pela proposição 2.4.3, como $(A|B)$ é equivalente a $(R|S)$, então o conjunto solução de $(A|B)$ é igual ao conjunto solução de $(R|S)$. A matriz $(R|S)$ está associada a *apenas um* dos três tipos de sistema a seguir, que serão **classificados de acordo com o Teorema do Posto**:

1º tipo: a matriz $(R|S)$ possui um pivô na última coluna. Então $(R|S)$ possui a última linha com a forma $(0|1)$, então $p_{AB} > p_A$, e portanto, o sistema $AX = B$ não tem solução, isto é, o sistema $AX = B$ é chamado *sistema impossível*, ou simplesmente SI.

2º tipo: o número de equações de $(R|S)$ é igual ao número de variáveis. Neste caso tem-se que $p_{AB} = p_A = n$. Logo, o sistema é possível e determinado (SPD). A solução do sistema é obtida partindo da última equação, obtendo x_p , substitui-se este valor na equação anterior, obtendo-se x_{p-1} , e assim sucessivamente.

3º tipo: O número de equações de $(R|S)$ é menor que o número de variáveis. Portanto, $p_{AB} = p_A < n$. Neste caso, $n - p_A$ é o número de variáveis livres do sistema. Apesar de terem quantidade definida, essas variáveis podem ser escolhidas com certa liberdade. Para resolver este sistema, basta transpor as variáveis livres para o segundo membro e a elas arbitrar valores. O novo sistema assim obtido recai em um sistema do 2º tipo e, portanto, *determinado*. Como as variáveis livres podem assumir qualquer valor em K , o sistema linear terá infinitas soluções e por isto é chamado *sistema possível e indeterminado*, ou somente SPI.

Observação: o método descrito para a resolução dos sistemas lineares chama-se método de eliminação de Gauss-Jordan, que se resume a:

1. Escrever a matriz completa do sistema de equações lineares.
2. Usar operações elementares com as linhas para reduzir a matriz completa à forma escalonada reduzida por linhas.
3. Usar substituição de trás para a frente para resolver o sistema equivalente que corresponde à matriz linha-reduzida.

2.5 Espaços Vetoriais

Definição 2.5.1: Um conjunto E , cujos elementos são chamados de *vetores*, é um *espaço vetorial* sobre um corpo K se possui as seguintes operações:

- *Adição:* a todo par de vetores $u, v \in E$, corresponde o vetor $u + v \in E$, chamado a *soma* de u e v ;
- *Multiplicação por escalar:* a cada número $\alpha \in K$, e a cada vetor $v \in E$ corresponde um vetor $\alpha \cdot v \in E$ (ou $\alpha v \in E$), chamado de produto de α por v .

Essas operações devem satisfazer às condições a seguir, chamadas os *Axiomas de Espaço Vetorial*, para todos $\alpha, \beta \in K$ e $u, v, w \in E$:

A1 Comutatividade da adição: $u + v = v + u$;

A2 Associatividade da adição: $(u + v) + w = u + (v + w)$;

A3 Elemento neutro: existe um vetor $0 \in E$, chamado *vetor nulo* ou *vetor zero*, tal que

$$v + 0 = 0 + v = v;$$

A4 Simétrico ou inverso aditivo: para todo $v \in E$ existe um vetor $-v \in E$, tal que

$$-v + v = v + (-v) = 0;$$

M1 Distributividade: $\alpha(u + v) = \alpha u + \alpha v$;

M2 Distributividade: $(\alpha + \beta)v = \alpha v + \beta v$;

M3 Associatividade da multiplicação: $(\alpha\beta)v = \alpha(\beta v)$

M4 Multiplicação por 1: $1 \cdot v = v$.

Exemplos 2.5.2:

a) Dado um corpo K qualquer, e n um inteiro positivo, o espaço K^n é um espaço vetorial sobre K em relação às seguintes operações:

para qualquer $a \in K$ e $x, y \in K^n$ tal que $x = (x_1, x_2, \dots, x_n)$ e $y = (y_1, y_2, \dots, y_n)$:

(i) *Adição de dois vetores:*

$$x + y = (x_1, x_2, \dots, x_n) + (y_1, y_2, \dots, y_n) = (x_1 + y_1, x_2 + y_2, \dots, x_n + y_n);$$

(ii) *Multiplicação do vetor x pelo número real a , chamado de escalar:*

$$a(x_1, x_2, \dots, x_n) = (ax_1, ax_2, \dots, ax_n).$$

Em particular, para $K = \mathbb{Z}_p$, onde p é primo, então \mathbb{Z}_p^n é um espaço vetorial sobre \mathbb{Z}_p .

b) O conjunto $M_{m \times n}(K)$ de todas as matrizes $m \times n$ com elementos em K é um espaço vetorial sobre K com as operações de adição e multiplicação por escalar definidas em 2.3.12 e 2.3.13 respectivamente.

Para as definições a seguir considere F um subconjunto qualquer de um espaço vetorial E e v_1, v_2, \dots, v_r vetores de F .

Definição 2.5.3: Se $v \in F$, v é uma *combinação linear* de $v_1, v_2, \dots, v_r \in F$ se existirem $\alpha_1, \alpha_2, \dots, \alpha_r$ escalares de K tais que

$$v = \alpha_1 v_1 + \alpha_2 v_2 + \dots + \alpha_r v_r$$

Definição 2.5.4: Os vetores v_1, v_2, \dots, v_r são *linearmente independentes* (LI) se a equação

$$\alpha_1 v_1 + \alpha_2 v_2 + \dots + \alpha_r v_r = 0$$

é satisfeita apenas para $\alpha_1 = \alpha_2 = \dots = \alpha_r = 0$. Caso exista algum $\alpha_i \neq 0$, então os vetores v_1, v_2, \dots, v_r são chamados *linearmente dependentes* (LD). O conjunto $\{v_1, v_2, \dots, v_r\}$ é chamado LI ou LD se os vetores v_1, v_2, \dots, v_r forem LI ou LD, respectivamente.

Note que, se um dos vetores v_1, v_2, \dots, v_r for o vetor nulo, então v_1, v_2, \dots, v_r serão LD.

Definição 2.5.5: O conjunto F gera o espaço vetorial E se todo vetor de E for combinação linear de vetores de F . Neste caso, o espaço vetorial E é chamado de um *espaço gerado por F* .

Definição 2.5.6: Uma *base* de um espaço vetorial E é um subconjunto \mathcal{B} de E que é *linearmente independente e gera E* . Isto significa que todo vetor v de E é escrito de modo *único* como combinação linear $v = \alpha_1 v_1 + \alpha_2 v_2 + \dots + \alpha_n v_n$ de vetores v_1, v_2, \dots, v_n da base \mathcal{B} .

Exemplo 2.5.7: Os vetores $e_1 = (1, 0, 0, \dots, 0)$, $e_2 = (0, 1, 0, \dots, 0)$, ..., $e_n = (0, 0, 0, \dots, 1)$ formam uma base $\{e_1, e_2, \dots, e_n\}$ de \mathbb{R}^n , chamada de *base canônica*.

Teorema 2.5.8: Se um espaço vetorial E admite uma base com n elementos, então todas as bases de E têm o mesmo número n de elementos, que é chamado de *dimensão de E* , ou simplesmente *dim E* .

Demonstração: Veja Lima (2001, p.28).

Definição 2.5.9: O espaço vetorial E tem *dimensão finita* quando admite uma base $\mathcal{B} = \{v_1, v_2, \dots, v_n\}$ com um número finito n de elementos. Um espaço vetorial E tem *dimensão infinita* quando ele não tem dimensão finita, isto é, quando nenhum subconjunto finito de E é uma base.

Exemplo 2.5.10:

- a) O espaço vetorial $M_{m \times n}(K)$ das matrizes $m \times n$ tem dimensão finita, igual a $m.n$. Uma base para $M_{m \times n}(K)$ é formada pelas matrizes e_{ij} , cuja ij -ésima entrada (entrada da linha i e coluna j) é igual a 1 e as demais entradas são iguais a zero.
- b) O espaço vetorial \mathbb{Z}_p^n sobre \mathbb{Z}_p , p primo, tem dimensão finita igual a n . Uma base para \mathbb{Z}_p^n é o conjunto formado pelos vetores

$$v_1 = \begin{bmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \quad v_2 = \begin{bmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \quad \dots, \quad v_n = \begin{bmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 1 \end{bmatrix}$$

Teorema 2.5.11: Se a dimensão de E é n , um conjunto com n vetores gera E se, e somente se, é LI.

Demonstração: Veja Lima (2001, p.30).

2.6 Transformações Lineares

Definição 2.6.1: Considere E, F espaços vetoriais. Uma *transformação linear* $T: E \rightarrow F$ é uma correspondência que associa a cada vetor $v \in E$ um único vetor $T(v) = T.v = Tv \in F$ de modo que se verifiquem, para todos $u, v \in E$ e $k \in K$, as relações:

- (i) $T(u + v) = T(u) + T(v)$
- (ii) $T(kv) = kT(v)$.

O vetor $T.v$ chama-se a *imagem* (ou o *transformado*) de v pela transformação T .

Definição 2.6.2 : Uma transformação linear $T: E \rightarrow F$ é um *isomorfismo* quando é bijetora, e neste caso os espaços vetoriais E e F são ditos *isomorfos*.

É fácil ver que um isomorfismo leva base em base e portanto, no caso de E e F serem espaços vetoriais de dimensão finita, um isomorfismo entre eles somente é possível quando ambos tiverem a mesma dimensão. Por outro lado, se E e F forem espaços vetoriais da mesma dimensão, um isomorfismo entre eles é fácil de ser construído. Para isso basta estender linearmente qualquer correspondência biunívoca entre uma base qualquer de E e uma base qualquer de F . Disto, segue o importante resultado:

Teorema 2.6.3: Sejam E e F dois espaços vetoriais de dimensão finita. Então, E e F são isomorfos se, e somente se, $\dim E = \dim F$.

3 JOGOS LINEARES FINITOS

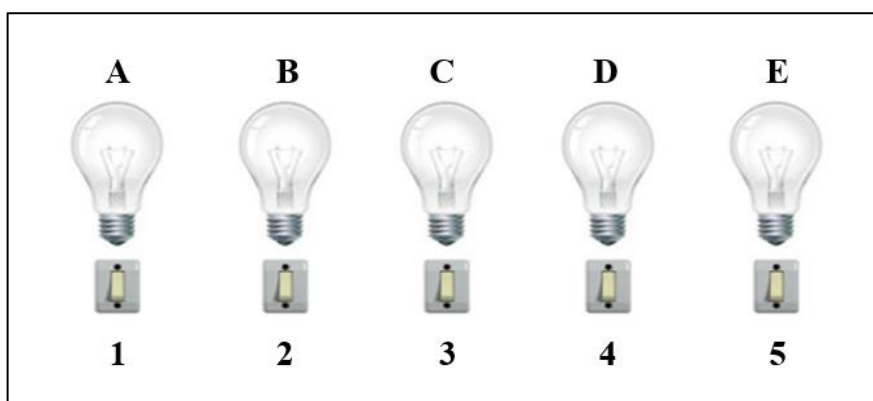
Conforme mencionado anteriormente, jogos lineares finitos são situações que possam ser representadas por um sistema físico com um número finito de estados, que possam ser alterados através de certos processos, cada um dos quais produzindo uma quantidade de resultados também finita.

O Sistema de Lâmpadas abaixo é um claro exemplo de jogo linear finito e o motivo do estudo a seguir.

3.1 Sistema de Lâmpadas

O sistema é formado por uma fileira horizontal de cinco lâmpadas, identificadas pelas letras **A**, **B**, **C**, **D**, **E**. Essas lâmpadas são controladas por cinco interruptores, identificados pelos números **1**, **2**, **3**, **4** e **5**, posicionados abaixo delas, como mostra a Figura 1. Cada interruptor muda o estado (ligada ou desligada) da lâmpada posicionada diretamente sobre ele e os estados das lâmpadas imediatamente adjacentes à esquerda e à direita.

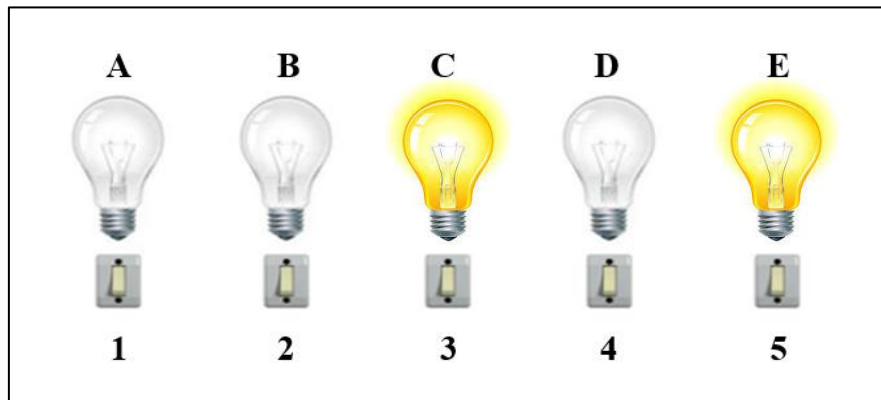
Figura 1 – Sistema de Lâmpadas



Fonte: Modificado de Poole, 2004.

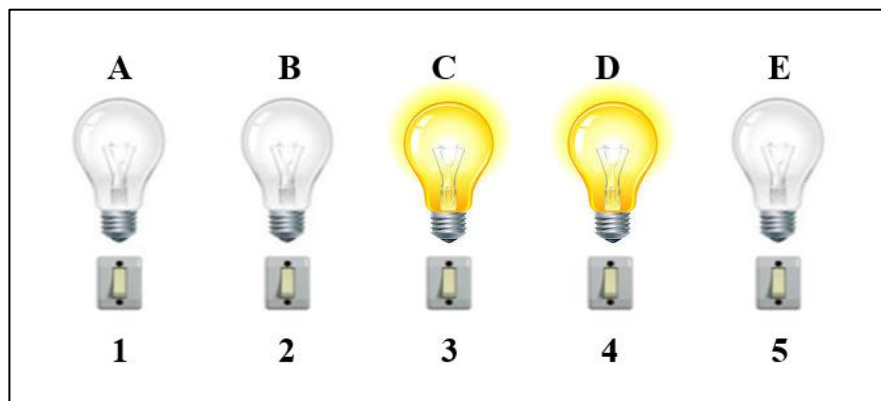
Por exemplo, se apenas as lâmpadas **C** e **E** estiverem acesas, como na Figura 2, ao pressionar-se o interruptor **5**, a lâmpada **D** acende e a lâmpada **E** apaga-se, mostrado na Figura 3. Se depois o interruptor **3** for pressionado, a lâmpada **B** acende e as lâmpadas **C** e **D** apagam-se, conforme a Figura 4.

Figura 2 – Sistema de Lâmpadas com lâmpadas **C** e **E** acesas.



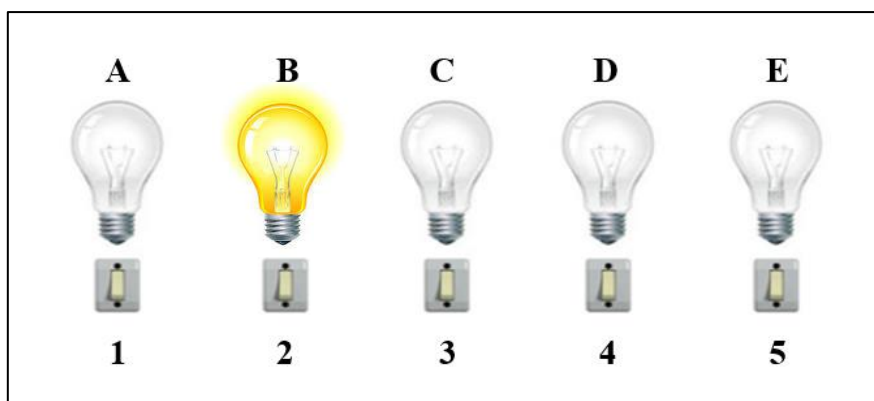
Fonte: Modificado de Poole, 2004.

Figura 3 – Sistema de Lâmpadas com lâmpadas **C** e **D** acesas.



Fonte: Modificado de Poole, 2004.

Figura 4 – Sistema de Lâmpadas com lâmpada **B** acesa



Fonte: Modificado de Poole, 2004.

A fim de explorar o Sistema de Lâmpadas à luz da Álgebra Linear, e considerando-se inicialmente que todas as lâmpadas estejam *apagadas*, propõe-se duas questões:

- (a) pode-se pressionar os interruptores em alguma ordem de modo que apenas as lâmpadas **A**, **C** e **E** fiquem acesas?
- (b) pode-se pressionar os interruptores em alguma ordem de modo que apenas a lâmpada **A** fique acesa?

Solução:

(a) Como cada lâmpada apresenta apenas dois estados, ligada ou desligada, pode-se usar a notação binária, trabalhando em \mathbb{Z}_2 . Assim, considerando um vetor \mathbf{v} que represente o estado das cinco lâmpadas, $\mathbf{v} \in \mathbb{Z}_2^5$, tal que

$$\mathbf{v} = (v_A, v_B, v_C, v_D, v_E)$$

onde v_A = estado da lâmpada **A**, v_B = estado da lâmpada **B**, e assim sucessivamente.

Como vetores são n-uplas ordenadas e possuem as regras de adição e multiplicação por escalar semelhantes às de matrizes, para efeito de facilitar os cálculos, os vetores pertencentes a \mathbb{Z}_2^n serão representados como *matrizes coluna* de ordem $n \times 1$. Dessa forma, \mathbf{v} poderá ser representado como

$$\mathbf{v} = \begin{bmatrix} v_A \\ v_B \\ v_C \\ v_D \\ v_E \end{bmatrix}$$

Cada um desses estados será representado por 0 para desligado, e 1 para ligado. Por exemplo, o vetor que representa apenas as lâmpadas **C** e **E** acesas, é escrito como:

$$\begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 1 \end{bmatrix}$$

A ação de cada interruptor também pode ser representada por vetores em \mathbb{Z}_2^5 . Então, se um interruptor muda o estado de uma lâmpada, a componente correspondente será igual a 1. Senão, a componente será igual a zero.

Desse modo, fazendo:

a = ação do interruptor **1** sobre as lâmpadas,

b = ação do interruptor **2** sobre as lâmpadas,

e assim sucessivamente, tem-se:

$$\mathbf{a} = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \quad \mathbf{b} = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 0 \end{bmatrix}, \quad \mathbf{c} = \begin{bmatrix} 0 \\ 1 \\ 1 \\ 1 \\ 0 \end{bmatrix}, \quad \mathbf{d} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 1 \end{bmatrix}, \quad \mathbf{e} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{bmatrix}.$$

Por exemplo, considerando o estado inicial das lâmpadas como o vetor

$$\begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 0 \end{bmatrix}$$

isto é, apenas as lâmpadas **B** e **D** acesas, ao apertar-se o interruptor **2**, tem-se:

$$\begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 0 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

Ou seja, ao final da operação, tem-se agora acesas as lâmpadas **A**, **C** e **D**.

Observe que se quer partir de uma determinada configuração e obter uma outra. Mas, pelo exemplo 2.5.10 item b, do capítulo 2,

“Se p é primo, o conjunto \mathbb{Z}_p^n (com as operações usuais de adição e multiplicação por escalar), é um espaço vetorial sobre \mathbb{Z}_p , para todo inteiro n positivo”.

Como 2 é primo, então \mathbb{Z}_2^5 é um espaço vetorial sobre \mathbb{Z}_2 . Isto garante a comutatividade da adição, ou seja, pressionar os interruptores **1** e depois **2**, é o mesmo que pressionar os interruptores **2**, e depois **1**. Fato, pois, em \mathbb{Z}_2^5 ,

$$\mathbf{a} + \mathbf{b} = \mathbf{b} + \mathbf{a}$$

Mas ainda resta uma pergunta: “quantas vezes pode-se acionar cada interruptor?”. Observe: ao pressionar os interruptores **1, 3, 2, 1, 3, 3**, nesta ordem, a ação por eles provocada é o resultado da soma vetorial

$$\mathbf{a} + \mathbf{c} + \mathbf{b} + \mathbf{a} + \mathbf{c} + \mathbf{c}$$

Como vale a propriedade comutativa, tem-se, então

$$2\mathbf{a} + \mathbf{b} + 3\mathbf{c}$$

Mas $2\mathbf{a}$ é o mesmo que pressionar duas vezes o mesmo interruptor. Ao pressionar-se a segunda vez, desfaz-se a ação da primeira vez. É fácil, pois como

$2 \in \mathbb{Z}_2$, e $2 \equiv 0 \pmod{2}$, tem-se que 2 corresponde a 0 em \mathbb{Z}_2 . Então $2\mathbf{a} = 0\mathbf{a} = 0$.

Isto vale para qualquer um dos interruptores. Logo, *pressionar um número par de vezes qualquer interruptor equivale a não apertá-lo.*

E o que dizer de $3\mathbf{c}$? Este pode ser escrito como

$$3\mathbf{c} = 1\mathbf{c} + \overset{0}{\widehat{2\mathbf{c}}} = 1\mathbf{c} .$$

Além disso,

$$5\mathbf{c} = 1\mathbf{c} + 2.2\mathbf{c} = 1\mathbf{c} + 2.0 = 1\mathbf{c}$$

$$7\mathbf{c} = 1\mathbf{c} + 3.2\mathbf{c} = 1\mathbf{c} + 3.0 = 1\mathbf{c}$$

⋮

Ou seja, como isto vale para qualquer interruptor, então *pressionar um número ímpar de vezes qualquer interruptor equivale a pressioná-lo uma única vez.*

Daí, conclui-se que, qualquer um dos interruptores, se pressionado, será uma única vez.

Chamando de \mathbf{x} o vetor solução do problema, onde $\mathbf{x} = (x_1, x_2, \dots, x_5)$, $x_i \in \mathbb{Z}_2$, x_i é o número de vezes que cada interruptor i será acionado ($i = 1, 2, 3, 4, 5$). Partindo da configuração \mathbf{s} , uma configuração inicial qualquer das lâmpadas, e sendo \mathbf{t} a configuração final desejada, tem-se:

$$\mathbf{s} + x_1 \cdot \mathbf{a} + x_2 \cdot \mathbf{b} + x_3 \cdot \mathbf{c} + x_4 \cdot \mathbf{d} + x_5 \cdot \mathbf{e} = \mathbf{t} ,$$

ou ainda,

$$x_1 \cdot \mathbf{a} + x_2 \cdot \mathbf{b} + x_3 \cdot \mathbf{c} + x_4 \cdot \mathbf{d} + x_5 \cdot \mathbf{e} = \mathbf{t} - \mathbf{s} ,$$

Cada uma das componentes de \mathbf{s} pertencem a \mathbb{Z}_2 . Como $-0 = 0$ e $-1 \equiv 1 \pmod{2}$, então

$$\mathbf{t} - \mathbf{s} = \mathbf{t} + (-1) \cdot \mathbf{s} = \mathbf{t} + 1 \cdot \mathbf{s} = \mathbf{t} + \mathbf{s} .$$

Logo,

$$x_1 \cdot \mathbf{a} + x_2 \cdot \mathbf{b} + x_3 \cdot \mathbf{c} + x_4 \cdot \mathbf{d} + x_5 \cdot \mathbf{e} = \mathbf{t} + \mathbf{s} . \quad (1)$$

Assim, o problema com as configurações \mathbf{s} (inicial) e \mathbf{t} (final) terá solução se, e somente se, o sistema de equações lineares (1) for um Sistema Possível (SP). Equivalentemente se, e somente se, o vetor $\mathbf{t} + \mathbf{s}$ for uma combinação linear dos vetores $\mathbf{a}, \mathbf{b}, \mathbf{c}, \mathbf{d}, \mathbf{e}$.

É fácil ver que o conjunto $\{\mathbf{a}, \mathbf{b}, \mathbf{c}, \mathbf{d}, \mathbf{e}\}$ não é uma base de \mathbb{Z}_2^5 e portanto nem sempre o sistema será possível.

No caso em questão:

$$\mathbf{s} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} \quad \mathbf{t}_1 = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 1 \end{bmatrix}$$

e substituindo na equação (1) anterior, vem:

$$x_1 \cdot \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} + x_2 \cdot \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 0 \end{bmatrix} + x_3 \cdot \begin{bmatrix} 0 \\ 1 \\ 1 \\ 1 \\ 0 \end{bmatrix} + x_4 \cdot \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 1 \end{bmatrix} + x_5 \cdot \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 1 \end{bmatrix}$$

Ou equivalentemente:

$$\begin{cases} x_1 + x_2 & = 1 \\ x_1 + x_2 + x_3 & = 0 \\ x_2 + x_3 + x_4 & = 1 \\ x_3 + x_4 + x_5 & = 0 \\ x_4 + x_5 & = 1 \end{cases}$$

Este sistema pode ser representado pela equação matricial

$$M \cdot \mathbf{x} = \mathbf{t},$$

onde $M_{5 \times 5}$ é a matriz incompleta do sistema, ou matriz dos coeficientes, sendo suas colunas os vetores **a**, **b**, **c**, **d**, **e**. Ou seja:

$$M = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix}.$$

Os valores \mathbf{x} e \mathbf{t} , onde $\mathbf{t} = \mathbf{s} + \mathbf{t}_1$ são respectivamente:

$$\mathbf{x} = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{bmatrix} ; \quad \mathbf{t} = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 1 \end{bmatrix}$$

A dimensão do espaço \mathbb{Z}_2^5 é igual a 5 (conforme exemplo 2.5.10, item b e Teorema 2.5.8) e o conjunto $\{\mathbf{a}, \mathbf{b}, \mathbf{c}, \mathbf{d}, \mathbf{e}\}$ tem a mesma quantidade de elementos que uma base para esse espaço vetorial. Se os vetores $\mathbf{a}, \mathbf{b}, \mathbf{c}, \mathbf{d}, \mathbf{e}$ forem L.I., pelo Teorema 2.5.11, esses vetores geram \mathbb{Z}_2^5 . Logo, todo vetor de \mathbb{Z}_2^5 será escrito de forma *única* como combinação linear de $\{\mathbf{a}, \mathbf{b}, \mathbf{c}, \mathbf{d}, \mathbf{e}\}$. Dessa forma, o sistema será SPD (sistema possível e determinado).

No item (b), o processo para obter apenas a lâmpada \mathbf{A} acesa, considerando inicialmente todas as lâmpadas apagadas, é análogo a este processo descrito. O que difere é somente o resultado desejado, representado pelo vetor \mathbf{t}_2 , onde

$$\mathbf{t}_2 = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

Substituindo na equação (1), tem-se:

$$x_1 \cdot \mathbf{a} + x_2 \cdot \mathbf{b} + x_3 \cdot \mathbf{c} + x_4 \cdot \mathbf{d} + x_5 \cdot \mathbf{e} = \mathbf{t}_2 + \mathbf{s} = \mathbf{t}' \quad (2)$$

Os sistemas em (a) e (b) possuem a mesma matriz M incompleta. Então suas respectivas matrizes completas $(M|\mathbf{t})$ e $(M|\mathbf{t}')$ podem ser resolvidas simultaneamente considerando de uma vez o sistema $(M|\mathbf{t}|\mathbf{t}')$:

$$\begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix} \xrightarrow{L_2 \rightarrow L_2 + L_1} \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix} \xrightarrow{\begin{matrix} L_1 \rightarrow L_1 + L_3 \\ L_2 \leftrightarrow L_3 \end{matrix}}$$

$$\begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix} \xrightarrow{\begin{matrix} L_1 \rightarrow L_1 + L_4 \\ L_2 \rightarrow L_2 + L_4 \end{matrix}} \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix} \xrightarrow{L_4 \rightarrow L_4 + L_3}$$

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix} \xrightarrow{L_5 \rightarrow L_5 + L_4} \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Voltando à solução do item (a):

A última linha da matriz reduzida acima é nula. Chamando de p_M o posto da matriz escalonada reduzida de M e de p_{Mt} o posto da matriz escalonada reduzida da matriz ampliada $(M|\mathbf{t})$, pelo Teorema do Posto, $p_{Mt} = p_M = 4 < 5$. Logo, o sistema é SPI, e, portanto, o conjunto $\{\mathbf{a}, \mathbf{b}, \mathbf{c}, \mathbf{d}, \mathbf{e}\}$ não é uma base para \mathbb{Z}_2^5 , e existe $5 - 4 = 1$ variável livre.

Como x_5 é a única variável livre, o sistema terá exatamente duas soluções, pois $x_5 \in \mathbb{Z}_2$. Logo, $x_5 = 0$ ou $x_5 = 1$.

Resolvendo o sistema da matriz escalonada reduzida de $(M|\mathbf{t})$, vem:

$$x_1 + x_5 = 0$$

$$x_2 + x_5 = 1$$

$$x_3 = 1$$

$$x_4 + x_5 = 1$$

Logo,

$$x_1 = x_5$$

$$x_2 = 1 + x_5$$

$$x_3 = 1$$

$$x_4 = 1 + x_5$$

1ª solução: para $x_5 = 0$,

$$x_1 = 0$$

$$x_2 = 1$$

$$x_3 = 1$$

$$x_4 = 1$$

Ou seja, o vetor solução $\mathbf{x} = (0, 1, 1, 1, 0)$ indica que basta pressionar uma única vez os interruptores **2, 3 e 4**.

2ª solução: para $x_5 = 1$,

$$x_1 = 1$$

$$x_2 = 0$$

$$x_3 = 1$$

$$x_4 = 0$$

Ou seja, o vetor solução $\mathbf{x} = (1, 0, 1, 0, 1)$ indica que basta pressionar uma única vez os interruptores **1, 3 e 5**.

(b) Para obter apenas a lâmpada **A** acesa, considerando inicialmente todas as lâmpadas apagadas, foi usado raciocínio análogo, chegando à matriz escalonada reduzida de $(M|\mathbf{t}')$:

$$\left[\begin{array}{ccccc|c} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{array} \right]$$

Observando a última linha dessa matriz, vê-se que $p_{Mt'} > p_M$, logo, pelo Teorema do posto, o sistema é impossível (SI). Isto é óbvio, pois $0 = 1$ é ABSURDO!

Logo, não é possível obter apenas a primeira lâmpada acesa, iniciando o processo com todas as lâmpadas apagadas.

3.2 Generalização do Sistema de Lâmpadas

Na seção anterior foram vistos dois casos do sistema de lâmpadas com resultados distintos. O primeiro, possível e indeterminado, e o segundo, impossível. A fim de identificar quando o sistema de lâmpadas encontra solução, o presente estudo será generalizado. Para isto, a configuração inicial \mathbf{s} e a configuração desejada \mathbf{t} são dadas como:

$$\mathbf{s} = \begin{bmatrix} s_1 \\ s_2 \\ s_3 \\ s_4 \\ s_5 \end{bmatrix} \qquad \mathbf{t} = \begin{bmatrix} t_1 \\ t_2 \\ t_3 \\ t_4 \\ t_5 \end{bmatrix}$$

O raciocínio é análogo ao descrito na resolução da questão (a). Então, sabe-se pela equação (1) que:

$$x_1 \cdot \mathbf{a} + x_2 \cdot \mathbf{b} + x_3 \cdot \mathbf{c} + x_4 \cdot \mathbf{d} + x_5 \cdot \mathbf{e} = \mathbf{t} + \mathbf{s}$$

Resolvendo essa equação, o desenvolvimento do primeiro membro levou à matriz escalonada reduzida de M . Então basta escalonar o segundo membro da equação, representado pela matriz coluna $\mathbf{t} + \mathbf{s}$, usando as mesmas operações elementares que foram aplicadas à matriz M . Assim, escalonando $(\mathbf{t} + \mathbf{s})$:

$$\begin{bmatrix} t_1 + s_1 \\ t_2 + s_2 \\ t_3 + s_3 \\ t_4 + s_4 \\ t_5 + s_5 \end{bmatrix} \xrightarrow{L_2 \rightarrow L_2 + L_1} \begin{bmatrix} t_1 + s_1 \\ (t_1 + t_2) + (s_1 + s_2) \\ t_3 + s_3 \\ t_4 + s_4 \\ t_5 + s_5 \end{bmatrix} \xrightarrow{\begin{matrix} L_1 \rightarrow L_1 + L_3 \\ L_2 \leftrightarrow L_3 \end{matrix}}$$

$$\begin{bmatrix} (t_1 + t_3) + (s_1 + s_3) \\ t_3 + s_3 \\ (t_1 + t_2) + (s_1 + s_2) \\ t_4 + s_4 \\ t_5 + s_5 \end{bmatrix} \xrightarrow{\begin{matrix} L_1 \rightarrow L_1 + L_4 \\ L_2 \rightarrow L_2 + L_4 \end{matrix}} \begin{bmatrix} (t_1 + t_3 + t_4) + (s_1 + s_3 + s_4) \\ (t_3 + t_4) + (s_3 + s_4) \\ (t_1 + t_2) + (s_1 + s_2) \\ t_4 + s_4 \\ t_5 + s_5 \end{bmatrix} \xrightarrow{L_4 \rightarrow L_4 + L_3}$$

$$\begin{bmatrix} (t_1 + t_3 + t_4) + (s_1 + s_3 + s_4) \\ (t_3 + t_4) + (s_3 + s_4) \\ (t_1 + t_2) + (s_1 + s_2) \\ (t_1 + t_2 + t_4) + (s_1 + s_2 + s_4) \\ t_5 + s_5 \end{bmatrix} \xrightarrow{L_5 \rightarrow L_5 + L_4} \begin{bmatrix} (t_1 + t_3 + t_4) + (s_1 + s_3 + s_4) \\ (t_3 + t_4) + (s_3 + s_4) \\ (t_1 + t_2) + (s_1 + s_2) \\ (t_1 + t_2 + t_4) + (s_1 + s_2 + s_4) \\ (t_1 + t_2 + t_4 + t_5) + (s_1 + s_2 + s_4 + s_5) \end{bmatrix}$$

Logo, a matriz escalonada reduzida de $(M|\mathbf{t} + \mathbf{s})$ é:

$$\left[\begin{array}{ccccc|c} 1 & 0 & 0 & 0 & 1 & (t_1 + t_3 + t_4) + (s_1 + s_3 + s_4) \\ 0 & 1 & 0 & 0 & 1 & (t_3 + t_4) + (s_3 + s_4) \\ 0 & 0 & 1 & 0 & 0 & (t_1 + t_2) + (s_1 + s_2) \\ 0 & 0 & 0 & 1 & 1 & (t_1 + t_2 + t_4) + (s_1 + s_2 + s_4) \\ 0 & 0 & 0 & 0 & 0 & (t_1 + t_2 + t_4 + t_5) + (s_1 + s_2 + s_4 + s_5) \end{array} \right]$$

Chamando de p_M o posto da matriz escalonada reduzida de M e p_{Mts} o posto da matriz escalonada reduzida de $(M|\mathbf{t} + \mathbf{s})$, conclui-se que $p_M = 4 < 5$ (número de variáveis do sistema acima). Logo, o sistema **não** será SPD. Para que haja solução, isto é, para que o sistema seja SPI, é necessário que $p_{Mts} = p_M$. Portanto:

$$(t_1 + t_2 + t_4 + t_5) + (s_1 + s_2 + s_4 + s_5) = 0$$

Concluindo: o sistema de lâmpadas proposto, independentemente das configurações inicial e final, não terá solução única. Para que existam soluções, a condição acima deverá ser satisfeita. Como as variáveis são elementos do corpo finito \mathbb{Z}_2 , as soluções, quando houver, serão também finitas: exatamente duas.

4 ATIVIDADES

As atividades propostas neste capítulo constituem uma sugestão de trabalho para as turmas de segundo ano do ensino médio.

Devido ao alto custo da construção de material concreto para o Sistema de Lâmpadas, este foi adaptado pela autora do trabalho como um jogo de cartas, conforme descrito na Atividade 1. Caso possível, esta atividade pode ser proposta antes do estudo teórico de Matrizes e Sistemas Lineares, como estratégia para despertar a curiosidade do aluno.

As demais atividades encontram-se no livro *Álgebra Linear*, de Poole, 2004, p.112.

4.1 Atividade 1 – Jogo de Cartas

O jogo é formado por um baralho com 37 cartas. Entre elas, 5 cartas possuem *duas* faces, com apenas uma das letras **A, B, C, D, E**. Uma das faces tem a letra preta, conforme figura 5, e a outra face tem a mesma letra, vazada, que será chamada de *branca*, conforme figura 6. As demais 32 cartas possuem apenas uma face, com as letras **A, B, C, D, E** listadas em coluna. Cada letra é preta ou branca, tornando as 32 cartas diferentes entre si. Estas cartas, chamadas de *configurações*, são as possíveis maneiras de organizar as 5 cartas de duas faces. Veja algumas delas na figura 7. O conjunto das cartas de duas faces precisa ser reproduzido em quantidade suficiente para que cada grupo possa utilizar um deles.

A proposta é que o professor faça um jogo com a turma, dividindo-a em pequenos grupos, como, por exemplo, 2 ou 3 alunos. Depois, siga as etapas descritas:

- 1) Cada grupo recebe um conjunto de 5 cartas de duas faces;
- 2) O professor escolhe, entre o baralho das 32 cartas, duas delas. Uma será a *configuração inicial* e a outra, a *configuração final*;
- 3) Os alunos são orientados a arrumar as 5 cartas do conjunto que receberam, de acordo com a configuração inicial;
- 4) Com o objetivo de alcançar a configuração final, cada grupo, independente dos demais, **escolhe uma letra, anotando qual foi**. Cada escolha permite virar *apenas* as letras relativas a ela, conforme informado abaixo;

5) A escolha prossegue, até o grupo obter a configuração final, quando informa ao professor que conseguiu;

6) O professor confere se a sequência informada pelo grupo leva ao resultado desejado.

Fica a critério do professor quantas vezes cada grupo poderá chamá-lo para a conferência.

Escolha de uma letra: vire esta letra e as imediatamente acima e abaixo. Assim:

Escolha da letra **A**: vire as letras **A** e **B**;

Escolha da letra **B**: vire as letras **A B** e **C**;

Escolha da letra **C**: vire as letras **B, C** e **D**;

Escolha da letra **D**: vire as letras **C, D** e **E**;

Escolha da letra **E**: vire as letras **D** e **E**.

A ideia é reproduzir o resultado semelhante ao do Sistema de Lâmpadas. Para isto, é interessante que a configuração final da primeira rodada seja possível de ser alcançada. E em uma próxima rodada, não. Além disso, espera-se que os alunos percebam que:

- Para mudar a cor de alguma carta, é necessário que ela seja virada um número *ímpar* de vezes;
- Existem partidas onde a configuração final *não* é alcançada;
- Para cada configuração, o número máximo de escolhas de cartas que cada grupo *precisa* fazer, é cinco: cada uma das cartas **A, B, C, D** ou **E**. A partir disso, começariam a *desfazer* alguma jogada;
- Existem configurações finais onde a solução não é única.

Figura 5 – Cartas com letras pretas.



Fonte: O Autor, 2016.

Figura 6 – Cartas com letras brancas.



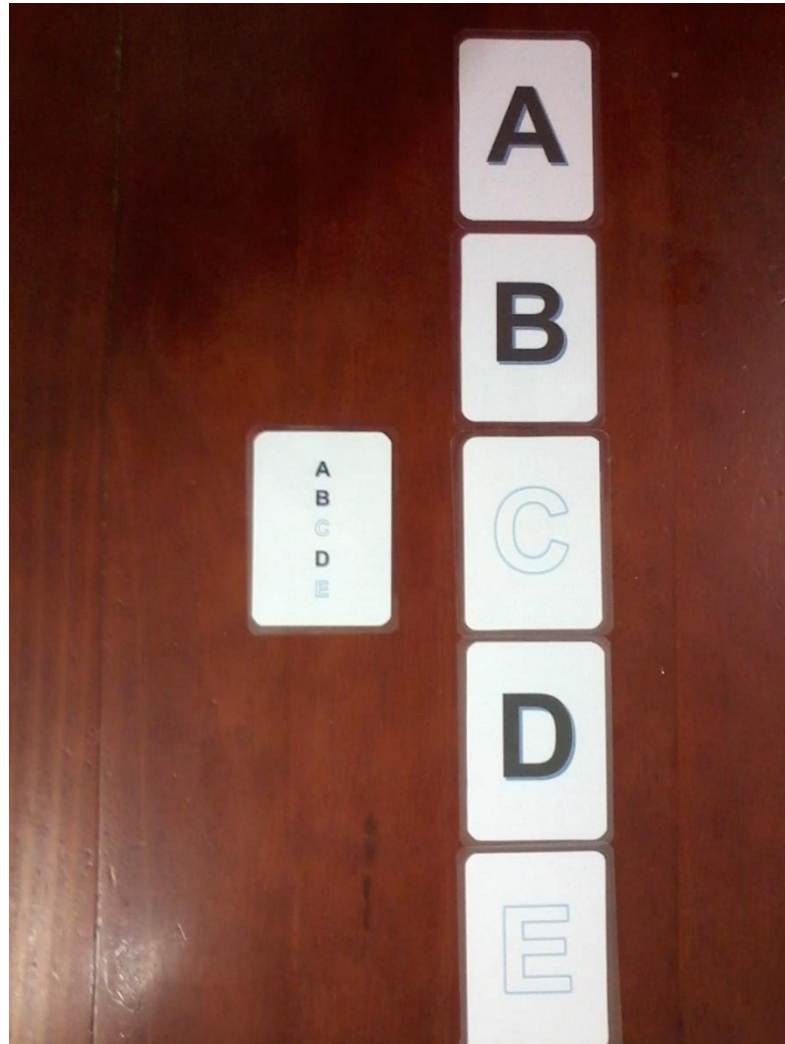
Fonte: O Autor, 2016

Figura 7 - Cartas com configurações.



Fonte: O Autor, 2016.

Figura 8 - Disposição das cartas após a escolha da configuração

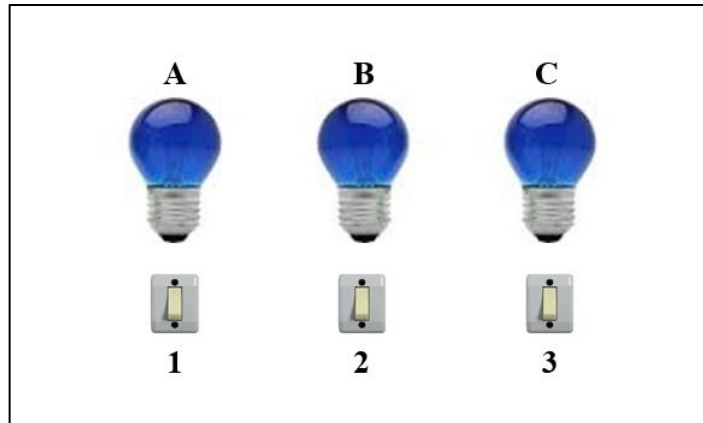


Fonte: O Autor, 2016.

4.2 Atividade 2

Considere uma fileira com apenas três lâmpadas, conforme figura 9, que podem estar apagadas, acesas com luz azul-clara ou azul-escura. Sob as lâmpadas estão três interruptores, **1**, **2** e **3**, cada um deles muda o estado das lâmpadas, para o próximo estado, segundo o ciclo desligada → azul-clara → azul-escura → desligada. O interruptor **1** muda o estado das duas primeiras lâmpadas, o interruptor **2** muda todas as três lâmpadas e o interruptor **3** muda as últimas duas. Se todas as três lâmpadas estiverem inicialmente desligadas, é possível pressionar os interruptores de um modo que as lâmpadas fiquem nesta ordem: desligada, azul-clara e azul-escura?

Figura 9 – Sistema de lâmpadas azuis.



Fonte: Modificado de Poole, 2004.

Solução:

Nesta atividade é necessário utilizar \mathbb{Z}_3 e a solução desejada é um vetor de \mathbb{Z}_3^3 . Como 3 é primo, então \mathbb{Z}_3^3 é um espaço vetorial sobre \mathbb{Z}_3 , com as operações usuais de adição e multiplicação. Novamente a mudança de estado de uma lâmpada é representada por 1, caso contrário, zero. *Atenção: agora pressionar duas vezes o mesmo interruptor não é o mesmo que não apertá-lo!* Basta verificar as operações de adição e multiplicação definidas anteriormente.

Fazendo:

a = ação do interruptor **1** sobre as lâmpadas;

b = ação do interruptor **2** sobre as lâmpadas e

c = ação do interruptor **3** sobre as lâmpadas,

então **a**, **b**, **c** são vetores em \mathbb{Z}_3^3 , tais que:

$$\mathbf{a} = \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}, \quad \mathbf{b} = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}, \quad \mathbf{c} = \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}$$

Os estados das lâmpadas serão representados por 0 para desligada, 1 para azul-clara e 2 para azul-escura. Assim, deseja-se encontrar o número de vezes que cada interruptor é pressionado, representado pelos escalares x_1, x_2, x_3 , em \mathbb{Z}_3 , onde:

$$x_1 \mathbf{a} + x_2 \mathbf{b} + x_3 \mathbf{c} = \mathbf{t}$$

sendo \mathbf{t} a configuração final desejada, isto é $\mathbf{t} = \begin{bmatrix} 0 \\ 1 \\ 2 \end{bmatrix}$. Substituindo os valores na equação acima,

a matriz completa do sistema é $[\mathbf{a} \ \mathbf{b} \ \mathbf{c} | \mathbf{t}]$, cuja redução por linhas segue abaixo:

$$\begin{bmatrix} 1 & 1 & 0 & | & 0 \\ 1 & 1 & 1 & | & 1 \\ 0 & 1 & 1 & | & 2 \end{bmatrix} \xrightarrow{L_2 \rightarrow L_2 + 2L_1} \begin{bmatrix} 1 & 1 & 0 & | & 0 \\ 0 & 0 & 1 & | & 1 \\ 0 & 1 & 1 & | & 2 \end{bmatrix} \xrightarrow{L_2 \leftrightarrow L_3} \begin{bmatrix} 1 & 1 & 0 & | & 0 \\ 0 & 1 & 1 & | & 2 \\ 0 & 0 & 1 & | & 1 \end{bmatrix} \xrightarrow{L_1 \rightarrow L_1 + 2L_2}$$

$$\begin{bmatrix} 1 & 0 & 2 & | & 1 \\ 0 & 1 & 1 & | & 2 \\ 0 & 0 & 1 & | & 1 \end{bmatrix} \xrightarrow{\begin{matrix} L_1 \rightarrow L_1 + L_3 \\ L_2 \rightarrow L_2 + 2L_3 \end{matrix}} \begin{bmatrix} 1 & 0 & 0 & | & 2 \\ 0 & 1 & 0 & | & 1 \\ 0 & 0 & 1 & | & 1 \end{bmatrix}$$

Os vetores coluna da matriz incompleta reduzida são uma base para \mathbb{Z}_3^3 . Logo, qualquer vetor pode ser escrito de **forma única** como combinação linear dos vetores \mathbf{a} , \mathbf{b} , \mathbf{c} , inclusive o vetor \mathbf{t} . Então o sistema é SPD e a solução é:

$$x_1 = 2$$

$$x_2 = 1$$

$$x_3 = 1$$

ou seja, o interruptor **1** deve ser pressionado duas vezes e os outros interruptores uma única vez.

Observe que a ação dos interruptores **1**, **2** e **3** sobre as lâmpadas, é de tal forma que os vetores \mathbf{a} , \mathbf{b} e \mathbf{c} que os representam formam uma base para \mathbb{Z}_3^3 . Daí, qualquer que sejam as configurações inicial e final desta atividade, o problema será sempre possível e determinado (com solução única).

De modo mais geral, supondo que \mathbf{s} e \mathbf{t} sejam as configurações inicial e final, respectivamente, propõe-se aqui que o leitor interessado em aplicar essa atividade em sala de aula acrescente mais duas variantes a ela. Escolha a ação dos interruptores de tal forma que forneçam um conjunto $\{\mathbf{a}, \mathbf{b}, \mathbf{c}\}$ de vetores linearmente dependentes em \mathbb{Z}_3^3 . Em seguida:

a) escolha vetores \mathbf{s} e \mathbf{t} de tal forma que $\mathbf{t} - \mathbf{s}$ seja uma combinação linear do conjunto

$\{\mathbf{a}, \mathbf{b}, \mathbf{c}\}$, obtendo assim um problema possível indeterminado (com mais de uma solução);

b) escolha vetores \mathbf{s} e \mathbf{t} tais que $\mathbf{t} - \mathbf{s}$ não seja uma combinação linear de $\{\mathbf{a}, \mathbf{b}, \mathbf{c}\}$ obtendo assim um problema impossível (que não admite qualquer solução).

4.3 Atividade 3

Supondo que as lâmpadas do sistema desenvolvido no capítulo 3 possam estar desligadas, azul-claras ou azul-escuras, e que os interruptores funcionem como na atividade anterior. Isto é, cada interruptor controla a lâmpada diretamente sobre ele e as lâmpadas imediatamente adjacentes à esquerda e à direita, mas pelo ciclo desligada \rightarrow azul-clara \rightarrow azul-escura \rightarrow desligada. Mostre que é possível começar com todas as lâmpadas apagadas e pressionar os interruptores em alguma ordem de modo que as lâmpadas fiquem nesta ordem: azul-escura, azul-clara, azul-escura, azul-clara, azul-escura.

Solução:

Esta atividade exige que se trabalhe em \mathbb{Z}_3 . Os estados das lâmpadas serão representados por 0 para desligada, 1 para azul-clara e 2 para azul-escura. Então a solução procurada é o vetor

$$\mathbf{t} = \begin{bmatrix} 2 \\ 1 \\ 2 \\ 1 \\ 2 \end{bmatrix}$$

Deve-se observar que *pressionar duas vezes o mesmo interruptor não é o mesmo que não apertá-lo!* Como no capítulo 3, os vetores \mathbf{a} , \mathbf{b} , \mathbf{c} , \mathbf{d} , \mathbf{e} são a ação dos interruptores sobre as lâmpadas e cada x_i ($i = 1, \dots, 5$) representa o número de vezes que cada interruptor i deverá ser pressionado. Como as lâmpadas iniciam-se apagadas, substituindo os valores na equação (1), pág. 42, tem-se:

$$x_1 \cdot \mathbf{a} + x_2 \cdot \mathbf{b} + x_3 \cdot \mathbf{c} + x_4 \cdot \mathbf{d} + x_5 \cdot \mathbf{e} = \mathbf{t}$$

Substituindo os valores, a matriz completa do sistema é $[\mathbf{a} \ \mathbf{b} \ \mathbf{c} \ \mathbf{d} \ \mathbf{e} | \mathbf{t}] = [M | \mathbf{t}]$ cuja redução por linhas segue abaixo:

$$\left[\begin{array}{ccccc|c} 1 & 1 & 0 & 0 & 0 & 2 \\ 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 2 \\ 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 2 \end{array} \right] \xrightarrow{L_2 \rightarrow L_2 + 2L_1} \left[\begin{array}{ccccc|c} 1 & 1 & 0 & 0 & 0 & 2 \\ 0 & 0 & 1 & 0 & 0 & 2 \\ 0 & 1 & 1 & 1 & 0 & 2 \\ 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 2 \end{array} \right] \xrightarrow{\begin{array}{l} L_1 \rightarrow L_1 + 2L_3 \\ L_2 \leftrightarrow L_3 \end{array}}$$

$$\left[\begin{array}{ccccc|c} 1 & 0 & 2 & 2 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 2 \\ 0 & 0 & 1 & 0 & 0 & 2 \\ 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 2 \end{array} \right] \xrightarrow{\begin{array}{l} L_1 \rightarrow L_1 + L_3 \\ L_2 \rightarrow L_2 + 2L_3 \\ L_4 \rightarrow L_4 + 2L_3 \end{array}} \left[\begin{array}{ccccc|c} 1 & 0 & 0 & 2 & 0 & 2 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 2 \\ 0 & 0 & 0 & 1 & 1 & 2 \\ 0 & 0 & 0 & 1 & 1 & 2 \end{array} \right] \xrightarrow{\begin{array}{l} L_1 \rightarrow L_1 + L_4 \\ L_2 \rightarrow L_2 + 2L_4 \\ L_5 \rightarrow L_5 + 2L_4 \end{array}}$$

$$\left[\begin{array}{ccccc|c} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 2 & 1 \\ 0 & 0 & 1 & 0 & 0 & 2 \\ 0 & 0 & 0 & 1 & 1 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array} \right]$$

O posto da matriz ampliada reduzida é igual ao posto da matriz M reduzida, que é 4, porém menor que o número de variáveis. Logo, o sistema é SPI, com uma única variável livre. Resolvendo, vem:

$$x_1 + x_5 = 1$$

$$x_2 + 2x_5 = 1$$

$$x_3 = 2$$

$$x_4 + x_5 = 2$$

A variável livre é $x_5 \in \mathbb{Z}_3$. Logo, $x_5 = 0$ ou $x_5 = 1$ ou $x_5 = 2$. Então:

para $x_5 = 0$: o vetor solução é $(1, 1, 2, 2, 0)$, isto é, basta apertar uma vez os interruptores **1** e **2** e apertar duas vezes os interruptores **3** e **4**, em qualquer ordem;

para $x_5 = 1$: o vetor solução é $(0, 2, 2, 1, 1)$, isto é, basta apertar duas vezes os interruptores **2** e **3** e apertar uma vez os interruptores **4** e **5**, em qualquer ordem;

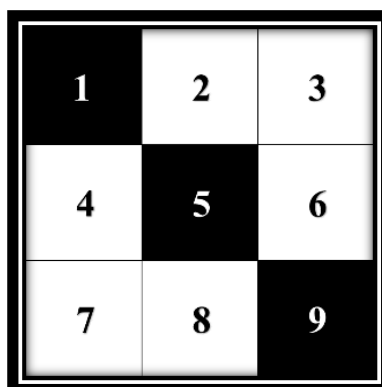
para $x_5 = 2$: o vetor solução é $(2, 0, 2, 0, 2)$, isto é, basta apertar duas vezes os interruptores **1**, **3** e **5**, em qualquer ordem.

Observe que nesta atividade 3, os interruptores forneceram o conjunto de vetores $B = \{\mathbf{a}, \mathbf{b}, \mathbf{c}, \mathbf{d}, \mathbf{e}\}$ que é linearmente dependente no espaço vetorial \mathbb{Z}_3^5 . Além disso, como o vetor $\mathbf{t} - \mathbf{s} = \mathbf{t} - \mathbf{0} = \mathbf{t}$ é uma combinação linear do conjunto B , o sistema é possível e indeterminado, e portanto possui mais de uma solução, que no caso foram exatamente três soluções.

4.4 Atividade 4

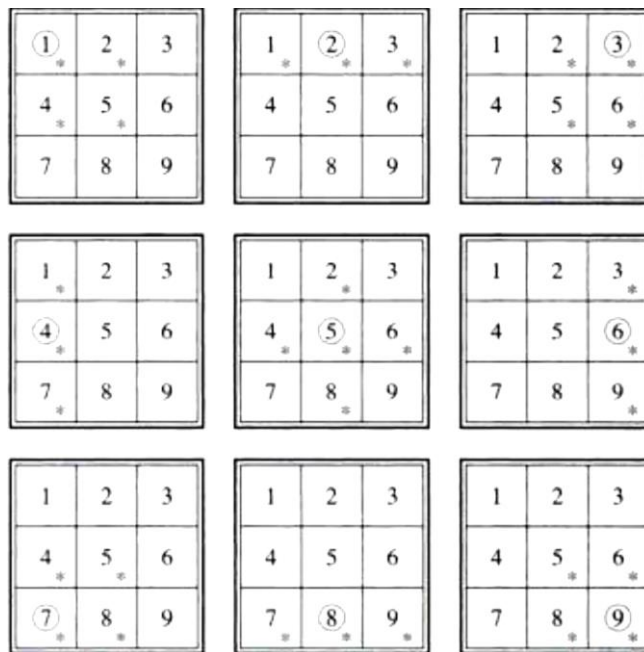
Nove quadrados, enumerados de 1 até 9, cada um deles branco ou preto, estão organizados em uma grade 3 x 3. A Figura 10 mostra uma configuração possível. Quando tocado, cada quadrado muda a sua própria cor e a cor de alguns vizinhos (preto \rightarrow branco; branco \rightarrow preto), conforme mostra a Figura 11. (Ao se tocar nos quadrados cujo número está circulado, mudam as cores dos quadrados marcados com *.) O objetivo do jogo é fazer todos os nove quadrados ficarem pretos. Este exercício foi adaptado do quebra-cabeças que pode ser encontrado no CD-ROM de jogos interativos *The seventh guest* (Trilobyte Software/Virgin Games, 1992).

Figura 10 - O quebra-cabeça.



Fonte: Poole, 2004.

Figura 11 - Mudanças de estados para o quebra-cabeças dos nove quadrados.



Fonte: Poole, 2004.

- (a) Se a configuração inicial é a mostrada na figura 10, mostre que o jogo pode ser ganho e descreva uma sequência de movimentos vencedora.
- (b) Prove que o jogo pode ser ganho, independentemente das configurações inicial e final.

Solução:

Este problema pode ser considerado dentro do espaço vetorial $V = M_{3 \times 3}(\mathbb{Z}_2)$ das matrizes de ordem 3×3 , com entradas em \mathbb{Z}_2 , sobre o corpo \mathbb{Z}_2 . Ou ainda, como V possui dimensão 9, pode-se considerar, via o seguinte isomorfismo T , no espaço vetorial \mathbb{Z}_2^9 :

$$T: V \rightarrow \mathbb{Z}_2^9 \text{ tal que } T \left(\begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix} \right) = (a_{11}, a_{12}, a_{13}, a_{21}, a_{22}, a_{23}, a_{31}, a_{32}, a_{33}).$$

Será utilizado \mathbb{Z}_2^9 .

- a) Cada um dos nove quadrados pode ficar apenas nas cores preta ou branca. Novamente a notação binária será útil, e deve-se trabalhar em \mathbb{Z}_2 . Assim, considere um vetor w que represente o estado dos nove quadrados, $w \in \mathbb{Z}_2^9$, tal que

$w = (w_1, w_2, \dots, w_9)$, onde $w_1 = \text{cor do quadrado n}^\circ 1$; $w_2 = \text{cor do quadrado n}^\circ 2$; ... ; $w_9 = \text{cor do quadrado n}^\circ 9$.

Para efeito de facilitação dos cálculos, às vezes serão representados os vetores como uma matriz coluna de ordem 9×1 . Por exemplo, o vetor w acima poderá ser escrito como segue:

$$w = \begin{bmatrix} w_1 \\ w_2 \\ w_3 \\ w_4 \\ w_5 \\ w_6 \\ w_7 \\ w_8 \\ w_9 \end{bmatrix}$$

A cor branca em cada quadrado será representada pelo 0, assim como a cor preta será representada pelo 1.

O toque em cada um dos quadrados será representado por vetores em \mathbb{Z}_2^9 . Então, a mudança de cor provocada pelo toque em algum quadrado será representada pela componente 1. Senão, a componente será igual a zero.

Desse modo, fazendo:

a = ação do toque do quadrado **1** sobre todos os quadrados;

b = ação do toque do quadrado **2** sobre todos os quadrados;

c = ação do toque do quadrado **3** sobre todos os quadrados;

⋮

i = ação do toque do quadrado **9** sobre todos os quadrados,

tem-se:

$$\mathbf{a} = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \mathbf{b} = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \mathbf{c} = \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \mathbf{d} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \mathbf{e} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}, \mathbf{f} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}, \mathbf{g} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \end{bmatrix}, \mathbf{h} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}, \mathbf{i} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 1 \end{bmatrix}.$$

Como 2 é primo, então \mathbb{Z}_2^9 é um espaço vetorial sobre \mathbb{Z}_2 . Novamente a comutatividade da adição é garantida, ou seja, tocar os quadrados 3 depois 5, por exemplo, é o mesmo que pressionar os quadrados 5 e depois 3. Fato, pois, em \mathbb{Z}_2^9 ,

$$\mathbf{a} + \mathbf{b} = \mathbf{b} + \mathbf{a}.$$

Raciocínio semelhante faz-se quanto ao número de vezes que um quadrado precisa ser tocado: *pressionar um número par de vezes qualquer quadrado equivale a não pressioná-lo; pressionar um número ímpar de vezes qualquer quadrado equivale a pressioná-lo uma única vez*. Logo, qualquer um dos quadrados, se tocado, será uma única vez.

Primeiramente resolve-se o problema usando apenas os conhecimentos sobre sistemas lineares.

Chamando de \mathbf{x} o vetor solução do problema, onde $\mathbf{x} = (x_1, x_2, \dots, x_9)$, $x_i \in \mathbb{Z}_2$, x_i é o número de vezes que cada interruptor i será acionado ($i = 1, 2, 3, \dots, 9$). Partindo da configuração \mathbf{s} , uma configuração inicial qualquer da cor dos quadrados, e sendo \mathbf{t} a configuração final desejada, tem-se:

$$\begin{aligned} \mathbf{s} + x_1 \cdot \mathbf{a} + x_2 \cdot \mathbf{b} + x_3 \cdot \mathbf{c} + x_4 \cdot \mathbf{d} + x_5 \cdot \mathbf{e} + x_6 \cdot \mathbf{f} + x_7 \cdot \mathbf{g} + x_8 \cdot \mathbf{h} + x_9 \cdot \mathbf{i} &= \mathbf{t} \Leftrightarrow \\ x_1 \cdot \mathbf{a} + x_2 \cdot \mathbf{b} + x_3 \cdot \mathbf{c} + x_4 \cdot \mathbf{d} + x_5 \cdot \mathbf{e} + x_6 \cdot \mathbf{f} + x_7 \cdot \mathbf{g} + x_8 \cdot \mathbf{h} + x_9 \cdot \mathbf{i} &= \mathbf{t} - \mathbf{s} \Leftrightarrow \\ x_1 \cdot \mathbf{a} + x_2 \cdot \mathbf{b} + x_3 \cdot \mathbf{c} + x_4 \cdot \mathbf{d} + x_5 \cdot \mathbf{e} + x_6 \cdot \mathbf{f} + x_7 \cdot \mathbf{g} + x_8 \cdot \mathbf{h} + x_9 \cdot \mathbf{i} &= \mathbf{t} + \mathbf{s} \end{aligned} \quad (2)$$

O problema tem solução se, e somente se, o sistema representado pela equação (2) for um Sistema Possível (SP). Isto é equivalente a dizer que o vetor $\mathbf{t} + \mathbf{s}$ é uma combinação linear do conjunto de vetores $B = \{\mathbf{a}, \mathbf{b}, \mathbf{c}, \mathbf{d}, \mathbf{e}, \mathbf{f}, \mathbf{g}, \mathbf{h}, \mathbf{i}\}$.

No caso em questão:

$$\mathbf{s} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} \quad \mathbf{t} = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}$$

e substituindo na equação (2), vem:

$$x_1 \cdot \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} + x_2 \cdot \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} + x_3 \cdot \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} + x_4 \cdot \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} + x_5 \cdot \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} + x_6 \cdot \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} + x_7 \cdot \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \end{bmatrix} + x_8 \cdot \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} + x_9 \cdot \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 1 \end{bmatrix} =$$

$$= \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 0 \end{bmatrix} .$$

Isso equivale a:

$$\begin{aligned}
 x_1 + x_2 + \quad x_4 &= 0 \\
 x_1 + x_2 + x_3 + \quad x_5 &= 1 \\
 \quad x_2 + x_3 + \quad \quad x_6 &= 1 \\
 x_1 + \quad \quad x_4 + x_5 + \quad x_7 &= 1 \\
 x_1 + \quad x_3 + \quad x_5 + \quad x_7 + \quad x_9 &= 0 \\
 \quad \quad x_3 + \quad x_5 + x_6 + \quad \quad x_9 &= 1 \\
 \quad \quad \quad x_4 + \quad \quad \quad x_7 + x_8 &= 1 \\
 \quad \quad \quad \quad x_5 + \quad x_7 + x_8 + x_9 &= 1 \\
 \quad \quad \quad \quad \quad x_6 + \quad x_8 + x_9 &= 0
 \end{aligned}$$

Este sistema pode ser representado pela equação matricial

$$M \cdot \mathbf{x} = \mathbf{t}_1 ,$$

onde $M_{9 \times 9}$ é a matriz incompleta do sistema, ou matriz dos coeficientes, sendo suas colunas os vetores $\mathbf{a}, \mathbf{b}, \mathbf{c}, \dots, \mathbf{i}$. Ou seja:

$$\mathbf{M} = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} .$$

Os valores \mathbf{x} e \mathbf{t}_1 , onde $\mathbf{t}_1 = \mathbf{s} + \mathbf{t}$, são, respectivamente:

$$\mathbf{x} = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \\ x_8 \\ x_9 \end{bmatrix} ; \quad \mathbf{t}_1 = \begin{bmatrix} 0 \\ 1 \\ 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

Observe que como $\dim(\mathbb{Z}_2^9)$ é 9 e B possui exatamente 9 vetores, se B for L.I. então B será uma base para \mathbb{Z}_2^9 e, portanto, o jogo sempre poderá ser ganho e existirá apenas uma única sequência vencedora. Deve-se verificar se este é o caso.

Escalonando a matriz completa $[M|\mathbf{t}_1]$ por linhas, tem-se:

$$\begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & | & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & | & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & | & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & | & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & | & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & | & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & | & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & | & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & | & 0 \end{bmatrix} \xrightarrow{\begin{matrix} L_2 \rightarrow L_2 + L_1 \\ L_4 \rightarrow L_4 + L_1 \\ L_5 \rightarrow L_5 + L_1 \end{matrix}} \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & | & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & | & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & | & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & | & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & | & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & | & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & | & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & | & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & | & 0 \end{bmatrix} \xrightarrow{L_2 \leftrightarrow L_3}$$

$$\begin{array}{c}
 \left[\begin{array}{cccccccc|c}
 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\
 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\
 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\
 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 \\
 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\
 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\
 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\
 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0
 \end{array} \right]
 \xrightarrow{\begin{array}{l} L_4 \rightarrow L_4 + L_2 \\ L_5 \rightarrow L_5 + L_2 \end{array}}
 \left[\begin{array}{cccccccc|c}
 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\
 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\
 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\
 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 \\
 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\
 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\
 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\
 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0
 \end{array} \right]
 \xrightarrow{\begin{array}{l} L_4 \rightarrow L_4 + L_3 \\ L_6 \rightarrow L_6 + L_3 \end{array}}
 \end{array}$$

$$\begin{array}{c}
 \left[\begin{array}{cccccccc|c}
 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\
 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\
 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\
 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 \\
 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\
 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\
 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\
 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0
 \end{array} \right]
 \xrightarrow{\begin{array}{l} L_5 \rightarrow L_5 + L_4 \\ L_6 \rightarrow L_6 + L_4 \\ L_7 \rightarrow L_7 + L_4 \end{array}}
 \left[\begin{array}{cccccccc|c}
 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\
 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\
 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\
 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\
 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\
 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\
 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\
 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0
 \end{array} \right]
 \xrightarrow{\begin{array}{l} L_6 \leftrightarrow L_7 \\ L_8 \rightarrow L_8 + L_5 \end{array}}
 \end{array}$$

$$\begin{array}{c}
 \left[\begin{array}{cccccccc|c}
 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\
 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\
 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\
 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\
 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\
 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\
 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\
 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0
 \end{array} \right]
 \xrightarrow{\begin{array}{l} L_8 \rightarrow L_8 + L_7 \\ L_9 \rightarrow L_9 + L_6 \end{array}}
 \left[\begin{array}{cccccccc|c}
 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\
 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\
 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\
 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\
 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\
 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\
 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\
 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0
 \end{array} \right]
 \xrightarrow{\begin{array}{l} L_5 \rightarrow L_5 + L_9 \\ L_7 \rightarrow L_7 + L_9 \\ L_8 \rightarrow L_8 + L_9 \end{array}}
 \end{array}$$

Aqui já aparece a primeira parte desta questão (a), pois como $p_M = 9 = p_{Mt_1}$ o Teorema 2.4.5 (Teor. do Posto) garante que o sistema é possível. E mais: como o número de incógnitas também é 9, esse Teorema diz que o sistema é um SPD. Isto também prova que o conjunto B é uma base para \mathbb{Z}_2^9 . Para achar a solução única continua-se reduzindo a matriz dos coeficientes até sua forma escalonada reduzida, que será a matriz identidade de ordem 9:

Concluindo a resolução:

$$x_1 = x_2 = x_4 = x_5 = x_6 = x_8 = x_9 = 0$$

e

$$x_3 = x_7 = 1$$

Ou seja, o vetor solução é $\mathbf{x} = (0, 0, 1, 0, 0, 0, 1, 0, 0)$, que equivale a tocar apenas os quadrados 3 e 7.

(b) Dos argumentos da parte (a) acima, já se sabia que o jogo tem sempre solução independente das condições iniciais pois qualquer vetor de \mathbb{Z}_2^9 será sempre uma combinação linear de uma base. Mas, será provado este fato independentemente dos conceitos da álgebra linear. Seja $\mathbf{t}_1 = \mathbf{s} + \mathbf{t}$, onde \mathbf{s} é uma configuração inicial qualquer e \mathbf{t} uma configuração final qualquer. Como a matriz completa $[M|\mathbf{t}_1]$ do sistema possui uma coluna a mais que a matriz M dos coeficientes, e ambas possuem 9 linhas, então $p_M \leq p_{M\mathbf{t}_1} \leq 9$. Como foi visto no item (a) acima que $p_M = 9$, segue que $p_M = p_{M\mathbf{t}_1} = 9$. Logo, pelo Teorema 2.4.5, tem-se o resultado.

Observação: Quando a atividade proposta recai em um sistema cuja matriz dos coeficientes é uma matriz quadrada, pode-se usar o determinante como ferramenta, principalmente quando o determinante é diferente de zero. Por exemplo, na atividade 4 acima, tem-se que $\det(M) = 1 \in \mathbb{Z}_2$, disto segue imediatamente que:

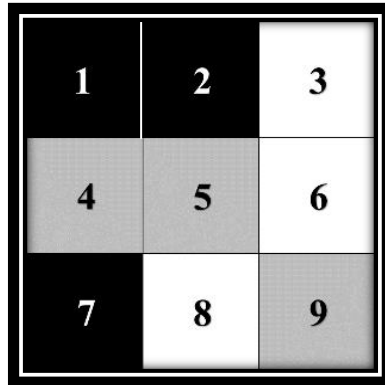
- O sistema é um SPD;
- O conjunto B dos vetores coluna de M forma uma base para \mathbb{Z}_2^9 ;
- A matriz M é invertível e, portanto, a solução única do sistema linear $M\mathbf{x} = \mathbf{t}_1$ é dada por $\mathbf{x} = M^{-1}\mathbf{t}_1$.

4.5 Atividade 5

Considere uma variação do quebra-cabeças dos nove quadrados. O jogo é como descrito na atividade 4, exceto que há três estados de cores possíveis para cada quadrado: branco, cinza ou preto. Os quadrados mudam de cor, como mostra a figura 11, mas agora as mudanças de

estado seguem o ciclo branco \rightarrow cinza \rightarrow preto \rightarrow branco. Mostre como a configuração vencedora toda preta pode ser obtida a partir da configuração inicial mostrada na figura 12.

Figura 12 – O quebra-cabeça dos nove quadrados com três estados.



Fonte: Poole, 2004.

Solução:

Este problema será resolvido dentro do espaço vetorial $V = M_{3 \times 3}(\mathbb{Z}_3)$ das matrizes de ordem 3×3 , com entradas sobre o corpo \mathbb{Z}_3 , pois cada quadrado apresenta três estados de cores. Como V possui dimensão 9, poderia ser considerado no espaço vetorial \mathbb{Z}_3^9 , análogo à atividade 4, via o isomorfismo T , onde:

$$T: V \rightarrow \mathbb{Z}_3^9 \text{ tal que } T \left(\begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix} \right) = (a_{11}, a_{12}, a_{13}, a_{21}, a_{22}, a_{23}, a_{31}, a_{32}, a_{33}).$$

Considere M_i como a matriz que representa o toque do quadrado i sobre todos os quadrados, onde $i = 1, \dots, 9$. O vetor solução do problema é o vetor $\mathbf{x} = (x_1, x_2, \dots, x_9)$, $x_i \in \mathbb{Z}_3$, onde x_i é o número de vezes que cada interruptor i será acionado. Representando por 0 a cor branca, por 1 a cor cinza e por 2 a cor preta, chamando de s , a configuração inicial da cor dos quadrados, e sendo t a configuração final desejada, precisa-se resolver:

$$s + x_1 \cdot M_1 + x_2 \cdot M_2 + x_3 \cdot M_3 + x_4 \cdot M_4 + x_5 \cdot M_5 + x_6 \cdot M_6 + x_7 \cdot M_7 + x_8 \cdot M_8 + x_9 \cdot M_9 = t$$

Ou ainda:

$$x_1 \cdot M_1 + x_2 \cdot M_2 + x_3 \cdot M_3 + x_4 \cdot M_4 + x_5 \cdot M_5 + x_6 \cdot M_6 + x_7 \cdot M_7 + x_8 \cdot M_8 + x_9 \cdot M_9 = t - s$$

Substituindo, vem:

$$\begin{aligned} & x_1 \cdot \begin{bmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix} + x_2 \cdot \begin{bmatrix} 1 & 1 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} + x_3 \cdot \begin{bmatrix} 0 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{bmatrix} + x_4 \cdot \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix} + x_5 \cdot \begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 0 \end{bmatrix} + \\ & + x_6 \cdot \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{bmatrix} + x_7 \cdot \begin{bmatrix} 0 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 0 \end{bmatrix} + x_8 \cdot \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 1 & 1 \end{bmatrix} + x_9 \cdot \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix} = \\ & \begin{bmatrix} 2 & 2 & 2 \\ 2 & 2 & 2 \\ 2 & 2 & 2 \end{bmatrix} - \begin{bmatrix} 2 & 2 & 0 \\ 1 & 1 & 0 \\ 2 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 2 \\ 1 & 1 & 2 \\ 0 & 2 & 1 \end{bmatrix} \end{aligned}$$

Desenvolvendo:

$$\begin{bmatrix} x_1 + x_2 + x_4 & x_1 + x_2 + x_3 + x_5 & x_2 + x_3 + x_6 \\ x_1 + x_4 + x_5 + x_7 & x_1 + x_3 + x_5 + x_7 + x_9 & x_3 + x_5 + x_6 + x_9 \\ x_4 + x_7 + x_8 & x_5 + x_7 + x_8 + x_9 & x_6 + x_8 + x_9 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 2 \\ 1 & 1 & 2 \\ 0 & 2 & 1 \end{bmatrix}, \text{ isto é:}$$

$$\begin{aligned} x_1 + x_2 + \quad x_4 + & & & & & & = 0 \\ x_1 + x_2 + x_3 + \quad x_5 + & & & & & & = 0 \\ \quad x_2 + x_3 + \quad \quad \quad x_6 & & & & & & = 2 \\ x_1 + \quad \quad \quad x_4 + x_5 + \quad x_7 & & & & & & = 1 \\ x_1 + \quad x_3 + \quad x_5 + \quad x_7 + \quad x_9 & & & & & & = 1 \\ \quad \quad \quad x_3 + \quad x_5 + x_6 + & & & & & & x_9 = 2 \\ \quad \quad \quad \quad \quad \quad x_4 + \quad \quad \quad x_7 + x_8 & & & & & & = 0 \end{aligned}$$

$$\begin{aligned}x_5 + x_7 + x_8 + x_9 &= 2 \\x_6 + x_8 + x_9 &= 1\end{aligned}$$

Este sistema pode ser representado pela equação matricial

$$M \cdot \mathbf{x} = \mathbf{t}_1$$

onde $M_{9 \times 9}$ é a matriz incompleta do sistema, ou matriz dos coeficientes. Note que, embora a matriz M aparente ser a mesma que a matriz incompleta da atividade 4, aquela possui entradas em \mathbb{Z}_2 . Então, fazendo o escalonando da matriz completa $[M|\mathbf{t}_1]$, vem:

$$\left[\begin{array}{cccccccc|c} 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 2 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 2 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{array} \right] \xrightarrow{\begin{array}{l} L_2 \rightarrow L_2 - L_1 \\ L_4 \rightarrow L_4 - L_1 \\ L_5 \rightarrow L_5 - L_1 \end{array}} \left[\begin{array}{cccccccc|c} 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 2 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 2 \\ 0 & 2 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 2 & 1 & 2 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 2 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{array} \right] \xrightarrow{L_2 \leftrightarrow L_3}$$

$$\left[\begin{array}{cccccccc|c} 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 2 \\ 0 & 0 & 1 & 2 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 2 & 1 & 2 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 2 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{array} \right] \xrightarrow{\begin{array}{l} L_1 \rightarrow L_1 - L_2 \\ L_4 \rightarrow L_4 + L_2 \\ L_5 \rightarrow L_5 + L_2 \end{array}} \left[\begin{array}{cccccccc|c} 1 & 0 & 2 & 1 & 0 & 2 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 2 \\ 0 & 0 & 1 & 2 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 2 & 2 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 2 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{array} \right] \xrightarrow{\begin{array}{l} L_1 \rightarrow L_1 + L_3 \\ L_2 \rightarrow L_2 - L_3 \\ L_4 \rightarrow L_4 - L_3 \\ L_5 \rightarrow L_5 + L_3 \\ L_6 \rightarrow L_6 - L_3 \end{array}}$$

$$\begin{array}{c}
 \left[\begin{array}{cccccccc|c}
 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 \\
 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 2 & 1 \\
 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\
 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 1 & 0 \\
 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 2 \\
 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 1 & 2 \\
 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\
 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2
 \end{array} \right]
 \begin{array}{l}
 L_1 \rightarrow L_1 - L_9 \\
 L_2 \rightarrow L_2 - L_9 \\
 L_3 \rightarrow L_3 + L_9 \\
 L_4 \rightarrow L_4 - L_9 \\
 L_5 \rightarrow L_5 - L_9 \\
 L_7 \rightarrow L_7 - L_9 \\
 \hline
 \rightarrow
 \end{array}
 \begin{array}{c}
 \left[\begin{array}{cccccccc|c}
 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 2 \\
 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 1 \\
 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 2 \\
 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 \\
 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\
 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2
 \end{array} \right]
 \begin{array}{l}
 L_6 \rightarrow 2L_6 \\
 L_7 \rightarrow 2L_7 \\
 \hline
 \rightarrow
 \end{array}
 \end{array}$$

$$\left[\begin{array}{cccccccc|c}
 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 2 \\
 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 1 \\
 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\
 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\
 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2
 \end{array} \right] .$$

Como $2x_5 = 1$, então $x_5 = 2$. Então, os valores são:

$$x_1 = x_3 = x_7 = 0$$

$$x_2 = x_6 = x_8 = 1 \quad ,$$

$$x_4 = x_5 = x_9 = 2$$

ou seja, o vetor solução é $\mathbf{x} = (0, 1, 0, 2, 2, 1, 0, 1, 2)$, que equivale a tocar os quadrados 2, 6 e 8 uma vez e os quadrados 4, 5 e 9 duas vezes, em qualquer ordem.

CONCLUSÃO

A ideia central deste trabalho foi apresentar uma ferramenta útil para impulsionar o estudo de Matrizes e Sistemas Lineares. Para isto, inicialmente pensou-se na construção de material concreto do Sistema de Lâmpadas descrito no capítulo 3. Devido ao alto custo do material e tendo como intenção que este possa ser reproduzido sem grande custo, optou-se pelo Jogo de Cartas, como descrito na Atividade 1.

Os principais aspectos históricos abordados no capítulo 1 visam fornecer ao leitor alguns dados para, caso queira, mostrar aos alunos como se deu o desenvolvimento dos principais conteúdos aqui estudados. A tecnologia de que dispomos, apesar do grande desenvolvimento durante o século XX, vem sendo construída há milhares de anos. Sob esse olhar, os avanços científicos em cada geração só fazem sentido se puderem ser transmitidos a outras gerações. Às vezes, saber como o conhecimento que está sendo visto em sala de aula chegou até cada um motiva os alunos a uma frequência maior nos estudos. O conforto que encontram na manipulação de seus aparelhos retrata longos e contínuos anos de estudos de muitos.

O referencial teórico descrito no capítulo 2 utiliza uma linguagem não totalmente adequada aos alunos do Ensino Médio. Entretanto, foi pensado para aprofundar ou recordar os conhecimentos dos docentes que se interessarem em utilizar este trabalho em sala de aula.

As atividades desenvolvidas no capítulo 4, assim como o capítulo 3, utilizam congruência módulo 2 ou módulo 3. Essas, por envolverem apenas números inteiros, possibilitam que o estudo inicial de Matrizes e Sistemas Lineares seja mais atraente para os alunos. Optar por trabalhar com o Teorema do Posto foi, antes de tudo, estratégia para agilizar o escalonamento das matrizes, uma vez que este precisaria ser feito, para encontrar as soluções dos problemas. E, como todo bom problema matemático, essas atividades não têm uma única forma de serem resolvidas.

Quanto ao que foi descrito na atividade 1, espera-se que as demais atividades possam ser trabalhadas com o uso de material concreto adequado.

É importante ressaltar que este trabalho não pretende direcionar como o leitor deve conduzir sua prática docente. Até porque alguns conteúdos relativos ao estudo de Matrizes e Sistemas Lineares não foram aqui trabalhados. Mas espera-se que seja uma contribuição positiva para um estudo preliminar destes assuntos.

Por se tratar de um trabalho teórico, apesar de pensado na prática em sala de aula, conforme cada atividade for aplicada, modificações surgirão. Melhorias já encerram em si o seu próprio significado. Afinal, nada em Matemática é estático. Ela está em crescente movimento, sujeita às necessidades dos indivíduos. Está em toda parte, onde quer que você vá.

REFERÊNCIAS

- BERTOLINI, Marcel Vinhas. *Aspectos da Matemática Chinesa: Os Nove Capítulos*. Disponível em www.ime.usp.br/~cpq/main/.../Marcel%20Vinhas%20Bertolini%20resumo2.pdf. Acesso em 21/07/2016.
- BOYER, Carl Benjamin. *História da Matemática*. 2. ed. São Paulo: Edgard Blucher, 1996.
- BRANDEMBERG, João Cláudio. *Emmy Noether e a Teoria dos Anéis*. Disponível em http://www.each.usp.br/ixsnhm/Anaisixsnhm/Posterres/2_Brandemberg_J_C_Emmy_Noether_e_a_Teoria_dos_An%C3%A9is.pdf. Acesso em 21/07/2016.
- BUENO, Hamilton Prado. *Álgebra Linear, Um Segundo Curso*. 1. ed. Rio de Janeiro: SBM, 2006.
- COUTINHO, Severino Collier. *Números Inteiros e Criptografia RSA*. 2. ed. Rio de Janeiro: IMPA, 2009.
- CRUZ, Luiz Francisco da. *Introdução ao Estudo da Álgebra Linear*. Disponível em www.fc.unesp.br/~lfcruz/AL_CAP_01_pdf. Acesso em 21/07/2016.
- DOMINGUES, Hygino H. *Emmy Noether e a Álgebra Moderna*. Disponível em <https://www.obaricentrodamente.com/2014/11/emmy-noether-e-algebra-moderna.html>. Acesso em 21/07/2016.
- DUMMIT, David S.; FOOTE, Richard M. *Abstract Algebra*. 3. ed. USA: Wiley, 2004.
- GONÇALVES, Adilson. *Introdução à Álgebra*. 5. ed. Rio de Janeiro: IMPA, 2015.
- HEFEZ, Abramo; FERNANDEZ, Cecília de Souza. *Introdução à Álgebra Linear*. PROFMAT, 2012.
- IEZZI, Gelson; HAZZAN, Samuel. *Fundamentos da Matemática Elementar 4*. 7. ed. São Paulo: Atual, 2004.
- KOLMAN, Bernard; HILL, David R. *Introdução à Álgebra Linear com Aplicações*. 8. ed. Rio de Janeiro: LTC, 2006.
- LIDL, Rudolf; NIEDERREITER, Harald. *Introduction to Finite Fields and Their Applications*. 1. ed. rev. United Kingdom: Cambridge: Cambridge University Press, 1994.
- LIMA, Elon Lages. *Álgebra Linear*. 5. ed. Rio de Janeiro: IMPA, 2001.
- POOLE, David. *Álgebra Linear*. 1. ed. São Paulo: Cengage Learning, 2004.