UFSC UNIVERSIDADE FEDERAL DE SANTA CATARINA

UNIVIMA

UNIVERSIDADE VIRTUAL DO ESTADO DO MARANHÃO

ESPECIALIZAÇÃO EM MATEMÁTICA NA MODALIDADE A DISTÂNCIA

TRANSFORMAÇÕES LINEARES E ISOMORFISMOS: UM EXEMPLO EM CRIPTOGRAFIA

LÚCIO HÉLIO OLIVEIRA DA SILVA

IMPERATRIZ – MA

2009

LÚCIO HÉLIO OLIVEIRA DA SILVA

TRANSFORMAÇÕES LINEARES E ISOMORFISMOS:

UM EXEMPLO EM CRIPTOGRAFIA

Trabalho de Conclusão de Curso apresentado ao curso de Especialização em Matemática, do Departamento de Matemática, Centro de Ciências Físicas e Matemáticas, Coordenadoria de Ensino à Distância, da Universidade Federal de Santa Catarina, conveniada a Universidade Virtual do Maranhão.

Professor/Orientador: Dr.Roberto Corrêa da Silva

IMPERATRIZ – MA

Agosto de 2009

UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO DE CIÊNCIAS FÍSICAS E MATEMÁTICAS
Departamento de Matemática
Curso de Especialização em Matemática-Formação de Professor na modalidade a distância

"Transformações Lineares e Isomorfismos: Um Exemplo em Criptografia"

Monografia submetida a Comissão de avaliação do Curso de Especialização em Matemática-Formação do professor em cumprimento parcial para a obtenção do título de Especialista em Matemática.

APROVADA PELA COMISSÃO EXAMINADORA em 17/08/2009

Dr. Roberto Correa da Silva (CFM/UFSC - Orientador) _____

Drª. Silvia Martini de Holanda Janesch (CFM/UFSC - Examinador) _____

Drª. Sonia Elena Palomino Bean (CFM/UFSC – Examinador) _____

Dra. Neri Terezinha Both Carvalho
Coordenadora do Curso de Especialização em Matemática-Formação de Professor

Florianópolis, Santa Catarina, agosto de 2009.

AGRADECIMENTOS

A todos os professores do curso em especial ao meu Orientador Professor Doutor Roberto Corrêa da Silva, que mesmo na Modalidade à Distância, contribuiu muito para esta realização.

DEDICATÓRIA

Ao Arquiteto do Universo, à Minha Esposa Alzira Cassimiro, e a todos que de alguma forma contribuíram para este Trabalho.

"Não há ramo da Matemática, por mais abstrato que seja que não possa um dia vir a ser aplicado aos fenômenos do mundo real."

(NICOLAI LOBACHEVSKY, matemático russo, trabalhou em álgebra, 1792 – 1856.)

SUMÁRIO

INTRODUÇÃO

O presente trabalho tem como base os estudos das Transformações Lineares de Espaços Vetoriais do curso de Álgebra Linear. No essencial, assumimos que o leitor já possua alguma familiaridade com os conceitos mais fundamentais da Teoria dos Espaços Vetoriais de Álgebra Linear. No entanto, abordaremos vez por outra esses conceitos que serão de suma importância no entendimento dos conceitos de Transformações Lineares.

Em Transformações Lineares nos deteremos mais nas exemplificações de Operadores Lineares no $\mathbb{R}^n$ e suas representações matriciais, buscando por em evidência essa cumplicidade de notações no que diz respeito as propriedades operatórias. Com isso, conceituaremos o Isomorfismo como uma Transformação Linear inversível.

Discorremos um pouco sobre a história da criptografia, abordando os principais fatos e um pouco de sua linguagem técnica, mostrando a importância da proteção das informações no meio de comunicação globalizado dos dias de hoje. Nos exemplos em criptografia faremos uso do Isomorfismo de Operadores Lineares no $\mathbb{R}^n$ como algoritmos criptográficos.

Faremos assim, uma abordagem das estruturas algébricas e bem como na criptografia de dados, através de exemplos para cada definição teórica de maneira didática e objetiva.

1. TRANSFORMAÇÃO LINEAR

Neste trabalho consideramos conhecida a teoria de espaços vetoriais sobre $\mathbb{R}$, cuja definição e resultados elementares são encontrados nos livros [1] e [2] de nossa referência.

Estamos familiarizados com funções ordinárias tais como as funções do cálculo. Mas, aqui veremos funções especiais que são as Transformações Lineares (ou também ditas aplicações lineares).

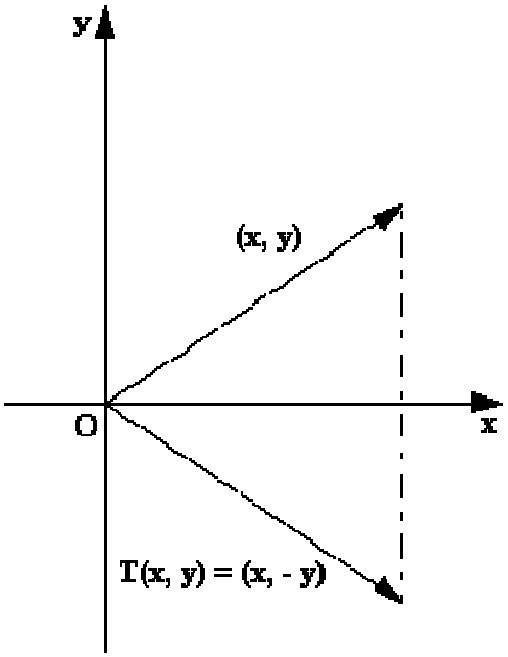
1.1. Conceito de Transformação Linear. Como introdução à definição de Transformação Linear, consideremos os dois seguintes exemplos:

1.1.1. Exemplo. (Reflexão em torno do eixo dos *x*).

Seja em $\mathbb{R}^2$ a função T definida por:

$$T(x, y) = (x, -y).$$

Geometricamente, T toma cada vetor do $\mathbb{R}^2$ e o reflete em torno do eixo dos *x*.



Observe que essa função goza das seguintes propriedades:

Dados os vetores $u = (x_1, y_1)$ e $v = (x_2, y_2) \in \mathbb{R}^2$ e $k \in \mathbb{R}$, temos:

i) $T(u + v) = (x_1 + x_2, -[y_1 + y_2])$

$T(u + v) = (x_1 + x_2, -y_1 - y_2) = (x_1, - y_1) + (x_2, - y_2) = T(u) + T(v)$

ii) $T(kv) = (kx_1, -ky_1) = k(x_1, -y_1) = kT(u)$

Que são as propriedades de linearidade.

1.1.2. Exemplo. Consideremos a expressão matricial de um sistema de equações:

$$Ax = b,$$

Onde A é uma matriz *mxn*, x $\in \mathbb{R}^n$ e b $\in \mathbb{R}^m$. Na equação buscamos conhecer x quando A e b são dados. De outro modo, dada a matriz A, a equação Ax = b, a matriz A representa a função com domínio $\mathbb{R}^n$ e contra domínio $\mathbb{R}^m$, onde a imagem de cada x $\in \mathbb{R}^n$ é b = Ax $\in \mathbb{R}^m$, considerando como coordenadas a base canônica do $\mathbb{R}^m$, teremos um vetor do $\mathbb{R}^m$ associado a b. E essa função terá as seguintes propriedades:

- A(x + y) = Ax + Ay,
- A(α x) = αAx, com $\alpha \in \mathbb{R}$.

1.1.3. *Definição de Transformação Linear.* Considere U e V espaços vetoriais sobre $\mathbb{R}$. Chamaremos de **Transformação Linear** a relação T: U $\longrightarrow$ V, pela qual cada elemento de U é associado a um único elemento em V, satisfazendo as seguintes condições:

i) Para quaisquer u_1 e u_2 em U,

$$T(u_1 + u_2) = T(u_1) + T(u_2)$$

ii) E para quaisquer que sejam $\alpha \in \mathbb{R}$ e u em U,

$$T(\alpha u) = \alpha T(u)$$

1.1.4. Exemplos:

1. Seja: T: $\mathbb{R}^2 \longrightarrow \mathbb{R}^3$, dada por T(x, y) = (x – y, 2y, -x) é uma Transformação Linear, pois leva cada elemento do $\mathbb{R}^2$ em apenas um elemento no $\mathbb{R}^3$, e:

i) Para (x_1, y_1) e (x_2, y_2) em $\mathbb{R}^2$ temos que:

$$\begin{aligned} T((x_1, y_1) + (x_2, y_2)) &= T(x_1 + x_2,\ y_1 + y_2) \\ &= ((x_1 + x_2) - (y_1 + y_2),\ 2.(y_1 + y_2),\ -(x_1 + x_2)) \\ &= ((x_1 - y_1) + (x_2 - y_2),\ 2y_1 + 2y_2,\ (-x_1) + (-x_2)) \\ &= (x_1 - y_1,\ 2y_1,\ -x_1) + (x_2 - y_2,\ 2y_2,\ -x_2) \\ &= T(x_1, y_1) + T(x_2, y_2) \end{aligned}$$

ii) Para (x_1, y_1) em $\mathbb{R}^2$ e $\kappa \in \mathbb{R}$, temos que:

$$\begin{aligned} T(\kappa\,(x_1, y_1)) &= T(\kappa x_1, \kappa y_1) \\ &= (\kappa x_1 - \kappa y_1,\ \kappa\, 2y_1,\ -\kappa x_1) \\ &= \kappa\,(x_1 - y_1,\ 2y_1,\ -x_1) \\ &= \kappa\, T(x_1, y_1) \end{aligned}$$

■

2. Seja T: $\mathbb{R} \longrightarrow \mathbb{R}$ definida por T(x) = αx, é uma Transformação Linear, onde α é fixado, de fato:

i) Para x_1 e x_2 em $\mathbb{R}$ temos que:

$$T(x_1+x_2) = \alpha\,(x_1+x_2)$$
$$= \alpha x_1 + \alpha x_2$$
$$= T(x_1) + T(x_2)$$

ii) Para x_1 em $\mathbb{R}$ e $\gamma \in \mathbb{R}$ temos que:

$$T(\gamma\, x_1) = \alpha(\gamma\, x_1) = \gamma(\alpha\, x_1)$$
$$= \gamma\, T(x_1)$$ ■

3. Seja T: $\mathbb{R} \longrightarrow \mathbb{R}^2$ definida por T(x) = (x, 2), não é uma Transformação Linear, de fato:

i) Para $x_1 = 4$ e $x_2 = -3$ em $\mathbb{R}$,temos que:

$$T(4 + [-3]) = (4 + [-3], 2) = (1, 2)$$
$$T(4) + T(-3) = (4, 2) + (-3, 2)$$
$$T(4) + T(-3) = (1, 4) \text{ , assim,}$$
$$T(x_1 + x_2) \neq T(x_1) + T(x_2)$$

Logo, T não é uma Transformação Linear. ■

4. A aplicação N: U $\longrightarrow$ V, que N(u) = 0, é uma Transformação Linear e designa-se por **Transformação Linear Nula**, de fato:

i) Para u_1 e u_2 em U, temos que:

$$N(u_1 + u_2) = 0$$
$$0 = 0 + 0 = N(u_1) + N(u_2)$$

ii) Para u_1 em U e $\alpha \in \mathbb{R}$, temos que:

$$N(\alpha.u_1) = 0$$
$$0 = \alpha.0 = \alpha.N(u_1)$$ ■

1.1.5. ***Definição de Operador Linear***. Uma Transformação Linear T de U em V é chamada de **Operador Linear** se os espaços vetoriais U e V são iguais.

1.1.6. Exemplo: Seja T: $\mathbb{R}^2 \longrightarrow \mathbb{R}^2$, T(x, y) = (y, x), é um Operador Linear, de fato:

i) Para u = (a, b) e v = (c, d) $\in \mathbb{R}^2$, temos que:

T(u + v) = T(a + c, b + d) = (b + d, a + c) = (b, a) + (d, c) = T(u) + T(v)

ii) Para u = (a, b) $\in \mathbb{R}^2$ e $\omega \in \mathbb{R}$, temos que:

T(ωu) = T(ωa, ωb) = (ωb, ωa) = ω(b, a) = ωT(u) ■

1.2. Propriedades de uma Transformação Linear.

Sejam U e V espaços vetoriais sobre $\mathbb{R}$ e considerando T: U $\longrightarrow$ V uma Transformação Linear, são válidas as seguintes proposições:

1.2.1. Proposição. T(0) = 0 (T leva o vetor nulo de U no vetor nulo de V)

Demonstração:

O fato de T ser Transformação Linear e o fato de 0 ser o vetor nulo de U nos leva a:

$$T(0) = T(0 + 0) = T(0) + T(0)$$

Assim temos:

$$T(0) + 0 = T(0) + T(0)$$

Adicionando - T(0) a ambos os membros desta igualdade chegamos a

$$0 = T(0)$$ ■

Observe que a **Proposição 1.2.1.** é decorrente da definição de Transformação Linear, isso nos auxilia a detectar transformações não lineares, ou seja, se $T(0) \neq 0$, T não é linear. Mas, devemos ter cuidado, pois, T(0) = 0, não é suficiente para que T seja linear.

1.2.2. Proposição. $T(-u) = -T(u)$, $\forall\ u \in U$.

***Demonstração*:** $T(u) + (-T(u)) = 0 = T(0) = T(u + (-u)) = T(u) + T(-u)$

Assim temos:

$$T(u) + T(-u) = T(u) + (-T(u))$$

Adicionando - T(u) a ambos os membros desta igualdade chegamos a:

$$T(-u) = -T(u)$$ ■

Observe que da definição de Transformação Linear, a **Proposição 1.2.2.** é um caso específico para $\alpha = -1$.

1.2.3. Proposição. $T(u_1 - u_2) = T(u_1) - T(u_2)$, $\forall\ u_1, u_2 \in U$.

***Demonstração*:** T é uma Transformação Linear, assim:

$$T(u_1) + T(-u_2) = T(u_1 + (-u_2)) = T(u_1 - u_2)$$

Pela **Proposição 1.2.2.** Temos que $T(-u_2) = -T(u_2)$, assim obtemos:

$$T(u_1) + T(-u_2) = T(u_1) + (-T(u_2)) = T(u_1) - T(u_2)$$

Daí pode-se concluir que:

$$T(u_1 - u_2) = T(u_1) - T(u_2)$$ ■

1.2.4. Proposição. $T(\sum_{i=1}^{n} \alpha_i u_i) = \sum_{i=1}^{n} a_i T(u_i)$.

$\forall\ u_i \in U$ e $\forall\ a_i \in \mathbb{R}$, onde $i \in \mathbb{N}^*$.

***Demonstração*:** Pela definição de Transformação Linear, podemos considerar:

$$T(a_1u_1 + a_2u_2) = a_1T(u_1) + a_2T(u_2),\ \forall\ u_1, u_2 \in U \text{ e } \forall\ a_1, a_2 \in \mathbb{R}.$$

Estendendo-se gradativamente:

$$T((a_1u_1 + a_2u_2) + a_3u_3) = (a_1T(u_1) + a_2T(u_2)) + a_3T(u_3)$$

$$T((a_1u_1 + a_2u_2 + a_3u_3) + a_4u_4) = (a_1T(u_1) + a_2T(u_2) + a_3T(u_3)) + a_4T(u_4), \text{ até}$$

$$T((a_1u_1 + a_2u_2 + a_3u_3 + ...) + a_nu_n) = (a_1T(u_1) + a_2T(u_2) + a_3T(u_3) + ...) + a_nT(u_n), \text{ ou seja,}$$

$$T(a_1u_1 + a_2u_2 + a_3u_3 + ... + a_nu_n) = a_1T(u_1) + a_2T(u_2) + a_3T(u_3) + ... + a_nT(u_n)$$

O que é equivalente a:

$$T(\sum_{i=1}^{n} a_i u_i) = \sum_{i=1}^{n} a_i T(u_i)$$

$\forall\ u_i \in U$ e $\forall\ \alpha_i \in \mathbb{R}$, onde $i \in \mathbb{N}^*$. ■

1.2.5. Teorema. Uma Transformação Linear T: U ⟶ V é totalmente caracterizada pelos seus valores em uma base de U. Ou seja, se B = $\{u_1, u_2, u_3, ... ,u_n\}$ é uma base de U e uma Transformação Linear T está definida para valores em B,

$$T(u_i) = v_i, \text{ para } i \in \mathbb{N}^*.$$

Então, existe uma única Transformação Linear definida em todo o espaço U, T: U ⟶ V, tal que $T(u_i) = v_i$, para $i \in \mathbb{N}^*$.

***Demonstração*:** Vamos ter como hipótese que B = $\{u_1, u_2, u_3, ... ,u_n\}$ seja a base do domínio e que se saiba quais são as imagens $T(u_1), T(u_2), T(u_3), ... , T(u_n)$ dos vetores dessa base:

Para $u \in U$, u é combinação linear da base B, assim:

$u = a_1u_1 + a_2u_2 + a_3u_3 + ... + a_nu_n$

a linearidade de T(u) decorre da maneira como:

$T(u) = a_1T(u_1) + a_2T(u_2) + a_3T(u_3) + ... + a_nT(u_n)$

Logo, conhecendo os vetores $T(u_1), T(u_2), T(u_3), ... , T(u_n)$ a expressão de T(u) só dependerá das coordenadas de u na base B. Fica assim determinada a expressão de T(u), e a linearidade desta função T(u) da maneira como a definimos acima.

Isto significa que as Transformações Lineares são determinadas conhecendo-se apenas seus valores nos elementos de uma base.

Por outro lado, se F: U ⟶ V é outra Transformação Linear, tal que: $F(u_i) = T(u_i)$ para $i \in \mathbb{N}^*$, então aplicando o mesmo raciocínio da proposição **1.2.5.** temos que:

$$F(u) = T(u), \text{ para todo } u \in U, \text{ ou seja, } F = T.$$ ■

1.3. Núcleo e Imagem

1.3.1. ***Definição de Núcleo.*** Sejam U e V dois espaços vetoriais sobre $\mathbb{R}$ e T: U ⟶ V uma Transformação Linear, indica-se por Ker(T) e denomina-se **núcleo** de T o seguinte subconjunto de U:

$$Ker(T) = \{u \in U / T(u) = 0\}$$

1.3.2. ***Definição de Imagem*****.** Sejam U e V espaços vetoriais sobre $\mathbb{R}$ e T: U ⟶ V uma Transformação Linear, indica-se por Im(T) e denomina-se **imagem** de T, o seguinte subconjunto de V:

$$Im(T) = \{T(u) / u \in U\}$$

1.3.3. ***Definição de subespaço vetorial:*** Seja U um espaço vetorial sobre $\mathbb{R}$, um **subespaço vetorial** de U é um subconjunto W ⊂ U, tal que:

i) $0 \in W$, (o elemento nulo de U pertence ao subespaço vetorial W),

ii) $\forall\ w_1, w_2 \in W,\ w_1 + w_2 \in W$,

iii) $\forall\ \alpha \in \mathbb{R}$ e $\forall\ w \in W,\ \alpha.w \in W$.

1.3.4. ***Proposição.*** A imagem de uma Transformação Linear T: U ⟶ V é um subespaço vetorial de V:

Demonstração.

Sejam v_1 e v_2 vetores pertencentes a Im(T) e β um número real qualquer. Devemos mostrar que $v_1 + v_2 \in Im(T)$ e que $\beta v_1 \in Im(T)$, isto é, devemos mostrar que existem u_m e u_k pertencentes a U, tais que $T(u_m) = v_1 + v_2$ e $T(u_k) = \beta v_1$.

Como v_1 e v_2 pertencem a Im(T), existem $u_1, u_2 \in U$ tais que $T(u_1) = v_1$ e $T(u_2) = v_2$. Fazendo $u_m = u_1 + u_2$ e $u_k = \beta u_1$, temos que:

$$T(u_m) = T(u_1 + u_2) = T(u_1) + T(u_2) = v_1 + v_2$$

$$T(u_k) = T(\beta u_1) = \beta T(u_1) = \beta v_1,$$

além disso, o vetor nulo pertence a Im(T).

Portanto, Im(T) é um subespaço vetorial de V. ■

1.3.5. ***Proposição*****.** Seja T: U ⟶ V uma Transformação Linear, então Ker(T) é um subespaço vetorial de U:

Demonstração.

i) Como T(0) = 0, então $0 \in$ Ker(T).

ii) Sejam $u_1 \in$ Ker(T), $u_2 \in$ Ker(T), então $T(u_1) = T(u_2) = 0$.

Assim, $T(u_1 + u_2) = T(u_1) + T(u_2) = 0 + 0 = 0$.

Portanto, $u_1 + u_2 \in$ Ker(T).

iii) Sejam $u \in$ Ker(T) e $\alpha \in \mathbb{R}$, então T(u) = 0, multiplicando a igualdade por α, temos que: α.T(u) = α.0. Assim α.T(u) = 0. Como T é uma Transformação Linear, α.T(u) = T(α.u), daí podemos afirmar que: T(α.u) = α.T(u) = 0 e que α.u $\in$ Ker(T). ■

1.3.6. ***Definição de Transformação Linear Injetora.*** Dada uma Transformação Linear T: U ⟶ V, dizemos que **T é injetora** se dados $u_1 \in$ U, $u_2 \in$ U com $T(u_1) = T(u_2)$ tivermos $u_1 = u_2$, ou equivalentemente, T é injetora se dados $u_1, u_2 \in$ U com $u_1 \neq u_2$, então $T(u_1) \neq T(u_2)$.

1.3.7. ***Teorema.*** A Transformação Linear T é injetora se, somente se, Ker(T) = {0}.

Demonstração.

i) Suponhamos T injetora e seja u $\in$ Ker(T). Então T(u) = 0, mas, pela **Proposição 1.2.1.** T(0) = 0, logo T(u) = T(0). Usando a hipótese que T é injetora em T(u) = T(0), tiramos que u = 0. Assim o núcleo de T será o vetor nulo de U.

ii) Suponhamos que Ker(T)= {0} e dados u_1 e $u_2 \in$ U, então:

$$T(u_1) = T(u_2) \implies T(u_1) - T(u_2) = 0 \implies$$

$$\implies T(u_1 - u_2) = 0 \implies u_1 - u_2 \in \text{Ker}(T) \implies$$

$$\implies u_1 - u_2 = 0 \implies u_1 = u_2$$

O que mostra que T é injetora. ■

1.3.8. ***Definição de uma Transformação Linear Sobrejetora.*** Dada uma Transformação Linear T: U ⟶ V, **T é sobrejetora** se a imagem de T coincidir com V (o contradomínio), ou seja, T(U) = V.

1.3.9. **Nota.** Observe que podemos escrever T é sobrejetora se, somente se, Im(T) = V. Observe também que T é injetora se dim Ker (T) = 0 e T é sobrejetora se dim Im (T) = dim V. Pois, como Ker(T) e Im(T) são subespaços vetoriais podemos encontrar base e dimensão desses espaços.

1.3.10. Teorema do Núcleo e da Imagem. Sejam U e V espaços vetoriais sobre $\mathbb{R}$ de dimensões finitas e T: U $\longrightarrow$ V uma Transformação Linear então:

$$\dim U = \dim Ker(T) + \dim Im(T).$$

Demonstração: Seja $B_1 = \{u_1, u_2, u_3, \ldots, u_n\}$ uma base de Ker(T). Como Ker(T) $\subset$ U é subespaço de U, essa base pode ser estendida a uma base $B_2 = \{u_1, u_2, u_3, \ldots, u_n, v_1, v_2, v_3, \ldots, v_m\}$ de U. Devemos mostrar que $B_3 = \{T(v_1), T(v_2), T(v_3), \ldots, T(v_m)\}$ é uma base para Im(T), ou seja,

i) $[T(v_1), T(v_2), T(v_3), \ldots, T(v_m)] = Im(T)$

ii) $\{T(v_1), T(v_2), T(v_3), \ldots, T(v_m)\}$ é linearmente independente.

Prova de i)

Dado v $\in$ Im(T), existe u $\in$ U tal que T(u) = v. Se u $\in$ U, então:

$u = a_1u_1 + a_2u_2 + a_3u_3 + \ldots + a_nu_n + b_1v_1 + b_2v_2 + b_3v_3 + \ldots + b_mv_m$, assim,

$v = T(u) = T(a_1u_1 + a_2u_2 + a_3u_3 + \ldots + a_nu_n + b_1v_1 + b_2v_2 + b_3v_3 + \ldots + b_mv_m)$

$T(u) = a_1T(u_1) + a_2T(u_2) + a_3T(u_3) + \ldots + a_nT(u_n) + b_1T(v_1) + b_2T(v_2) + b_3T(v_3) + \ldots + b_mT(v_m)$

Como $u_1, u_2, u_3, \ldots, u_n$ pertencem ao Ker(T), $T(u_i) = 0$ para i = 1, 2, 3, ... , n. Assim,

$$v = b_1T(v_1) + b_2T(v_2) + b_3T(v_3) + \ldots + b_mT(v_m)$$

e a imagem de T é gerada pelos vetores $T(v_1), T(v_2), T(v_3), \ldots, T(v_m)$.

Prova de ii)

Consideramos agora, a combinação linear

$$a_1T(v_1) + a_2T(v_2) + a_3T(v_3) + \ldots + a_mT(v_m) = 0$$

e mostraremos que os a_i são nulos.

Como T é Transformação Linear, $T(a_1v_1 + a_2v_2 + a_3v_3 + \ldots + a_mv_m) = 0$.

Logo, $a_1v_1 + a_2v_2 + a_3v_3 + \ldots + a_mv_m \in Ker(T)$.

Então, $a_1v_1 + a_2v_2 + a_3v_3 + \ldots + a_mv_m$ pode ser escrito como combinação linear da base B_1 de Ker(T), ou seja, existem $b_1, b_2, b_3, \ldots, b_n$ tais que:

$$a_1v_1 + a_2v_2 + a_3v_3 + \ldots + a_mv_m = b_1u_1 + b_2u_2 + b_3u_3 + \ldots + b_nu_n$$

ou ainda, $a_1v_1 + a_2v_2 + a_3v_3 + \ldots + a_mv_m - b_1u_1 - b_2u_2 - b_3u_3 - \ldots - b_nu_n = 0$

mas, B_2 é uma base U,

todos os coeficientes são nulos em particular $a_1 = a_2 = a_3 = \ldots = a_m = 0$ ■

1.3.11. Corolário: Seja T: $\mathbb{R}^n \longrightarrow \mathbb{R}^n$ um Operador Linear.

a) Se T é sobrejetiva, então T é injetiva.

b) Se T é injetiva, então T é sobrejetiva.

a) Se T é sobrejetiva, temos que:

$$\text{Im}(T) = \mathbb{R}^n \Longrightarrow \dim \text{Im}(T) = \dim \mathbb{R}^n$$

$$\dim \text{Im}(T) = \dim \mathbb{R}^n$$

$$\dim \text{Ker}(T) = 0 \text{ (pelo } \textbf{Teorema 1.3.10.}\text{)}$$

Logo, T é injetiva.

b) Se T é injetiva, temos que:

$$\text{Ker}(T) = \{0\} \Longrightarrow 0 + \dim \text{Im}(T) = \dim \mathbb{R}^n \text{ (pelo } \textbf{Teorema 1.3.10.}\text{)}$$

$$\dim \text{Im}(T) = \dim \mathbb{R}^n$$

$$\text{Im}(T) = \mathbb{R}^n$$

Logo, T é sobrejetiva.

1.3.12. Exemplo: Vamos analisar a Transformação Linear T: $\mathbb{R}^2 \longrightarrow \mathbb{R}^2$ definida por:

$$T(x, y) = (3x - y, -3x + y)$$

a) Qual o núcleo de T? T é injetora?

$(3x - y, -3x + y) = (0, 0) \Longrightarrow \begin{cases} 3x - y = 0 \\ -3x + y = 0 \end{cases} \Longrightarrow y = 3x$

$\text{Ker}(T) = \{(x, 3x) / x \in \mathbb{R}\}$

como $\text{Ker}(T) \neq \{(0, 0)\}$, T não é injetora.

Além disso, uma base para Ker(T) é [(1, 3)] , logo dim Ker(T) = 1

b) Qual a imagem de T? T é sobrejetora?

$(3x - y, -3x + y) = (a, b) \Longrightarrow \begin{cases} 3x - y = a \\ -3x + y = b \end{cases} \Longrightarrow a = -b$

$\text{Im}(T) = \{(a, b) \in \mathbb{R}^2 / a + b = 0\}$

Pelo teorema da dimensão temos:

$$\dim U = \dim \text{Ker}(T) + \dim \text{Im}(T)$$

$$\dim R^2 = \dim \text{Ker}(T) + \dim \text{Im}(T)$$

$$2 = 1 + \dim \text{Im}(T)$$

$$\dim \text{Im}(T) = 2 - 1$$

$$\dim \text{Im}(T) = 1$$

como, $\dim \text{Im}(T) \neq \dim \mathbb{R}^2$, logo, T não é sobrejetora.

1.3.13. Posto e Nulidade. Seja T: U $\longrightarrow$ V uma Transformação Linear, são válidas as seguintes definições:

i) O posto de T é a dimensão de Im(T);

ii) A nulidade de T é a dimensão de Ker(T).

Assim, o teorema **1.3.10.** pode ser escrito para uma Transformação Linear T: U ⟶ V, quando U tem dimensão finita, da seguinte maneira:

$$\text{Posto}(T) + \text{Nulidade}(T) = \dim U$$

1.4. Matriz Associada a uma Transformação Linear.

Denotamos a matriz da Transformação Linear T por $[T]_{AB}$, que é a notação da matriz associada de T da base A para base B e por $[T]_{can}$ que é a notação da matriz associada a um Operador Linear no R^n da base canônica para a base canônica, assim, deve-se tomar o cuidado de percebermos que a matriz associada é um objeto que depende da base escolhida, enquanto a Transformação Linear T é um objeto intrínseco, ou seja, não depende de escolha de bases.

1.4.1. ***Definição de Matriz Associada***. Seja T: U ⟶ V uma Transformação Linear e A= $\{u_1, u_2, u_3,...,u_n\}$ base para U e B= $\{v_1, v_2, v_3,...,v_m\}$ base para V:

$$T(u_1) = \alpha_{11} v_1 + \alpha_{21} v_2 + \alpha_{31} v_3 + ... + \alpha_{m1} v_m$$

$$T(u_2) = \alpha_{12} v_1 + \alpha_{22} v_2 + \alpha_{32} v_3 + ... + \alpha_{m2} v_m$$

$$T(u_1) = \alpha_{13} v_1 + \alpha_{23} v_2 + \alpha_{33} v_3 + ... + \alpha_{m3} v_m$$

.....

$$T(u_n) = \alpha_{1n} v_1 + \alpha_{2n} v_2 + \alpha_{3n} v_3 + ... + \alpha_{mn} v_m$$

A matriz da Transformação Linear T em relação às bases A e B é denotada por $[T]_{AB}$ e definida por:

$$\begin{pmatrix} \alpha_{11} & \alpha_{12} & \cdots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \cdots & \alpha_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ \alpha_{m1} & \alpha_{m2} & \cdots & \alpha_{mn} \end{pmatrix}$$

Reciprocamente dada uma matriz M, dizemos que uma Transformação Linear T é associada a M, se $M = [T]_{AB}$ em relação às bases A e B.

1.4.2. Exemplos:

1. Seja T: $\mathbb{R}^2 \longrightarrow \mathbb{R}^3$ a Transformação Linear definida por:

$$T(x, y) = (2x - y, x + y, 3x)$$

Com B= {(1, 1), (2, 1)} e C= {(1, 0, 0), (0, 2, 0), (0, 0, 3)}, determine a matriz de T de B para C, $[T]_{BC}$.

Solução: $T(1, 1) = (1, 2, 3) = a_1(1, 0, 0)+a_2(0, 2, 0)+a_3(0, 0, 3)$

$T(2, 1) = (3, 3, 6) = b_1(1, 0, 0)+b_2(0, 2, 0)+b_3(0, 0, 3)$

$$\begin{cases} a_1 = 1 \\ 2a_2 = 2 \\ 3a_3 = 3 \end{cases} \quad \text{e} \quad \begin{cases} b_1 = 3 \\ 2b_2 = 3 \\ 3b_3 = 6 \end{cases}$$

$$[T]_{BC} = \begin{pmatrix} 1 & 3 \\ 1 & 3/2 \\ 1 & 2 \end{pmatrix}$$

Observamos que o resultado é uma matriz 3x2, onde o índice 3 é a dimensão do contradomínio e o índice 2 é a dimensão do domínio.

2. Considerando as bases canônicas A = {(1, 0, 0), (0, 1, 0), (0, 0, 1)} e B = {(1, 0), (0, 1)} do $\mathbb{R}^3$ e do $\mathbb{R}^2$, respectivamente, e a transformação linear T: $\mathbb{R}^3 \longrightarrow \mathbb{R}^2$definida por T(x, y, z) = (x + y, y – z). Determinar a matriz de T nas bases A e B:

Solução:

$T(1, 0, 0) = (1, 0)$

$T(0, 1, 0) = (1, 1)$

$T(0, 0, 1) = (0, – 1)$

$$[T]_{AB} = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & -1 \end{pmatrix}$$

1.5. Matriz de uma Transformação Linear Composta.

1.5.1. ***Definição.*** Sejam U, V e W espaços vetoriais sobre $\mathbb{R}$, de dimensões m, n, e p que admitem as respectivas bases: B = {u_1, u_2, u_3,..., u_m}, C = {v_1, v_2, v_3,..., v_n} e D = {w_1, w_2, w_3,..., w_p} fixas, supondo F: U $\longrightarrow$ V; G: V $\longrightarrow$ W Transformações Lineares que $[F]_{B,C} = [\alpha_{ij}]$ e $[G]_{C,D} = [\beta_{ki}]$, podemos determinar $[G \circ F]_{B,D}$, usando a linearidade de G, temos:

$$[G \circ F](u_j) = G(F(u_j)) =$$

$$= G\left(\sum_{i=1}^{m} \alpha_{ij} v_i\right) =$$

$$= \sum_{i=1}^{m} \alpha_{ij} G(v_i) =$$

$$= \sum_{i=1}^{m} \alpha_{ij} \sum_{k=1}^{p} \beta_{ki} w_k =$$

$$= \sum_{k=1}^{p} \left(\sum_{i=1}^{m} \beta_{ki}\, \alpha_{ij}\right) w_k$$

Tendo assim, como termo geral de $[G \circ F]_{B,D}$ o valor $\gamma_{kj} = \sum_{i=1}^{m} \beta_{ki}\, \alpha_{ij}$ que também é termo geral de $[G]_{C,D}.[F]_{B,C}$ o que implica:

$$[G \circ F]_{B,D} = [G]_{C,D}.[F]_{B,C}$$

Dizemos que a matriz de G∘F é igual ao produto da matriz associada de G pela matriz associada de F, seguindo essa ordem de composição.

1.5.2. Exemplo: Dadas as Transformações Lineares do $\mathbb{R}^3$ no $\mathbb{R}^3$ definidas por: F(x, y, z) = (x + z, x – z, y) e G(x, y, z) = (x, x – y, 2x + y – z). Determinar a Matriz Transformação Composta [F∘G] na base canônica do $\mathbb{R}^3$:

Solução:

F(1, 0, 0) = (1 + 0, 1 – 0, 0) = (1, 1, 0)

F(0, 1, 0) = (0 + 0, 0 – 0, 1) = (0, 0, 1)

F(0, 0, 1) = (0 + 1, 0 – 1, 0) = (1, -1, 0)

$$[F] = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix}$$

G(1, 0, 0) = (1, 1 – 0, 2.1 + 0 – 0) = (1, 1, 2)

G(0, 1, 0) = (0, 0 – 1, 2.0 + 1 – 0) = (0, -1, 1)

G(0, 0, 1) = (0, 0 – 0, 2.0 + 0 – 1) = (0, 0, -1)

$$[G] = \begin{pmatrix} 1 & 0 & 0 \\ 1 & -1 & 0 \\ 2 & 1 & -1 \end{pmatrix}$$

Como [F∘G] = [F].[G] ; temos:

$$[F \circ G] = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix} . \begin{pmatrix} 1 & 0 & 0 \\ 1 & -1 & 0 \\ 2 & 1 & -1 \end{pmatrix} = \begin{pmatrix} 3 & 1 & -1 \\ -1 & -1 & 1 \\ 1 & -1 & 0 \end{pmatrix}$$

2. ISOMORFISMO

2.1. História.

> "Sabemos que toda a matemática tradicional se fundamenta na Teoria dos Conjuntos. Podemos dizer, na verdade, que todas as idéias matemáticas são definíveis em termos da noção de conjunto e que as linguagens de todas as teorias matemáticas são particularizações da linguagem da Teoria dos Conjuntos.
>
> A Matemática Pura atual pode ser definida como o estudo das estruturas conjuntistas. Isto ficou patente, principalmente após os trabalhos de N. Bourbaki [um grupo de matemáticos franceses (1957 e 1968)]. Após a obra desse grupo de matemáticos, a Matemática se converteu na investigação de estruturas bem definidas, as quais Bourbaki tratou minuciosamente nos seus *Elements de Mathématique,* que hoje já possui mais de 30 volumes. Com efeito, Bourbaki escreve: "É, portanto, tentador asseverar que a moderna noção de 'estrutura' existia substancialmente por volta de 1900, mas de fato outros trinta anos de preparação se evidenciaram necessários, antes de sua completa aparição.
>
> Uma estrutura matemática se origina quando se definem certas funções, relações ou coleções de conjuntos, a partir de certos conjuntos básicos dados. Na Álgebra, nos ocupamos das chamadas estruturas algébricas que, numa primeira aproximação, se reduzem a conjuntos sobre os quais se definem certas operações determinadas por propriedades convenientes." (JAIR MINORO ABE, 1989)

Certamente, não é difícil reconhecer estruturas da mesma espécie isto é entendido como o conceito de Isomorfismo. Uma aplicação T: U $\rightarrow$ V, entre dois espaços vetoriais U e V sobre $\mathbb{R}$, dotados do mesmo tipo de estrutura são um Isomorfismo quando cada elemento de V resultante de um único elemento de U por T transformam as operações, relações, etc. que há em U nessas que estão em V. Quando entre duas estruturas há um Isomorfismo, ambos são indistinguíveis para Álgebra Linear, eles têm as mesmas propriedades, e qualquer enunciado é simultaneamente certo ou falso, para cada uma delas.

2.2. Introdução ao Isomorfismo. Antes de escrever este conceito formalmente, vamos ver um exemplo simples, embora fora de nosso contexto de estudo.

Vamos supor que nós estamos em um planeta distante onde os habitantes só conhecem dois "números", o 0 e o 1, e a única forma de operar que eles definiram foi a seguinte:

$\oplus$	0	1
0	0	1
1	1	0

Mas, em vez de números, eles recebem as cartas de outro lugar do espaço, com *e* para 1 e *a* para 0, e inclusive eles sabem uma forma de operar estas cartas, assim:

*	*e*	*a*
e	*e*	*a*
a	*a*	*e*

Não é difícil de perceber isso em ambos os lugares, de fato eles estão definindo uma operação que, embora não é exatamente a mesma, mas, tem o mesmo fundo. Para especificar esta idéia, nós podemos definir uma função:

$$\Psi: \{ 0 , 1 \} \longrightarrow \{ e , a \}$$

dado para:

$$\Psi(0) = e$$

$$\Psi(1) = a$$

Nesta parte, nós estamos identificando o 0 com *e*, e o 1 com *a*. O que realmente importa desta função que nós definimos, é que preserva as operações de ambos os conjuntos, e que:

$$\Psi(0 \oplus 0) = \Psi(0) * \Psi(0)$$

$$\Psi(0 \oplus 1) = \Psi(0) * \Psi(1)$$

$$\Psi(1 \oplus 0) = \Psi(1) * \Psi(0)$$

$$\Psi(1 \oplus 1) = \Psi(1) * \Psi(1)$$

Pensaremos nisto, como que o quadro de somar de um grupo, corresponde exatamente à tábua de multiplicar do outro grupo.

Neste ponto, podemos dizer que nossa função é tal que preserva as operações de ambos os grupos. De fato, neste exemplo em álgebra abstrata, a função Ψ é conhecida como homomorfismo de grupos.

Em vez de grupos, nos deteremos em espaços vetoriais em nosso contexto, e em vez de homomorfismos de grupos, Transformações Lineares. Isto é, uma Transformação Linear não é outra coisa, mas uma forma de mudança de um espaço vetorial para outro, de tal modo que a forma de operar de um lado preservará a forma de operar do outro, se ela for bijetora, pois caso contrário, não poderia preservar as operações de todos os elementos do contradomínio.

Finalmente, nós vemos que a função Ψ, não só preserva as operações, mas, também é bijetiva. O que realmente nos mostra que os dois grupos são semelhantes.

Podemos ainda introduzir os seguintes conceitos:

Seja T: U ⟶ V, uma Transformação Linear:

i) Nós dizemos que T é um monomorfismo, se T é injetiva.

ii) Nós dizemos que T é um epimorfismo, se T é sobrejetiva.

iii) Nós dizemos que T é um isomorfismo, se T é bijetiva.

Deste modo, um Isomorfismo não é somente uma Transformação Linear, mas também é uma função inversível, e então, pela luz de nossa discussão prévia, está entre dois espaços vetoriais como uma identificação.

Em outras palavras, dois espaços vetoriais são isomorfos, se eles são indistinguíveis como tal. É então importante, desejar saber quando dois espaços vetoriais são isomorfos, porque talvez no princípio pareçam diferentes, mas de fato eles são "a mesma coisa".

2.3. Etimologia da palavra isomorfismo.

A palavra "Isomorfismo" é composta dos termos gregos "iso"(igual) e "morphos"(forma).

2.4. ***Definição de Isomorfismo***. Denominaremos **Isomorfismo** do espaço vetorial U no espaço vetorial V (ambos sobre $\mathbb{R}$) uma Transformação Linear T: U ⟶ V que seja bijetora.

2.5. ***Definição de Espaços Vetoriais Isomorfos.*** Diremos que **dois espaços vetoriais U e V são isomorfos** se houver um Isomorfismo T: U → V.

Em outras palavras, quando a correspondência biunívoca entre dois espaços vetoriais preserva as operações de adição e multiplicação por escalar, $T(u_1 + u_2) = T(u_1) + T(u_2)$ e $T(ku_1) = k\,T(u_1)$, diz-se que esses espaços são isomorfos.

2.5.1. Exemplos:

1. (Operador Idêntico). I: U⟶ U dada por I(u) = u para todo vetor u do espaço vetorial U, é um Isomorfismo trivial.

2. (Exemplo de Isomorfismo). Seja a Transformação Linear T: $\mathbb{R}^2 \to \mathbb{R}^2$ definida por: (x, y) → (2x – y, x+ y) é um Isomorfismo. De fato:

i) $T((x_1, y_1) +(x_2, y_2)) = T(x_1 + x_2, y_1 + y_2) = (2(x_1 + x_2) –(y_1 + y_2), (x_1 + x_2)+(y_1 + y_2))$

$= (2x_1 + 2x_2 - y_1 - y_2, x_1 + x_2 + y_1 + y_2)$

$= ((2x_1 - y_1) + (2x_2 - y_2), (x_1 + y_1) + (x_2 + y_2))$

$= T(x_1, y_1) + T(x_2, y_2)$

ii) $T(\alpha (x_1, y_1)) = T (\alpha x_1, \alpha y_1) = (2(\alpha x_1)+(\alpha y_1), (\alpha x_1)+(\alpha y_1))$

$= (\alpha(2x_1 - y_1), \alpha(x_1 + y_1))$

$= \alpha\, T(x_1, y_1)$

iii) $T(x_1, y_1) = T(x_2, y_2) \implies (2x_1 - y_1, x_1 + y_1) = (2x_2 - y_2, x_2 + y_2)$

$$\implies \begin{cases} 2x1 - y1 = 2x2 - y2 \\ x1 + y1 = x2 + y2 \end{cases}$$

$\implies x_1 = x_2$ e $y_1 = y_2$, logo T é Injetora.

iv) Dado (x, y) pertencente ao contradomínio, existe (a, b) pertencente ao domínio, tal que, T(a, b) = (x, y). De fato:

Basta tomar (x, y) = (a + b/3, 2b –a/3) para que se tenha T(a, b) = T(x, y).

Logo, T é sobrejetora.

i) e ii) garante que T é uma Transformação Linear.

iii) e iv) prova que T é Isomorfismo. ■

3. (Contra exemplo de Isomorfismo). Mostrar que T: $\mathbb{R}^3 \longrightarrow \mathbb{R}^4$ dada por:

T(x, y, z) = (x – y – z, x + y + z, 2x – y, - y) é uma Transformação Linear, mas, não é um Isomorfismo. De fato:

i) $T((x_1, y_1, z_1) + (x_2, y_2, z_2)) = T((x_1 + x_2, y_1 + y_2, z_1 + z_2)) =$

$= ((x_1+x_2) - (y_1+y_2) - (z_1+z_2), (x_1+x_2) + (y_1+y_2) + (z_1+z_2), 2(x_1+x_2) - (y_1+y_2), - (y_1+y_2)) =$

$= (x_1+x_2 - y_1 - y_2 - z_1 - z_2, x_1+x_2 + y_1+y_2 + z_1+z_2, 2x_1+ 2x_2 - y_1 - y_2, - y_1 - y_2) =$

$= ((x_1 - y_1 - z_1)+(x_2 - y_2 - z_2), (x_1 + y_1 + z_1) + (x_2 + y_2 + z_2), (2x_1 - y_1)+(2x_2 - y_2), (-y_1)+(-y_2)) =$

$= T(x_1, y_1, z_1) + T(x_2, y_2, z_2)$

ii) $T(\alpha(x_1, y_1, z_1)) = (\alpha(x_1 - y_1 - z_1), \alpha(x_1 + y_1 + z_1), \alpha(2x_1 - y_1), \alpha(-y_1)) =$

$= \alpha(x_1 - y_1 - z_1, x_1 + y_1 + z_1, 2x_1 - y_1, -y_1) = \alpha\, T(x_1, y_1, z_1)$

Até aqui mostramos que T é Transformação Linear.

iii) $Ker(T) = \{(x, y, z) \in \mathbb{R}^3 / T(x, y, z) = (0, 0, 0)\}$

Se T(x, y, z) = (0, 0, 0), então:

(x – y – z, x + y + z, 2x – y, - y) = (0, 0, 0, 0)

$$\begin{cases} x - y - z = 0 \\ x + y + z = 0 \\ 2x - y = 0 \\ -y = 0 \end{cases}$$

O sistema só admite a solução trivial, logo Ker(T) = {(0, 0, 0)}, o que prova T não é

sobrejetora, pois, dim Im (T) = dim $\mathbb{R}^3$ - dim Ker(T) = 3, tendo como conseqüência Im(T) $\neq \mathbb{R}^4$. Assim podemos afirmar que T não é um Isomorfismo.

2.6. Teorema. Se uma Transformação Linear T: U $\longrightarrow$ V, com U e V espaços vetoriais sobre $\mathbb{R}$, é um Isomorfismo, então: dim U = dim V.

Demonstração: Como T é um Isomorfismo, T é injetora, então:

Considere $\{u_1, u_2, \ldots, u_n\}$ base de U, e que o conjunto $\{T(u_1), T(u_2), \ldots, T(u_n)\} \subset$ V é Linearmente Independente. Pois, dados os escalares $a_1, a_2, \ldots, a_n \in \mathbb{R}$ tais que:

$a_1T(u_1) + a_2T(u_2) + \ldots + a_nT(u_n) = 0$, temos que,

$T(a_1u_1 + a_2u_2 + \ldots + a_nu_n) = 0$, assim,

$a_1u_1 + a_2u_2 + \ldots + a_nu_n = 0$, como $\{u_1, u_2, \ldots, u_n\}$ é Linearmente Independente, logo, $a_1 = a_2 = \ldots = a_n = 0$.

Então se, dim U = dim V = n, $\{T(u_1), T(u_2), \ldots, T(u_n)\}$ é base de V. ■

2.7. Teorema da Transformação Linear Inversa. Se T:U $\longrightarrow$V é uma Transformação Linear e um Isomorfismo, sua inversa T^{-1}: V $\longrightarrow$ U, também será uma Transformação Linear e um Isomorfismo.

Demonstração:

Como T é um Isomorfismo, temos que T é bijetora, logo existe sua inversa T^{-1}.

i) Dados v_1 e v_2 em V, como T é sobrejetora, temos que:

$T(u_1) = v_1$ e $T(u_2) = v_2$, logo,

$T^{-1}(v_1 + v_2) = T^{-1}(T(u_1) + T(u_2)) = T^{-1}(T(u_1 + u_2)) = u_1 + u_2 = T^{-1}(v_1) + T^{-1}(v_2)$

Pois, $T^{-1}(T(u_1))=T^{-1}(v_1) \Longrightarrow u_1 = T^{-1}(v_1)$ e $T^{-1}(T(u_2))=T^{-1}(v_2) \Longrightarrow u_2 = T^{-1}(v_2)$

ii) Dados $v_1 \in$ V e $\alpha \in \mathbb{R}$, como T é sobrejetora, temos que:

$T(u_1) = v_1$, logo,

$T^{-1}(\alpha v_1) = T^{-1}(\alpha T(u_1)) = T^{-1}(T(\alpha u_1)) = \alpha u_1 = \alpha T^{-1}(v_1)$

iii) Como $T^{-1}(T(u)) = u$ os vetores $Ker(T^{-1})$ são os vetores T(u) = 0,

mas, como T é injetora, u = 0.

Logo, $Ker(T^{-1}) = \{ 0 \}$ e pelo ***Teorema* 1.3.6.** temos que:

T^{-1} também é injetora.

iv) Como T é sobrejetora, para todo v $\in$ V, existe u $\in$ U, tal que T(u) = v.

Então, $T^{-1}(T(u)) = u \Longrightarrow T^{-1}(v) = u$

Assim para todo u $\in$ U, existe v $\in$ V, tal que $T^{-1}(v) = u$.

Logo, T^{-1} também é sobrejetora.

Por i) e ii) garantimos que T^{-1} é uma Transformação Linear.

Por iii) e iv) provamos que T^{-1} é Isomorfismo. ∎

2.7.1. ***Definição:*** Sejam U e V espaços vetoriais sobre $\mathbb{R}$ de dimensões n, se B e C são bases de U e V, respectivamente, e T: U $\longrightarrow$ V é um Isomorfismo, então: $[T]_{B,C}$ é inversível e sua inversa será $[T^{-1}]_{C,B}$. Pois:

$$[T]_{B,C}.[T^{-1}]_{C,B} = [T \circ T^{-1}]_C = In$$
$$[T^{-1}]_{C,B}.[T]_{B,C} = [T^{-1} \circ T]_B = In$$

Isso é decorrente da definição **1.5.1.**

2.7.2. Exemplo: Considere o Operador Linear T do $\mathbb{R}^3$ satisfazendo as seguintes condições T(1, 0, 0) = (1, 1, 1), T(0, 1, 0) = (1, 0, 1) e T(0, 1, 2) = (0, 0, 4). T é um Isomorfismo? Se for determine o Isomorfismo inverso.

a) Observamos que B = {(1, 0, 0), (0, 1, 0), (0, 1, 2)} é uma base do $\mathbb{R}^3$, assim vamos encontrar as coordenadas (x, y, z) em relação à base B:

(x, y, z) = a(1, 0, 0) + b(0, 1, 0) + c(0, 1, 2)

$$\begin{cases} a = x \\ b + c = y \\ 2c = z \end{cases} \leftrightarrow \begin{cases} a = x \\ b = y - z/2 \\ c = z/2 \end{cases}$$

Logo, (x, y, z) = x(1, 0, 0) + (y – z/2)(0, 1, 0) + z/2(0, 1, 2)

b) Podemos agora encontrar a lei que rege T:

T(x, y, z) = x.T(1, 0, 0) + (y – z/2).T(0, 1, 0) + (z/2).T(0, 1, 2)

T(x, y, z) = x.(1, 1, 1) + (y – z/2).(1, 0, 1) + (z/2).(0, 0, 4)

T(x, y, z) = (x, x, x) + (y – z/2, 0, y – z/2) + (0, 0, 2z)

T(x, y, z) = (x + y – z/2, x, x + y + 3z/2)

c) Provaremos agora, que T é um Isomorfismo:

i)
$$\begin{cases} x + y - \frac{z}{2} = 0 \\ x = 0 \\ x + y + \frac{3z}{2} = 0 \end{cases}$$

o sistema só admite a solução trivial, assim Ker(T) = {(0, 0, 0)} e T é injetora.

ii) Como Im(T) = $\mathbb{R}^3$, T é sobrejetora.

i) e ii) garante que T é um Isomorfismo.

d) Encontremos o Isomorfismo inverso de T:

$$(T^{-1} \circ T)(a, b, c) = (a, b, c)$$
$$T^{-1}(T(a, b, c)) = (a, b, c)$$

Assim fazendo T(a, b, c) = (x, y, z), temos a seguinte igualdade:

$$(a + b - c/2,\ a,\ a + b + 3c/2) = (x, y, z)$$

$$\begin{cases} a + b - \frac{c}{2} = x \\ a = y \\ a + b + \frac{3c}{2} = z \end{cases} \Leftrightarrow \begin{cases} b - \frac{c}{2} = x - y \\ b + \frac{3c}{2} = z - y \end{cases}$$

$$b = \tfrac{1}{4}(3x - 4y + z) \quad \text{e} \quad c = \tfrac{1}{2}(z - x)$$

se $T(a, b, c) = (x, y, z)$, então $T^{-1}(x, y, z) = (a, b, c)$,

e finalmente, $T^{-1}(x, y, z) = (\ y, \tfrac{1}{4}(3x - 4y + z), \tfrac{1}{2}(z - x)\ )$ é o Isomorfismo Inverso.

2.8. Definições de Alguns conjuntos de Aplicações:

2.8.1. ***Definição:*** Denominamos de **conjunto de todas as Transformações Lineares**, o seguinte conjunto, caracterizado e denotado a seguir:

$$L(\mathbb{R}^n) = \{\ T: \mathbb{R}^n \longrightarrow \mathbb{R}^n \ /\ T \text{ é uma Transformação Linear }\}$$

2.8.2. ***Definição:*** Denominamos de **conjunto de todos os Isomorfismos**, o subconjunto de $L(\mathbb{R}^n)$, caracterizado e denotado a seguir:

$$\text{Isom}(\mathbb{R}^n) = \{\ T \in L(\mathbb{R}^n) / \ T \text{ é um Isomorfismo }\}$$

2.8.3. ***Definição:*** Denominamos de **conjunto de todas as Matrizes Inversíveis no $\mathbb{R}^n$**, o subconjunto das Matrizes de $(M_n(\mathbb{R}))$, cujos determinantes são diferentes de zero, caracterizado e denotado a seguir:

$$G\,L_n(\mathbb{R}) = \{\ A \in M_n(\mathbb{R}) / \ A \text{ é inversível }\}$$

2.9. Exemplos de algumas associações entre conjuntos de aplicações:

2.9.1. Teorema: A associação $F: L(\mathbb{R}^2) \longrightarrow M_2(\mathbb{R})$

$$T \mapsto [T]_{can}$$

onde $[T]_{can}$ é a matriz associada na base canônica do $\mathbb{R}^2$. É um Isomorfismo.

Demonstração:

Observamos que $L(\mathbb{R}^2)$ e $M_2(\mathbb{R})$ são espaços vetoriais sobre $\mathbb{R}$, conforme definição encontrada no capítulo 2 do livro [2] de nossa referência.

Vamos mostrar que F é uma Transformação Linear:

i) O conjunto $L(\mathbb{R}^2)$ é o conjunto das Transformações Lineares no $\mathbb{R}^2$, assim um elemento de $L(\mathbb{R}^2)$ será do tipo:

$$\Psi : \mathbb{R}^2 \longrightarrow \mathbb{R}^2 \qquad \text{e} \quad F(\Psi) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

$$(x, y) \mapsto (ax + by, cx + dy)$$

e $\Omega: \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ e $F(\Omega) = \begin{pmatrix} g & h \\ j & l \end{pmatrix}$, assim:

$$(x, y) \mapsto (gx + hy, jx + ly)$$

$$\Psi + \Omega: \mathbb{R}^2 \longrightarrow \mathbb{R}^2$$

$$(x, y) \mapsto ((a + g).x + (b + h).y, (c + j).x + (d + l).y), \text{ com}$$

$$F(\Psi + \Omega) = \begin{pmatrix} a+g & b+h \\ c+j & d+l \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} g & h \\ j & l \end{pmatrix} = F(\Psi) + F(\Omega)$$

ii) E se $\alpha \in R$, temos:

$$\alpha\Psi: \mathbb{R}^2 \longrightarrow \mathbb{R}^2$$

$$\alpha(x, y) \mapsto (\alpha(ax + by), \alpha(cx + dy))$$

$$F(\alpha\Psi) = \begin{pmatrix} \alpha a & \alpha b \\ \alpha c & \alpha d \end{pmatrix} = \alpha \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \alpha F(\Psi),$$

i) e ii) prova que F é Transformação Linear.

iii) $Ker(F) = \{U \in L(\mathbb{R}^2) / F(U) = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}\}$

Se $U: \mathbb{R}^2 \longrightarrow \mathbb{R}^2$, tal que: $[U]_{can} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, logo:

$$(x, y) \mapsto U(x, y)$$

U(1, 0) = 0.(1, 0) + 0.(0, 1) = (0, 0)
U(0, 1) = 0.(1, 0) + 0.(0, 1) = (0, 0) e,
U(x, y) = U(x.(1, 0) + y.(0, 1)) = x.U(1, 0) + y.U(0, 1) = x.(0, 0) + y.(0, 0) = (0, 0)
Logo, U(x, y) = (0, 0)
Assim, U(x, y) é a função nula em $L(\mathbb{R}^2)$.
Portanto, Ker(F) possui somente a função nula em $L(\mathbb{R}^2)$, logo F é injetora.

iv) Dada $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(R)$, existe $T: \mathbb{R}^2 \longrightarrow \mathbb{R}^2$, tal que: $[T]_{can} = A$,

De fato, tomando T(x, y) = (ax + by, cx + dy), temos que:
T(1, 0) = (a, c) e T(0, 1) = (b, d) e finalmente:

$[T]_{can} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, o que garante que F é sobrejetora.

iii) e iv), prova que F é um Isomorfismo.

Com um procedimento análogo é possível provar que a associação:

$$\Phi : L(\mathbb{R}^n) \longrightarrow M_n(\mathbb{R})$$

$$T \mapsto [T]_{can}$$

onde $[T]_{can}$ é a matriz associada na base canônica do $\mathbb{R}^n$

é um Isomorfismo.

2.9.2. Associação H: $Isom(\mathbb{R}^n) \longrightarrow GL_n(\mathbb{R})$

$$T \mapsto [T]_{can}$$

Não é um Isomorfismo, de fato:

$Isom(\mathbb{R}^n)$ e $GL_n(\mathbb{R})$ não são espaços vetoriais, pois, uma das propriedades de espaço vetorial é a existência do elemento neutro da adição, assim, a Transformação Linear nula não pertence a $Isom(\mathbb{R}^n)$ e a matriz nula não pertence a $GL_n(\mathbb{R})$.

Logo, H é apenas uma função.

2.9.3. Associação $\lambda: L(\mathbb{R}^3) \longrightarrow M_3(\mathbb{R})$

$$T \mapsto [T^t]_{can}$$

Onde $[T^t]_{can}$ é a matriz transposta associada na base canônica do $\mathbb{R}^3$.

Consideremos as Transformações Lineares J e L no $\mathbb{R}^3$, e suas respectivas matrizes associadas na base canônica do $\mathbb{R}^3$:

$$[J] = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} = A \qquad \text{e}$$

$$[L] = \begin{pmatrix} b_{11} & b_{12} & b_{13} \\ b_{21} & b_{22} & b_{23} \\ b_{31} & b_{32} & b_{33} \end{pmatrix} = B$$

Logo,

$$\lambda(J) = \begin{pmatrix} a_{11} & a_{21} & a_{31} \\ a_{12} & a_{22} & a_{32} \\ a_{13} & a_{23} & a_{33} \end{pmatrix} = A^t \qquad \text{e}$$

$$\lambda(\,L\,) = \begin{pmatrix} b_{11} & b_{21} & b_{31} \\ b_{12} & b_{22} & b_{32} \\ b_{13} & b_{23} & b_{33} \end{pmatrix} = B^t$$

i) $\lambda(\,J\,) + \lambda(\,L\,) = A^t + B^t = (A + B)^t = \lambda(\,J + L\,)$

ii) $\lambda(\alpha J\,) = (\alpha A^t) = \alpha(\,A^t\,) = \alpha.\,\lambda(\,J\,)$

iii) Ker(λ) = { U ∈ L(R^3) / $\lambda(\,U\,) = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ }

U(1, 0, 0) = 0.(1, 0, 0) + 0.(0, 1, 0) + 0.(1, 0, 0) = (0, 0, 0)
U(0, 1, 0) = 0.(1, 0, 0) + 0.(0, 1, 0) + 0.(1, 0, 0) = (0, 0, 0)
U(0, 0, 1) = 0.(1, 0, 0) + 0.(0, 1, 0) + 0.(1, 0, 0) = (0, 0, 0) e,

U(x, y, z) = U(x.(1, 0, 0) + y.(0, 1, 0) + z.(0, 0, 1)) = (0, 0, 0)
U(x, y, z) = x.U(1, 0, 0) + y.U(0, 1, 0) + z.U(0, 0, 1) = (0, 0, 0)
U(x, y, z) = x.(0, 0 ,0) + y.(0, 0, 0) + z.(0, 0, 0) = (0, 0, 0)
Logo, U será o operador linear nulo do $\mathbb{R}^3$.
Ker(λ) = (0x, 0y , 0z) assim, λ é injetora.

iv) Dada A = $\begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix}$ ∈ $M_3(\mathbb{R})$, existe U ∈ L($\mathbb{R}^3$),tal que λ(U) = A, vejamos:

Como $(A^t)^t$ = A, temos:

Se, A^t = $\begin{pmatrix} a & d & g \\ b & e & h \\ c & f & i \end{pmatrix}$ = U, a associação λ é sobrejetora.

Com isso fica provado que λ é uma Transformação Linear Bijetora e, portanto um Isomorfismo. ■

3. ISOMORFISMO - UM EXEMPLO EM CRIPTOGRAFIA

3.1. Um passeio na história da criptografia.

O primeiro método para criptografia de dados surgiu mais ou menos há 4000 anos e durante toda a história da humanidade, pessoas e governos vêm trabalhando de diversas formas, para proteger suas comunicações através desses métodos de cifragem. Foram construídos modelos criptográficos cada vez mais complexos e eficazes. Novos métodos e novos algoritmos vêm sendo desenvolvidos e como conseqüência desse trabalho e da alta demanda de segurança, a criptografia tornou-se de fato parte integrante do mundo das Transferências de Informações.

Os métodos de criptografia começaram com mensagens esculpidas em madeiras ou pedras e passadas para as pessoas que tinham os meios necessários para decifrar as mensagens.

Mas, o primeiro registro de alguém que usou um mecanismo para cifrar dados, aconteceu no Egito em 2000 a.C. Nessa época, hieróglifos eram usados na decoração de túmulos (eles contavam histórias da vida dos faraós). Só que a intenção naquela época na verdade, não era de esconder as mensagens em si, mas sim de fazê-las parecerem mais nobres e majestosas.

Foi então que um método hebraico de criptografia utilizou o alfabeto invertido para cifrar as mensagens. Cada caractere da mensagem é substituído por outro do alfabeto invertido.

Vejam o exemplo abaixo:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A

Baseando-se no método acima a palavra **SEGURANÇA = HVTFIZMXZ**

Por volta de 400 a.C., os espartanos usavam um sistema de cifragem de informações onde era utilizada uma folha de papiro enrolada em um cilindro de madeira. A mensagem só poderia ser lida, se esse papiro fosse enrolado em um cilindro exatamente do mesmo diâmetro do cilindro onde a mensagem havia sido escrita originalmente.

Pouco depois, o Imperador Julio César desenvolveu um método chamado Caesar Cipher. Era um método simples de deslocamento das letras do alfabeto

(sistema mono alfabético), similar ao método hebraico. Tudo o que ele fez foi simplesmente deslocar o alfabeto em três posições. Aos nossos olhos, é obviamente um método muito simples pra ser efetivo, mas estamos falando de um alto nível de proteção de dados para aquela época.

No final do século XVIII, os sistemas de criptografia eram amplamente usados para as comunicações militares e ao longo de muitos anos, outros métodos de criptografia foram surgindo. Na segunda guerra mundial, dispositivos de cifragem simples de uso militar evoluíram bastante com a tecnologia eletromecânica (comunicação via telégrafo e rádio). Em 1918, Arthur Scherbius criou a máquina de cifragem mais famosa do mundo que se chamava Enigma, que foi usada pelo exército alemão. Pouco depois um grupo de criptógrafos poloneses quebrou o código e revelou aos britânicos os planos de ataque e movimentação das tropas alemãs.

A IBM (International Business Machines) também contribuiu e muito para o desenvolvimento das tecnologias de cifragem de dados. Em 1976 foi criado o DES que depois foi modificado pela Agência Nacional de Segurança dos Estados Unidos (NSA) dando origem ao DES (Data Encryption Standard). O mesmo governo americano depois criou o Clipper Chip para ser implantado em todos os sistemas de comunicação.

Em 1977 foi criado por Ron Rivest, Adi Shamir e Len Adleman nos laboratórios do MIT (Massachusetts Institute of Technology), o RSA (Rivest, Shamir and Adleman) que é um dos algoritmos criptográficos mais usados. Nele, números primos são utilizados da seguinte forma: dois números primos são multiplicados para se obter um terceiro valor. Porém, descobrir os dois primeiros números a partir do terceiro (ou seja, fazer uma fatoração) é muito trabalhoso. Se dois números primos grandes (realmente grandes) forem usados na multiplicação, será necessário usar muito processamento para descobrí-los, tornando essa tarefa praticamente inviável.

3.2. Apresentando a criptografia de dados.

A criptografia, nada mais é que um método de armazenar e transmitir dados de uma forma que somente às pessoas autorizadas como, por exemplo, os destinatários, possam ler e processar. É considerada a ciência de proteção da informação através da codificação em um formato ilegível. Contudo, a maioria dos algoritmos (na realidade todos) podem ser quebrados e a informação revelada se o atacante tiver tempo e recursos suficientes. Com isso, chegamos então às duas conclusões muito importantes:

i) Não existe um método de criptografia que não possa ser quebrado.

ii) O real objetivo da criptografia é fazer com que conseguir acesso à informação, seja tão trabalhoso e leve tanto tempo, que o atacante sinta-se desestimulado e desista.

3.3. Etimologia da palavra criptografia.

A palavra ”criptografia” é composta dos termos gregos ”kryptos”(secreto, oculto, não inteligível) e ”grapho”(escrita, escrever).

3.4. Terminologias aplicadas em criptografia.

a) Mensagem ou texto: é o pedaço da informação que se pretende proteger.
b) Texto Puro: é o texto original antes de ser cifrado.
c) Encriptação ou Cifragem: é ação de cifrar os dados usando qualquer seja o sistema de criptografia. É quando o texto puro pode assumir uma nova forma que é o texto cifrado.
d) Remetente: é quem envia a mensagem cifrada.
e) Destinatário: usará um processo chamando Decifragem ou Desencriptação (o ato de desencriptar ou desencriptografar).
f) **Algoritmo**: é o conjunto de regras que definem como são feitas as cifragem e decifragem. Na maioria das vezes é de poder público. Neste caso a parte secreta do sistema é a chave. Neste trabalho os algoritmos utilizados serão **Isomorfismos**.
g) Chave: é um valor composto de uma grande seqüência de bits randômicos. E é a informação que o remetente e o destinatário possuem.
h) O Espaço Chave: é o conjunto de valores usados para gerar a chave. Quanto maior o Espaço Chave, mais randômicas são as chaves.
i) Meio ou Local não seguro: é onde a mensagem transita ou onde é armazenada.
j) 3º Personagem: é o inimigo. Que pode ser passivo ou ativo.
k) O inimigo passivo: ganha conhecimento e não interfere somente intercepta a mensagem.
l) O inimigo ativo: interfere no processo de comunicação com interrupção, modificação, fabricação de mensagens falsas, impersonificação (disfarce), repetição e negação do serviço.

3.5. Exemplos da aplicação de Isomorfismo em Criptografia.

O Isomorfismo pode ser definido aqui, de uma maneira simplificada como um dicionário que permite traduzir uma sentença de um idioma, numa sentença com o mesmo significado, em outro idioma. Mas simplesmente, dizer que uma dada sentença num idioma pode ser expressa em outro é pouco significativo, é necessário o dicionário para efetuar a tradução. Da mesma forma pode ter pouco significado saber que dois espaços vetoriais são isomorfos, o objeto de interesse pode ser o próprio isomorfismo. A aplicação desse conceito de Isomorfismo como algoritmo criptográfico, embora de maneira simplificada em comparação a outros trabalhos

neste gênero, revela a didática do Isomorfismo que desempenha papel fundamental na representação do mundo.

3.5.1. (Operador Linear no $\mathbb{R}^2$). Imaginemos que a mensagem a seguir tenha grande valor de especulação, e que seu remetente e seu destinatário sejam conhecidos:

O texto puro é: C-O-N-V-E-N-I-O-U-N-I-V-I-M-A-U-F-S-C-M-T-M

Tabela de randomização:

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**
6	14	-2	7	-8	-6	13	-7	2	-4	-3	3	10
N	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
15	1	-9	8	-5	11	0	4	9	-1	12	21	5

A tabela acima é o que chamamos de randômizar, cada letra está relacionada com um número na linha logo abaixo.

Vamos fazer a primeira cifragem:

-2_1_15_9_-8_15_2_1_4_15_2_9_2_10_6_4_-6_11_-2_10_0_10

O algoritmo que usaremos é o Operador Linear do $\mathbb{R}^2$:

$$T(x, y) = (3x - y, 2x + y)$$

Primeiramente, vamos confirmar que T é um Isomorfismo, através de sua matriz associada na base canônica do $\mathbb{R}^2$, é inversível, ou seja, se seu determinante é diferente de zero:

$$[T]_{can} = \begin{pmatrix} 3 & -1 \\ 2 & 1 \end{pmatrix} \text{ e } \det[T] = 3 - (-2) = 5,$$

realmente, $[T]_{can}$ é inversível, logo, T é um Isomorfismo.

Tomando de dois em dois números, e fazendo as contas:

T (-2, 1) = (3.(-2) – 1, 2(-2) + 1) = (-7, -3)

T (15, 9) = (3.(15) – 9, 2(15) + 9) = (36, 39)

T (-8, 15) = (3.(-8) – 15, 2(-8) + 15) = (-39, -1)

T (2, 1) = (3.(2) – 1, 2(2) + 1) = (5, 5)

T (4, 15) = (3.(4) – 15, 2(4) + 15) = (-3, 23)

T (2, 9) = (3.(2) – 9, 2(2) + 9) = (-3, 13)

T (2, 10) = (3.(2) – 10, 2(2) + 10) = (-4, 14)

T (6, 4) = (3.(6) – 4, 2(6) + 4) = (14, 16)

T (-6, 11) = (3.(-6) – 11, 2(-6) + 11) = (-29, -1)

T (-2, 10) = (3.(-2) – 10, 2(-2) + 10) = (-16, 6)

T (0, 10) = (3.(0) – 10, 2(0) + 10) = (-10, 10)

Aqui fazemos a segunda cifragem:

-7_-3_36_39_-39_-1_5_5_-3_23_-3_13_-4_14_14_16_-29_-1_-16_6_-10_10

Este é o texto recebido pelo destinatário.

Cabe ao destinatário decifrar, o texto recebido.

São de domínio comum ao remetente e do destinatário, a tabela de randomização que faz parte do algoritmo criptográfico.

Neste caso T (x, y) = (3x – y, 2x + y), assim o destinatário deverá encontrar o Isomorfismo Inverso de T, aqui usaremos o processo prático via escalonamento de matrizes, para obtermos a inversa de $[T]_{can}$ e assim chegarmos a T^{-1}:

$$\begin{pmatrix} 3 & -1 & 1 & 0 \\ 2 & 1 & 0 & 1 \end{pmatrix} \sim 1/3\ L_1 \longrightarrow L_1 \sim \begin{pmatrix} 1 & -1/3 & 1/3 & 0 \\ 2 & 1 & 0 & 1 \end{pmatrix} \sim 1/2\ L_2 \longrightarrow L_2 \sim$$

$$\begin{pmatrix} 1 & -1/3 & 1/3 & 0 \\ 1 & 1/2 & 0 & 1/2 \end{pmatrix} \sim L_2 - L_1 \longrightarrow L_1 \sim \begin{pmatrix} 1 & -1/3 & 1/3 & 0 \\ 0 & 5/6 & -1/3 & 1/2 \end{pmatrix} \sim 6/5\ L_2 \longrightarrow L_2 \sim$$

$$\begin{pmatrix} 1 & -1/3 & 1/3 & 0 \\ 0 & 1 & -2/5 & 3/5 \end{pmatrix} \sim L_1 + 1/3\ L_2 \sim \begin{pmatrix} 1 & 0 & 1/5 & 1/5 \\ 0 & 1 & -2/5 & 3/5 \end{pmatrix}$$

então, $[T^{-1}] = 1/5.\begin{pmatrix} 1 & 1 \\ -2 & 3 \end{pmatrix}$ e

assim, $1/5.\begin{pmatrix} 1 & 1 \\ -2 & 3 \end{pmatrix}.\begin{pmatrix} x \\ y \end{pmatrix} = 1/5.(x + y \quad 3y - 2x)$

Logo, $T^{-1}(x, y) = (1/5(x + y), 1/5(3y – 2x))$

$T^{-1}(-7, -3) = (1/5(-7-3), 1/5(3[-3] – 2[-7])) = (-2, 1)$

$T^{-1}(36, 39) = (1/5(36+39), 1/5(3[39] – 2[36])) = (15, 9)$

$T^{-1}(-39, -1) = ((1/5(-39-1), 1/5(3[-1] – 2[-39])) = (-8, 15)$

$T^{-1}(5, 5) = (1/5(5 + 5), 1/5(3[5] – 2[5])) = (2, 1)$

$T^{-1}(-3, 23) = (1/5(-3+23), 1/5(3[23] – 2[-3])) = (4, 15)$

$T^{-1}(-3, 13) = (1/5(-3+13), 1/5(3[13] – 2[-3])) = (2, 9)$

$T^{-1}(-4, 14) = (1/5(-4+14), 1/5(3[14] – 2[-4])) = (2, 10)$

$T^{-1}(14, 16) = (1/5(14+16), 1/5(3[16] – 2[14])) = (6, 4)$

$T^{-1}(-29, -1) = ((1/5(-29-1), 1/5(3[-1] – 2[-29])) = (-6, 11)$

$T^{-1}(-16, 6) = (1/5(-16+6), 1/5(3[6] – 2[-16])) = (-2, 10)$

$T^{-1}(-10, 10) = (1/5(-10+10), 1/5(3[10] – 2[-10])) = (0, 10)$

Aplicando a tabela de randomização:

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**
6	14	-2	7	-8	-6	13	-7	2	-4	-3	3	10
N	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
15	1	-9	8	-5	11	0	4	9	-1	12	21	5

e finalmente, o texto desencriptografado:

CONVENIO UNIVIMA UFSC MTM

Observe que nosso algoritmo, “mistura” de duas em duas letras.

3.5.2. Nota. Random é palavra inglesa, de origem francesa, usada na expressão at random, cujo sentido é "ao acaso", "a esmo", "sem seleção ou critério de escolha". De random, em inglês, deriva o verbo randomizar, o equivalente poderia ser aleatorizar.

3.5.3. (Operador Linear no $\mathbb{R}^2$). É comum a grande especulação nas bolsas de valores mundiais, uma informação pode significar a ascensão ou a total falência de investidores, vejamos uma suposta informação desse âmbito:

Texto Puro: preço-ação-bb-sobe-fevereiro

Tabela de randomização:

p	**r**	**e**	**ç**	**o**	**a**
5	11	9	3	8	7
ç	**a**	**o**	**b**	**b**	**s**
3	7	8	1	1	4
o	**b**	**e**	**f**	**e**	**v**
8	1	9	2	9	6
e	**r**	**e**	**i**	**r**	**o**
9	11	9	10	11	8

Cifragem(I) : 5_11_9_3_8_7_3_7_8_1_1_4_8_1_9_2_9_6_9_11_9_10_11_8

1º algoritmo: no lugar da Transformação Linear podemos usar sua matriz associada da seguinte maneira:

$$[T] = \begin{pmatrix} 1 & 2 \\ 1 & -1 \end{pmatrix}$$

como det [T] = (-1) – (2) = -3, garante que [T] é inversível.

Tomando dois a dois números, e fazendo as contas:

$$\begin{pmatrix} 1 & 2 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 5 \\ 11 \end{pmatrix} = \begin{pmatrix} 27 \\ -6 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 9 \\ 3 \end{pmatrix} = \begin{pmatrix} 15 \\ 6 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 8 \\ 7 \end{pmatrix} = \begin{pmatrix} 22 \\ 1 \end{pmatrix}$$

$$\begin{pmatrix}1 & 2\\ 1 & -1\end{pmatrix}\begin{pmatrix}3\\ 7\end{pmatrix}=\begin{pmatrix}17\\ -4\end{pmatrix}$$
$$\begin{pmatrix}1 & 2\\ 1 & -1\end{pmatrix}\begin{pmatrix}8\\ 1\end{pmatrix}=\begin{pmatrix}10\\ 7\end{pmatrix}$$
$$\begin{pmatrix}1 & 2\\ 1 & -1\end{pmatrix}\begin{pmatrix}1\\ 4\end{pmatrix}=\begin{pmatrix}9\\ -3\end{pmatrix}$$
$$\begin{pmatrix}1 & 2\\ 1 & -1\end{pmatrix}\begin{pmatrix}8\\ 1\end{pmatrix}=\begin{pmatrix}10\\ 7\end{pmatrix}$$
$$\begin{pmatrix}1 & 2\\ 1 & -1\end{pmatrix}\begin{pmatrix}9\\ 2\end{pmatrix}=\begin{pmatrix}13\\ 7\end{pmatrix}$$
$$\begin{pmatrix}1 & 2\\ 1 & -1\end{pmatrix}\begin{pmatrix}9\\ 6\end{pmatrix}=\begin{pmatrix}21\\ 3\end{pmatrix}$$
$$\begin{pmatrix}1 & 2\\ 1 & -1\end{pmatrix}\begin{pmatrix}9\\ 11\end{pmatrix}=\begin{pmatrix}31\\ -2\end{pmatrix}$$
$$\begin{pmatrix}1 & 2\\ 1 & -1\end{pmatrix}\begin{pmatrix}9\\ 10\end{pmatrix}=\begin{pmatrix}29\\ -1\end{pmatrix}$$
$$\begin{pmatrix}1 & 2\\ 1 & -1\end{pmatrix}\begin{pmatrix}11\\ 8\end{pmatrix}=\begin{pmatrix}27\\ 3\end{pmatrix}$$

Cifragem(II):

27_-6_15_6_22_1_17_-4_10_7_9_-3_10_7_13_7_21_3_31_-2_29_-1_27_3

A Cifragem(II) será a mensagem recebida pelo destinatário; o qual conhecerá a Cifragem(I) e a matriz transformação inversa $[T^{-1}]$:

$$\left(\begin{array}{cc|cc}1 & 2 & 1 & 0\\ 1 & -1 & 0 & 1\end{array}\right)\sim L_2 - L_1 \mapsto L_2 \sim \left(\begin{array}{cc|cc}1 & 2 & 1 & 0\\ 0 & -3 & -1 & 1\end{array}\right)$$
$$\left(\begin{array}{cc|cc}1 & 2 & 1 & 0\\ 0 & -3 & -1 & 1\end{array}\right)\sim -1/3\ L_2 \mapsto L_2 \sim \left(\begin{array}{cc|cc}1 & 2 & 1 & 0\\ 0 & 1 & 1/3 & 1/3\end{array}\right)$$
$$\left(\begin{array}{cc|cc}1 & 2 & 1 & 0\\ 0 & 1 & 1/3 & 1/3\end{array}\right)\sim L_1 - 2L_2 \mapsto L_1 \sim \left(\begin{array}{cc|cc}1 & 0 & 1/3 & 2/3\\ 0 & 1 & 1/3 & 1/3\end{array}\right)$$

2º algoritmo: será a matriz Transformação Linear:

$$[T^{-1}]=\begin{pmatrix}1/3 & 2/3\\ 1/3 & -1/3\end{pmatrix}$$

Decifragem (I):

$$\begin{pmatrix}1/3 & 2/3\\ 1/3 & -1/3\end{pmatrix}\begin{pmatrix}27\\ -6\end{pmatrix}=\begin{pmatrix}5\\ 11\end{pmatrix}$$
$$\begin{pmatrix}1/3 & 2/3\\ 1/3 & -1/3\end{pmatrix}\begin{pmatrix}15\\ 6\end{pmatrix}=\begin{pmatrix}9\\ 3\end{pmatrix}$$
$$\begin{pmatrix}1/3 & 2/3\\ 1/3 & -1/3\end{pmatrix}\begin{pmatrix}22\\ 1\end{pmatrix}=\begin{pmatrix}8\\ 7\end{pmatrix}$$
$$\begin{pmatrix}1/3 & 2/3\\ 1/3 & -1/3\end{pmatrix}\begin{pmatrix}17\\ -4\end{pmatrix}=\begin{pmatrix}3\\ 7\end{pmatrix}$$
$$\begin{pmatrix}1/3 & 2/3\\ 1/3 & -1/3\end{pmatrix}\begin{pmatrix}10\\ 7\end{pmatrix}=\begin{pmatrix}8\\ 1\end{pmatrix}$$
$$\begin{pmatrix}1/3 & 2/3\\ 1/3 & -1/3\end{pmatrix}\begin{pmatrix}9\\ -3\end{pmatrix}=\begin{pmatrix}1\\ 4\end{pmatrix}$$

$$\begin{pmatrix} 1/3 & 2/3 \\ 1/3 & -1/3 \end{pmatrix}\begin{pmatrix} 10 \\ 7 \end{pmatrix} = \begin{pmatrix} 8 \\ 1 \end{pmatrix}$$

$$\begin{pmatrix} 1/3 & 2/3 \\ 1/3 & -1/3 \end{pmatrix}\begin{pmatrix} 13 \\ 7 \end{pmatrix} = \begin{pmatrix} 9 \\ 2 \end{pmatrix}$$

$$\begin{pmatrix} 1/3 & 2/3 \\ 1/3 & -1/3 \end{pmatrix}\begin{pmatrix} 21 \\ 3 \end{pmatrix} = \begin{pmatrix} 9 \\ 6 \end{pmatrix}$$

$$\begin{pmatrix} 1/3 & 2/3 \\ 1/3 & -1/3 \end{pmatrix}\begin{pmatrix} 31 \\ -2 \end{pmatrix} = \begin{pmatrix} 9 \\ 11 \end{pmatrix}$$

$$\begin{pmatrix} 1/3 & 2/3 \\ 1/3 & -1/3 \end{pmatrix}\begin{pmatrix} 29 \\ -1 \end{pmatrix} = \begin{pmatrix} 9 \\ 10 \end{pmatrix}$$

$$\begin{pmatrix} 1/3 & 2/3 \\ 1/3 & -1/3 \end{pmatrix}\begin{pmatrix} 27 \\ 3 \end{pmatrix} = \begin{pmatrix} 11 \\ 8 \end{pmatrix}$$

Decifragem (II): Utiliza-se a tabela da cifragem (I)

Decifragem final: preço ação BB sobe fevereiro.

Observamos que os algoritmos utilizados na cifragem e decifragem é um código de criptografia baseado em um Isomorfismo.

3.5.4. (Operador Linear no $\mathbb{R}^3$). Ocultar uma informação já conhecida, no mundo das especulações, pode valorizar essa informação:

Texto puro: Isomorfismo de Operadores Lineares um exemplo em criptografia.

Tabela de randomização:

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**
-4	15	7	2	4	-1	9	-9	3	-10	17	6	1
N	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
-5	5	-3	12	0	-2	8	-6	18	14	-8	13	10

Obtemos assim a 1ª cifragem:

3_-2_5_1_5_0_-1_3_-2_

1_5_2_4_5_-3_4_0_-4_

2_5_0_4_-2_6_3_-5_4_

-4_0_4_-2_-6_1_4_-8_4_

1_-3_6_5_4_1_7_0_3_

-3_8_5_9_0_-4_-1_3_-4

Usaremos para a 2ª cifragem o Operador Linear do $\mathbb{R}^3$:

$$T(x, y, z) = (2x + y, 2x + y + z, x + z),$$

Determinando a representação matricial de T, na base canônica do $\mathbb{R}^3$, obtemos:

$$[T]_{can} = \begin{pmatrix} 2 & 1 & 0 \\ 2 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}$$

Primeiramente vamos garantir que T é um Isomorfismo:

$$[T]_{can} = \begin{pmatrix} 2 & 1 & 0 \\ 2 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} \text{ e } \det [T] = (2 + 1 + 0) – (0 + 0 + 2) = 1$$

como det [T] ≠ 0, [T] é uma matriz inversível e T é um Isomorfismo.

Tomando de três a três números, considerando o vetor associado a matriz produto e fazendo as contas:

$\begin{pmatrix} 2 & 1 & 0 \\ 2 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}.\begin{pmatrix} 3 \\ -2 \\ 5 \end{pmatrix}$ = (2.3 + 1.(-2) + 0.5, 2.3 + 1.(-2) + 1.5, 1.3 + 0.(-2) + 1.5) = (4, 9, 8)

$\begin{pmatrix} 2 & 1 & 0 \\ 2 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}.\begin{pmatrix} 1 \\ 5 \\ 0 \end{pmatrix}$ = (2.1 + 1.5 + 0.0, 2.1 + 1.5 + 1.0, 1.1 + 0.5 + 1.0) = (7, 7, 1)

$\begin{pmatrix} 2 & 1 & 0 \\ 2 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}.\begin{pmatrix} -1 \\ 3 \\ -2 \end{pmatrix}$=(2.(-1)+1.3 +0.(-2), 2.(-1)+1.3 + 1.(-2), 1.(-1)+0.3 + 1.(-2)) = (1, -1, -3)

$\begin{pmatrix} 2 & 1 & 0 \\ 2 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}.\begin{pmatrix} 1 \\ 5 \\ 2 \end{pmatrix}$ = (2.1 + 1.5 + 0.2, 2.1 + 1.5 + 1.2, 1.1 + 0.5 + 1.2) = (7, 9, 3)

$\begin{pmatrix} 2 & 1 & 0 \\ 2 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}.\begin{pmatrix} 4 \\ 5 \\ -3 \end{pmatrix}$ = (2.4 + 1.5 + 0.(-3), 2.4 + 1.5 + 1.(-3), 1.4 + 0.5 + 1.(-3)) = (13, 10, 1)

$\begin{pmatrix} 2 & 1 & 0 \\ 2 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}.\begin{pmatrix} 4 \\ 0 \\ -4 \end{pmatrix}$ = (2.4 + 1.0 + 0.(-4), 2.4 + 1.0 + 1.(-4), 1.4 + 0.0 + 1.(-4)) = (8, 4, 0)

$\begin{pmatrix} 2 & 1 & 0 \\ 2 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}.\begin{pmatrix} 2 \\ 5 \\ 0 \end{pmatrix}$ = (2.2 + 1.5 + 0.0, 2.2 + 1.5 + 1.0, 1.2 + 0.5 + 1.0) = (9, 9, 2)

$\begin{pmatrix} 2 & 1 & 0 \\ 2 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}.\begin{pmatrix} 4 \\ -2 \\ 6 \end{pmatrix}$ = (2.4 + 1.(-2) + 0.6, 2.4 + 1.(-2) + 1.6, 1.4 + 0.(-2) + 1.6) = (6, 12, 10)

$\begin{pmatrix} 2 & 1 & 0 \\ 2 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}.\begin{pmatrix} 3 \\ -5 \\ 4 \end{pmatrix}$ = (2.3 + 1.(-5) + 0.4, 2.3 + 1.(-5) + 1.4, 1.3 + 0.(-5) + 1.4) = (1, 5, 7)

$\begin{pmatrix} 2 & 1 & 0 \\ 2 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}.\begin{pmatrix} -4 \\ 0 \\ 4 \end{pmatrix}$ = (2.(-4) + 1.0 + 0.4, 2.(-4) + 1.0 + 1.4, 1.(-4) + 0.0 + 1.4) = (-8, -4, 0)

$\begin{pmatrix}2&1&0\\2&1&1\\1&0&1\end{pmatrix}.\begin{pmatrix}-2\\-6\\1\end{pmatrix}$=(2.(-2)+1.(-6)+0.1, 2.(-2)+1.(-6)+1.1, 1.(-2)+0.(-6)+1.1) = (-10, -9, -1)

$\begin{pmatrix}2&1&0\\2&1&1\\1&0&1\end{pmatrix}.\begin{pmatrix}4\\-8\\4\end{pmatrix}$ = (2.4 + 1.(-8) + 0.4, 2.4 + 1.(-8) + 1.4, 1.4 + 0.(-8) + 1.4) = (0, 4, 8)

$\begin{pmatrix}2&1&0\\2&1&1\\1&0&1\end{pmatrix}.\begin{pmatrix}1\\-3\\6\end{pmatrix}$ = (2.1 + 1.(-3) + 0.6, 2.1 + 1.(-3) + 1.6, 1.1 + 0.(-3) + 1.6) = (-1, 5, 7)

$\begin{pmatrix}2&1&0\\2&1&1\\1&0&1\end{pmatrix}.\begin{pmatrix}5\\4\\1\end{pmatrix}$ = (2.5 + 1.4 + 0.1, 2.5 + 1.4 + 1.1, 1.5 + 0.4 + 1.1) = (14, 15, 6)

$\begin{pmatrix}2&1&0\\2&1&1\\1&0&1\end{pmatrix}.\begin{pmatrix}7\\0\\3\end{pmatrix}$ = (2.7 + 1.0 + 0.3, 2.7 + 1.0 + 1.3, 1.7 + 0.0 + 1.3) = (14, 17, 10)

$\begin{pmatrix}2&1&0\\2&1&1\\1&0&1\end{pmatrix}.\begin{pmatrix}-3\\8\\5\end{pmatrix}$ = (2.(-3) + 1.8 + 0.5, 2.(-3) + 1.8 + 1.5, 1.(-3) + 0.8 + 1.5) = (2, 7, 2)

$\begin{pmatrix}2&1&0\\2&1&1\\1&0&1\end{pmatrix}.\begin{pmatrix}9\\0\\-4\end{pmatrix}$ = (2.9 + 1.0 + 0.(-4), 2.9 + 1.0 + 1.(-4), 1.9 + 0.0 + 1.(-4)) = (18, 14, 5)

$\begin{pmatrix}2&1&0\\2&1&1\\1&0&1\end{pmatrix}.\begin{pmatrix}-1\\3\\-4\end{pmatrix}$ =(2.(-1)+1.3 +0.(-4), 2.(-1)+1.3 + 1.(-4), 1.(-1)+0.3 +1.(-4)) = (1, -3, -5)

Obtemos assim a 2ª cifragem:

4_9_8_7_7_1_1_-1_-3_

7_9_3_13_10_1_8_4_0_

9_9_2_6_12_10_1_5_7_

-8_-4_0_-10_-9_-1_0_4_8_

-1_5_7_14_15_6_14_17_10_

2_7_2_18_14_5_1_-3_-5

O conjugado de números acima é o texto criptografado que o destinatário receberá.

Observe que a ordem que os números aparecem na mensagem cifrada, que circulará ou ficará arquivada, deve ser sempre a mesma, pois a troca da ordem causará interferência na sua decifragem.

Vamos imaginar um pequeno ataque de um inimigo, o qual interceptou a mensagem recebida pelo destinatário e conseguiu se apossar da tabela de randomização:

A mensagem recebida pelo inimigo seria:

E_G_T_C_C_M_M_F_P_

C_G_I_Y_Z_M_T_E_R_

G_G_D_L_Q_Z_M_O_C_

X_A_R_J_H_F_R_E_T_

F_O_C_W_B_L_W_K_Z_

D_C_D_V_W_O_M_P_N

O que já traria um pouco de dificuldade para tal inimigo decifrar completamente a mensagem, e chegar ao texto puro.

O destinatário tem posse do algoritmo T(x, y, z) = (2x + y, 2x + y + z, x + z), que é um Operador Linear, através de sua representação matricial chegará a $[T^{-1}]$ da seguinte maneira:

$$\left(\begin{array}{ccc|ccc} 2 & 1 & 0 & 1 & 0 & 0 \\ 2 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{array}\right) \sim L2 - L1 \longrightarrow L2 \sim \left(\begin{array}{ccc|ccc} 2 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & -1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{array}\right)$$

$$\left(\begin{array}{ccc|ccc} 2 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & -1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{array}\right) \sim L2 \longrightarrow L3 \text{ e } L3 \longrightarrow L2 \sim \left(\begin{array}{ccc|ccc} 2 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & -1 & 1 & 0 \end{array}\right)$$

$$\left(\begin{array}{ccc|ccc} 2 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & -1 & 1 & 0 \end{array}\right) \sim L2 - L3 \longrightarrow L2 \sim \left(\begin{array}{ccc|ccc} 2 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & -1 & 1 \\ 0 & 0 & 1 & -1 & 1 & 0 \end{array}\right)$$

$$\left(\begin{array}{ccc|ccc} 2 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & -1 & 1 \\ 0 & 0 & 1 & -1 & 1 & 0 \end{array}\right) \sim L1 \longrightarrow L2 \text{ e } L2 \longrightarrow L1 \sim \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & -1 & 1 \\ 2 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & -1 & 1 & 0 \end{array}\right)$$

$$\left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & -1 & 1 \\ 2 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & -1 & 1 & 0 \end{array}\right) \sim L2 - 2L1 \longrightarrow L2 \sim \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & -1 & 1 \\ 0 & 1 & 0 & -1 & 2 & -2 \\ 0 & 0 & 1 & -1 & 1 & 0 \end{array}\right)$$

Então $[T^{-1}] = \begin{pmatrix} 1 & -1 & 1 \\ -1 & 2 & -2 \\ -1 & 1 & 0 \end{pmatrix}$ é a matriz associada do Operador Linear T^{-1} na base canônica do $\mathbb{R}^3$:

Assim, $\begin{pmatrix} 1 & -1 & 1 \\ -1 & 2 & -2 \\ -1 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} x - y + z \\ -x + 2y - 2z \\ -x + y \end{pmatrix}$

Logo, $T^{-1}(x, y, z) = (x – y + z, -x + 2y -2z, -x + y)$

De posse de T^{-1} o destinatário decifrará o texto criptografado.

3.5.5. (Operador Linear no $\mathbb{R}^4$, sua Matriz Associada na base canônica do $\mathbb{R}^4$ e a Associação λ para o $\mathbb{R}^4$). Senhas de acesso também muito são visadas por terceiros, vamos a um exemplo de quatro letras e quatro algarismos:

Senha original: FASL 2 1 0 5

Tabela de randomização:

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**
-1	10	6	-8	13	2	-12	-5	-11
J	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**
12	-7	3	17	-14	19	18	11	-15
S	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	**1**
1	15	-13	-18	16	-17	14	-16	-2
2	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**0**
5	-6	7	0	8	-10	4	-4	-3

1ª Cifragem: 2_-1_1_3_5_-2_-3_0_

Na 2ª cifragem usaremos o Operador Linear do $\mathbb{R}^4$:

T(x, y, z, w) = (x + 2z – w, 2x + y + 3z – 2w, 2z + 3w, x – y + 2w)

Com sua representação matricial na base canônica do $\mathbb{R}^4$:

$$[T]_{can} = \begin{pmatrix} 1 & 0 & 2 & -1 \\ 2 & 1 & 3 & -2 \\ 0 & 0 & 2 & 3 \\ 1 & -1 & 0 & 2 \end{pmatrix}$$

Tomando de quatro em quatro números, considerando o vetor associado a matriz produto, faremos a 2ª cifragem:

$$[T]_{can}.\begin{pmatrix} 2 \\ -1 \\ 1 \\ 3 \end{pmatrix} = (1, 0, 11, 9)$$

$$[T]_{can}.\begin{pmatrix} 5 \\ -2 \\ -3 \\ 0 \end{pmatrix} = (-1, -1, -6, 7)$$

2ª Cifragem: 1_0_11_9_-1_-1_-6_7

Para a 3ª cifragem, nos beneficiaremos da associação λ da seção **2.10.3.** no $\mathbb{R}^4$:

$$\lambda: L(\mathbb{R}^4) \longrightarrow M_4(\mathbb{R})$$

$$T \mapsto [T^t]_{can}$$

Onde $[T^t]_{can}$ é a matriz transposta associada na base canônica do $\mathbb{R}^4$.

Da qual obtemos a representação matricial:

$$[\lambda(T)] = \begin{pmatrix} 1 & 2 & 0 & 1 \\ 0 & 1 & 0 & -1 \\ 2 & 3 & 2 & 0 \\ -1 & -2 & 3 & 2 \end{pmatrix} = [T^t]$$

Assim, faremos a 3ª cifragem:

$$[T^t]_{can}.\begin{pmatrix} 1 \\ 0 \\ 11 \\ 9 \end{pmatrix} = (10, -9, 24, 50)$$

$$[T^t]_{can}.\begin{pmatrix} -1 \\ -1 \\ -6 \\ 7 \end{pmatrix} = (4, -8, -17, -1)$$

A senha circulará no sistema da seguinte forma:

10_-9_24_50_4_-8_-17_-1

Como decifrar, se foram usados dois Operadores Lineares, no algoritmo criptográfico?

Encontraremos primeiramente a inversa de $[T]_{can}$, através do método prático de escalonamento de matrizes:

$$\left(\begin{array}{cccc|cccc} 1 & 0 & 2 & -1 & 1 & 0 & 0 & 0 \\ 2 & 1 & 3 & -2 & 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 3 & 0 & 0 & 1 & 0 \\ 1 & -1 & 0 & 2 & 0 & 0 & 0 & 1 \end{array}\right) \sim L_2 - 2L_1 \longrightarrow L_2 \sim$$

$$\left(\begin{array}{cccc|cccc} 1 & 0 & 2 & -1 & 1 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 & -2 & 1 & 0 & 0 \\ 0 & 0 & 2 & 3 & 0 & 0 & 1 & 0 \\ 1 & -1 & 0 & 2 & 0 & 0 & 0 & 1 \end{array}\right) \sim L_4 - L_1 \longrightarrow L_4 \sim$$

$$\left(\begin{array}{cccc|cccc} 1 & 0 & 2 & -1 & 1 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 & -2 & 1 & 0 & 0 \\ 0 & 0 & 2 & 3 & 0 & 0 & 1 & 0 \\ 0 & -1 & -2 & 3 & -1 & 0 & 0 & 1 \end{array}\right) \sim L_4 + L_2 \longrightarrow L_4 \sim$$

$$\left(\begin{array}{cccc|cccc} 1 & 0 & 2 & -1 & 1 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 & -2 & 1 & 0 & 0 \\ 0 & 0 & 2 & 3 & 0 & 0 & 1 & 0 \\ 0 & 0 & -3 & 3 & -3 & 1 & 0 & 1 \end{array}\right) \sim 1/2L_3 \longrightarrow L_3 \sim$$

$$\left(\begin{array}{cccc|cccc} 1 & 0 & 2 & -1 & 1 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 & -2 & 1 & 0 & 0 \\ 0 & 0 & 1 & 3/2 & 0 & 0 & 1/2 & 0 \\ 0 & 0 & -3 & 3 & -3 & 1 & 0 & 1 \end{array}\right) \sim -1/3L_4 \longrightarrow L_4 \sim$$

$$\left(\begin{array}{cccc|cccc} 1 & 0 & 2 & -1 & 1 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 & -2 & 1 & 0 & 0 \\ 0 & 0 & 1 & 3/2 & 0 & 0 & 1/2 & 0 \\ 0 & 0 & 1 & -1 & 1 & -1/3 & 0 & -1/3 \end{array}\right) \sim L_4 - L_3 \longrightarrow L_4 \sim$$

$$\left(\begin{array}{cccc|cccc} 1 & 0 & 2 & -1 & 1 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 & -2 & 1 & 0 & 0 \\ 0 & 0 & 1 & 3/2 & 0 & 0 & 1/2 & 0 \\ 0 & 0 & 0 & -5/2 & 1 & -1/3 & -1/2 & -1/3 \end{array}\right) \sim -2/5L_4 \longrightarrow L_4 \sim$$

$$\left(\begin{array}{cccc|cccc} 1 & 0 & 2 & -1 & 1 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 & -2 & 1 & 0 & 0 \\ 0 & 0 & 1 & 3/2 & 0 & 0 & 1/2 & 0 \\ 0 & 0 & 0 & 1 & -2/5 & 2/15 & 1/5 & 2/15 \end{array}\right) \sim L_3 - 3/2L_3 \longrightarrow L_4 \sim$$

$$\left(\begin{array}{cccc|cccc} 1 & 0 & 2 & -1 & 1 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 & -2 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 3/5 & -1/5 & 1/5 & -1/5 \\ 0 & 0 & 0 & 1 & -2/5 & 2/15 & 1/5 & 2/15 \end{array}\right) \sim L_2 + L_3 \longrightarrow L_2 \sim$$

$$\left(\begin{array}{cccc|cccc} 1 & 0 & 2 & -1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & -7/5 & 4/5 & 1/5 & -1/5 \\ 0 & 0 & 1 & 0 & 3/5 & -1/5 & 1/5 & -1/5 \\ 0 & 0 & 0 & 1 & -2/5 & 2/15 & 1/5 & 2/15 \end{array}\right) \sim L_1 - 2L_3 \longrightarrow L_1 \sim$$

$$\left(\begin{array}{cccc|cccc} 1 & 0 & 0 & -1 & -1/5 & 2/5 & -2/5 & 2/5 \\ 0 & 1 & 0 & 0 & -7/5 & 4/5 & 1/5 & -1/5 \\ 0 & 0 & 1 & 0 & 3/5 & -1/5 & 1/5 & -1/5 \\ 0 & 0 & 0 & 1 & -2/5 & 2/15 & 1/5 & 2/15 \end{array}\right) \sim L_1 + L_4 \longrightarrow L_1 \sim$$

$$\left(\begin{array}{cccc|cccc} 1 & 0 & 0 & -1 & -3/5 & 8/15 & -1/5 & 8/15 \\ 0 & 1 & 0 & 0 & -7/5 & 4/5 & 1/5 & -1/5 \\ 0 & 0 & 1 & 0 & 3/5 & -1/5 & 1/5 & -1/5 \\ 0 & 0 & 0 & 1 & -2/5 & 2/15 & 1/5 & 2/15 \end{array}\right)$$

Logo, $[T^{-1}] = \begin{pmatrix} -3/5 & 8/15 & -1/5 & 8/15 \\ -7/5 & 4/5 & 1/5 & -1/5 \\ 3/5 & -1/5 & 1/5 & -1/5 \\ -2/5 & 2/15 & 1/5 & 2/15 \end{pmatrix}$ ou,

$$[T^{-1}] = 1/15.\begin{pmatrix} -9 & 8 & -3 & 8 \\ -21 & 12 & 3 & -3 \\ 9 & -3 & 3 & -3 \\ -6 & 2 & 3 & 2 \end{pmatrix}$$

Calculada a inversa de $[T]_{can}$, pelas propriedades das matrizes transpostas encontradas na página 11 do livro [1] de nossa referência, concluímos que:

$$[T^{-1}]^t = [T^t]^{-1} = 1/15 \begin{pmatrix} -9 & -21 & 9 & -6 \\ 8 & 12 & -3 & 2 \\ -3 & 3 & 3 & 3 \\ 8 & -3 & -3 & 2 \end{pmatrix}$$

- Determinamos assim, a 1ª decifragem:

$$[T^t]^{-1}.\begin{pmatrix} 10 \\ -9 \\ 24 \\ 50 \end{pmatrix} = (1, 0, 11, 9)$$

$$[T^t]^{-1}.\begin{pmatrix} 4 \\ -8 \\ -17 \\ -1 \end{pmatrix} = (-1, -1, -6, 7)$$

- Determinamos com $[T^{-1}]$, a 2ª decifragem:

$$[T^{-1}].\begin{pmatrix} 1 \\ 0 \\ 11 \\ 9 \end{pmatrix} = (2, -1, 1, 3)$$

$$[T^{-1}].\begin{pmatrix} -1 \\ -1 \\ -6 \\ 7 \end{pmatrix} = (5, -2, -3, 0)$$

- A última decifragem vem da tabela de randomização:
  A senha do cliente: FASL 2 1 0 5

Apesar da pequena complexidade de nosso algoritmo criptográfico, se determinarmos várias rodadas no processo, chegaremos a uma intratabilidade considerável, pois os espaços vetoriais no $\mathbb{R}^n$ nos dá uma infinidade de combinação de números, de um em um, dois em dois, até de n em n, o que dificulta consideravelmente a decifragem por terceiros, sendo assim, nosso objetivo de utilizar o Isomorfismo de Transformações Lineares como método criptográfico, se revela possível e de aplicação real.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] BOLDRINI, José Luiz, et. Al. **Álgebra Linear** - 3ª edição, HARBRA Editora, São Paulo: 1986.

[2] CALLIOLI, Carlos A.; DOMINGUES, Hygino H.; Costa, Roberto C. F. **Álgebra Linear e Aplicações** - 6ª edição, ATUAL Editora, São Paulo: 1990.

[3] CARVALHO, Daniel Balparda. **Criptografia: Métodos e Algoritmos** – 1ª edição, Book Espress, Rio de Janeiro: 2000.

[4] GONÇALVES, Adilson. **Introdução à Álgebra –** Projeto Euclides, Instituto de Matemática Pura e Aplicada, Rio de Janeiro: 1979.

[5] STEINBRUCH, Alfredo; WINTERLE, Paulo. **Álgebra Linear** - 2ª edição, Pearson Makron Books, São Paulo: 2008.

[6] ABE, Jair Minoro. **A noção de estrutura em matemática e física** - Estudos avançados vol.3, São Paulo - Maio/Agosto 1989. Disponível em: < www.scielo.br/scielo.php .> acesso em: 20 março 2009.

[7] MIERS, Charles Christian. **Modelo Simplificado do Cifrador AES** - Florianópolis, Julho de 2002. Disponível em: < www.tede.ufsc.br/teses/PGCC0376.pdf > acesso em: 15 abril 2009.

[8] SANTOS, Reginaldo J. **Introdução à Álgebra Linear** - Departamento de Matemática-ICEx (Universidade Federal de Minas Gerais) - Março 2008. Disponível em: < http://www.mat.ufmg.br/~regi > acesso em: 15 abril 2009.