Teoria de Grupos e Tensores

Matheus Pereira Coutinho
Instituto de Física da USP
matheus.coutinho9@usp.br

1 - Monóides, Semigrupos e Grupos

Antes de definir as estruturas algébricas básicas de monóides, semigrupos e grupos, é necessário introduzir algumas noções, mais elementares ainda, são essas, conjuntos em mapas.

Definição **[Conjunto]**

Um conjunto é uma coleção de elementos, e para se definir um conjunto específico é necessária uma regra que me permita verificar se um determinado objeto pertence ao conjunto ou não.

Definição **[Mapa]**

Consideremos dois conjuntos X e Y. Um mapa é uma regra que associa um elemento $y \in Y$ a cada $x \in X$

$$\varphi : X \longrightarrow Y$$
$$\varphi : x \mapsto \varphi(x)$$

O conjunto X é chamado de Domínio do mapa e Y de contradomínio do mapa. A imagem do mapa é o conjunto de elementos de Y, tais que $\varphi(x) = y$

Algumas definições

- Um mapa é dito ser injetivo se, quando $x \neq x' \;\Rightarrow \varphi(x) \neq \varphi(x')$
- Um mapa é dito ser sobrejetivo se, para cada elemento de $y \in Y$ existe um $x \in X$, tal que $\varphi(x) = y$
- Um mapa é dito ser bijetivo quando ele é injetivo e sobrejetivo

Dadas as definições acima, podemos definir um tipo especial de mapa, que também tem um nome particular, o produto ou operação.

Definição **[Produto]**

Consideremos um conjunto X qualquer e o conjunto $X \times X$ chamado de produto cartesiano, que o é conjunto formado por pares de elementos de X, ou seja, $X \times X := \{(a, b), a, b \in X\}$. Um **produto** em X é um mapa da forma

$$\varphi : X \times X \longrightarrow X$$
$$\varphi : (a, b) \longmapsto \varphi(a, b)$$

em outros termos, é um mapa que associa um elemento de X a cada par de elementos de X.

Por vezes, $\varphi(a, b)$ é denotado, simplesmente, por $a \star b$ ou $a \cdot b$

Dados os ingrediente, podemos definir as estruturas algébricas mais elementares

Definição **[Semigrupo]**

Um **semigrupo** é um conjunto não-vazio S dotado de um produto, ou seja, um mapa da forma $\varphi : S \times S \longrightarrow S$, tal que

$\varphi(\varphi(a,b),c) = \varphi(a,\varphi(b,c)) \quad \forall a,b,c \in S$ (Associatividade)

Ou, em notação simplificada $\quad (a \star b) \star c = a \star (b \star c))$

Deste modo, o semigrupo é representado pelo par, conjunto, produto $(S, \star)$

Definição **[Monóide]**

Um **monóide** é um conjunto não-vazio M dotado de um produto, ou seja, um mapa da forma $\varphi : M \times M \longrightarrow M$, tal que

- $(a \star b) \star c = a \star (b \star c)) \quad \forall a,b,c \in M$ (Associatividade)
- Existe um (único) elemento $e \in M$ tal que $e \star a = a \star e = a \; \forall a \in M$ (elemento neutro)

Deste modo, o monóide é representado pelo par, conjunto, produto $(M, \star)$

Definição **[Grupo]**

Um **grupo** é um conjunto não-vazio G dotado de um produto, ou seja, um mapa da forma $\varphi : G \times G \longrightarrow G$, tal que

- $(a \star b) \star c = a \star (b \star c)) \quad \forall a,b,c \in G$ (Associatividade)
- Existe um (único) elemento $e \in M$ tal que $e \star a = a \star e = a \; \forall a \in G$ (elemento neutro)
- Para cada $a \in G$ exite um (único) a^{-1} tal que $a \star a^{-1} = a^{-1} \star a = e \quad \forall a \in G$ (elemento inverso)

Deste modo, o grupo é representado pelo par, conjunto, produto $(G, \star)$

★ Um grupo é dito ser abeliano se o seu produto é comutativo, ou seja, $a \star b = b \star a \quad \forall a, b \in G$

Exemplos:

► O conjunto $GL(n, \mathbb{R})$ de todas as matrizes reais $n \times n$ com determinante não nulo (e, portanto, inversíveis) é um grupo em relação à operação de produto usual de matrizes. $GL(n, \mathbb{R})$ é não Abeliano se $n > 1$

► Sendo X um conjunto não-vazio qualquer e denotamos por $S = X^X$ o conjunto de todos os mapas $\varphi : X \longrightarrow X$, S então é um monóide com o produto sendo a composição de mapas e o elemento neutro sendo o mapa ou função identidade $id(x) = x\,, \quad \forall x \in X$.

► Sendo X um conjunto não-vazio qualquer e denotamos por $S = X^X$ o conjunto de todos os mapas bijetores $\varphi : X \longrightarrow X$, S então é um grupo não abeliano com o produto sendo a composição de mapas, o elemento neutro sendo o mapa ou função identidade $\mathrm{id}(x) = x\ , \quad \forall x \in X$ e o elemento inverso é o mapa inverso φ^{-1}. Esse grupo é chamado de grupo de permutações de X e é denotado por $\mathrm{Perm}(X)$

► O conjunto dos números reais $\mathbb{R}$ com a soma usual de números reais é um grupo abeliano, sendo 0 o elemento neutro e $-a$ o elemento inverso de cada elemento a. Este grupo é denominado de grupo aditivo dos reais $(\mathbb{R}, +)$

2 - Grupo de Permutações, Grupos $\mathbb{Z}_n$ e Homomorfismo

Grupo de Permutações

Os Grupos $\mathbb{Z}_n$

◇ **Divisão Euclidiana**
Seja $n \in \mathbb{N}$ um número fixo. Então todo número $z \in \mathbb{Z}$ pode ser escrito, unicamente, como $z = qn + r$, com $q \in \mathbb{Z}$ e $r \in \{0, 1, ..., n-1\}$. r é o resto da divisão de z por n e pode ser denotado por $r = z \bmod n$

Homomorfismo

Dados dois grupos G e H, um mapa $\phi : G \longrightarrow H$ é dito ser um homomorfismo se satisfazer o seguinte requerimento

$$\phi(a \star b) = \phi(a)\phi(b)\ , \quad \forall a, b \in G$$

★ Se um homomorfismo $\phi : G \longrightarrow H$ for bijetor, então ele é dito ser um isomorfismo entre os dois grupos.

3 - Homomorfismo, Grupo do Círculo e Semigrupos

4 - Corpos, Espaços Vetoriais, Álgebras e Álgebras de Lie

Definição **[Corpos]**

Um **corpo** é um conjunto não vazio dotado de dois mapas, ambos de forma $f : \mathbb{K} \times \mathbb{K} \longrightarrow \mathbb{K}$, denominados de soma e produto, e denotados por $+$ e $\cdot$, respectivamente, tais que valem as seguintes propriedades para todos $a, b, c \in \mathbb{K}$

- $a + b = b + a$
- $a + (b + c) = (a + b) + c$
- Existe um elemento $0 \in \mathbb{K}$ tal que $a + 0 = 0 + a = a\,, \quad \forall a \in \mathbb{K}$
- Para cada $a \in \mathbb{K}$ existe um elemento b tal que $a + b = 0$. Frequentemente esse elemento é denotado por $-a$
- $a \cdot b = b \cdot a$
- $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
- Existe um elemento $1 \in \mathbb{K}$ tal que $a \cdot 1 = 1 \cdot a = a\,, \quad \forall a \in \mathbb{K}$
- Para cada elemento a existe um elemento b tal que $a \cdot b = 1$. Frequentemente esse elemento é denotado por a^{-1}
- $a \cdot (b + c) = a \cdot b + a \cdot c$

Com isso, podemos representar um corpo pela tripla $(\mathbb{K}, +, \cdot)$

★ É comum, especialmente em fisica, chamar os elementos de um corpo de escalares.

★ Os corpos utilizados em física são, na grande maioria dos casos, $\mathbb{R}$ e $\mathbb{C}$

Definição **[Espaço Vetorial]**

Um **espaço vetorial** sobre um corpo $\mathbb{K}$ é um conjunto V não vazio dotado de dois mapas, de formas $\varphi : V \times V \longrightarrow V$ e $\psi : \mathbb{K} \times V \longrightarrow V$, cujos nomes são soma vetorial e produto por escalar, respectivamente, tais que valem as seguinte propriedades para todos $u, v, w \in V$ e $a, b \in \mathbb{K}$

- $u + v = v + u$
- $u + (v + w) = (u + v) + w$
- Existe um elemento $0 \in V$ tal que $u + 0 = 0 + u = u\,, \quad \forall u \in V$
- Para cada $u \in V$ existe um elemento v tal que $u + v = 0$. Frequentemente esse elemento é denotado por $-u$
- $a \cdot (b \cdot u) = (a \cdot b) \cdot u$
- Existe um único elemento $1 \in \mathbb{K}$ tal que $u \cdot 1 = 1 \cdot u = u\,, \quad \forall u \in V$
- $a \cdot (u + v) = a \cdot u + a \cdot v$
- $(a + b) \cdot u = a \cdot u + b \cdot u$

Com isso, podemos representar um espaço vetorial pela tripla $(V, +, \cdot)$

★ Os elementos de um espaço vetorial são chamados de vetores.

Exemplos:

► Se $\mathbb{K}$ é um corpo, então ele também é um espaço vetorial sob as ele mesmo e com as operações nele definidas.

► Um exemplo muito relevante me física é o conjunto $\mathbb{R}^n := \{(x_1, ..., x_n), x_i \in \mathbb{R}, i = 1, ..., n\}$ com as operações soma

$$(x_1, ..., x_n) + (y_1, ..., y_n) = (x_1 + y_1, ..., x_n + y_n)$$

e produto por escalar

$$a \cdot (x_1, ..., x_n) = (a \cdot x_1, ..., a \cdot x_n)$$

Frequentemente um elemento de $\mathbb{R}^n$ é denotado por uma matriz coluna

$$(x_1, ..., x_n) \quad \longrightarrow \quad \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

► O mesmo exemplo do espaço $\mathbb{R}^n$ também pode ser considerado para o espaço $\mathbb{C}^n$

► Um exemplo de fundamental importância é o espaço vetorial formado pelo conjunto de funções $f : X \longrightarrow \mathbb{R}$, onde X é um conjunto qualquer, e com a soma vetorial e produto por escalar definidos por

$$(f + g)(x) = f(x) + g(x) \ , \quad \forall x \in X$$
$$(a \cdot f)(x) = a \cdot f(x)$$

Esse exemplo demonstra o quão amplo é o conceito de espaço vetorial.

Definição **[Álgebra]**

Uma álgebra é um espaço vetorial V sobre um corpo $\mathbb{K}$ e com um terceiro mapa, denominado de produto da álgebra, e de forma $\varphi : V \times V \longrightarrow V$. A notação para esse produto será, a priori, $\varphi(u, v) := u \times v$. Tal produto deve ainda satisfazer os seguintes requerimentos para todos $u, v, w \in V$

$$u \times (v + w) = u \times v + u \times w \quad \text{e} \quad (u + v) \times w = u \times w + v \times w$$
$$a \cdot (u \times v) = (a \cdot u) \times v = u \times (a \cdot v) \ , \quad \forall a \in \mathbb{K}$$

★ Uma álgebra é dita ser comutativa se $u \times v = v \times u$

★ Uma álgebra é dita ser associativa se $u \times (v \times w) = (u \times v) \times w$

Um exemplo de álgebra, muito utilizada em física, é a a álgebra do produto vetorial, que é o espaço vetorial $\mathbb{R}^3 := \{(x_1, x_2, x_3), x_i \in \mathbb{R}\}$ com o produto da álgebra

$$(x_1, x_2, x_3) \times (y_1, y_2, y_3) = (x_2 y_3 - x_3 y_2, x_1 y_3 - x_3 y_1, x_1 y_2 - x_2 y_1)$$

Propriedades notáveis dessa álgebra,em partícular, são

$$u \times v = -v \times u$$

$$u \times (v \times w) \neq (u \times v) \times w$$
$$u \times (v \times w) + v \times (w \times u) + w \times (u \times v) = 0$$

A ultima propriedade é chamada de identidade de Jacobi.

Constantes de Estrutura

Se A é uma álgebra de dimensão n, portanto é também um espaço vetorial, podemos considerar o conjunto $B := \{b_1, ..., b_n\}$. Com base na noção de base da álgebra, sabemos que qualquer elemento dela pode ser escrito como uma combinação linear dos elementos da base. Em especial, podemos escrever o produto de dois elementos da base como combinação dos elementos da base

$$b_i \cdot b_j = \sum_{k=1}^{n} c_{ij}^{k} b_k$$

Os coeficientes c_{ij}^{k} são denominados constantes de estrutura da álgebra A na base B. Por meio dessas constantes nós podemos determinar o produto de dois elementos da álgebra, pois dados dois elementos u e v escritos na base B.

$$u = \sum_{i=1}^{n} u_i b_i \quad \text{e} \quad v = \sum_{j=1}^{n} v_j b_j$$

O produto $u \times v$ será

$$u \times v = \sum_{k=1}^{n} \lambda_k b_k$$

com

$$\lambda_k = \sum_{i=1}^{n} \sum_{j=1}^{n} u_i v_j c_{ij}^{k}$$

E, portanto

$$u \times v = \sum_{k=1}^{n} \left(\sum_{i=1}^{n} \sum_{j=1}^{n} u_i v_j c_{ij}^{k} \right) b_k$$

Nosso próximo passo definir uma álgebra de Lie. Mas antes disso é preciso falar de notação, pois o o produto em álgebras de Lie é denotado por $[u, v]$

Definição [Álgebras de Lie]

Uma álgebra L é dita ser uma álgebra de Lie se satisfazer as seguintes condições

- $\forall a \in L \quad [a, a] = 0$
- $\forall a, b, c \in L \quad [a, [b, c]] + [c, [a, b]] + [b, [c, a]] = 0$ (identidade Jacobi)

Alternativamente, podemos escrever a primeira condição como

$$[a, b] = -[b, a] \quad \text{(anticomutatividade)}$$

► Como já apresentado, é direta a conclusão de que o espaço vetorial $\mathbb{R}^3 := \{(x_1, x_2, x_3), x_i \in \mathbb{R}, i = 1, ..., n\}$ com o produto vetorial é um exemplo de álgebra de Lie

Álgebra Associativa

Dada uma álgebra A associativa, isto é, $a \times (b \times c) = (a \times b) \times c \;\; \forall a, b, c \in A$. Como por exemplo a álgebra formado pelo conjunto de matrizes reais $n \times n$, denotado por $Mat(\mathbb{R}, n)$, com o produto usual de matrizes. É sempre possível construir, a partir dela, uma álgebra de Lie. Para tanto, é necessário definir o produto da álgebra como sendo o comutador

$$[a, b] = ab - ba$$

É fácil ver que, com esse novo produto definido, as condições que definem uma álgebra de Lie são naturalmente satisfeitas

$$[a, a] = aa - aa = 0$$

$$\begin{aligned}
&[a, [b, c]] + [c, [a, b]] + [b, [c, a]] \\
&\qquad = a(bc - cb) - (bc - cb)a + c(ab - ba) - (ab - ba)c + b(ca - ac) - (ca - ac)b \\
&\qquad = abc - acb - bca + cba + cab - cba - abc + bac + bca - bac - cab + acb \\
&\qquad = 0
\end{aligned}$$

É notável, que a última propriedade só é satisfeita se a álgebra for associativa

Definição **[Álgebra de Poisson]**

Definição **[Álgebra de Jordan]**

Definição **[Álgebra de Grassmann]**

Definição **[Álgebra de Clliford]**

5 - Relações, Relações de Equivalência e Classes de Equivalência

Definição **[Relação]**

Dados dois conjuntos não vazios quaisquer A e B, o produto cartesiano entre esses dois conjuntos é simplesmente o conjunto formado por todos os pares ordenados de elementos de A e B, denotado por $A \times B := \{(a,b), a \in A, b \in B\}$. Uma **relação** R entre A e B é simplesmente um subconjunto de $A \times B$. $R \subset A \times B$

Definição **[Relação de Equivalência em um Conjunto]**

Consideremos A um conjunto não vazio qualquer e o produto cartasiano $A \times A := \{(a,a'),\ a,a' \in A\}$. Uma **relação de equivalência** em A é uma relação $E \subset A \times A$, tal que

- $(a,a) \in E$, $\forall a \in A$ (reflexividade)
- se $(a,b) \in E$, então $(b,a) \in E$ (simetria)
- se $(a,b) \in E$ e $(b,c) \in E$, então $(a,c) \in E$ (transitividade)

Se um par (a,b) pertence a uma relação de equivalência E então dizemos que a é equivalente a b seguindo E. Uma notação comum é $a \sim b$. Segunda essa notação as propriedades que uma relação deve possuir para ser considerada uma relação de equivalência escrevem-se

- $a \sim a$ para todo $a \in A$ (Reflexividade)
- Se $a \sim b$ então $b \sim a$ (simetria)
- Se $a \sim b$ e $b \sim c$ então $a \sim c$ (transitividade)

Exemplo:

Consideremos V um espaço vetorial e U um subespaço qualquer de V

★ Só para se ter intuição, o exemplo acima pode ser pensado, simplesmente, considerando V o espaço $\mathbb{R}^2$ e U os pontos que pertencem à uma reta que cruza a origem, por exemplo.

Consideremos a relação $E = \{(a,b),\ a,b \in V,\ b-a \in U\}$, isto é, $a \sim b$ se $b - a \in U$

Chequemos se as condições são satisfeitas

$a \sim a$ se $a - a \in U$, e portanto se $0 \in U$. Essa condição é satisfeita, pois U contém o elemento neutro (do contrário não seria subespaço)

$a \sim b$ implica que $b - a \in U$ e $b \sim a$ implica que $a - b \in U$. Mas $a - b = -(b-a)$ e $b - a \in U$, e como trata-se de um subespaço vetorial um elemento multiplicado por um escalar também é um elemento do subespaço. Logo $a - b \in U$

$a \sim b \ \Rightarrow b - a \in U$ e $b \sim c \ \Rightarrow c - b \in U$. $a \sim c$ implica que $c - a \in U$, para ver com clareza que $c - a \in U$ basta considerar $b - a = u_1 \in U$ e $c - b = u_2 \in U$, se u_1 e u_2 pertencem a U, certamente a subtração deles também pertence a U. Logo, $u_2 - u_1 = c - b - (b-a) = c - a \in U$

Definição **[Classe de Equivalência]**

Sendo A um conjunto e $E \subset A \times A$ uma relação de equivalência em A, definimos, para cada $a \in A$, sua **classe de equivalência** como sendo o conjunto de todos os elementos que são equivalente a a, isto é

$$E(a) := \{a' \in A \text{ tal que } (a, a') \in E\}$$

Uma outra notação para a classe de equivalência de a é $[a]$

$$[a] = \{a' \in A,\ a' \sim a\}$$

★ É notável que, pela reflexividade, um elemento a sempre é equivalente a ele mesmo, $a \sim a$, e, por isso uma classe de equivalência nunca é um conjunto vazio, pois contém, no mínimo, o próprio elemento.

★ Com base na observação acima, temos que, o conjunto A pode ser escrito a partir da união das classes de equivalência dos seus elementos

$$A = \bigcup_{a \in A} [a]$$

★ Além do mais, se $a, b \in A$ e $a \sim b$, então $[a] = [b]$. Isso é trivial, pois se $[a] \neq [b]$, então existiria algum elemento, digamos c, que pertence a $[a]$ mas não pertence a b ($c \in [a]$ e $c \notin [b]$) , isso significa que esse suposto elemento é equivalente a a mas não é equivalente a b, essa conidção, porém, não pode ser verdade, uma vez que, pela transitividade, se $c \sim a$ e $a \sim b$, então, necessariamente, $c \sim b$, e portanto $c \in [b]$. Logo, as classes de equivalência de dois elementos equivalentes tem de ser iguais.

★ Segue-se disso que, se $a \nsim b$ então $[a] \cap [b] = \varnothing$

6 - Relações de Equivalência e o Espaço Quociente

Notação: O conjunto de todas as classes de equivalência em um conjunto A, segundo uma relação $\sim$ é denotado por:

$$A/\sim = \{[a], a \in A\}$$

Definição **[Espaço Vetorial Quociente]**

Consideremos V um espaço vetorial, U um subespaço de V, a relação de equivalência, $x \sim y$ se $y - x \in U$ e o conjunto das classes de equivalência $V/\sim = V/U = \{[x], \quad x \in V\}$. O **espaço quociente** é um espaço vetorial formado pelo conjunto V/U com a soma definida por

$$[x] + [y] := [x + y]$$

e o produto por escalar

$$a \cdot [x] := [a \cdot x]$$

7 - Grupo de Permutações e Grupos Matriciais

Grupo de Matrizes

Notação: Conjuntos de matrizes reais e complexas $n \times n$ são denotados por $Mat(\mathbb{R}, n)$ e $Mat(\mathbb{C}, n)$, respectivamente.

★ Ambos os conjuntos acima são grupos abelianos sob a operação de soma usual de matrizes, mas não sob a operação de multiplicação usual de matrizes, pois nem toda matriz possui elemento inverso.

★ Se considerarmos agora o subconjunto de $Mat(\mathbb{R}, n)$ formado por matrizes inversíveis, então esse conjunto é um grupo não abeliano sob a operação de multiplicação usual de matrizes. Esse grupo é denominado de grupo linear real $GL(\mathbb{R}, n)$. Analogamente, tem-se o grupo linear complexos $GL(\mathbb{C}, n)$. Uma forma de garantir que uma matriz tenha inversa é dizendo que seu determinante é não nulo, com isso, podemos escrever os grupos lineares como

$$GL(n, \mathbb{R}) := \{A \in Mat(n, \mathbb{R}), det(A) \neq 0\} \quad \text{e} \quad GL(n, \mathbb{C}) := \{A \in Mat(n, \mathbb{C}), det(A) \neq 0\}$$

★ Além destes, devido à propriedade do determinante $det(A \cdot B) = det(A) \cdot det(B)$, o produto de duas matrizes com determinante 1 também possui determinante igual a 1, por isso podemos forma um subgrupo de $GL(n, \mathbb{R})$, formado pelas matrizes de determinante 1

$$SL(n, \mathbb{R}) := \{A \in Mat(n, \mathbb{R}), det(A) = 1\}$$

Analogamente, para matrizes complexas

$$SL(n, \mathbb{C}) := \{A \in Mat(n, \mathbb{C}), det(A) = 1\}$$

Esses grupos são chamados de grupos lineares especiais

Grupo de Heisenberg $GH_3(\mathbb{C})$

O grupo de Heisenberg é composto pelo conjunto de matrizes da forma

$$H(a, b, c) = \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix}$$

com a operação usual de multiplicação de matrizes, e $a, b, c \in \mathbb{C}$

★ É fácil ver que a matriz identidade está no grupo, pois $H(0, 0, 0) = \mathbb{I}$, e é o elemento neutro

$$H(a, b, c) \cdot H(x, y, z) = H(a + x, b + y, c + z + a \cdot y) = H(a, b, c)$$

$$\begin{aligned} a + x = a &\Rightarrow x = 0 \\ b + y = b &\Rightarrow y = 0 \\ c + z + ay = c &\Rightarrow z = 0 \end{aligned}$$

$$e = H(0,0,0)$$

Além disso, o produto de duas matrizes do grupo de Heisenberg é

$$H(a,b,c) \cdot H(a',b',c') = \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & a' & c' \\ 0 & 1 & b' \\ 0 & 0 & 1 \end{pmatrix}$$

$$H(a,b,c) \cdot H(a',b',c') = \begin{pmatrix} 1 & a+a' & c'+a \cdot b'+c \\ 0 & 1 & b'+b \\ 0 & 0 & 1 \end{pmatrix}$$

$$H(a,b,c)H(a',b',c') = H(a+a', b+b', c+c'+ab')$$

A inversa de uma matriz $H(a,b,c)$ é dada por

$$H(a,b,c)^{-1} = H(-a,-b,ab-c) = \begin{pmatrix} 1 & -a & ab-c \\ 0 & 1 & -b \\ 0 & 0 & 1 \end{pmatrix}$$

Pois

$$H(a,b,c) \cdot H(x,y,z) = H(0,0,0)$$

$$H(a+x, b+y, c+z+a \cdot y) = H(0,0,0)$$

$$\begin{aligned} x &= -a \\ y &= -b \\ z &= a \cdot b - c \end{aligned}$$

$$H^{-1}(a,b,c) = H(-a,-b,ab-c)$$

★ Podemos identificar um subgrupo do grupo de Heisenberg formado pelas matrizes

$$H_1(t) := H(t,0,0) = \begin{pmatrix} 1 & t & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$H_2(t) := H(0,t,0) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & t \\ 0 & 0 & 1 \end{pmatrix}$$

$$H_3(t) := H(0,0,t) = \begin{pmatrix} 1 & 0 & t \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$H_j(t)H_j\left(t'\right) = H_j\left(t + t'\right)$$

Cada matriz $H_j(t)$ gera um subgrupo uniparamétrico. Que podem ser representados a partir de seus geradores

$$h_j := \left.\frac{d}{dt}H_j(t)\right|_{t=0}$$

Exponenciação de Matrizes

$$e^x = 1 + \sum_{n=1}^{\infty} \frac{x^n}{n!}$$

$$e^x e^y = e^{x+y}$$

$$e^0 = 1$$

$$\frac{d}{dx}e^x = e^x$$