UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
CURSO DE LICENCIATURA EM MATEMÁTICA

GABRIELLY HALAS

RELAÇÕES ENTRE TEORIA DE REPRESENTAÇÕES DE GRUPOS E A ÁLGEBRA MULTILINEAR: UMA INTRODUÇÃO NAÏF

TRABALHO DE CONCLUSÃO DE CURSO

CURITIBA

2015

GABRIELLY HALAS

RELAÇÕES ENTRE TEORIA DE REPRESENTAÇÕES DE GRUPOS E A ÁLGEBRA MULTILINEAR: UMA INTRODUÇÃO NAÏF

Trabalho de Conclusão de Curso apresentado ao Curso de Licenciatura em Matemática da Universidade Tecnológica Federal do Paraná como requisito parcial para a disciplina Trabalho de Conclusão de Curso 2.

Orientadora: Mari Sano, Prof.ª Dr.ª

CURITIBA

2015

Ministério da Educação
UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
Câmpus Curitiba
Diretoria de Graduação e Educação Profissional
Departamento Acadêmico de Matemática
Coordenação do Curso de Licenciatura em Matemática

TERMO DE APROVAÇÃO

"RELAÇÕES ENTRE TEORIA DE REPRESENTAÇÕES DE GRUPOS E A ÁLGEBRA MULTILINEAR: UMA INTRODUÇÃO NAIF"

por

"Gabrielly Halas"

Este Trabalho de Conclusão de Curso foi apresentado às 14 horas do dia 11 de Dezembro de 2015 na sala V2-102 como requisito parcial à obtenção do grau de Licenciado em Matemática na Universidade Tecnológica Federal do Paraná - UTFPR - Câmpus Curitiba. O(a) aluno(a) foi arguido pela Banca de Avaliação abaixo assinados. Após deliberação, de acordo com o parágrafo 1º do art. 37 do Regulamento Específico do trabalho de Conclusão de Curso para o Curso de Licenciatura em Matemática da UTFPR do Câmpus Curitiba, a Banca de Avaliação considerou o trabalho aprovado.

_____ Profa. Dra. Mari Sano **(Presidente - UTFPR/Curitiba)**	_____ Prof. Dr. Ronie Peterson Dario **(Avaliador 1 - UTFPR/Curitiba)**
_____ Profa. Dra. Paula Olga Gneri **(Avaliador 2 - UTFPR/Curitiba)**	_____ Prof. Dr. Marco Aurélio Kalinke **(Professor Responsável pelo TCC – UTFPR/Curitiba)**
_____ Profa. Dra. Neusa Nogas Tocha **(Coordenador do curso de Licenciatura em Matemática – UTFPR/Curitiba)**	

"A Folha de Aprovação assinada encontra-se na Coordenação do Curso."

SUMÁRIO

1 INTRODUÇÃO

O conceito abstrato de *grupo* surgiu depois de muitos anos, a partir de situações *concretas* de *grupos de transformações*. Segundo Wussing (2007), a Teoria de Grupos tem suas origens em três áreas:

1. Na teoria da resolubilidade de equações, onde o representante mais conhecido é o *Grupo de Galois*, apesar de Lagrange, Vandermonde, Ruffini e outros matemáticos também terem realizados estudos importantes. Nessa teoria, o grupo é definido como um subgrupo do grupo de permutações das raízes de uma equação.

2. Na teoria de números, na qual Euler, por exemplo, estudou a aritmética modular e, dentre muitos trabalhos, mostrou um caso especial do Teorema de Lagrange, de maneira implícita.

3. Na geometria, especialmente com os trabalhos de Klein e Möbius, com os grupos de transformações associados às geometrias projetiva, hiperbólica, entre outras.

Nessas origens da teoria de Grupos, o grupo sempre agia como um conjunto de transformações de uma estrutura, seja como permutações das raízes de uma equação, seja como simetrias de uma estrutura geométrica.

Com o passar do tempo, na segunda metade do século XIX, trabalhos de Cayley, Frobenius e Burnside evidenciaram a importância da estrutura *abstrata* de grupo, e esta foi desenvolvendo-se como uma das principais áreas da Álgebra, com grande sucesso, como a classificação completa dos grupos finitos simples, um trabalho de décadas que ainda está sendo simplificado.

Porém, a roda da história continua dando voltas, e o caminho inverso é muito importante: dado um grupo abstrato G, como ele pode agir como grupo de transformações de um espaço? Esse caso, em que o grupo age como transformações lineares de um espaço vetorial, é chamado de *Teoria de Representações de Grupos*.

A Teoria de Representações nasceu nos trabalhos do matemático alemão Ferdinand Georg Frobenius. Esses trabalhos originaram-se a partir de uma carta enviada a ele por Julius Wilhelm Richard Dedekind. Na mesma, o remetente fez a seguinte observação: Considere a tabela de multiplicação de um grupo finito G e transforme-a em uma matriz X_G substituindo cada entrada g, da tabela, por uma variável x_g. Então, o determinante de X_G se decompõe em um produto de polinômios irredutíveis em x_g.

Dedekind verificou esse fato em alguns casos especiais, mas não conseguiu demonstrá-lo em geral. Assim, o objetivo de sua carta foi apresentar o problema para Frobenius. A fim de encontrar uma solução, Frobenius criou a Teoria das Representações de grupos finitos.

Nesse trabalho, essas teorias serão estudadas junto à *Álgebra Multilinear*, a qual fornece soluções da seguinte pergunta: a partir de um espaço vetorial V, como produzir espaços vetoriais "novos" associados de maneira natural a V? Existem algumas construções óbvias, tais como o espaço produto $V \times V$, porém serão apresentadas outras mais sofisticadas.

O objetivo desse trabalho é, primeiramente, introduzir as teorias citadas com seus conceitos, definições e alguns teoremas, bem como ilustrá-las com alguns exemplos de um caso muito clássico: a teoria de representações do grupo linear geral $GL_n(\mathbb{K})$ de matrizes $n \times n$ invertíveis sobre um corpo $\mathbb{K}$. Será visto como representações interessantes de $GL_n(\mathbb{K})$ são produzidas por construções da Álgebra Multilinear, tais como a potência simétrica e a potência exterior. Também, será mostrado no Teorema 4.4.24 que o produto tensorial $V \otimes V$ é isomorfo a soma direta dessas potências. É notável como essa teoria evolui, já que modernamente é utilizada a Álgebra Homológica para dar estrutura ao *conjunto de todas as representações*. (BUCHBAUM, 1994), (SANO, 2003), (SANO, 2006)

O trabalho está organizado da seguinte maneira: após essa introdução, no primeiro capítulo serão abordadas noções básicas da teoria de grupos. No capítulo seguinte serão descritas as construções universais da Álgebra Multilinear. E no último capítulo, acredita-se que haverá a contribuição mais significativa deste trabalho, ou seja, relacionar essas duas áreas da Álgebra, fazendo rudimentos da Teoria de Representações de Grupos, e dando como exemplo principal as representações do grupo $GL_n(\mathbb{K})$ induzidas pelas construções da Álgebra Multilinear.

2 TEORIA BÁSICA DE GRUPOS

Neste capítulo serão apresentadas as definições e os resultados básicos, referentes à teoria de grupos, necessários para o desenvolvimento deste trabalho. O mesmo é desenvolvido seguindo Domingues e Iezzi (2003) e Garcia e Lequain (2003).

2.1 GRUPOS

Para definir um grupo é necessário o conceito de operação binária.

Definição 2.1.1. *Seja G um conjunto não vazio. Uma* ***operação binária*** *sobre G é uma função*

$$\begin{aligned} * : G \times G &\to G \\ (a,b) &\mapsto a * b \end{aligned}$$

para todos $a, b \in G$.

Definição 2.1.2. *Seja G um conjunto não vazio e* $*$ *uma operação binária sobre G. Diz-se que G tem estrutura de* ***grupo*** *em relação a essa operação, se são satisfeitas as seguintes condições:*

(i) associatividade: a(b*c)=(a*b)*c*

(ii) existência do elemento neutro: existe $e \in G$ *tal que* $a * e = e * a = a$

(iii) existência do elemento inverso: existe $g \in G$ *tal que* $a * g = g * a = e$

para todos $a, b, c \in G$.

Diz-se que um grupo $(G, *)$ é **comutativo** (ou abeliano) quando a operação $*$ é comutativa.

Nota 2.1.3. *Se* $a \in G$*, então o seu elemento inverso g é denotado por* a^{-1}*. O grupo formado por G e pela operação* $*$ *sobre G é representado por* $(G, *)$*. A fim de facilitar a notação, quando não houver ambiguidade, a operação binária* $a * b$ *será denotada pela notação de multiplicação, ou seja, ab. E o grupo* $(G, *)$ *será representado somente por G.*

Observação 2.1.4. *Se G é um grupo, então o elemento neutro é único e o elemento inverso é único.*

Seguem algumas propriedades de grupos:

Propriedade 2.1.5. *Seja G um grupo. Então,*

(i) Para todo $a \in G$, tem-se $(a^{-1})^{-1} = a$.

(ii) Se $a_i \in G$, para $i \in \{1,2,...,n-1,n\}$, tem-se

$$(a_1 a_2 ... a_{n-1} a_n)^{-1} = a_n^{-1} a_{n-1}^{-1} ... a_2^{-1} a_1^{-1}.$$

(iii) Sendo $a,b,c \in G$, se $ab = ac$, tem-se $b = c$. (Se isso ocorre, diz-se que todo elemento de G é regular para a operação).

Demonstração:

(i) Considere a^{-1} o elemento inverso de a. Por definição, $aa^{-1} = a^{-1}a = e$. Note que a é o inverso de a^{-1}, ou seja, $a = (a^{-1})^{-1}$.

(ii) A propriedade será demonstrada por indução sobre i. Para $i = 2$, tem-se que

$$(a_1 a_2)(a_2^{-1} a_1^{-1}) = a_1 (a_2 a_2^{-1}) a_1^{-1} = a_1 e a_1^{-1} = a_1 a_1^{-1} = e.$$

Analogamente,

$$(a_2^{-1} a_1^{-1})(a_1 a_2) = a_2^{-1} (a_1^{-1} a_1) a_2 = a_2^{-1} e a_2 = a_2^{-1} a_2 = e.$$

Pela transitividade da igualdade,

$$(a_1 a_2)(a_2^{-1} a_1^{-1}) = (a_2^{-1} a_1^{-1})(a_1 a_2) = e.$$

Segue que $a_2^{-1} a_1^{-1}$ é o elemento inverso de $a_1 a_2$, ou seja, $(a_1 a_2)^{-1} = a_2^{-1} a_1^{-1}$. Logo, vale a propriedade para $i = 2$. Suponha, por hipótese de indução, que a igualdade é válida para algum número natural n, ou seja,

$$(a_1 a_2 ... a_{n-1} a_n)^{-1} = a_n^{-1} a_{n-1}^{-1} ... a_2^{-1} a_1^{-1}.$$

Desse modo, o objetivo é mostrar que a afirmação é válida para $n+1$,

$$(a_1 a_2 ... a_{n-1} a_n a_{n+1})^{-1} = a_{n+1}^{-1} (a_1 a_2 ... a_{n-1} a_n)^{-1} = a_{n+1}^{-1} a_n^{-1} a_{n-1}^{-1} ... a_2^{-1} a_1^{-1}.$$

Portanto, vale a igualdade para todo $i \geqslant 2$, $i \in \mathbb{N}$.

(iii) Por hipótese, $ab = ac$. Considere $a^{-1} \in G$ o inverso de a. Então, $a^{-1}(ab) = a^{-1}(ac)$, ou seja, $(a^{-1}a)b = (a^{-1}a)c$. Daí, $eb = ec$. Logo, $b = c$.

□

Seguem alguns exemplos de grupos.

Exemplo 2.1.6. *Os conjuntos $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ munidos da operação de adição usual são grupos abelianos, já que a adição é associativa e comutativa para todos os números complexos, existe o elemento neutro denotado por 0, e todos os números complexos possuem oposto.*

Exemplo 2.1.7. *Os conjuntos $\mathbb{Q}\setminus\{0\}$, $\mathbb{R}\setminus\{0\}$ e $\mathbb{C}\setminus\{0\}$ munidos da operação de multiplicação usual são grupos abelianos, pois a multiplicação é associativa e comutativa para todos os números complexos existe o elemento neutro denotado por 1, e todos os números complexos não nulos possuem inverso.*

Exemplo 2.1.8. *Seja $GL_n(\mathbb{K})$ o conjunto das matrizes $A \in M_n(\mathbb{K})$ que são invertíveis. Esse conjunto munido da operação de multiplicação de matrizes tem estrutura de grupo e é denominado **grupo linear geral sobre** $\mathbb{K}$. De fato, $GL_n(\mathbb{K})$ é fechado para a multiplicação de matrizes. A operação é associativa, o elemento neutro é a matriz identidade e existe a matriz inversa para todo elemento de $GL_n(\mathbb{K})$.*

Exemplo 2.1.9. *Seja $\mathbb{Z}_m = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}$ o conjunto das classes de restos módulo m. Esse conjunto munido da operação de adição é grupo abeliano. Com efeito, $\mathbb{Z}_m$ é fechado para a adição já que $\overline{a} + \overline{b} = \overline{a+b}$, para todo $a, b \in \mathbb{Z}_m$. Vale a associatividade dos elementos do conjunto, o elemento neutro é $\overline{0}$ e o elemento inverso de $a \in \mathbb{Z}_m$ é $\overline{m-a} \in \mathbb{Z}_m$.*

Para o próximo exemplo é necessária a seguinte definição:

Definição 2.1.10. *Considere um polígono regular T. Diz-se que a aplicação bijetora $f\colon T \to T$ é uma **simetria** quando preserva distâncias no polígono.*

Exemplo 2.1.11. *Considere um triângulo equilátero de vértices 1, 2, 3, de baricentro O e as medianas m_1, m_2, m_3 que passam pelos vértices 1, 2 e 3, respectivamente, como pode-se observar na figura 1.*

Denote por R_0, $R_{\frac{2\pi}{3}}$ e $R_{\frac{4\pi}{3}}$ as rotações de 0, $\frac{2\pi}{3}$, $\frac{4\pi}{3}$ radianos em torno de O, respectivamente, no sentido anti-horário. Sejam M_1, M_2 e M_3 as reflexões de π radianos em torno das medianas m_1, m_2 e m_3, respectivamente.

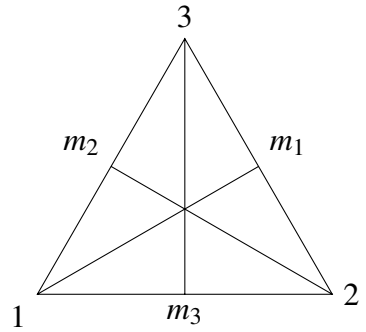


Figura 1: Triângulo Equilátero

O conjunto das simetrias no triângulo equilátero $D_3 = \left\{R_0, R_{\frac{2\pi}{3}}, R_{\frac{4\pi}{3}}, M_1, M_2, M_3\right\}$ *munido da composição de transformações é um grupo não abeliano.*
Com efeito, efetuando-se todas as composições possíveis, obtêm-se a seguinte tábua:

$\circ$	R_0	$R_{\frac{2\pi}{3}}$	$R_{\frac{4\pi}{3}}$	M_1	M_2	M_3
R_0	R_0	$R_{\frac{2\pi}{3}}$	$R_{\frac{4\pi}{3}}$	M_1	M_2	M_3
$R_{\frac{2\pi}{3}}$	$R_{\frac{2\pi}{3}}$	$R_{\frac{4\pi}{3}}$	R_0	M_3	M_1	M_2
$R_{\frac{4\pi}{3}}$	$R_{\frac{4\pi}{3}}$	R_0	$R_{\frac{2\pi}{3}}$	M_2	M_3	M_1
M_1	M_1	M_3	M_2	R_0	$R_{\frac{4\pi}{3}}$	$R_{\frac{2\pi}{3}}$
M_2	M_2	M_1	M_3	$R_{\frac{2\pi}{3}}$	R_0	$R_{\frac{4\pi}{3}}$
M_3	M_3	M_2	M_1	$R_{\frac{4\pi}{3}}$	$R_{\frac{2\pi}{3}}$	R_0

Sabe-se que a composição de transformações é associativa. Pela tábua é possível observar que R_0 *é o elemento neutro e que existem os elementos inversos de todos os elementos do conjunto. Note que a tábua não é simétrica. Segue que a operação não é comutativa.*
Além disso,

$$R^2_{\frac{2\pi}{3}} = R_{\frac{4\pi}{3}}$$
$$M_1 \circ R_{\frac{2\pi}{3}} = M_3$$
$$M_1 \circ R^2_{\frac{2\pi}{3}} = M_2$$

Então, $D_3 = \left\{R^0_{\frac{2\pi}{3}},\ R_{\frac{2\pi}{3}},\ R^2_{\frac{2\pi}{3}},\ M_1,\ M_1 \circ R_{\frac{2\pi}{3}},\ M_1 \circ R^2_{\frac{2\pi}{3}}\right\}$*, ou seja,* D_3 *é gerado* $R_{\frac{2\pi}{3}}$ *e* M_1.

Exemplo 2.1.12. *Considere um quadrado de vértices 1, 2, 3, 4, as retas* m_1 *e* m_2 *que passam pelas diagonais 13 e 24 do quadrado, respectivamente, e as retas* m_3 *e* m_4 *perpendiculares aos lados 12 e 34 e, 23 e 14, que passam pelos pontos médios desses lados, respectivamente, sendo O o ponto de interseção entre essas retas, como pode-se observar na figura 2.*

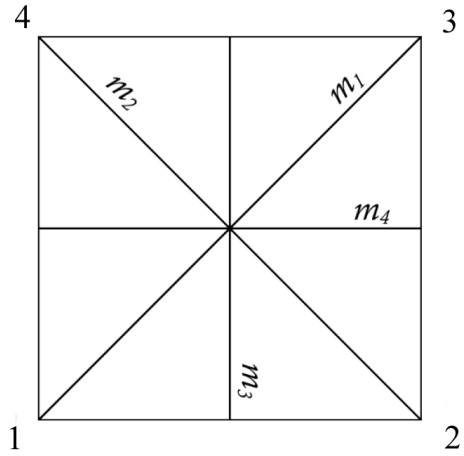


Figura 2: Quadrado

Denote por R_0, $R_{\frac{\pi}{2}}$, R_π *e* $R_{\frac{3\pi}{2}}$ *as rotações de* 0, $\frac{\pi}{2}$, π *e* $\frac{3\pi}{2}$ *radianos em torno de O, respectivamente, no sentido anti-horário. Sejam* M_1 *e* M_2 *as reflexões de* π *radianos em torno das diagonais* m_1 *e* m_2, M_3 *e* M_4 *as reflexões de* π *radianos em torno das perpendiculares* m_3 *e* m_4. *O conjunto das simetrias do quadrado* $D_4 = \left\{R_0, R_{\frac{\pi}{2}}, R_\pi, R_{\frac{3\pi}{2}}, M_1, M_2, M_3, M_4\right\}$ *munido da composição de transformações é um grupo não abeliano.*

De fato, efetuando todas as composições possíveis, obtêm-se a seguinte tábua:

$\circ$	R_0	$R_{\frac{\pi}{2}}$	R_π	$R_{\frac{3\pi}{2}}$	M_1	M_2	M_3	M_4
R_0	R_0	$R_{\frac{\pi}{2}}$	R_π	$R_{\frac{3\pi}{2}}$	M_1	M_2	M_3	M_4
$R_{\frac{\pi}{2}}$	$R_{\frac{\pi}{2}}$	R_π	$R_{\frac{3\pi}{2}}$	R_0	M_3	M_4	M_2	M_1
R_π	R_π	$R_{\frac{3\pi}{2}}$	R_0	$R_{\frac{\pi}{2}}$	M_2	M_1	M_4	M_3
$R_{\frac{3\pi}{2}}$	$R_{\frac{3\pi}{2}}$	R_0	$R_{\frac{\pi}{2}}$	R_π	M_4	M_3	M_1	M_2
M_1	M_1	M_3	M_2	M_4	R_0	R_π	$R_{\frac{\pi}{2}}$	$R_{\frac{3\pi}{2}}$
M_2	M_2	M_4	M_1	M_3	R_π	R_0	$R_{\frac{3\pi}{2}}$	$R_{\frac{\pi}{2}}$
M_3	M_3	M_2	M_4	M_1	$R_{\frac{3\pi}{2}}$	$R_{\frac{\pi}{2}}$	R_0	R_π
M_4	M_4	M_1	M_3	M_2	$R_{\frac{\pi}{2}}$	$R_{\frac{3\pi}{2}}$	R_π	R_0

Sabe-se que a composição de transformações é associativa. Pela tábua é possível observar que R_0 *é o elemento neutro e que existem os elementos inversos de todos os elementos do conjunto. Note que a tábua não é simétrica. Segue que a operação não é comutativa.*

Além disso,

$$\begin{aligned} R_{\frac{\pi}{2}}^2 &= R_\pi \\ R_{\frac{\pi}{2}}^3 &= R_{\frac{3\pi}{2}} \\ M_1 \circ R_{\frac{\pi}{2}} &= M_3 \\ M_1 \circ R_{\frac{\pi}{2}}^2 &= M_2 \\ M_1 \circ R_{\frac{\pi}{2}}^3 &= M_4 \end{aligned}$$

Então, $D_4 = \left\{R_{\frac{\pi}{2}}^0,\, R_{\frac{\pi}{2}},\, R_{\frac{\pi}{2}}^2,\, R_{\frac{\pi}{2}}^3,\, M_1,\, M_1 \circ R_{\frac{\pi}{2}},\, M_1 \circ R_{\frac{\pi}{2}}^2,\, M_1 \circ R_{\frac{\pi}{2}}^3\right\}$*, ou seja,* D_4 *é gerado por* $R_{\frac{\pi}{2}}$ *e* M_1*.*

É possível estender o conceito de grupo de simetrias para polígonos regulares de lado n.

Exemplo 2.1.13. *Com base nos exemplos anteriores de grupo de simetrias, nota-se que o número de simetrias de um polígono regular de n lados é* $2n$*.*
Denote os vértices desse polígono por $1,2,\ldots,n$ *e considere* D_n *o conjunto das simetrias desse polígono.* D_n *é gerado pela rotação* $R_{\frac{2\pi}{n}}$ *de* $\frac{2\pi}{n}$ *radianos em torno do centro O do polígono, e pela reflexão* M_1 *de* π *radianos em torno da reta* m_1 *que passa pelo vértice 1 e por O.*
O conjunto $D_n = \left\{R_{\frac{2\pi}{n}}^0, R_{\frac{2\pi}{n}}, R_{\frac{2\pi}{n}}^2, \ldots, R_{\frac{2\pi}{n}}^{n-1}, M_1, M_1 \circ R_{\frac{2\pi}{n}}, M_1 \circ R_{\frac{2\pi}{n}}^2, \ldots, M_1 \circ R_{\frac{2\pi}{n}}^{n-1}\right\}$ *munido da operação de composição é um grupo não abeliano, denominado* ***grupo diedral****.*

Exemplo 2.1.14. *Sejam* $(G,\circ)$ *e* $(H,\cdot)$ *grupos. Considere o produto cartesiano de G e H,* $G \times H = \{(g,h) \colon g \in G, h \in H\}$*. Defina a operação* $*$ *de* $G \times H$ *como*

$$(g_1,h_1) * (g_2,h_2) = (g_1 \circ g_2, h_1 \cdot h_2)$$

para todo $g_1,g_2 \in G$ *e* $h_1,h_2 \in H$*. Afirma-se que o conjunto* $G \times H$ *munido da operação* $*$ *é um grupo. De fato, a associatividade da operação* $*$ *decorre da associatividade das operações dos grupos G e H. O elemento neutro de* $G \times H$ *é* (e_G,e_H)*, sendo* e_G *e* e_H *elementos neutros de G e H, respectivamente. O inverso de* $(g,h) \in G \times H$ *é dado por* (g^{-1},h^{-1})*, sendo* $g^{-1} \in G$ *o inverso de g e* $h^{-1} \in H$ *o inverso de h.*

Definição 2.1.15. *Seja G um grupo. Diz-se que G é um* ***grupo finito*** *quando G é um conjunto finito.*

Definição 2.1.16. *Seja G um grupo finito. O número de elementos do conjunto G é denominado* ***ordem*** *do grupo G, e é denotado por* $o(G)$ *ou* $|G|$*.*

Observação 2.1.17. *Nesse texto, a notação para ordem do grupo G será* $o(G)$*.*

2.2 SUBGRUPOS

É interessante encontrar subconjuntos de grupos que tenham as mesmas propriedades desses grupos.

Definição 2.2.1. *Sejam G um grupo e H um subconjunto não vazio de G. Diz-se que H é um* ***subgrupo*** *de G, e denota-se por $H < G$, quando H é grupo com respeito a mesma operação de G.*

Observação 2.2.2. *O elemento neutro do subgrupo e o inverso de um elemento do subgrupo são os mesmos do grupo.*

Para facilitar a prova de que um subconjunto não vazio de um grupo é um subgrupo, pode ser utilizado o resultado abaixo, que decorre da definição.

Proposição 2.2.3. *Seja G um grupo e H um subconjunto não vazio de G. Então, H é subgrupo de G se, e somente se, as condições abaixo são satisfeitas:*

(i) $ab \in H$

(ii) $a^{-1} \in H$

para todo $a, b \in H$.

Demonstração:
$(\Rightarrow)$ Por hipótese H é subgrupo de G. Então, H é grupo e é fechado em relação a sua operação. Logo, vale a condição (i). Como H é grupo, então existe o elemento inverso $a^{-1} \in H$, para todo $a \in H$. Logo, vale a condição (ii).
$(\Leftarrow)$ Por hipótese, são satisfeitas as condições (i) e (ii). Da condição (i), decorre que H é fechado em relação à operação. Falta mostrar que H é grupo.
Vale a associatividade para todo elemento de G. Como $H \subset G$, então vale a associatividade para todo elemento de H.
Como H é não vazio, então existe $a \in H$. Pela condição (ii), existe o elemento inverso $a^{-1} \in H$ de a. Pela condição (i), $a^{-1}a \in H$. Sabendo que $a^{-1}a = e$, tem-se que $e \in H$. Conclui-se a existência do elemento neutro e em H.
A existência do elemento inverso de $a \in H$ segue da condição (ii).
Logo, H é grupo. Portanto, H é subgrupo de G.

□

Seguem alguns exemplos de subgrupos.

Exemplo 2.2.4. *Seja G um grupo. Sendo e o elemento neutro de G, tem-se que $\{e\}$ e G são subgrupos de G, denominados subgrupos triviais de G.*

Exemplo 2.2.5. *Seja $\mathbb{Z}$ um grupo. Então, $n\mathbb{Z} = \{n\alpha : \alpha \in \mathbb{Z}\}$ é subgrupo de $\mathbb{Z}$, para todo $n \in \mathbb{Z}$. De fato,*

(i) *$n\mathbb{Z} \neq \emptyset$, já que $n \in n\mathbb{Z}$.*

(ii) *Sendo na, $nb \in n\mathbb{Z}$, tem-se que $na + nb = n(a+b) \in n\mathbb{Z}$.*

(iii) *Sendo $na \in n\mathbb{Z}$, tem-se que $-na = n(-a) \in n\mathbb{Z}$ é o inverso de na.*

Exemplo 2.2.6. *Considere o grupo $D_3 = \left\{R^0_{\frac{2\pi}{3}}, R_{\frac{2\pi}{3}}, R^2_{\frac{2\pi}{3}}, M_1, M_1 \circ R_{\frac{2\pi}{3}}, M_1 \circ R^2_{\frac{2\pi}{3}}\right\}$. Note que o subconjunto das rotações de D_3 dado por $R_{D_3} = \left\{R^0_{\frac{2\pi}{3}}, R_{\frac{2\pi}{3}}, R^2_{\frac{2\pi}{3}}\right\}$ é um subgrupo de D_3. Basta observar na tábua do grupo D_3.*

Exemplo 2.2.7. *O conjunto $SL_n(\mathbb{C}) = \{A \in GL_n(\mathbb{C}) : \det(A) = 1\}$ é subgrupo de $GL_n(\mathbb{C})$. Com efeito,*

(i) *$SL_n(\mathbb{C}) \neq \emptyset$, pois a matriz identidade I pertence a esse conjunto.*

(ii) *Sejam A, $B \in SL_n(\mathbb{C})$, então $\det(A) = \det(B) = 1$. Mas $\det(AB) = \det(A)\det(B) = 1$. Portanto, $AB \in SL_n(\mathbb{C})$.*

(iii) *Seja $A \in SL_n$, então $\det(A) = 1 \neq 0$. Segue que existe A^{-1} tal que $AA^{-1} = A^{-1}A = I$, sendo $\det(A^{-1}) = \frac{1}{1} = 1$. Logo, $A^{-1} \in SL_n(\mathbb{C})$.*

Exemplo 2.2.8. *Seja G um grupo. Se H_1 e H_2 são subgrupos de G, então $H_1 \cap H_2$ também é subgrupo de G. De fato,*

(i) *Seja e o elemento neutro de G. Como H_1 e H_2 são subgrupos de G, tem-se $e \in H_1$, $e \in H_2$. Logo, $e \in H_1 \cap H_2$. Segue que $H_1 \cap H_2 \neq \emptyset$.*

(ii) *Considere a, $b \in H_1 \cap H_2$, então a, $b \in H_1$ e a, $b \in H_2$. Pelo fato de H_1 e H_2 serem subgrupos, $ab \in H_1$ e $ab \in H_2$. Logo, $ab \in H_1 \cap H_2$.*

(iii) *Sendo $a \in H_1 \cap H_2$, tem-se que $a \in H_1$ e $a \in H_2$. Pelo fato de H_1 e H_2 serem subgrupos, $a^{-1} \in H_1$ e $a^{-1} \in H_2$. Logo, $a^{-1} \in H_1 \cap H_2$.*

Observação 2.2.9. *Em geral, a união de subgrupos não é diretamente um subgrupo. São necessárias algumas condições. Sendo G um grupo, se H_1 e H_2 são subgrupos de G, então $H_1 \cup H_2$ é subgrupo de G se, e somente se, $H_1 \subset H_2$ ou $H_2 \subset H_1$.*

2.3 HOMOMORFISMO DE GRUPOS

Considere as tábuas dos grupos $(G,\cdot)$ e $(\mathbb{Z}_2,+)$, sendo $G=\{-1,1\}$ e $\mathbb{Z}_2=\{\bar{0},\bar{1}\}$.

Tabela 1: Tábua do grupo $(G,\cdot)$

$\cdot$	1	-1
1	1	-1
-1	-1	1

Tabela 2: Tábua do grupo $(\mathbb{Z}_2,+)$

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

Perceba que eles têm a mesma estrutura, como pode ser generalizado na tábua de uma operação qualquer $*$.

Tabela 3: Tábua da operação $*$

$*$	a	b
a	a	b
b	b	a

Quando um grupo tem a mesma estrutura de outro, eles são ditos isomorfos.

A definição de homomorfismo de grupos permite definir isomorfismo de grupos, um conceito bastante importante.

Definição 2.3.1. *Sejam $(G,*)$ e $(J,\cdot)$ grupos. Diz-se que uma aplicação f é **homomorfismo** de G em J quando*

$$\begin{aligned} f: \quad & G \to J \\ & a*b \mapsto f(a)\cdot f(b) \end{aligned}$$

para todos $a,b \in G$.

Observação 2.3.2. *Se um homomorfismo é uma aplicação injetora, então é dito homomorfismo injetor (ou monomorfismo). Se um homomorfismo é uma aplicação sobrejetora, então é dito homomorfismo sobrejetor (ou epimorfismo).*

Considere G e J grupos, sendo e e e_J os elementos neutros de G e J, respectivamente. Se $f: G \to J$ é um homomorfismo de G em J, então valem as seguintes propriedades:

Propriedade 2.3.3. $f(e) = e_J$.

Demonstração:
Como f é um homomorfismo, então

$$f(e)f(e) = f(ee) = f(e) = e_J f(e)$$

Sabendo que todo elemento do grupo é regular para a operação, segue que $f(e) = e_J$.

□

Propriedade 2.3.4. $f(a^{-1}) = f(a)^{-1}$, $\forall a \in G$.

Demonstração:
Como f é homomorfismo, então

$$f(a)f(a^{-1}) = f(aa^{-1}) = f(e) = e_J = f(a)f(a)^{-1}$$

Sabendo que todo elemento do grupo é regular para a operação, segue que $f(a^{-1}) = f(a)^{-1}$.

□

Corolário 2.3.5. $f(ab^{-1}) = f(a)f(b)^{-1}$, *para todo* $a, b \in G$.

Demonstração:
Como f é homomorfismo, então

$$f(ab^{-1}) = f(a)f(b^{-1}) = f(a)f(b)^{-1}.$$

□

O próximo resultado afirma que se f é um homomorfismo, então f transforma subgrupo de G em subgrupo de J.

Proposição 2.3.6. *Se* H *é subgrupo de* G, *então* $f(H)$ *é subgrupo de* J.

Demonstração:
Por hipótese H é subgrupo de G, então $e \in H$ é elemento neutro de H. Daí,

$$e_J = f(e) \in f(H) \subset J.$$

Logo, $f(H) \neq \emptyset$.
Para mostrar que $f(H)$ é subgrupo de J, utiliza-se a proposição 2.2.3.
O fato de H ser subgrupo de G implica que $H \neq \emptyset$. Se $a, b \in H$, então, $f(a), f(b) \in f(H)$. Como f é homomorfismo, $f(a)f(b) = f(ab)$. Note que $ab \in H$, pois H é subgrupo de G. Segue que, $f(ab) = f(a)f(b) \in f(H)$.
Como H é subgrupo de G, existe o elemento inverso $a^{-1} \in H$ de $a \in H$. Daí, $f(a^{-1}) \in f(H)$. Mas, $f(a^{-1}) = f(a)^{-1}$. Logo, $f(a)^{-1} \in f(H)$.
Portanto, $f(H)$ é subgrupo de J.

□

Exemplo 2.3.7. *Seja G um grupo e $Id\colon G \to G$ a aplicação definida por $Id(a) = a$, para todo $a \in G$. Se a, $b \in G$, então $Id(ab) = ab = Id(a)Id(b)$. Logo, Id é homomorfismo de G em G denominado* ***homomorfismo identidade****.*

Exemplo 2.3.8. *Seja G um grupo e $e\colon G \to G$ a aplicação definida por $e(a) = e_G$, para todo $a \in G$, sendo e_G o elemento neutro de G. Se a, $b \in G$, então $e(ab) = e_G = e_G e_G = e(a)e(b)$. Logo, e é homomorfismo de G em G denominado* ***homomorfismo trivial****.*

Exemplo 2.3.9. *Sejam $(\mathbb{R}_+, \cdot)$ e $(\mathbb{R}, +)$ grupos. Considere $f\colon (\mathbb{R}_+, \cdot) \to (\mathbb{R}, +)$ a aplicação definida por $f(a) = \log_{10}(a)$, para todo $a \in G$. Se a, $b \in G$, então*

$$f(ab) = \log_{10}(ab) = \log_{10}(a) + \log_{10}(b) = f(a) + f(b).$$

Logo, f é homomorfismo de $\mathbb{R}_+$ em $\mathbb{R}$.

Exemplo 2.3.10. *Sejam $GL_n(\mathbb{R})$ e $(\mathbb{R} \setminus \{0\}, \cdot)$ grupos. Considere $f\colon GL_n(\mathbb{R}) \to (\mathbb{R} \setminus \{0\}, \cdot)$ a aplicação definida por $f(A) = \det(A)$, para todo $A \in GL_n(\mathbb{R})$. Se A, $B \in GL_n(\mathbb{R})$, então*

$$f(AB) = \det(AB) = \det(A)\det(B) = f(A)f(B).$$

Logo, f é homomorfismo de $GL_n(\mathbb{R})$ em $(\mathbb{R} \setminus \{0\}, \cdot)$.

Se G e J são grupos e $f\colon G \to J$ é um homomorfismo, define-se o **núcleo** do homomorfismo f como sendo o conjunto:

$$Nu(f) = Ker(f) = \{a \in G\colon f(a) = e_J\},$$

onde e_J o elemento neutro de J.

Observação 2.3.11. *Nesse trabalho, será utilizada a notação $Nu(f)$ para representar o núcleo de um homomorfismo f.*

Proposição 2.3.12. *Sejam G e J grupos e seja $f\colon G \to J$ um homomorfismo de grupos. Então, $Nu(f)$ é um subgrupo de G.*

Demonstração:
Para demonstrar essa propriedade será utilizada a proposição (2.2.3). Como f é um homomorfismo, então $f(e) = e_J$. Logo, pela definição de núcleo de homomorfismo, $e \in Nu(f)$, ou seja, $Nu(f) \neq \emptyset$. Sejam $a, b \in Nu(f)$, então $f(a) = f(b) = e_J$. Daí,

$$f(ab) = f(a)f(b) = e_J e_J = e_J.$$

Logo, $ab \in Nu(f)$. Como G é grupo, então existe o inverso de $a^{-1} \in G$ de $a \in G$. Assim,

$$f(a^{-1}) = f(a)^{-1} = e_J^{-1} = e_J.$$

Segue que, $a^{-1} \in Nu(f)$. Portanto, $Nu(f)$ é subgrupo de G.

□

Proposição 2.3.13. *Sejam G e J grupos e seja $f\colon G \to J$ um homomorfismo de grupos. Então, f é um homomorfismo injetor se, e somente se, $Nu(f) = \{e\}$.*

Demonstração:
($\Rightarrow$) Se $a \in Nu(f)$, então $f(a) = e_J$. Mas $f(e) = e_J$. Daí, $f(a) = f(e)$. Por hipótese, f é homomorfismo injetor, $a = e$. Portanto, $Nu(f) = \{e\}$.
($\Leftarrow$) Por outro lado, sejam $a, b \in G$ tal que $f(a) = f(b)$. Então, $f(ab^{-1}) = f(a)f(b)^{-1} = f(b)f(b)^{-1} = e_J$. Segue que, $ab^{-1} \in Nu(f)$. Por hipótese, $Nu(f) = \{e\}$, então $ab^{-1} = e$, ou seja, $ab^{-1}b = eb$. Logo, $a = b$. Portanto, f é homomorfismo injetor.

□

Conhecendo homomorfismo de grupos é possível introduzir a definição de isomorfismo de grupos. A ideia de isomorfismo de grupos é que se existem dois grupos isomorfos, então eles têm as mesmas características, ou seja, um pode ser substituído pelo outro.

Definição 2.3.14. *Sejam G e J grupos e seja $f\colon G \to J$ um homomorfismo de grupos. Diz-se que f é um **isomorfismo** de G em J quando f é bijetor.*

A proposição a seguir afirma que se uma aplicação é um isomorfismo, então a aplicação inversa também é.

Proposição 2.3.15. *Sejam G e J grupos. Se $f\colon G \to J$ é isomorfismo, então $f^{-1}\colon J \to G$ é isomorfismo.*

Demonstração:
Para demonstrar que f^{-1} é isomorfismo é necessário mostrar que é bijetor e que é um homomorfismo.
Como f é uma aplicação bijetora, então f^{-1} é bijetora.
Por hipótese f é isomorfismo, então f é sobrejetor. Logo, para todo $c,d \in J$, existem $a,b \in G$, tais que $c = f(a)$ e $d = f(b)$. Como f admite inversa, porque é bijetora, segue que $f^{-1}(c) = a$ e $f^{-1}(d) = b$. Daí,

$$f^{-1}(cd) = f^{-1}(f(a)f(b)) = f^{-1}(f(ab)) = ab = f^{-1}(c)f^{-1}(d)$$

Logo, f^{-1} é homomorfismo. Portanto, f^{-1} é isomorfismo.

□

Observação 2.3.16. *Sejam G e J grupos e $f\colon G \to J$ um isomorfismo de grupos. Diz-se que G e J são **grupos isomorfos**, e denota-se por $G \cong J$.*

Exemplo 2.3.17. *O grupo $(\mathbb{R},+)$ é isomorfo ao grupo $(\mathbb{R}_+,\cdot)$. De fato, considere a aplicação $f\colon (\mathbb{R},+) \to (\mathbb{R}_+,\cdot)$ dada por $f(a) = e^a$, para todo $a \in \mathbb{R}$.*

(i) Sendo a, $b \in \mathbb{R}$, tem-se $f(a+b) = e^{a+b} = e^a e^b = f(a)f(b)$. Logo, f é homomorfismo.

(ii) Suponha $f(a) = f(b)$, para a, $b \in \mathbb{R}$, então $e^a = e^b$. Segue que $a\ln e = \ln e^a = \ln e^b = b\ln e$, ou seja, $a = b$. Logo, f é injetora.

(iii) Dado $b \in \mathbb{R}_+$, objetiva-se mostrar que existe $a \in \mathbb{R}$ tal que $f(a) = b$. Assim, basta considerar $a = \ln b$, pois $f(a) = f(\ln b) = e^{\ln b} = b$. Logo, f é sobrejetora.

2.4 GRUPOS CÍCLICOS

Um fato sobre os grupos cíclicos é a possibilidade de caracterizá-los, isto é, ou eles são isomorfos a $\mathbb{Z}$ ou a $\mathbb{Z}_m$. Para definir um grupo cíclico é necessário conhecer os conceitos de potência e múltiplo.

Definição 2.4.1. *Seja G um grupo multiplicativo e considere $a \in G$ e $m \in \mathbb{Z}$. A **potência***

m-ésima *de a é denotada por* a^m *e definida por*

$$a^m = \begin{cases} e, & m = 0 \\ a^{m-1}a, & m > 0 \\ (a^{-m})^{-1}, & m < 0 \end{cases}$$

sendo e o elemento neutro de G.

Observação 2.4.2. *Tem-se que* $e^m = e$*, para todo* $m \in \mathbb{Z}$*.*

Proposição 2.4.3. *Seja G um grupo multiplicativo. Se* $m,n \in \mathbb{Z}$ *e* $a \in G$*, então valem as seguintes propriedades:*

(i) $a^m a^n = a^{m+n}$

(ii) $a^{-m} = (a^m)^{-1}$

(iii) $(a^m)^n = a^{mn}$

Demonstração:
A demonstração é feita utilizando indução.

Corolário 2.4.4. *Sejam G um grupo multiplicativo,* $a \in G$ *e* $m,n \in \mathbb{Z}$*, então* $a^m a^n = a^n a^m$*.*

Demonstração:
Esse corolário decorre diretamente do item (i) da proposição 2.4.3 e da comutatividade da soma no conjunto $\mathbb{Z}$, pois

$$a^m a^n = a^{m+n} = a^{n+m} = a^n a^m$$

para todo $m,n \in \mathbb{Z}$ e $a \in G$.

□

Definição 2.4.5. *Seja G um grupo aditivo e considere* $a \in G$ *e* $m \in \mathbb{Z}$*. O* ***múltiplo m-ésimo*** *de a é denotado por ma e definido por*

$$ma = \begin{cases} e, & m = 0 \\ (m-1)a + a, & m > 0 \\ -((-m)a), & m < 0 \end{cases}$$

sendo e o elemento neutro de G.

Proposição 2.4.6. *Seja G um grupo aditivo. Se $m,n \in \mathbb{Z}$ e $a \in G$, então valem as seguintes propriedades:*

(i) $ma + na = (m+n)a$

(ii) $(-m)a = -(ma)$

(iii) $n(ma) = (nm)a$

Demonstração:
A demonstração é feita utilizando indução.

Definição 2.4.7. *Sejam G um grupo e H um subconjunto qualquer de G. O conjunto*

$$\{h_1 h_2 \dots h_i : h_i \in H,\ i \in \mathbb{N}\}$$

é um subgrupo de G denominado ***subgrupo gerado por*** *H, e denotado por $\langle H \rangle$.*

Definição 2.4.8. *Seja G um grupo multiplicativo e $a \in G$. O conjunto das* ***potências inteiras*** *de a é denotado por $\langle a \rangle$ e definido por*

$$\langle a \rangle = \{a^m : m \in \mathbb{Z}\}.$$

A proposição a seguir afirma que se G é um grupo e $a \in G$, então $\langle a \rangle$ é subgrupo de G, e mais, $\langle a \rangle$ é o menor subgrupo de G que contém a.

Proposição 2.4.9. *Seja G um grupo multiplicativo e $a \in G$, então*

(i) *$\langle a \rangle$ é subgrupo de G;*

(ii) *Se H é subgrupo de G e $a \in H$, então $\langle a \rangle \subset H$.*

Demonstração:

(i) Note que $e = a^0 \in \langle a \rangle$. Logo, $\langle a \rangle \neq \emptyset$. Sejam $r,s \in \langle a \rangle$, tal que $r = a^m$ e $s = a^n$, sendo $m,n \in \mathbb{Z}$. Assim, $rs = a^m a^n = a^{m+n} \in \langle a \rangle$. E, $r^{-1} = (a^m)^{-1} = a^{-m} \in \langle a \rangle$. Logo, $\langle a \rangle$ é subgrupo de G.

(ii) Por hipótese, H é subgrupo de G e $a \in H$, então $a^n \in H$, para todo $n \in \mathbb{Z}$. Portanto, $\langle a \rangle \subset H$.

□

A definição abaixo afirma que um grupo é cíclico quando todos os seus elementos podem ser escritos como potência de um único elemento do grupo.

Definição 2.4.10. *Seja G um grupo multiplicativo e $a \in G$. Diz-se que G é um* ***grupo cíclico*** *quando G é igual ao conjunto das potências inteiras de a, ou seja,*

$$G = \langle a \rangle = \{a^m : m \in \mathbb{Z}\}.$$

Observação 2.4.11. *A definição de grupo cíclico vale para qualquer grupo. Então, se G é um grupo aditivo, diz-se que G é um grupo cíclico quando $G = \langle a \rangle = \{ma : m \in \mathbb{Z}\}$, para $a \in G$. Nesse texto, serão utilizados o grupo multiplicativo e as potências, para facilitar a notação.*

Tem-se que todo subgrupo de um grupo cíclico é cíclico. E se um grupo é cíclico, então é abeliano. A demonstração pode ser vista em Domingues e Iezzi (2003).

Definição 2.4.12. *Seja G um grupo e $a \in G$. A* ***ordem de a****, denotada por $o(a)$, é a ordem do subgrupo cíclico $\langle a \rangle$.*

Exemplo 2.4.13. *O grupo $\mathbb{Z}$ é cíclico, pois $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$.*

Exemplo 2.4.14. *O grupo $\mathbb{Z}_4$ é cíclico, pois $\mathbb{Z}_4 = \langle \overline{1} \rangle = \langle \overline{3} \rangle$.*

2.5 CLASSES LATERAIS

O conceito de classes laterais permite estender a definição de congruência.

Definição 2.5.1. *Sejam $m \in \mathbb{Z} \setminus \{0\}$ e $a, b \in \mathbb{Z}$. Diz-se que a é* ***congruente*** *b módulo m, e denota-se por $a \equiv b \mod m$, quando os restos das divisões de a e b por m são iguais.*

A proposição a seguir é importante em relação às congruências. Ela fornece um método prático para verificar se dois números são congruentes módulo m. A demonstração pode ser vista em Hefez (2011).

Proposição 2.5.2. *Sejam $a, b \in \mathbb{Z}$ tais que $b \geqslant a$. Tem-se que $a \equiv b \mod m$ se, e somente se, $m | b - a$, ou seja, $b - a = mk$, para algum $k \in \mathbb{Z}$.*

Agora, seja H um subgrupo não trivial de $\mathbb{Z}$. Como $\mathbb{Z}$ é um grupo cíclico, tem-se que H é cíclico, ou seja, existe $h \in H$ tal que $H = \langle h \rangle = \{hk : k \in \mathbb{Z}\}$. Então, para todo $a, b \in \mathbb{Z}$ segue que $a \equiv b \mod h$ se, e somente se, $b - a = hk$, para algum $k \in \mathbb{Z}$, ou seja, $b - a \in H$.

Note que $b-a=b+(-a)\in H$, isto é, b operação com o inverso de a deve estar em H. Desse modo, segue a proposição abaixo.

Proposição 2.5.3. *Sejam G um grupo e H um subgrupo de G. Defina a relação $\equiv$ sobre G de forma que $a\equiv b$ se, e somente se, $a^{-1}b\in H$. Tem-se que:*

1. *$\equiv$ é uma relação de equivalência.*
2. *Se $a\in G$, então $\overline{a}=aH=\{ah\colon h\in H\}$.*

Demonstração:

1. Considere $a,b,c\in G$.
   Como $e=a^{-1}a\in H$, segue que $a\equiv a$, ou seja, $\equiv$ é reflexiva.
   Supondo que $a\equiv b$, tem-se que $a^{-1}b\in H$, então $(a^{-1}b)^{-1}\in H$. Como H é subgrupo, $(a^{-1}b)^{-1}=b^{-1}(a^{-1})^{-1}\in H$. Segue que $b^{-1}a\in H$. Logo, $b\equiv a$. Assim, $\equiv$ é simétrica.
   Considere que $a\equiv b$ e $b\equiv c$. Tem-se que $a^{-1}b\in H$ e $b^{-1}c\in H$. Como H é subgrupo, $(a^{-1}b)(b^{-1}c)\in H$. Segue que $(a^{-1}b)(b^{-1}c)=a^{-1}(bb^{-1})c=a^{-1}c\in H$. Logo, $\equiv$ é transitiva.
   Portanto, $\equiv$ é uma relação de equivalência.

2. Se $x\in\overline{a}=\{x\in G\colon x\equiv a\}$, então $x\equiv a$. Por definição, $x^{-1}a\in H$, ou seja, $x^{-1}a=h,h\in H$. Daí,

$$xx^{-1}a=xh\implies ah^{-1}=xhh^{-1}\implies x=ah^{-1}.$$

   Como $h^{-1}\in H$, segue que $x\in aH$. Logo, $\overline{a}\subset aH$.
   Por outro lado, se $x\in aH$, ou seja, $x=ah,h\in H$, vem que,

$$x^{-1}xh^{-1}=x^{-1}ahh^{-1}\implies h^{-1}=x^{-1}a$$

   Sendo H subgrupo, então $h^{-1}=x^{-1}a\in H$. Por definição, $x\equiv a$. Logo, $x\in\overline{a}$. Assim, $aH\subset\overline{a}$.

   Portanto, $\overline{a}=aH$.

□

Com base na proposição anterior, a definição de congruência estende-se do seguinte modo:

Definição 2.5.4. *Sejam G um grupo e H um subgrupo de G. Diz-se que a é **congruente** b módulo H, e denota-se por $a \equiv b \mod H$, quando $a^{-1}b \in H$, para $a, b \in G$.*

E define-se a classe de equivalência $\overline{a}$ de $a \in G$ da seguinte maneira:

Definição 2.5.5. *Seja G um grupo. Para cada $a \in G$, a classe de equivalência $\overline{a} \in H$, dada por*

$$\{x \in G : x \equiv a\} = \overline{a} = aH = \{ah : h \in H\}, \text{ sendo } \equiv \text{ definida por : } a \equiv b \iff a^{-1}b \in H$$

*é denominada **classe lateral** à esquerda módulo H determinada por a (ou classe lateral à esquerda de H em G que contém a).*

Exemplo 2.5.6. *Considere o grupo $\mathbb{Z}_8$. Um subgrupo de $\mathbb{Z}_8$ é $H = \{\overline{0}, \overline{4}\}$. As classes laterais são dadas pelo conjunto $\overline{a} + H = \{\overline{a} + h : h \in H\}$. Assim,*

$$\overline{0} + H = \{\overline{0} + h : h \in H\} = \{\overline{0} + \overline{0},\ \overline{0} + \overline{4}\} = \{\overline{0}, \overline{4}\}$$
$$\overline{1} + H = \{\overline{1} + h : h \in H\} = \{\overline{1} + \overline{0},\ \overline{1} + \overline{4}\} = \{\overline{1}, \overline{5}\}$$
$$\overline{2} + H = \{\overline{2} + h : h \in H\} = \{\overline{2} + \overline{0},\ \overline{2} + \overline{4}\} = \{\overline{2}, \overline{6}\}$$
$$\overline{3} + H = \{\overline{3} + h : h \in H\} = \{\overline{3} + \overline{0},\ \overline{3} + \overline{4}\} = \{\overline{3}, \overline{7}\}$$

As classes laterais $\overline{a} + H$, para $a \in \{4, 5, 6, 7, 8\}$ serão repetições das classes já encontradas.

O conjunto das classes laterais à esquerda módulo H é denominado conjunto quociente de G pela relação $\equiv$.

Definição 2.5.7. *Sejam G um grupo e H um subgrupo de G. O conjunto quociente de G por essa relação $\equiv$, denotado por G/H, é o conjunto das classes laterais aH, para algum $a \in G$. Em símbolos,*

$$G/H = \{aH : a \in G\}.$$

Observação 2.5.8. *Note que $eH = H \in G/H$, logo $G/H \neq \emptyset$.*

Desse modo, G/H é uma partição de G, ou seja,

1. Se $a \in G$, então $aH \neq 0$
2. Se $a, b \in G$, então $aH = bH$ ou $aH \cap bH = \emptyset$
3. A união de todas as classes laterais é igual a G.

Para que seja possível afirmar que G/H é um grupo, é necessário o conceito de subgrupo normal, o qual garante a boa definição da operação, e será visto mais adiante.

Se G é um grupo e H é um subgrupo de G, então duas classes laterais quaisquer módulo H têm a mesma cardinalidade de H.

Definição 2.5.9. *O número de elementos distintos pertencentes a G/H é denominado* ***índice*** *de H em G e denotado por $(G\colon H)$.*

Observação 2.5.10. *É possível desenvolver a teoria de classes laterais tanto para classes laterais à direita, quanto para classes laterais à esquerda, já que a aplicação*

$$f\colon \{\textit{classes laterais à esquerda}\} \to \{\textit{classes laterais à direita}\}$$
$$aH \mapsto Ha^{-1}$$

é bijetora.

2.6 TEOREMA DE LAGRANGE

O teorema a seguir relaciona a teoria de grupos finitos com a teoria de divisibilidade dos inteiros.

Teorema 2.6.1. *(Teorema de Lagrange) Sejam G um grupo finito e H um subgrupo de G, então $o(G) = o(H)(G:H)$, ou seja, $o(H)|o(G)$.*

Demonstração:
Seja $(G:H) = r$, então $G/H = \{a_1H, a_2H, \ldots, a_rH\}$. Como G/H é uma partição de G,

$$G = a_1H \cup a_2H \cup \ldots \cup a_rH,$$

sendo $a_iH \cap a_jH = \emptyset$, $i, j \in \{1, \ldots, r\colon i \neq j\}$. Segue que

$$o(G) = o(a_1H) + o(a_2H) + \ldots + o(a_rH).$$

Mas $o(a_1H) = o(a_2H) = \ldots = o(a_rH) = o(H)$. Logo, $o(G) = o(H)r = o(H)(G:H)$.

□

Corolário 2.6.2. *Seja G um grupo finito tal que $o(G) = p$, p primo. Então, G é cíclico e os únicos subgrupos de G são os triviais.*

Demonstração:
Sendo $o(G) = p$, então $p > 1$, ou seja, existe $a \in G$ tal que $a \neq e$. Logo, $H = \langle a \rangle$ é um subgrupo de G tal que $o(H) \geqslant 2$. Pelo teorema de Lagrange, $o(H)|o(G) = p$. Assim, $o(H) = p$. Considerando o fato de que $H \subset G$, segue que $\langle a \rangle = G$, isto é, G é cíclico.
É claro que os únicos subgrupos de G são os triviais.

□

Proposição 2.6.3. *Seja G um grupo. Se $o(G) \leqslant 5$, então G é abeliano.*

Demonstração:
Sendo $o(G) = 1$, então $G = \{e\}$. Logo, G é abeliano.
Suponha $o(G) = 2, 3$ ou 5, pelo corolário anterior, G é cíclico. Daí, G é abeliano. (Os grupos de ordem 2, 3 e 5 são isomorfos a $\mathbb{Z}_2$, $\mathbb{Z}_3$ e $\mathbb{Z}_5$, respectivamente).
Se $o(G) = 4$, considere $H = \langle a \rangle$ subgrupo de G. Seguem dois casos:

1. Se G é cíclico (nesse caso, G é isomorfo a $\mathbb{Z}_4$), então G é abeliano.

2. Se G não é cíclico (nesse caso, G é isomorfo ao grupo de Klein), então não existe $a \in G$, $a \neq e$, tal que $H = \langle a \rangle$. Pelo Teorema de Lagrange, $o(\langle a \rangle) = 2$. Desse modo, $a^2 = e$, para todo $a \in G$. Portanto, G é abeliano.

□

Observação 2.6.4. *A recíproca do Teorema de Lagrange não é necessariamente verdadeira, ou seja, se G é um grupo finito e $m|o(G)$, não há garantia de que G contém um subgrupo cuja ordem é m. Porém, caso esse m seja um número primo p, então G irá conter um subgrupo de ordem p. Esses subgrupos são conhecidos como **subgrupos de Sylow** e esse resultado como **Teorema de Cauchy** (a demonstração não é o foco deste trabalho).*

2.7 SUBGRUPOS NORMAIS

Seja G um grupo e H um subgrupo de G. O objetivo é verificar se a operação de G induz naturalmente uma operação sobre o conjunto das classes laterais à esquerda de H em G, dado por G/H, ou seja, verificar com quais condições a operação $(aH, bH) \mapsto abH$ fica bem definida, no sentido de não depender da escolha dos representantes a e b das classes.

Note que a e ah são representantes da classe aH, b e bk são representantes da classe bH. Desse modo, a operação só está bem definida quando $abH = ahbkH$, isto é,

$$b^{-1}a^{-1}abH = b^{-1}a^{-1}ahbkH.$$

Logo, $H = b^{-1}hbH$, pois $k \in H$. Portanto, deve acontecer $b^{-1}hb \in H$, para todo $b \in G$ e para todo $h \in H$.

Proposição 2.7.1. *Sejam G um grupo e H um subgrupo de G, então as seguintes afirmações são equivalentes:*

(i) A operação induzida sobre as classes laterais à esquerda está bem definida.

(ii) $aHa^{-1} \subseteq H$*, para todo* $a \in G$*.*

(iii) $aHa^{-1} = H$*, para todo* $a \in G$*.*

(iv) $aH = Ha$*, para todo* $a \in G$*.*

Demonstração:
$(i) \iff (ii)$ Demonstrada acima.
$(ii) \iff (iii)$ Seja $h \in H$, então

$$ehe = aa^{-1}haa^{-1} = a(a^{-1}ha)a^{-1}$$

Como $a^{-1}ha \in H$, segue que $a(a^{-1}ha)a^{-1} \in aHa^{-1}$, para todo $a \in G$. Portanto $H \subseteq aHa^{-1}$. Por hipótese, $aHa^{-1} \subseteq H$. Portanto, $aHa^{-1} = H$.
$(iii) \iff (iv)$ Tem-se que $aHa^{-1} = H$ se, e somente se, $aHa^{-1}a = Ha$. Segue que, $aH = Ha$.

□

Dessa proposição, segue a seguinte definição:

Definição 2.7.2. *Seja G um grupo e N subgrupo de G. N é denominado* ***subgrupo normal*** *de G, e denotado por* $N \lhd G$*, se satisfaz alguma das condições da proposição acima.*

Exemplo 2.7.3. *Seja G um grupo abeliano e H um subgrupo de G, então H é subgrupo normal.*

Proposição 2.7.4. *Seja G um grupo e H um subgrupo de G. Se* $(G\colon H) = 2$*, então H é subgrupo normal.*

Demonstração:
Por hipótese, $(G\colon H) = 2$, então existem somente duas classes laterais em G/H. Considere $aH \in G/H$. O objetivo é mostrar que $aH = Ha$, para todo $a \in G$. Podem ocorrer dois casos:

1. Se $a \in H$, então $ah \in aH$, pois H é subgrupo. Segue que $H \subset aH$. Supondo $b \in aH$, tem-se $b = ah \in H$. Daí, $aH \subset H$. Logo, $aH = H$. Analogamente, $H = aH$. Portanto, $aH = Ha$.

2. Se $a \notin H$, então $aH \neq H$ e $H \neq aH$. Como $(G\colon H) = 2$, segue que $G/H = \{H, aH\}$, sendo $a \in G$. Pelo fato das classes laterais serem uma partição de G, então $aH = G \setminus H$ e $Ha = G \setminus H$. Portanto, $aH = Ha$.

□

2.8 GRUPOS QUOCIENTES

Nesse momento é possível demonstrar que G/H, sendo G um grupo, tem estrutura de grupo quando H é subgrupo normal de G.

Proposição 2.8.1. *Sejam G um grupo e N um subgrupo normal de G. Então, G/N com a operação induzida de G tem estrutura de grupo.*

Demonstração:
Sejam $aN, bN, cN \in G/N$, então

(i) $[(aN)(bN)](cN) = [(ab)N](cN) = [(ab)c]N = [a(bc)]N = (aN)[(bc)N] = (aN)[(bN)(cN)]$.

(ii) Existe $eN \in G/N$ tal que $(aN)(eN) = (ae)N = aN = (ea)N = (eN)(aN)$.

(iii) Existe $a^{-1} \in G/N$ tal que $(aN)(a^{-1}N) = (aa^{-1})N = (a^{-1}a)N = (a^{-1}N)(aN)$.

□

Assim, está demonstrado que G/N é um grupo cujo elemento neutro é eN e o elemento inverso de aN é $a^{-1}N$, para $aN \in G/N$.

Definição 2.8.2. *Sejam G um grupo e N um subgrupo normal de G. O grupo das classes laterais de G com a operação induzida de G é denominado **grupo quociente** de G por N, e denotado por G/N.*

Exemplo 2.8.3. *O conjunto de todas as classes laterais do exemplo 2.5.6 é o grupo quociente de $\mathbb{Z}_8$ por H. Simbolicamente, $\mathbb{Z}_8/H = \{\overline{0}+H, \overline{1}+H, \overline{2}+H, \overline{3}+H\}$.*

A proposição abaixo indica que o grupo G/N herda algumas propriedades do grupo G, sendo N subgrupo normal de G.

Proposição 2.8.4. *Seja G um grupo e N um subgrupo normal de G.*

(i) Se G é um grupo abeliano, então G/N é abeliano.

(ii) Se G é um grupo cíclico, então G/N é cíclico.

Demonstração:

(i) Considere $aN, bN \in G/N$, $a, b \in G$. Como G é grupo abeliano, $ab = ba$, logo $aNbN = abN = baN = bNaN$. Portanto, G/N é abeliano.

(ii) O objetivo é mostrar que $G/N = \langle \overline{a} \rangle$. Considere $\overline{b} \in G/N$, então $b \in G$. Como G é cíclico, então existe $a \in G$ tal que $G = \langle a \rangle$. Logo, $b = a^m$, para algum $m \in \mathbb{Z}$. Desse modo, $\overline{b} = \overline{a^m} = \overline{a}^m \in \langle \overline{a} \rangle$. Segue que $G/N \subset \langle \overline{a} \rangle$. Por outro lado, seja $\overline{a}^m \in \langle \overline{a} \rangle$, sendo $m \in \mathbb{Z}$. Sabe-se que $\overline{a} = aN \in G/N$. Como N é subgrupo normal de G, tem-se G/N grupo, logo, $\overline{a}^m \in G/N$. Assim, $\langle \overline{a} \rangle \subset G/N$. Portanto, $\langle \overline{a} \rangle = G/N$.

□

Com grupos quocientes é possível definir a seguinte aplicação:

Proposição 2.8.5. *Seja G um grupo. Se N é um subgrupo normal de G, então a aplicação*

$$\begin{aligned} \pi \colon G &\to G/N \\ a &\mapsto aN \end{aligned}$$

é um homomorfismo sobrejetor de grupos cujo núcleo é N.

Demonstração:
Sejam $a, b \in G$. Então, $\pi(ab) = (ab)N = (aN)(bN) = \pi(a)\pi(b)$. Então, π é homomorfismo.
Dado $y \in G/N$, então $y = bN$ o objetivo é mostrar que existe $a \in G$, tal que $\pi(a) = bN = y$.
Basta considerar $a = b$, pois $\pi(a) = \pi(b) = bN = y$. Segue que π é sobrejetora.

Agora, se $a \in Nu(\pi)$, então $\pi(a) = aN = eN = N$. Então, $a \in N$. Assim, $Nu(\pi) \subset N$. Por outro lado, se $a \in N$, então $aN = N$. Assim, $\pi(a) = aN = N$, ou seja, $a \in Nu(\pi)$. Logo, $N \subset Nu(\pi)$. Portanto, $Nu(\pi) = N$.

□

A aplicação definida na proposição acima é denominada projeção canônica.

2.9 TEOREMA DO HOMOMORFISMO

O Teorema do Homomorfismo é importante na Teoria de Grupos, pois permite construir isomorfismos entre grupos e grupos quocientes. Para demonstrá-lo, primeiramente é preciso mostrar que $G/Nu(\mu)$ tem estrutura de grupo. Isso acontece quando $Nu(\mu)$ é subgrupo normal de G.

Lema 2.9.1. *Sejam G e L grupos. Se $\mu : G \to L$ é um homomorfismo de grupos, então $Nu(\mu)$ é um subgrupo normal de G e, portanto, $G/Nu(\mu)$ tem uma estrutura de grupo.*

Demonstração:
Na seção de Homomorfismo de Grupos foi demonstrado que $Nu(\mu)$ é subgrupo de G. Falta mostrar que $aNu(\mu) = Nu(\mu)a$, para todo $a \in G$.
Seja $an \in aNu(\mu)$, tal que $an = (ana^{-1})a$. Como μ é homomorfismo,

$$\mu(ana^{-1}) = \mu(a)\mu(n)\mu(a^{-1}) = \mu(a)e_L\mu(a)^{-1} = \mu(a)\mu(a)^{-1} = e_L,$$

sendo e_L o elemento neutro de L. Então, $ana^{-1} \in Nu(\mu)$. Logo, $aNu(\mu) \subset Nu(\mu)a$.
Por outro lado, seja $c \in Nu(\mu)a$, então $c = na$, $n \in Nu(\mu)$. Mas $c = na = a(a^{-1}na)$. Como μ é homomorfismo,

$$\mu(a^{-1}na) = \mu(a^{-1})\mu(n)\mu(a) = \mu(a^{-1})e_L\mu(a) = e_L.$$

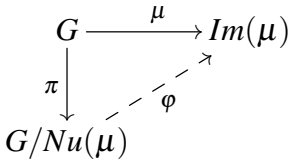
Então, $a^{-1}na \in Nu(\mu)$. Assim, $c = a(a^{-1}na) \in aNu(\mu)$. Logo, $Nu(\mu)a \subset aNu(\mu)$.
Portanto, $aNu(\mu) = Nu(\mu)a$, ou seja, $Nu(\mu)$ é normal.

□

Teorema 2.9.2. *(Teorema do Homomorfismo) Sejam G e L grupos e $\mu : G \to L$ um homomorfismo de grupos. Se $Nu(\mu)$ é o núcleo de μ, então existe um* ***único*** *isomorfismo*

$$\varphi : G/Nu(\mu) \to Im(\mu)$$

que torna comutativo o diagrama

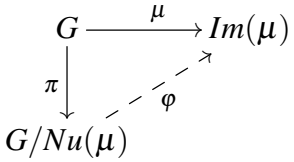


onde π é a projeção canônica.

Demonstração:
O objetivo é construir um isomorfismo de $G/Nu(\mu)$ em $Im(\mu)$. Desse modo, defina a seguinte aplicação:

$$\begin{aligned} \varphi\colon G/Nu(\mu) &\to Im(\mu) \\ aNu(\mu) &\mapsto \varphi(aNu(\mu)) = \mu(a) \end{aligned}$$

A qual faz o diagrama abaixo comutar:



Primeiramente, é necessário verificar se φ está bem definida.
Para isso, sejam $aNu(\mu), bNu(\mu) \in G/Nu(\mu)$ tais que $aNu(\mu) = bNu(\mu)$. Então,

$$b^{-1}aNu(\mu) = Nu(\mu),$$

ou seja, $b^{-1}a \in Nu(\mu)$. Logo, $\varphi(b^{-1}aNu(\mu)) = \mu(b^{-1}a) = e_L$, sendo e_L elemento neutro de L. Como μ é homomorfismo, segue que $e_L = \mu(b^{-1}a) = \mu(b)^{-1}\mu(a)$. Daí, $\mu(a) = \mu(b)$, isto é, $\varphi(aNu(\mu)) = \varphi(bNu(\mu))$. Logo, φ está bem definida.
Tem-se que φ é homomorfismo, porque μ é homomorfismo. Com efeito, considere $aNu(\mu), bNu(\mu) \in G/Nu(\mu)$, então

$$\varphi(aNu(\mu)bNu(\mu)) = \mu(ab) = \mu(a)\mu(b) = \varphi(aNu(\mu))\varphi(bNu(\mu)).$$

Além disso, φ é bijetora. De fato, seja $aNu(\mu), bNu(\mu) \in G/Nu(\mu)$, tais que $\varphi(aNu(\mu)) = \varphi(bNu(\mu))$, então $\mu(a) = \mu(b)$, sendo $a, b \in G$. Daí, $\mu(b)^{-1}\mu(a) = \mu(b)^{-1}\mu(b) = e_L$. Como μ é um homomorfismo, vem $e_L = \mu(b)^{-1}\mu(a) = \mu(b^{-1})\mu(a) = \mu(b^{-1}a)$. Segue que $b^{-1}a \in Nu(\mu)$. Logo, $aNu(\mu) = bNu(\mu)$. Decorre que, φ é injetora. Além disso, $Im(\varphi) = Im(\mu)$, ou

seja, φ é sobrejetora.
Portanto, φ é isomorfismo.

□

Exemplo 2.9.3. *O grupo $GL_n(\mathbb{R})/SL_n(\mathbb{R})$ é isomorfo a $\mathbb{R}\setminus\{0\}$. Basta considerar a aplicação*

$$\begin{aligned}\varphi\colon GL_n(\mathbb{R}) &\to \mathbb{R}\setminus\{0\}\\ A &\mapsto det(A)\end{aligned}$$

para $A \in GL_n(\mathbb{R})$.

Exemplo 2.9.4. *O grupo $\mathbb{R}/\mathbb{Z}$ é isomorfo a S^1. Basta considerar a aplicação*

$$\begin{aligned}\varphi\colon \mathbb{R} &\to S^1\\ t &\mapsto e^{2\pi it}\end{aligned}$$

para $t \in \mathbb{R}$.

Exemplo 2.9.5. *O grupo $\mathbb{R}\setminus\{0\}/\{-1,1\}$ é isomorfo a $\mathbb{R}_+\setminus\{0\}$. Basta considerar a aplicação*

$$\begin{aligned}\varphi\colon \mathbb{R}\setminus\{0\} &\to \mathbb{R}_+\setminus\{0\}\\ x &\mapsto |x|\end{aligned}$$

para $x \in \mathbb{R}\setminus\{0\}$.

Corolário 2.9.6. *Seja G um grupo. Se K e H são subgrupos normais de G, tal que $K \subset H$, então*

$$\frac{G/K}{H/K} \cong G/H.$$

Demonstração:
Para demonstração, ver Garcia e Lequain (2003).

□

Corolário 2.9.7. *Seja G um grupo. Se K é subgrupo de G e H é subgrupo normal de G, então*

$$\frac{K}{K\cap H} \cong \frac{KH}{H},$$

sendo $KH = \{kh\colon k \in K, h \in H\}$.

Demonstração:
Para demonstração, ver Garcia e Lequain (2003).

□

2.10 GRUPO DE PERMUTAÇÕES

Os grupos de permutações serão úteis nos próximos capítulos, a fim de conceituar as aplicações multilineares simétricas utilizadas na definição da potência simétrica. Além disso, serão utilizados em exemplos específicos de representações de grupos.

Definição 2.10.1. *Seja E um conjunto não vazio. Uma **permutação** é uma aplicação $\sigma\colon E \to E$ tal que σ é bijetora.*

Considere $S(E)$ o conjunto de todas as permutações $\sigma\colon E \to E$. Esse conjunto munido da operação de composição é um grupo. De fato, sejam $\sigma, \rho \in S(E)$. Como σ e ρ são bijetoras, então $\rho \circ \sigma$ é bijetora. Portanto, $S(E)$ é fechado para a composição. Sabe-se que a composição é associativa. O elemento neutro é a aplicação identidade e o elemento inverso é a aplicação inversa.

Definição 2.10.2. *O conjunto de todas as permutações $\sigma\colon E \to E$, denotado por $S(E)$, munido da operação de composição é denominado **grupo de permutações** sobre E.*

Exemplo 2.10.3. *Um caso particular e importante de grupo de permutações ocorre quando considera-se $E = I_n = \{1, 2, \dots n\}$, com $n \in \mathbb{N}^*$. O grupo formado é denominado **grupo simétrico de grau n** e denotado por S_n. Note que S_n é um grupo finito tal que $o(S_n) = n!$, pois esse é o número de permutações que podem ser construídas com n elementos.*

Considerando $\sigma \in S_n$, de modo que $\sigma(1) = i_1, \sigma(2) = i_2, ..., \sigma(n) = i_n$, para $i_j \in I_n$, com $j \in \{1, \dots, n\}$, uma maneira de visualizar a permutação σ é utilizar a seguinte notação:

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix} = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}.$$

Considere, além de σ, a permutação $\rho \in S_n$ tal que $\sigma(n) = i_n$ e $\rho(i_n) = j_{i_n}$. Desse modo, a composição dessas duas permutações é dada por:

$$(\rho \circ \sigma)(n) = \rho(\sigma(n)) = \rho(i_n) = j_{i_n}.$$

A notação introduzida facilita a operação com permutações.

$$\rho \circ \sigma = \begin{pmatrix} i_1 & \dots & i_r & \dots & i_n \\ j_1 & \dots & j_{i_r} & \dots & j_n \end{pmatrix} \begin{pmatrix} 1 & \dots & r & \dots & n \\ i_1 & \dots & i_r & \dots & i_n \end{pmatrix} = \begin{pmatrix} 1 & \dots & r & \dots & n \\ j_1 & \dots & j_{i_r} & \dots & j_n \end{pmatrix}.$$

Nessa notação, sendo

$$\sigma = \begin{pmatrix} a & \dots & r & \dots & b \\ 1 & \dots & i_r & \dots & n \end{pmatrix}$$

a permutação inversa de σ é dada por

$$\sigma^{-1} = \begin{pmatrix} 1 & \dots & i_r & \dots & n \\ a & \dots & r & \dots & b \end{pmatrix}.$$

Exemplo 2.10.4. *Considere o grupo de permutação S_3 tal que*

$$S_3 = \{\sigma_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$
$$\sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\}$$

Construindo a tábua desse grupo, tem-se

$\circ$	σ_0	σ_1	σ_2	σ_3	σ_4	σ_5
σ_0	σ_0	σ_1	σ_2	σ_3	σ_4	σ_5
σ_1	σ_1	σ_2	σ_0	σ_5	σ_3	σ_4
σ_2	σ_2	σ_0	σ_1	σ_4	σ_5	σ_3
σ_3	σ_3	σ_4	σ_5	σ_0	σ_1	σ_2
σ_4	σ_4	σ_5	σ_3	σ_2	σ_0	σ_1
σ_5	σ_5	σ_3	σ_4	σ_1	σ_2	σ_0

Note que $\sigma_1^2 = \sigma_2$, $\sigma_3 \circ \sigma_1 = \sigma_4$ e $\sigma_3 \circ \sigma_1^2 = \sigma_5$, ou seja, S_3 é gerado por σ_1 e σ_3. Assim,

$$S_3 = \{\sigma_1^0, \sigma_1, \sigma_1^2, \sigma_3, \sigma_3 \circ \sigma_1, \sigma_3 \circ \sigma_1^2\}.$$

Também é possível escrever S_3 da forma

$$S_3 = \{\sigma_0,\ \sigma_1,\ \sigma_1^{-1},\ \sigma_3,\ \sigma_3\sigma_1 = \sigma_1^{-1}\sigma_3,\ \sigma_1\sigma_3 = \sigma_3\sigma_1^{-1}\},$$

a qual será utilizada mais adiante, no capítulo de Representações de Grupos.

Observação 2.10.5. *É interessante observar que o grupo S_3 é isomorfo ao grupo D_3, definido no exemplo 2.1.11. Sabendo que S_3 é gerado por σ_1 e $\sigma 3$; e que D_3 é gerado por $R_{\frac{2\pi}{3}}$ e M_1, é*

possível construir o seguinte isomorfismo

$$\begin{aligned}\varphi\colon S_3 &\to D_3\\ \sigma_1 &\mapsto R_{\frac{2\pi}{3}}\\ \sigma_2 &\mapsto M_1.\end{aligned}$$

Definição 2.10.6. *Sejam $i_r \in I_n = \{1,2,\ldots,n\}$, $r > 1$ e $\sigma \in S_n$ uma permutação tal que*

$$\begin{aligned}&\sigma(i_1) = i_2\\ &\sigma(i_2) = \sigma^2(i_1) = i_3\\ &\vdots\\ &\sigma(i_{r-1}) = \sigma^{r-1}(i_1) = i_r\\ &\sigma(i_r) = \sigma^r(i_1) = i_1\\ &\sigma(j) = j,\end{aligned}$$

*para todo $j \in I_n \setminus \{i_1,\ldots,i_r\}$. Diz-se que σ é um **ciclo de comprimento r** ou um **r-ciclo**, denotado por $(i_1 \ldots i_r)$, sendo $\{i_1,\ldots,i_r\}$ denominado **conjunto suporte** de σ.*

Observação 2.10.7. *O ciclo de comprimento 2 ou 2-ciclo é denominado **transposição**.*

Como as permutações que são elementos do grupo simétrico de ordem n, S_n, são finitas, é possível afirmar o seguinte resultado sobre a ordem desses elementos.

Proposição 2.10.8. *Seja $\sigma \in S_n$ um r-ciclo, tal que $r > 1$, então $o(\sigma) = r$ e sendo id a permutação identidade de S_n, tem-se $\langle\sigma\rangle = \{id, \sigma, \sigma^2, \ldots, \sigma^{r-1}\}$.*

Observação 2.10.9. *A potência de um ciclo não é necessariamente um ciclo. Por exemplo: considere o ciclo (1 2 3 4), então (1 2 3 4)(1 2 3 4)=(1 3)(2 4).*

Definição 2.10.10. *Dois ciclos cujos conjuntos suportes são conjuntos disjuntos são denominados **ciclos disjuntos**.*

Proposição 2.10.11. *Sejam $\sigma, \rho \in S_n$ dois ciclos disjuntos, então σ e ρ comutam.*

Demonstração:
Sejam $\sigma = (i_1 \ldots i_r)$ e $\rho = (j_1 \ldots j_s)$ tais que $\{i_1,\ldots,i_r\} \cap \{j_1,\ldots,j_s\} = \emptyset$. Podem ocorrer três casos:

1. Se $k \in \{i_1, \ldots, i_r\}$, então

$$(\rho \circ \sigma)(k) = \rho(\sigma(k)) = \sigma(k)$$
$$(\sigma \circ \rho)(k) = \sigma(\rho(k)) = \sigma(k)$$

   Logo, $(\rho \circ \sigma)(k) = (\sigma \circ \rho)(k)$.

2. Se $k \in \{j_1, \ldots, j_s\}$, então a demonstração é análoga ao item 1.

3. Se $k \notin \{i_1, \ldots, i_r\}$ e $k \notin \{j_1, \ldots, j_s\}$, então

$$(\rho \circ \sigma)(k) = \rho(\sigma(k)) = k$$
$$(\sigma \circ \rho)(k) = \sigma(\rho(k)) = k$$

   Logo, $(\rho \circ \sigma)(k) = (\sigma \circ \rho)(k)$.

□

Proposição 2.10.12. *Toda permutação $\sigma \in S_n$, exceto a permutação idêntica id, (a menos da ordem dos fatores) pode ser escrita como um produto de ciclos disjuntos.*

Demonstração:
Para demonstração, ver Domingues e Iezzi (2003).

□

Corolário 2.10.13. *Se $n > 1$, então toda permutação $\sigma \in S_n$ pode ser expressa como um produto de transposições.*

Demonstração:
Pela proposição anterior é possível decompor σ em um produto de ciclos disjuntos. Após isso, basta aplicar a identidade

$$(i_1 i_2 i_3 \ldots i_{r-1} i_r) = (i_1 i_r)(i_1 i_{r-1}) \ldots (i_1 i_3)(i_1 i_2),$$

que é de fácil verificação.

□

Sabendo que é possível decompor uma permutação em um produto de transposições e que dois ciclos disjuntos comutam, tem-se que essa decomposição não é única. Mas se em

uma delas, o número de transposições é par ou ímpar, o mesmo acontece nas outras. Antes de demonstrar essa afirmação, são necessárias algumas definições e resultados.

Definição 2.10.14. *Seja $\sigma \in S_n$ uma permutação dada por*

$$\sigma = \begin{pmatrix} i_1 \dots i_n \\ j_1 \dots j_n \end{pmatrix}.$$

*A **assinatura** de σ é o número real denotado por $sgn\sigma$ e definido por*

$$sgn\sigma = \prod_{s>r} \frac{i_s - i_r}{j_s - j_r}.$$

Proposição 2.10.15. *A assinatura de uma transposição é -1.*

Demonstração:
Seja $\tau \in S_n$ uma transposição, tal que

$$\tau = \begin{pmatrix} i_1 & i_2 & i_3 & \dots & i_n \\ i_2 & i_1 & i_3 & \dots & i_n \end{pmatrix},$$

sem perda de generalidade.
Se (r,s) é um par de índices da primeira linha da transposição τ e $1 \leqslant r < s \leqslant n$, então podem acontecer os seguintes casos:

1. Se $(r,s) = (1,2)$, então o fator correspondente de (r,s) em $sgn\tau$ é $\dfrac{i_2 - i_1}{i_1 - i_2} = \dfrac{i_2 - i_1}{-(i_2 - i_1)} = -1$.
2. Se $r = 1$ e $s > 2$, então o fator correspondente de (r,s) em $sgn\tau$ é $\dfrac{i_s - i_1}{i_s - i_2}$.
3. Se $r = 2$ e $s > 2$, então o fator correspondente de (r,s) em $sgn\tau$ é $\dfrac{i_s - i_2}{i_s - i_1}$.
4. Se $r > 2$ e $s > 2$, então o fator correspondente de (r,s) em $sgn\tau$ é $\dfrac{i_s - i_r}{i_s - i_r} = 1$.

Note que os fatores correspondentes de (r,s) em $sgn\tau$ dos itens 2 e 3 virão aos pares, ou seja,

$$\frac{i_s - i_1}{i_s - i_2}\frac{i_s - i_2}{i_s - i_1},$$

para cada $s > 2$, então será possível cancelá-los, restando somente os fatores correspondentes de (r,s) em $sgn\tau$ dos itens 1 e 4.
Portanto, $sgn\tau = -1$.

□

Proposição 2.10.16. *Se $\sigma, \rho \in S_n$ são permutações, então $sgn(\rho \circ \sigma) = sqn\rho sgn\sigma$.*

Demonstração:
Considere as permutações $\sigma, \rho \in S_n$, dadas por

$$\sigma = \begin{pmatrix} i_1 & i_2 & i_3 & \dots & i_n \\ j_1 & j_2 & j_3 & \dots & j_n \end{pmatrix} \text{ e } \rho = \begin{pmatrix} j_1 & j_2 & j_3 \dots & j_n \\ k_1 & k_2 & k_3 & \dots & k_n \end{pmatrix},$$

então,

$$(sgn\sigma)(sgn\rho) = \prod_{s>r} \frac{i_s - i_r}{j_s - j_r} \prod_{s>r} \frac{j_s - j_r}{k_s - k_r} = \prod_{s>r} \frac{i_s - i_r}{k_s - k_r} = sgn(\rho \circ \sigma).$$

□

A proposição anterior pode ser estendida para o caso de mais permutações.

Corolário 2.10.17. *Se $\sigma \in S_n$, então $sgn\sigma = \pm 1$.*

Demonstração:
É possível decompor σ em um produto de transposições, ou seja,

$$\sigma = \tau_1 \circ \tau_2 \circ \ldots \circ \tau_r$$

tal que $\tau_1, \tau_2, \ldots, \tau_r \in S_n$, $r \in \mathbb{N}$. Pela proposição anterior

$$sgn\sigma = (sgn\tau_1)(sgn\tau_2)\ldots(sgn\tau_r) = (-1)^r.$$

Se $r = 2k+1$, então $sgn\sigma = -1$. Caso $r = 2k$, então $sgn\sigma = 1$, para $k \in \mathbb{Z}$.

□

Corolário 2.10.18. *Se $\sigma \in S_n$, então $sgn\sigma^{-1} = (sgn\sigma)^{-1}$.*

Demonstração:
Note que $(12)(12)$ indica a identidade de S_n, então

$$\sigma^{-1}\sigma = (12)(12).$$

Segue que,

$$(sgn\sigma^{-1})(sgn\sigma) = sgn(\sigma^{-1}\sigma) = sgn((12)(12)) = (sgn(12))(sgn(12)) = (-1)(-1) = 1.$$

De onde,

$$sgn\sigma^{-1} = \frac{1}{sgn\sigma} = (sgn\sigma)^{-1}.$$

□

Nesse momento, é possível demonstrar o resultado que refere-se a paridade de duas decomposições distintas de uma mesma permutação.

Definição 2.10.19. *O conjunto das permutações pares de S_n é denominado* ***grupo alternado*** *de S_n e denotado por A_n.*

Note que $(12)(12) = id$ é uma permutação par, então $A_n \neq \emptyset$. E pela proposição abaixo, confirma-se que esse conjunto é um grupo.

Proposição 2.10.20. *Seja $\sigma \in S_n$ e considere duas decomposições de σ em transposições: $\sigma = \tau_1 \circ \tau_2 \circ \ldots \circ \tau_r$ e $\sigma = \rho_1 \circ \rho_2 \circ \ldots \circ \rho_s$, $r,s \in \mathbb{Z}$. Então, r,s tem a mesma paridade.*

Demonstração:
Temos que $sgn\sigma = (-1)^r = (-1)^s$. Se r for par, então $(-1)^r = 1 = (-1)^s$. Logo, s também é par. Analogamente, se r for ímpar.

□

Sabendo que a paridade de diferentes decomposições de uma permutação é igual, é possível classificar as permutações de acordo com essa paridade.

Definição 2.10.21. *Seja $\sigma \in S_n$. A permutação σ é denominada* ***par*** *ou* ***ímpar*** *quando é expressa por um número par ou ímpar de transposições, respectivamente.*

Dessa definição e dos resultados anteriores, decorre que se $sgn\sigma = 1$, então σ é par, e se $sgn\sigma = -1$, então σ é ímpar.

Proposição 2.10.22. *Para todo $n > 1$, o conjunto das permutações pares de S_n, denotado por A_n é um subgrupo normal de S_n tal que $o(A_n) = \frac{n!}{2}$ e $(S_n : A_n) = 2$.*

Demonstração:
O objetivo é mostrar que A_n é o núcleo do homomorfismo $\mu : S_n \to \{-1,1\}$, pois pelo Lema 2.9.1 e pelo Teorema do Homomorfismo vem que $S_n/A_n \cong \{-1,1\}$ e A_n é subgrupo normal de

S_n, ou seja, $o(A_n) = \dfrac{n!}{2}$ e $(S_n : A_n) = 2$.
Considere a aplicação $\mu : S_n \to \{-1, 1\}$ dada por

$$\mu(\sigma) = \begin{cases} 1, & \text{se } \sigma \text{ é par} \\ -1, & \text{se } \sigma \text{ é ímpar} \end{cases}$$

É claro que μ está bem definida, μ é um homomorfismo sobrejetor e $A_n = Nu(\mu)$. Pelo Lema 2.9.1, A_n é um subgrupo normal de S_n. Pelo Teorema do Homomorfismo, $S_n/A_n \cong \{-1, 1\}$. Daí, $o(S_n/A_n) = 2$, ou seja, $(S_n : A_n) = 2$. Pelo Teorema de Lagrange, $o(S_n) = o(A_n)(S_n : A_n)$. Segue que $o(A_n) = \dfrac{n!}{2}$.

□

2.11 TEOREMA DE CAYLEY

Considere a tábua da operação do grupo $\mathbb{Z}_3$:

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

Note que cada coluna dessa tábua é uma permutação da outra. Desse modo, nessa seção será abordado o Teorema de Cayley, que afirma que todo grupo G é isomorfo a um subgrupo do grupo de permutações $S(E)$. Para demonstrar esse teorema, são necessários alguns conhecimentos preliminares.

Definição 2.11.1. *Seja G um grupo. A aplicação δ_a dada por*

$$\begin{aligned} \delta_a : G &\to G \\ b &\mapsto ab \end{aligned}$$

*para $a \in G$ e para todo $b \in G$, é denominada **translação à esquerda** definida por a.*

A translação à direita definida por a é dada de maneira análoga.

Proposição 2.11.2. *Seja G um grupo e $a \in G$. Se δ_a é uma translação, então δ_a é uma bijeção, ou seja, δ_a é uma permutação dos elementos do grupo G.*

Demonstração:
Sendo $b, c \in G$, considere $\delta_a(b), \delta_a(c) \in G$, tal que $\delta_a(b) = \delta_a(c)$, ou seja, $ab = ac$. Como G é

regular para a operação, $b = c$. Logo, δ_a é injetora.
Dado $g \in G$, o objetivo é mostrar que existe $d \in G$ tal que $\delta_a(d) = g$, ou seja, $ad = g$. No grupo, essa equação tem solução $d = a^{-1}g$. Então, basta considerar $d = a^{-1}g$. Assim, $\delta_a(d) = \delta_a(a^{-1}g) = a(a^{-1}g) = g$. Logo, δ_a é sobrejetora.
Portanto, δ_a é bijetora.

□

Observação 2.11.3. *Sendo $T(G)$ o conjunto das translações em G e $S(G)$ o conjunto das permutações em G, tem-se pela proposição anterior que $T(G) \subset S(G)$.*

Pela proposição abaixo, além de subconjunto, tem-se que $T(G)$ é subgrupo de $S(G)$.

Proposição 2.11.4. *Seja G um grupo, então $T(G)$ é subgrupo de $S(G)$.*

Demonstração:
O conjunto $T(G) \neq \emptyset$, pois $1_G = \delta_e \in T(G)$
Considere as translações $\delta_a, \delta_b \in T(G)$. Seja $d \in G$, então

$$(\delta_a \circ \delta_b)(d) = \delta_a(\delta_b(d)) = \delta_a(bd) = a(bd) = (ab)d = \delta_{ab}(d)$$

Logo, $\delta_a \circ \delta_b = \delta_{ab}$, ou seja, $T(G)$ é fechado para a composição.
Como δ_a é bijetora, então existe $\delta_a^{-1} \in T(G)$, sendo $a^{-1} \in G$ o elemento inverso de $a \in G$, tal que $\delta_a^{-1} = \delta_{a^{-1}}$. De fato,

$$(\delta_a \circ \delta_a^{-1})(d) = (\delta_a \circ \delta_{a^{-1}})(d) = \delta_a(\delta_{a^{-1}}(d)) = \delta_a(a^{-1}d) = a(a^{-1}d) = (aa^{-}1)d = d = \delta_e(d)$$
$$(\delta_a^{-1} \circ \delta_a)(d) = (\delta_{a^{-1}} \circ \delta_a)(d) = \delta_(a^{-1})(\delta_a(d)) = \delta_{a^{-1}}(ad)a^{-1}(ad) = (a^{-1}a)d = d = \delta_e(d).$$

Daí, $(\delta_a \circ \delta_a^{-1}) = (\delta_a^{-1} \circ \delta_a) = \delta_e$.
Portanto, $T(G)$ é subgrupo de $S(G)$.

□

Agora é possível demonstrar o Teorema de Cayley, um exemplo do que se chama teorema de representação.

Teorema 2.11.5. *(Teorema de Cayley) Seja G um grupo, então G é isomorfo a $T(G) \subset S(G)$.*

Demonstração:
Defina a aplicação $\mu : G \to T(G)$ dada por $\mu(a) = \delta_a$. O objetivo é mostrar que essa aplicação

é um isomorfismo.
É claro que μ está bem definida.
Considere $a,b \in G$, então,

$$\delta_{ab}(c) = (ab)c = a(bc) = \delta_a(bc) = (\delta_a \circ \delta_b)(c),$$

para todo $c \in G$. Logo, $\mu(ab) = \mu(a) \circ \mu(b)$. Segue que μ é homomorfismo.
Além disso, μ é bijetora. Com efeito, sejam $\mu(a), \mu(b) \in T(G)$, tais que $\mu(a) = \mu(b)$. Tem-se $\delta_a(c) = \delta_b(c)$, ou seja, $ac = bc$, para $c \in G$. Como G é regular para a operação, $a = b$. Logo, μ é injetora. É claro que μ é sobrejetora.
Portanto, μ é isomorfismo.

□

Observação 2.11.6. *A possibilidade de representar qualquer grupo por um grupo de permutações dá uma maior concretude ao grupo em estudo, por mais abstrato que seja. E pelo Teorema de Cayley, observa-se que é possível representar todo o grupo G por um grupo de permutações dos elementos de G, isto é, $T(G)$ é uma representação de G. Pode-se dizer que G age sobre si mesmo, no sentido de que cada $g \in G$ produz uma permutação de G.*

A definição de ação será vista na próxima seção, generalizando a noção de um grupo agindo sobre si mesmo.

A mesma é muito importante na Teoria de Representações de Grupos, abordada nesse trabalho.

2.12 AÇÃO DE GRUPOS

Definição 2.12.1. *Seja G um grupo e X um conjunto não-vazio. Diz-se que G* ***age*** *em X se para cada $g \in G$, existe uma aplicação*

$$\begin{aligned} f\colon G \times X &\to X \\ (g,x) &\mapsto f(g,x) = g \cdot x \end{aligned}$$

que satisfaz as seguintes condições:

(i) Tem-se $e \cdot x = x$, para todo $x \in X$, sendo e o elemento neutro de G.

(ii) $g \cdot (h \cdot x) = (gh) \cdot x$, para todo $g,h \in G$ e $x \in X$.

Exemplo 2.12.2. *O grupo $\mathbb{Z}$ age sobre $\mathbb{R}$ pela aplicação*

$$\begin{aligned} f\colon \mathbb{Z}\times\mathbb{R} &\to \mathbb{R} \\ (n,x) &\mapsto n\cdot x = (-1)^n x \end{aligned}$$

De fato,

(i) $0\cdot x = (-1)^0 x = x$;

(ii) $(n+m)\cdot x = (-1)^{n+m}x = (-1)^n((-1)^m x) = (-1)^n(m\cdot x) = n\cdot(m\cdot x)$, *para* $n,m\in\mathbb{Z}$ *e* $x\in\mathbb{R}$.

Exemplo 2.12.3. *Todo grupo G age sobre si mesmo por meio da operação usual do grupo. Considere a aplicação*

$$\begin{aligned} f\colon G\times G &\to G \\ (g,x) &\mapsto g\cdot x = gx \end{aligned}$$

Então, as condições de ação são satisfeitas pela associatividade da operação de G e pela existência do elemento neutro de G. Essa ação é denominada ***ação regular****.*

Exemplo 2.12.4. *Seja G um grupo e X um conjunto não-vazio. Defina a aplicação*

$$\begin{aligned} f\colon G\times X &\to X \\ (g,x) &\mapsto g\cdot x = x \end{aligned}$$

Tem-se que f é uma ação denominada ***ação trivial****.*

Exemplo 2.12.5. *Considere o grupo S_n e o conjunto não-vazio $I_n = \{1,2,\ldots,n\}$. Defina a aplicação*

$$\begin{aligned} f\colon S_n\times I_n &\to I_n \\ (\sigma,x) &\mapsto \sigma\cdot x = \sigma(x) \end{aligned}$$

Essa aplicação é uma ação natural de S_n em I_n.

Exemplo 2.12.6. *Seja G um grupo e H um subgrupo de G. Considere a aplicação*

$$\begin{aligned} f\colon H\times G &\to G \\ (h,x) &\mapsto h\cdot x = hxh^{-1} \end{aligned}$$

Essa ação de H em G é denominada ***conjugação por H*** *e hxh^{-1} é chamado* ***conjugado*** *de x por h.*

3 ALGUMAS CONSTRUÇÕES UNIVERSAIS

Considere V e W espaços vetoriais de dimensão finita sobre o corpo $\mathbb{K}$ e T uma transformação linear de V em W. Sabe-se que o conjunto imagem da transformação T, denotado por $Im(T)$, é subespaço vetorial de W. Porém, geralmente isso não acontece para aplicações multilineares. Usando a definição de produto tensorial, obtém-se que a imagem de uma aplicação multilinear é um espaço vetorial.

O produto tensorial será definido com a utilização de aplicações bilineares, pois com algumas adaptações é possível generalizá-lo para aplicações multilineares.

Esse capítulo foi baseado em Greub (1967) e seu objetivo é definir as estruturas - produto tensorial, potência simétrica e exterior - para utilizá-las como exemplos de representações de grupos e mostrar que o produto tensorial é isomorfo a soma direta da potência exterior com a simétrica, no caso de aplicações bilineares.

3.1 APLICAÇÕES BILINEARES

Definição 3.1.1. *Sejam V_1, V_2 e W espaços vetoriais sobre o corpo $\mathbb{K}$. A aplicação*

$$\varphi\colon V_1 \times V_2 \to W$$

*é denominada **aplicação bilinear** quando:*

$$\varphi(\alpha u_1 + \beta u_2, v) = \alpha\varphi(u_1, v) + \beta\varphi(u_2, v)$$
$$\varphi(u, \gamma v_1 + \lambda v_2) = \gamma\varphi(u, v_1) + \lambda\varphi(u, v_2)$$

para todo u, u_1, $u_2 \in V_1$, v, v_1, $v_2 \in V_2$, $\alpha, \beta, \gamma, \lambda \in \mathbb{K}$.

Observação 3.1.2. *Se $W = \mathbb{K}$, então φ é denominada **função bilinear**.*

Considere φ uma aplicação bilinear de V_1 e V_2 em W, sendo V_1, V_2 e W espaços vetoriais de dimensão finita sobre o corpo $\mathbb{K}$. Então, nem sempre o conjunto imagem de φ, dado

por

$$Im(\varphi) = \{\varphi(u,v) \in W : u \in V_1 \text{ e } v \in V_2\},$$

é subespaço vetorial do contradomínio W.

De fato, considere o caso em que $V_1 = V_2 = V$ e W são espaços vetoriais finitos tais que $dim(V) = 2$ e $dim(W) = 4$. Sejam $\{v_1, v_2\}$ e $\{w_1, w_2, w_3, w_4\}$ bases para V e W, respectivamente. Considere a aplicação bilinear $\varphi : V \times V \to W$ definida por

$$\varphi(\alpha_1 v_1 + \alpha_2 v_2, \beta_1 v_1 + \beta_2 v_2) = \alpha_1\beta_1 w_1 + \alpha_1\beta_2 w_2 + \alpha_2\beta_1 w_3 + \alpha_2\beta_2 w_4$$

para $\alpha_1, \alpha_2, \beta_1, \beta_2 \in \mathbb{K}$.

Afirma-se que o vetor $z = \gamma_1 w_1 + \gamma_2 w_2 + \gamma_3 w_3 + \gamma_4 w_4$ pertence a $Im(\varphi)$ se, e somente se, $\gamma_1\gamma_4 - \gamma_2\gamma_3 = 0$.

Com efeito, se $z \in Im(\varphi)$ então, $z = \varphi(\alpha_1 v_1 + \alpha_2 v_2, \beta_1 v_1 + \beta_2 v_2)$. Assim,

$$z = \alpha_1\beta_1 w_1 + \alpha_1\beta_2 w_2 + \alpha_2\beta_1 w_3 + \alpha_2\beta_2 w_4.$$

Denominando $\gamma_1 = \alpha_1\beta_1$, $\gamma_2 = \alpha_1\beta_2$, $\gamma_3 = \alpha_2\beta_1$ e $\gamma_4 = \alpha_2\beta_2$, vem

$$\gamma_1\gamma_4 - \gamma_2\gamma_3 = \alpha_1\beta_1\alpha_2\beta_2 - \alpha_1\beta_2\alpha_2\beta_1 = 0.$$

Por outro lado, se $\gamma_1\gamma_4 - \gamma_2\gamma_3 = 0$, então $\gamma_4 = \gamma_1^{-1}\gamma_2\gamma_3$. Supondo $\alpha_1 = \gamma_1$, $\beta_1 = 1$, $\beta_2 = \gamma_1^{-1}\gamma_2$, $\alpha_2 = \gamma_3$, segue que

$$\begin{aligned}
\varphi(\alpha_1 v_1 + \alpha_2 v_2, \beta_1 v_1 + \beta_2 v_2) &= \alpha_1\beta_1 w_1 + \alpha_1\beta_2 w_2 + \alpha_2\beta_1 w_3 + \alpha_2\beta_2 w_4 \\
&= \gamma_1 w_1 + \gamma_1\gamma_1^{-1}\gamma_2 w_2 + \gamma_3 w_3 + \gamma_1^{-1}\gamma_2\gamma_3 w_4 \\
&= \gamma_1 w_1 + \gamma_2 w_2 + \gamma_3 w_3 + \gamma_4 w_4 \\
&= z
\end{aligned}$$

Logo, $z \in Im(\varphi)$.

Suponha que $z_1 = 2w_1 + 2w_2 + w_3 + w_4$ e $z_2 = w_1 + w_3$. Então, z_1 e z_2 satisfazem as condições acima. Logo, $z_1, z_2 \in Im(\varphi)$. Porém, $z_1 - z_2 = w_1 + 2w_2 + w_4 \notin Im(\varphi)$. Portanto, $Im(\varphi)$ não é subespaço de W.

Considere o conjunto $B(V_1, V_2; W)$ das aplicações bilineares, dado por

$$B(V_1, V_2; W) = \{\varphi : V_1 \times V_2 \to W : \varphi \text{ é uma aplicação bilinear}\}$$

e defina a soma e o produto por escalar da seguinte maneira:

$$(\alpha\varphi_1 + \varphi_2)(u,v) = \alpha\varphi_1(u,v) + \varphi_2(u,v)$$

para todos φ_1, $\varphi_2 \in B$, $u \in V_1$, $v \in V_2$ e $\alpha \in \mathbb{K}$.

O conjunto $B(V_1,V_2;W)$ com a soma e o produto por escalar tem estrutura de espaço vetorial sobre $\mathbb{K}$.

Observação 3.1.3. *Se $W = \mathbb{K}$, então o conjunto $B(V_1,V_2;W)$ será denotado simplesmente por $B(V_1,V_2)$.*

É possível estender o conceito de aplicações bilineares para o que denomina-se aplicações multilineares.

3.2 APLICAÇÕES MULTILINEARES

Definição 3.2.1. *Sejam $V_1,\ldots,V_p$ e W espaços vetoriais sobre o corpo $\mathbb{K}$. A aplicação*

$$\varphi\colon V_1 \times \ldots \times V_p \to W$$

*é denominada **aplicação multilinear** quando:*

$$\varphi(u_1,\ldots,\alpha u_i + \beta v_i,\ldots,u_p) = \alpha\varphi(u_1,\ldots,u_i,\ldots,u_p) + \beta\varphi(u_1,\ldots,v_i,\ldots,u_p)$$

para todo u_i, $v_i \in V_i$, $i \in \{1,\ldots,n\}$ e $\alpha,\beta \in \mathbb{K}$.

Observação 3.2.2. *Se $W = \mathbb{K}$, então φ é denominada **função p-linear** ou **multilinear**.*

Considere o conjunto $L(V_1,\ldots,V_p;W)$ das aplicações multilineares, dado por

$$L(V_1,\ldots,V_p;W) = \{\varphi\colon V_1 \times \ldots \times V_p \to W\colon \varphi \text{ é uma aplicação multilinear}\}$$

e defina a soma e o produto por escalar da seguinte maneira:

$$(\alpha\varphi_1 + \varphi_2)(u_1,\ldots,u_p) = \alpha\varphi_1(u_1,\ldots,u_p) + \varphi_2(u_1,\ldots,u_p)$$

para todos φ_1, $\varphi_2 \in L$, $u_i \in V_i$, $i \in \{1,\ldots,p\}$ e $\alpha \in \mathbb{K}$.

O conjunto $L(V_1,\ldots,V_p;W)$ com a soma e o produto por escalar tem estrutura de espaço vetorial sobre $\mathbb{K}$.

Observação 3.2.3. *Se $W = \mathbb{K}$, então o conjunto $L(V_1,\ldots,V_p;W)$ será denotado simplesmente por $L(V_1,\ldots,V_p)$.*

3.3 PRODUTO TENSORIAL

Nesta seção, será introduzido o produto tensorial. As aplicações multilineares podem ser vistas como aplicações lineares sobre o produto tensorial.

Definição 3.3.1. *Sejam V_1, V_2 e W espaços vetoriais sobre o corpo $\mathbb{K}$ e seja φ uma aplicação bilinear dada por $\varphi\colon V_1 \times V_2 \to W$. O par (W, φ) é denominado* ***produto tensorial*** *de V_1 e V_2 quando:*

(i) $Im(\varphi) = W$;

(ii) Se $\psi\colon V_1 \times V_2 \to U$ é uma aplicação bilinear, sendo U um espaço vetorial arbitrário sobre $\mathbb{K}$, então existe uma aplicação linear $f\colon W \to U$ tal que $\psi = f \circ \varphi$, ou seja, tal que o diagrama

$$\begin{array}{ccc} V_1 \times V_2 & \xrightarrow{\psi} & U \\ {\scriptstyle\varphi}\downarrow & \nearrow_{f} & \\ W & & \end{array}$$

comuta.

As condições (i) e (ii) da definição 3.3.1 são equivalentes a condição a seguir, denominada **propriedade universal**: Se $\psi\colon V_1 \times V_2 \to U$ é uma aplicação bilinear, sendo U um espaço vetorial arbitrário sobre $\mathbb{K}$, então existe uma **única** aplicação linear $f\colon W \to U$ tal que $\psi = f \circ \varphi$.

De fato, vale a equivalência. Suponha, pela condição (ii), que existem as aplicações lineares $f_1\colon W \to U$ e $f_2\colon W \to U$ tais que $\psi = f_1 \circ \varphi$ e $\psi = f_2 \circ \varphi$. Então, $f_1 \circ \varphi = f_2 \circ \varphi$, ou seja, $f_1 \circ \varphi - f_2 \circ \varphi = 0$. Segue que, $(f_1 - f_2) \circ \varphi = 0$. Pela condição (i), $f_1 = f_2$. Logo, a aplicação linear é única e vale a propriedade universal.

Agora, suponha que vale a propriedade universal. A condição (ii) segue imediatamente. Para mostrar a validade da condição (i), considere a aplicação bilinear

$$\psi\colon V_1 \times V_2 \to Im(\varphi)$$

definida por $\psi(u,v) = \varphi(u,v)$, para todo $u \in V_1$ e $v \in V_2$, sendo φ a aplicação bilinear

$$\varphi\colon V_1 \times V_2 \to W.$$

Pela propriedade universal, existe $f\colon W \to Im(\varphi)$ tal que $\psi = f \circ \varphi$. Seja $g\colon Im(\varphi) \to W$ a aplicação de inclusão, o objetivo é mostrar que g é sobrejetora. Como g é aplicação de

inclusão, então $g \circ \psi = \varphi$. Segue que, $(g \circ f) \circ \varphi = g \circ (f \circ \varphi) = g \circ \psi = \varphi$. Considerando a aplicação identidade $i\colon W \to W$, sabe-se que $i \circ \varphi = \varphi$. Daí, que $(g \circ f) \circ \varphi = i \circ \varphi = \varphi$. Pela propriedade universal, existe única aplicação h tal que $\varphi = h \circ \varphi$. Então, $g \circ f = i$. Conclui-se que g é sobrejetora. Com efeito, dado $y \in W$, existe $x \in Im(\varphi)$ tal que $g(x) = y$, basta considerar $x = f(y)$, já que $g(x) = g(f(y)) = (g \circ f)(y) = i(y) = y$. Portanto, $Im(\varphi) = W$. Logo, vale a condição (i).

No exemplo a seguir será utilizada a definição 3.3.1 para mostrar que a multiplicação por escalar é um produto tensorial.

Exemplo 3.3.2. *Seja W um espaço vetorial arbitrário sobre o corpo $\mathbb{K}$. Defina a aplicação bilinear $\varphi\colon \mathbb{K} \times W \to W$ dada por $\varphi(\alpha, w) = \alpha w$. Então, (W, φ) é um produto tensorial de $\mathbb{K}$ e W.*

(i) $Im(\varphi) = W$. Com efeito, seja $y \in W$. O objetivo é mostrar que existe $(\alpha, w) \in \mathbb{K} \times W$ tal que $\varphi(\alpha, w) = y$. Considere $(\alpha, w) = (1, y)$. Daí,

$$\varphi(\alpha, w) = \varphi(1, y) = y.$$

(ii) Se $\psi\colon \mathbb{K} \times W \to U$ é uma aplicação bilinear, sendo U espaço vetorial arbitrário, então existe uma aplicação linear $f\colon W \to U$ tal que $\psi = f \circ \varphi$. De fato, considere a aplicação linear $f\colon W \to U$ definida por $f(w) = \psi(1, w)$, então

$$f \circ \varphi(\alpha, w) = f(\varphi(\alpha, w)) = f(\alpha w) = \alpha f(w) = \alpha \psi(1, w) = \psi(\alpha, w).$$

Observação 3.3.3. *Sejam V_1, V_2 e W espaços vetoriais sobre o corpo $\mathbb{K}$ e uma aplicação bilinear $\varphi\colon V_1 \times V_2 \to W$. Supondo que o par (W, φ) seja o produto tensorial de V_1 e V_2. Denota-se $W = V_1 \otimes V_2$ e $\varphi(u, v) = u \otimes v$, para $u \in V_1$ e $v \in V_2$. Caso $V = V_1 = V_2 = \ldots = V_n$, sendo V_i espaços vetoriais, para $i \in \{1, 2, \ldots, n\}$, denota-se $W = V_1 \otimes V_2 \otimes \ldots \otimes V_n = V^{\otimes n}$.*

O produto tensorial foi definido e exemplificado, porém é possível garantir sua existência? E se ele existe, é único? Para demonstrar esses fatos, é necessário entender a definição de espaço vetorial livre.

Observação 3.3.4. *Considere um conjunto arbitrário A, um corpo $\mathbb{K}$ e o conjunto $C(A)$ das funções $f\colon A \to \mathbb{K}$ tal que $f(a) \neq 0$ para uma quantidade finita de elementos $a \in A$. Em símbolos,*

$$C(A) = \{f\colon A \to \mathbb{K}\colon f(a_i) \neq 0, a_i \in A, i \in \{1, \ldots, n\}\}.$$

Defina a soma de dois elementos e o produto por escalar, sendo $f, g \in C(A)$, $\alpha \in \mathbb{K}$, *como*

$$(\alpha f + g)(x) = \alpha f(x) + g(x)$$

para todo $x \in A$.

O conjunto C(A) com a soma e o produto por escalar, definidos acima, tem estrutura de espaço vetorial sobre $\mathbb{K}$.

Para cada $a \in A$ *defina* $f_a \in C(A)$ *tal que:*

$$f_a(x) = \begin{cases} 1, & x = a \\ 0, & x \neq a \end{cases}$$

para $x \in A$.

Se $f \in C(A)$, *então existe uma quantidade finita de elementos* $a_i \in A$, *sendo* $i \in \{1, \ldots, n\}$, *tais que* $f(a_i) \neq 0$. *Desse modo, é possível definir* f *em um elemento* $x \in A$ *da seguinte maneira:*

$$f(x) = \sum_{i=1}^{n} f(a_i) f_{a_i}(x).$$

Denotando $f(a_i) = \alpha_i$, *obtêm-se*

$$f(x) = \sum_{i=1}^{n} \alpha_i f_{a_i}(x).$$

Note que foi possível escrever uma $f \in C(A)$ *genérica como combinação linear dos elementos do conjunto* $\{f_a\}_{a \in A}$. *Portanto,* $\{f_a\}_{a \in A}$ *gera* $C(A)$.

Agora, considerando $\beta_i \in \mathbb{K}$ *quaisquer,* $i \in \{1, \ldots, n\}$ *e*

$$\sum_{i=1}^{n} \beta_i f_{a_i}(x) = 0$$

tem-se para cada $j \in \{1, \ldots, n\}$ *e* $a_j \in A$

$$0 = \sum_{i=1}^{n} \beta_i f_{a_i}(a_j) = \beta_j f a_j(a_j) = \beta_j.$$

Logo, $\{f_a\}_{a \in A}$ *é linearmente independente.*

Portanto, $\{f_a\}_{a \in A}$ *é uma base para o conjunto* $C(A)$. *Fazendo a identificação* $a \mapsto f_a$, *obtém-se que A é uma base para* $C(A)$.

Daí, decorre a seguinte definição:

Definição 3.3.5. *O espaço vetorial $C(A)$ construído acima é denominado espaço vetorial livre sobre A.*

Observação 3.3.6. *Considerando $A = V_1 \times V_2$, obtêm-se que $\{f_{(a,b)}\}_{(a,b)\in A}$ é uma base para $C(V_1 \times V_2)$. Sendo $f \in C(V_1 \times V_2)$ é possível escrevê-lo como uma combinação linear dos elementos da base, isto é,*

$$f(u,v) = \sum_{i,j} \alpha_{i,j} f_{(a_i,b_j)}(u,v),$$

para $\alpha_{i,j} = f(a_i,b_j) \in \mathbb{K}$, $u \in V_1$ e $v \in V_2$.

Fazendo a identificação $(a,b) \mapsto f_{(a,b)}$, obtêm-se que $V_1 \times V_2$ é uma base para $C(V_1 \times V_2)$. Desse modo, se $z \in C(V_1 \times V_2)$, então

$$z = \sum_{i,j} \alpha_{i,j}(a_i,b_j),$$

para $\alpha_{i,j} = f(a_i,b_j) \in \mathbb{K}$.

Agora, é possível demonstrar a existência do produto tensorial.

Proposição 3.3.7. *Sejam V_1, V_2 e W espaços vetoriais sobre o corpo $\mathbb{K}$. Então, existe o produto tensorial $V_1 \otimes V_2$.*

Demonstração:
Considere o espaço vetorial livre $C(V_1 \times V_2)$, cuja base é $V_1 \times V_2$, e $N(V_1,V_2)$ o subespaço de $C(V_1 \times V_2)$ gerado pelos vetores:

$$(\alpha u_1 + \beta u_2, v) - \alpha(u_1,v) - \beta(u_2,v)$$
$$(u, \gamma v_1 + \lambda v_2) - \gamma(u,v_1) - \lambda(u,v_2)$$

sendo $u, u_1, u_2 \in V_1$, $v, v_1, v_2 \in V_2$ e $\alpha, \beta, \gamma, \lambda \in \mathbb{K}$.
Seja $W = C(V_1 \times V_2)/N(V_1,V_2)$ e π a projeção canônica de $C(V_1 \times V_2)$ em W e defina
$\varphi\colon V_1 \times V_2 \to W$ tal que $\varphi(u,v) = \pi(u,v)$.
A bilinearidade da aplicação φ decorre da definição de $N(V_1,V_2)$. Tem-se que

$$(\alpha u_1 + \beta u_2, v) - \alpha(u_1,v) - \beta(u_2,v) \in N(V_1,V_2),$$

então

$$\pi(\alpha u_1 + \beta u_2, v) = \alpha\pi(u_1,v) + \beta\pi(u_2,v),$$

assim,

$$\begin{aligned}\varphi(\alpha u_1+\beta u_2,v) &= \pi(\alpha u_1+\beta u_2,v)\\ &= \alpha\pi(u_1,v)+\beta\pi(u_2,v)\\ &= \alpha\varphi(u_1,v)+\beta\varphi(u_2,v)\end{aligned}$$

Analogamente, para $\varphi(u,\gamma v_1+\lambda v_2)=\gamma\varphi(u,v_1)+\lambda\varphi(u,v_2)$.
Para mostrar que a aplicação φ satisfaz a propriedade universal do produto tensorial, basta demonstrar que ela satisfaz as condições (i) e (ii) da definição 3.3.1.

(i) Seja $z\in C(V_1\times V_2)$, pela observação 3.3.6, tem-se que

$$z=\sum_{i,j}\alpha_{i,j}(a_i,b_j).$$

Como $\pi\colon C(V_1\times V_2)\to W$ é sobrejetora, tem-se que para $w\in W$, existe $z\in C(V_1\times V_2)$ tal que

$$\pi(z)=\pi\left(\sum_{i,j}\alpha_{i,j}(a_i,b_j)\right)=w,$$

Daí,

$$w=\pi\left(\sum_{i,j}\alpha_{i,j}(a_i,b_j)\right)=\sum_{i,j}\alpha_{i,j}\pi(a_i,b_j)=\sum_{i,j}\alpha_{i,j}\varphi(a_i,b_j)=\varphi\left(\sum_{i,j}\alpha_{i,j}(a_i,b_j)\right)$$

Logo, $w\in Im(\varphi)$, ou seja, $W\subset Im\varphi$. É claro que $Im\varphi\subset W$. Portanto, $Im\varphi=W$.

(ii) Considere a aplicação bilinear $\psi\colon V_1\times V_2\to U$, sendo U um espaço vetorial arbitrário. Pela observação 3.3.6, $V_1\times V_2$ é base de $C(V_1\times V_2)$, então existe uma única aplicação linear $g\colon C(V_1\times V_2)\to U$ dada por $g(u,v)=\psi(u,v)$. Da bilinearidade de ψ segue que $N(V_1,V_2)\subset Nu(g)$. De fato,

$$\begin{aligned}\psi(\alpha u_1+\beta u_2,v)&=\alpha\psi(u_1,v)+\beta\psi(u_2,v)\\ \psi(u,\gamma v_1+\lambda v_2)&=\gamma\psi(u,v_1)+\lambda\psi(u,v_2)\end{aligned}$$

De onde,

$$g(\alpha u_1 + \beta u_2, v) = \alpha g(u_1, v) + \beta g(u_2, v) = g(\alpha(u_1, v) + \beta(u_2, v))$$
$$g(u, \gamma v_1 + \lambda v_2) = \gamma g(u, v_1) + \lambda g(u, v_2) = g(\gamma(u, v_1) + \lambda(u, v_2))$$

Da linearidade da g, conclui-se que $N(V_1, V_2) \subset Nu(g)$.
Portanto, g induz uma aplicação linear $f\colon C(V_1 \times V_2)/N(V_1, V_2) \to U$ tal que $f \circ \pi = g$.
Como $\pi(u, v) = \varphi(u, v)$, segue que

$$f \circ \varphi = f \circ \pi = g = \psi.$$

Logo, (W, φ) é o produto tensorial de V_1 em V_2, sendo $W = C(V_1 \times V_2)/N(V_1, V_2)$ e $\varphi = \pi$.

□

Demonstrada a existência do produto tensorial, tem-se a proposição abaixo, a qual garante sua unicidade.

Proposição 3.3.8. *Sejam V_1, V_2, W e U espaços vetoriais sobre o corpo $\mathbb{K}$. Se $\varphi_1\colon V_1 \times V_2 \to W$ e $\varphi_2\colon V_1 \times V_2 \to U$ são aplicações bilineares que satisfazem a propriedade universal. Então, existe um isomorfismo linear $f\colon W \to U$ tal que $f(\varphi_1(u, v)) = \varphi_2(u, v)$, para todo $u \in V_1$ e $v \in V_2$.*

Demonstração:
Sabendo que φ_1 e φ_2 satisfazem a propriedade universal, é possível utilizar a notação instituída na observação 3.3.3. Assim, $\varphi_1(u, v) = u \otimes_1 v$ e $\varphi_2(u, v) = u \otimes_2 v$, para $u \in V_1$ e $v \in V_2$. Pela condição (ii) da definição 3.3.1, existem as aplicações lineares $f\colon W \to U$ e $g\colon U \to W$ tais que

$$f(u \otimes_1 v) = u \otimes_2 v \quad \text{e} \quad g(u \otimes_2 v) = u \otimes_1 v,$$

para todo $u \in V_1$ e $v \in V_2$. Assim,

$$f(g(u \otimes_2 v)) = f(u \otimes_1 v) = u \otimes_2 v \quad \text{e} \quad g(f(u \otimes_1 v)) = g(u \otimes_2 v) = u \otimes_1 v.$$

Considerando-se as aplicações identidade i_U e i_W, tem-se

$$i_U(u \otimes_2 v) = u \otimes_2 v \quad \text{e} \quad i_W(u \otimes_1 v) = u \otimes_1 v.$$

Pela condição (i) da definição 3.3.1, segue que f e g são isomorfismos lineares inversos.

□

Para construir uma base para o produto tensorial faz-se necessária a seguinte proposição:

Proposição 3.3.9. *Considere V e W espaços vetoriais sobre o corpo $\mathbb{K}$ e $(v_i)_{1\leqslant i\leqslant n}$ uma família de vetores de V. A família $(v_i)_{1\leqslant i\leqslant n}$ é linearmente independente se, e somente se, para cada família $(w_i)_{1\leqslant i\leqslant n}$ de vetores de W, existe uma aplicação linear $f\colon V\to W$ tal que $f(v_i)=w_i$, para todo $i\in\{1,\ldots,n\}$.*

Proposição 3.3.10. *Sejam V_1 e V_2 espaços vetoriais sobre o corpo $\mathbb{K}$. Se $\{v_i^1\}_{1\leqslant i\leqslant n}$ e $\{v_j^2\}_{1\leqslant j\leqslant m}$ são bases de V_1 e V_2, respectivamente, então o conjunto $\{(v_i^1\otimes v_j^2)\colon i\in\{1,\ldots,n\}\ e\ j\in\{1,\ldots,m\}\}$ é uma base para o produto tensorial $V_1\otimes V_2$.*

Demonstração:
Todo $v_1\in V_1$ pode ser escrito de maneira única como

$$v_1=\sum_{i=1}^{n}\alpha_i v_i^1.$$

Todo $v_2\in V_2$ pode ser escrito de maneira única como

$$v_2=\sum_{j=1}^{m}\beta_j v_j^2.$$

Considere um espaço vetorial qualquer W não trivial e $\{w_{1,1},\ldots,w_{n,m}\}\subset W$.
O objetivo é mostrar que existe uma aplicação linear $h\colon V_1\otimes V_2\to W$ tal que $h(v_i^1\otimes v_j^2)=w_{i,j}$.
Então, defina a aplicação $f\colon V_1\times V_2\to W$ tal que

$$f(v_1,v_2)=f\left(\sum_{i=1}^{n}\alpha_i v_i^1,\sum_{j=1}^{m}\beta_j v_j^2\right)=\sum_{i,j}\alpha_i\beta_j w_{i,j}$$

Note que f é bilinear.
Pela propriedade universal do produto tensorial existe $f_\otimes\colon V_1\otimes V_2\to W$ tal que

$$f=f_\otimes\circ\varphi,$$

onde $\varphi\colon V_1\times V_2\to V_1\otimes V_2$.
Logo, a h procurada é a $f_\otimes$.
Portanto, pela proposição anterior, $\{(v_i^1\otimes v_j^2)\colon i\in\{1,\ldots,n\};j\in\{1,\ldots,m\}\}$ é linearmente independente.
Pela demonstração do teorema da existência do produto tensorial, tem-se que

$$\begin{aligned}\varphi\colon V_1\times V_2&\to W=V_1\otimes V_2\\(u,v)&\mapsto\pi(u,v)=\varphi(u,v)=(u\otimes v)\end{aligned}$$

Desse modo, $\{(v_i^1, v_j^2) \colon i \in \{1,\ldots,n\}; j \in \{1,\ldots,m\}\}$ gera o espaço $V_1 \times V_2$ e $\{(v_i^1 \otimes v_j^2) \colon i \in \{1,\ldots,n\}; j \in \{1,\ldots,m\}\}$ gera o espaço $W = V_1 \otimes V_2$.
Portanto, $\{(v_i^1 \otimes v_j^2) i \in \{1,\ldots,n\}; j \in \{1,\ldots,m\}\}$ é uma base para $V_1 \otimes V_2$.

□

Conhecendo-se a base de um espaço vetorial, é interessante saber a dimensão desse espaço vetorial, que nesse caso decorre diretamente do princípio fundamental da contagem.

Proposição 3.3.11. *Sejam V_1 e V_2 espaços vetoriais sobre o corpo $\mathbb{K}$. Considere $dim(V_1) = n$ e $dim(V_2) = m$, então $dim(V_1 \otimes V_2) = nm$.*

Seguem alguns exemplos de produto tensorial.

Exemplo 3.3.12. *Sejam M_1, M_2, N_1, e N_2 espaços vetoriais sobre o corpo $\mathbb{K}$, com dimensões m_1, m_2, n_1, e n_2, respectivamente. Então, $L(M_1,M_2) \otimes L(N_1,N_2) \cong L(M_1 \otimes N_1, M_2 \otimes N_2)$. De fato, considere a aplicação*

$$\begin{aligned} \varphi \colon L(M_1,M_2) \times L(N_1,N_2) &\to L(M_1 \otimes N_1, M_2 \otimes N_2) \\ (f,g) &\mapsto \varphi(f,g) \end{aligned}$$

dada por $\varphi(f,g)(a \otimes b) = f(a) \otimes f(b)$. É claro que φ é bilinear.
Pela propriedade universal do produto tensorial existe uma única aplicação linear

$$\phi \colon L(M_1,M_2) \otimes L(N_1,N_2) \to L(M_1 \otimes N_1, M_2 \otimes N_2)$$

tal que $\phi(f \otimes g) = \varphi(f,g)$.
O objetivo é mostrar que ϕ leva base em base. Assim, considere $\{e_i\}$, $\{e_i'\}$, $\{e_j\}$ e $\{e_j'\}$ bases de M_1, M_2, N_1 e N_2, respectivamente. Então, $\{E_{i'i}\}$ e $\{\tilde{E}_{j'j}\}$ são bases de $L(M_1,M_2)$ e $L(N_1,N_2)$, respectivamente.
Definindo a aplicação linear $E_{i'i} \colon M_1 \to M_2$ tal que $E_{i'i}(e_i) = e_i'$ e $E_{i'i}(e_j) = 0$, para $j \neq i$. E definindo uma aplicação linear $\tilde{E}_{j'j}$ de maneira análoga, obtém-se que $\{E_{i'i} \otimes \tilde{E}_{j'j}\}$ é uma base para $L(M_1,M_2) \otimes L(N_1,N_2)$.
Dessa maneira,

$$\begin{aligned} \phi(E_{i'i} \otimes \tilde{E}_{j'j})(e_r \otimes E_s) &= E_{i'i}(e_r) \otimes \tilde{E}_{j'j}(E_s) \\ &= \begin{cases} e_i' \otimes E_j', & \text{se } r = i \text{ e } s = j \\ 0, & \text{caso contrário} \end{cases} \end{aligned}$$

Logo, $\phi(E_{i'i} \otimes \tilde{E}_{j'j})$ leva $e_i \otimes E_j$ em $e'_i \otimes E'_j$, e os outros elementos da base de $M_1 \otimes N_1$ leva em 0.
Portanto, obtém-se o resultado.

Exemplo 3.3.13. *Se m, n são inteiros positivos e $d = (m,n)$, então*

$$\mathbb{Z}/n\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/d\mathbb{Z}.$$

Em particular,

$$\mathbb{Z}/n\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/m\mathbb{Z} = 0$$

se, e somente se, $(m,n) = 1$.
De fato. Como $[1]_n$ gera $\mathbb{Z}/n\mathbb{Z}$ e $[1]_m$ gera $\mathbb{Z}/m\mathbb{Z}$, tem-se que $[1]_n \otimes [1]_m$ gera $Z/n\mathbb{Z} \otimes \mathbb{Z}/m\mathbb{Z}$. Agora, $n([1]_n \otimes [1]_m) = [n]_n \otimes [1]_m = 0 \otimes [1]_m = 0$ e $m([1]_n \otimes [1]_m) = [1]_n \otimes [m]_m = [1]_n \otimes 0 = 0$. A ordem de $[1]_n \otimes [1]_m$ divide n e m. Portanto, divide d. Logo, a ordem de $\mathbb{Z}/n\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/m\mathbb{Z}$ é menor ou igual a d.
Considere a aplicação $\psi\colon \mathbb{Z}/n\mathbb{Z} \times_{\mathbb{Z}} \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/d\mathbb{Z}$, dada por $\psi([a]_n, [b]_m) = [ab]_d$. Tem-se que ψ está bem definida, pois se $([a_1]_n, [b_1]_m) = ([a_2]_n, [b_2]_m)$, então $n|a_1 - a_2$ e $m|b_1 - b_2$. Assim, $d|a_1 - a_2$ e $d|b_1 - b_2$. Daí, $d|b_1(a_1 - a_2)$ e $d|(b_1 - b_2)a_2$. Segue que, $d|a_1b_1 - a_2b_2$, ou seja, $[a_1b_1]_d = [a_2b_2]_d$.
É claro que ψ é $\mathbb{Z}$-bilinear.
Pela propriedade universal do produto tensorial, existe uma única aplicação $\mathbb{Z}$-linear $h\colon \mathbb{Z}/n\mathbb{Z} \otimes \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/d\mathbb{Z}$ que faz o seguinte diagrama comutar.

$$\begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} \otimes \mathbb{Z}/m\mathbb{Z} & \xrightarrow{\psi} & \mathbb{Z}/d\mathbb{Z} \\ {\scriptstyle\otimes}\downarrow & \nearrow_{h} & \\ \mathbb{Z}/n\mathbb{Z} \otimes \mathbb{Z}/d\mathbb{Z} & & \end{array}$$

Assim, $h([a]_n \otimes [b]_m) = [ab]_d$.
Em particular, $h([a]_n, [1]_m) = [a]_d$. Desse modo, h é sobrejetora. Daí, $\mathbb{Z}/n\mathbb{Z} \otimes \mathbb{Z}/m\mathbb{Z}$ tem tamanho pelo menos d. Logo, o tamanho é d.

3.4 POTÊNCIA SIMÉTRICA

O objetivo em definir a potência simétrica é chegar a uma noção do produto tensorial que permita tratar aplicações multilineares simétricas como aplicações lineares.

Primeiramente, segue a definição de uma aplicação multilinear simétrica:

Definição 3.4.1. *Sejam V e W espaços vetoriais sobre o corpo $\mathbb{K}$ e seja $\varphi\colon V^n \to W$ uma aplicação multilinear. Diz-se que φ é uma* ***aplicação multilinear simétrica*** *quando*

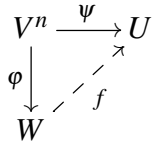
$$\varphi(v_{\sigma(1)},\ldots,v_{\sigma(n)}) = \varphi(v_1,\ldots,v_n)$$

com $v_i \in V$, para $i \in \{1,\ldots,n\}$ e $\sigma \in S_n$, sendo S_n o grupo simétrico.

O conjunto de todas as aplicações multilineares simétricas $\varphi\colon V^n \to W$ é denotado por $S^n(V,W)$. Esse conjunto com a composição de aplicações tem estrutura de espaço vetorial sobre o corpo $\mathbb{K}$.

A partir dos conceitos de produto tensorial e aplicação multilinear simétrica é possível construir a potência simétrica. Mas primeiramente, o que é uma potência simétrica? A resposta está na definição abaixo, que é muito semelhante a definição de produto tensorial. A diferença é que φ e ψ devem ser mais do que aplicações multilineares, precisam ser aplicações multilineares simétricas.

Definição 3.4.2. *Sejam V e W espaços vetoriais sobre o corpo $\mathbb{K}$ e seja φ uma aplicação multilinear simétrica dada por $\varphi\colon V^n \to W$. O par (W,φ) é denominado* ***potência simétrica*** *de V quando para cada aplicação multilinear simétrica $\psi\colon V^n \to U$, sendo U um espaço vetorial arbitrário, existe uma* ***única*** *aplicação linear $f\colon W \to U$ tal que $\psi = f \circ \varphi$, ou seja, tal que o diagrama*



comuta.

Para facilitar a escrita, é utilizada a seguinte notação:

Observação 3.4.3. *Sejam V e W espaços vetoriais sobre o corpo $\mathbb{K}$ e seja uma aplicação multilinear simétrica $\varphi\colon V^n \to W$. Supondo que o par (W,φ) seja a potência simétrica de V, denota-se $W = S^n(V)$ e $\varphi(v_1,v_2,\ldots,v_n) = v_1v_2\ldots v_n$, para $v_i \in V$, sendo $i \in \{1,\ldots,n\}$.*

Nesse ponto surge a mesma dúvida em relação ao produto tensorial: a potência simétrica existe? E se existe, ela é única?

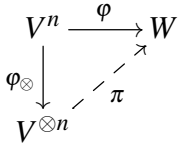
Proposição 3.4.4. *Sejam V e W espaços vetoriais sobre o corpo $\mathbb{K}$ e seja $\varphi\colon V^n \to W$ uma aplicação multilinear simétrica, então uma potência simétrica (W,φ) pode ser construída.*

Demonstração:
Seja $(V^{\otimes n},\varphi_{\otimes})$ o produto tensorial de V^n e considere C o subespaço vetorial de $V^{\otimes n}$ gerado

pelos vetores

$$v_1 \otimes \ldots \otimes v_n - v_{\sigma(1)} \otimes \ldots \otimes v_{\sigma(n)}.$$

Sejam $W = V^{\otimes n}/C$ e π a projeção canônica de $V^{\otimes n}$ em W. Defina a aplicação multilinear $\varphi\colon V^n \to W$ tal que $\varphi(v_1,\ldots,v_n) = \pi(v_1 \otimes \ldots \otimes v_n)$. Como $(V^{\otimes n}, \varphi_\otimes)$ é o produto tensorial, tem-se que $\varphi_\otimes(v_1,\ldots,v_n) = v_1 \otimes \ldots \otimes v_n$, então $\varphi = \pi \circ \varphi_\otimes$, ou seja, o diagrama



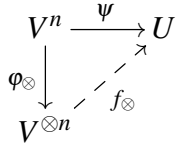
comuta.

Note que φ é simétrica.

Como os vetores $v_1 \otimes \ldots \otimes v_n$ geram $V^{\otimes n}$ e π é sobrejetora, então $\pi(v_1 \otimes \ldots \otimes v_n) = \varphi(v_1,\ldots,v_n)$ gera W.

O objetivo é mostrar que (W,φ) é a potência simétrica de V, ou seja, mostrar que dada uma aplicação multilinear simétrica $\psi\colon V^n \to U$, sendo U um espaço vetorial arbitrário sobre $\mathbb{K}$, existe uma única aplicação linear $f\colon W \to U$ tal que $\psi = f \circ \varphi$.

Agora, dada uma aplicação multilinear simétrica $\psi\colon V^n \to U$, pela propriedade universal do produto tensorial existe uma única aplicação linear $f_\otimes\colon V^{\otimes n} \to U$ tal que $\psi = f_\otimes \circ \varphi_\otimes$, ou seja, tal que o diagrama



comuta.

Sendo $v = v_1 \otimes \ldots \otimes v_n - v_{\sigma(1)} \otimes \ldots \otimes v_{\sigma(n)}$, pelo fato de ψ ser simétrica e $f_\otimes$ linear, tem-se que

$$\begin{aligned} f_\otimes(v) &= f_\otimes(v_1 \otimes \ldots \otimes v_n - v_{\sigma(1)} \otimes \ldots \otimes v_{\sigma(n)}) \\ &= f_\otimes(v_1 \otimes \ldots \otimes v_n) - f_\otimes(v_{\sigma(1)} \otimes \ldots \otimes v_{\sigma(n)}) \\ &= f_\otimes \circ \varphi_\otimes(v_1,\ldots,v_n) - f_\otimes \circ \varphi_\otimes(v_{\sigma(1)},\ldots,v_{\sigma(n)}) \\ &= \psi(v_1,\ldots,v_n) - \psi(v_{\sigma(1)},\ldots,v_{\sigma(n)}) \\ &= 0 \end{aligned}$$

Segue que $f_\otimes$ induz uma única aplicação linear $f\colon W \to U$ tal que $f(\overline{v}) = f_\otimes(v)$, sendo $\overline{v} \in W$, com $v \in V^{\otimes n}$. De fato, suponha $\overline{v_1}, \overline{v_2} \in W$, de modo que $\overline{v_1} = \overline{v_2}$, então $v_1 - v_2 \in C$. Assim, $f_\otimes(v_1 - v_2) = 0$, pela linearidade da aplicação, $f_\otimes(v_1) = f_\otimes(v_2)$. Logo, $f(\overline{v_1}) = f(\overline{v_2})$.

Portanto, (W, φ) é a potência simétrica de V, sendo $W = V^{\otimes n}/C$, tal que o diagrama

$$\begin{array}{ccc} V^n & \xrightarrow{\psi} & U \\ {\scriptstyle\varphi}\downarrow & \nearrow_{f} & \\ W & & \end{array}$$

comuta. É claro que a aplicação f é única.

□

Demonstrada a existência da potência simétrica, tem-se a proposição abaixo, a qual garante sua unicidade.

Proposição 3.4.5. *Sejam V, W e U espaços vetoriais sobre o corpo $\mathbb{K}$ e considere $\varphi_1 \colon V^n \to W$ e $\varphi_2 \colon V^n \to U$ aplicações multilineares simétricas tal que (W, φ_1) e (U, φ_2) são potências simétricas. Então, existe um isomorfismo $f \colon W \to U$ tal que*

$$f(\varphi_1(v_1, \ldots, v_n)) = \varphi_2(v_1, \ldots, v_n),$$

para todo $v_i \in V$, sendo $i \in \{1, \ldots, n\}$.

Demonstração:
A demonstração é análoga a demonstração da unicidade do produto tensorial.

□

Agora, será construída uma base para a potência simétrica, de modo semelhante a construção da base para o produto tensorial.

Proposição 3.4.6. *Seja V um espaço vetorial sobre o corpo $\mathbb{K}$ tal que $dim(V) = m$ e $\{e_1, \ldots, e_m\}$ é base de V. Então, $\beta = \{e_1^{i_1} \ldots e_m^{i_m} \colon i_1 + \ldots + i_m = n\}$ é uma base para $S^n(V)$.*

Demonstração:
Na demonstração da construção da potência simétrica foi demonstrado que o conjunto β gera $S^n(V)$. Para mostrar que é linearmente independente, será utilizada a proposição 3.3.9. O objetivo é considerar uma família arbitrária de vetores $(w_I)_{I \in A}$ de W, para $I = (i_1, \ldots, i_m)$, $A = \{(i_1, \ldots, i_m) \colon i_1 + \ldots + i_m = n\}$, sendo W qualquer espaço vetorial não trivial sobre $\mathbb{K}$, e mostrar que para cada família desse tipo existe uma aplicação linear $h \colon S^n(V) \to W$ tal que $h(e_1^{i_1} \ldots e_m^{i_m}) = w_I$.

Defina a aplicação $\psi\colon V^n \to W$ por

$$\psi(v_1,\ldots,v_n) = \psi\left(\sum_{i=1}^{m}\alpha_{1i}e_i,\ldots,\sum_{i=1}^{m}\alpha_{ni}e_i\right) = \sum(\alpha_{1i}\ldots\alpha_{ni})w_I$$

para todo $(v_1,\ldots,v_n) \in V^n$. A aplicação ψ é multilinear e simétrica. Então, sendo $(S^n(V),\varphi)$ a potência simétrica de V, pela definição de potência simétrica existe única transformação linear $f\colon S^n(V) \to W$ tal que $\psi = f\circ\varphi$, onde $\varphi\colon V^n \to S^n(V)$.
Desse modo, a h procurada é a f. Portanto, o conjunto é linearmente independente.

□

A dimensão de $S^n(V)$ é igual a quantidade de elementos na base desse espaço vetorial. Encontrar essa quantidade é semelhante a resolver o problema de encontrar soluções inteiras e não negativas cuja soma é um determinado número, por exemplo $x_1+x_2+x_3+x_4 = 11$. Sabe-se que a quantidade de soluções da forma (x_1,x_2,x_3,x_4) é igual a $\begin{pmatrix} 14 \\ 3 \end{pmatrix}$. Generalizando, se a equação é $x_1+\ldots+x_m = p$, então o número de soluções inteiras não negativas $(x_1,\ldots,x_n)$ é $\begin{pmatrix} p+m-1 \\ m-1 \end{pmatrix}$.

Proposição 3.4.7. *Seja V um espaço vetorial sobre o corpo $\mathbb{K}$ tal que $dim(V) = m$, então* $dim(S^n(V)) = \begin{pmatrix} n+m-1 \\ m-1 \end{pmatrix}$.

Exemplo 3.4.8. *Tem-se que $S^k(V)$ pode ser pensada como o espaço dos polinômios de grau k nos elementos de V com a operação usual de produto comutativo de polinômios. Quando os elementos são escritos em termos de uma base, o produto resulta em um polinômio. Por exemplo, considere o produto*

$$(1,1,1)\cdot(-1,1,1)\cdot(0,1,-1) \in S^3(\mathbb{R}^3).$$

Sejam $x = (1,0,0)$, $y = (0,1,0)$, $z = (0,0,1)$. Calculando o produto em termos de x, y e z, segue que

$$(1,1,1)\cdot(-1,1,1)\cdot(0,1,-1) = (x+y+z)(-x+y+z)(y-z) = x^2y-x^2z+y^3+y^2z-yz^2-z^3.$$

3.5 POTÊNCIA EXTERIOR

Primeiramente, será definida a aplicação multilinear alternada.

Definição 3.5.1. *Sejam V e W espaços vetoriais sobre o corpo $\mathbb{K}$ e seja $\varphi\colon V^n \to W$ uma aplicação multilinear. Diz-se que φ é uma* ***aplicação multilinear alternada*** *se*

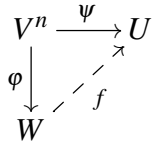
$$\varphi(v_1,\ldots,v_i,\ldots,v_j,\ldots,v_n) = 0$$

sempre que algum $v_i = v_j$, com $i \neq j$, para $v_i, v_j \in V$ e $i, j \in \{1,\ldots,n\}$.

O conjunto de todas as aplicações multilineares alternadas $\varphi\colon V^n \to W$ é denotado por $Alt^n(V,W)$. Esse conjunto com a composição de aplicações tem estrutura de espaço vetorial sobre o corpo $\mathbb{K}$.

A partir da definição de aplicação multilinear alternada e tendo noção de produto tensorial é possível construir a potência exterior. Segue abaixo a definição.

Definição 3.5.2. *Sejam V e W espaços vetoriais sobre o corpo $\mathbb{K}$ e seja φ uma aplicação multilinear alternada dada por $\varphi\colon V^n \to W$. O par (W,φ) é denominado* ***potência exterior*** *de V quando para cada aplicação multilinear alternada $\psi\colon V^n \to U$, sendo U um espaço vetorial arbitrário, existe uma* ***única*** *aplicação linear $f\colon W \to U$ tal que $\psi = f \circ \varphi$, ou seja, tal que o diagrama*



comuta.

Para facilitar a escrita, utiliza-se a seguinte notação:

Observação 3.5.3. *Sejam V e W espaços vetoriais sobre o corpo $\mathbb{K}$ e seja uma aplicação multilinear alternada $\varphi\colon V^n \to W$. Supondo que o par (W,φ) seja a potência exterior de V, denota-se $W = \bigwedge^n(V)$ e $\varphi(v_1,v_2,\ldots,v_n) = v_1 \wedge v_2 \wedge \ldots \wedge v_n$, para $v_i \in V$, sendo $i \in \{1,\ldots,n\}$.*

Uma dúvida é: a potência exterior existe? E se existe, ela é única?

Proposição 3.5.4. *Sejam V e W espaços vetoriais sobre o corpo $\mathbb{K}$ e seja $\varphi\colon V^n \to W$ uma aplicação multilinear alternada, então uma potência exterior (W,φ) pode ser construída.*

Demonstração:
Seja $(V^{\otimes n}, \varphi_{\otimes})$ o produto tensorial de V^n e considere C o subespaço vetorial de $V^{\otimes n}$ gerado pelos vetores

$$v_1 \otimes \ldots \otimes v_i \otimes \ldots \otimes v_i \otimes \ldots \otimes v_n.$$

Sejam $W = V^{\otimes n}/C$ e π a projeção de $V^{\otimes n}$ em W dada por $\pi\colon V^{\otimes n} \to W$. Defina a aplicação multilinear $\varphi\colon V^n \to W$ tal que $\varphi(v_1,\ldots,v_n) = \pi(v_1 \otimes \ldots \otimes v_n)$. Como $(V^{\otimes n}, \varphi_\otimes)$ é o produto tensorial, tem-se que $\varphi_\otimes(v_1,\ldots,v_n) = v_1 \otimes \ldots \otimes v_n$, então $\varphi = \pi \circ \varphi_\otimes$, ou seja, o diagrama

$$\begin{array}{ccc} V^n & \xrightarrow{\varphi} & W \\ {\scriptstyle\varphi_\otimes}\downarrow & \nearrow_{\pi} & \\ V^{\otimes n} & & \end{array}$$

comuta.

Note que φ é alternada.

Como os vetores $v_1 \otimes \ldots \otimes v_n$ geram $V^{\otimes n}$ e π é sobrejetora, então $\pi(v_1 \otimes \ldots \otimes v_n) = \varphi(v_1,\ldots,v_n)$ gera W.

O objetivo é mostrar que (W,φ) é a potência exterior de V, ou seja, mostrar que dada uma aplicação multilinear alternada $\psi\colon V^n \to U$, sendo U um espaço vetorial arbitrário sobre $\mathbb{K}$, existe uma única aplicação linear $f\colon W \to U$ tal que $\psi = f \circ \varphi$.

Agora, dada uma aplicação multilinear alternada $\psi\colon V^n \to U$, pela propriedade universal do produto tensorial existe uma única aplicação linear $f_\otimes\colon V^{\otimes n} \to U$ tal que $\psi = f_\otimes \circ \varphi_\otimes$, ou seja, tal que o diagrama

$$\begin{array}{ccc} V^n & \xrightarrow{\psi} & U \\ {\scriptstyle\varphi_\otimes}\downarrow & \nearrow_{f_\otimes} & \\ V^{\otimes n} & & \end{array}$$

comuta.

Sendo $v = v_1 \otimes \ldots \otimes v_i \otimes \ldots \otimes v_i \otimes \ldots \otimes v_n$, pelo fato de ψ ser alternada e $f_\otimes$ linear, tem-se que

$$\begin{aligned} f_\otimes(v) &= f_\otimes(v_1 \otimes \ldots \otimes v_i \otimes \ldots \otimes v_i \otimes \ldots \otimes v_n) \\ &= f_\otimes \circ \varphi_\otimes(v_1,\ldots,v_i,\ldots,v_i,\ldots,v_n) \\ &= \psi(v_1,\ldots,v_i,\ldots,v_i,\ldots,v_n) \\ &= 0 \end{aligned}$$

Segue que $f_\otimes$ induz uma única aplicação linear $f\colon W \to U$ tal que $f(\overline{v}) = f_\otimes(v)$, sendo $\overline{v} \in W$, com $v \in V^{\otimes n}$. De fato, suponha $\overline{v_1}, \overline{v_2} \in W$, de modo que $\overline{v_1} = \overline{v_2}$, então $v_1 - v_2 \in C$. Assim, $f_\otimes(v_1 - v_2) = 0$, pela linearidade da aplicação, $f_\otimes(v_1) = f_\otimes(v_2)$. Logo, $f(\overline{v_1}) = f(\overline{v_2})$.

Portanto, (W,φ) é a potência exterior de V, sendo $W = V^{\otimes n}/C$, tal que o diagrama

$$\begin{array}{ccc} V^n & \xrightarrow{\psi} & U \\ {\scriptstyle\varphi}\downarrow & \nearrow_{f} & \\ W & & \end{array}$$

comuta. É claro que a aplicação f é única.

□

Demonstrada a existência da potência exterior, segue a proposição abaixo, a qual garante sua unicidade.

Proposição 3.5.5. *Sejam V, W e U espaços vetoriais sobre o corpo $\mathbb{K}$ e considere $\varphi_1 : V^n \to W$ e $\varphi_2 : V^n \to U$ aplicações multilineares alternadas tal que (W, φ_1) e (U, φ_2) são potências exteriores. Então, existe um isomorfismo linear $f : W \to U$ tal que $f(\varphi_1(v_1, \ldots, v_n)) = \varphi_2(v_1, \ldots, v_n)$, para todo $v_i \in V$, sendo $i \in \{1, \ldots, n\}$.*

Demonstração:
A demonstração é análoga a demonstração da unicidade do produto tensorial.

□

Agora, será construída uma base para a potência exterior:

Proposição 3.5.6. *Seja V um espaço vetorial sobre o corpo $\mathbb{K}$ tal que $dim(V) = m$. Se $\{e_1, \ldots, e_m\}$ é uma base de V, então $\beta = \{e_{i_1} \wedge \ldots \wedge e_{i_n}\}$ é uma base para $\bigwedge^n(V)$, sendo $1 \leqslant i_1 < \ldots < i_n \leqslant m$.*

Demonstração:
Pela demonstração da existência da potência exterior, tem-se que β gera $\bigwedge^n(V)$. Falta mostrar que β é linearmente independente.
Considere $(v_1, \ldots, v_n) \in V^n$. Então,

$$v_i = \sum_{j=1}^{m} a_{ji} e_j$$

para $a_{ji} \in \mathbb{K}$, sendo $i = 1, \ldots, n$.
Desse modo, será obtida uma matriz A composta pelos coeficiente de cada v_i,

$$A = \begin{pmatrix} a_{11} & \ldots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \ldots & a_{mn} \end{pmatrix}$$

Defina, para cada n-upla ordenada $I = (i_1, \ldots, i_n)$ com $1 \leqslant i_1 < \ldots < i_n \leqslant m$, a aplicação $\mu_I : V^n \to \mathbb{K}$ tal que

$$\mu_I(v_1, \ldots, v_n) = det(a_{i_r j})_{1 \leqslant r < j \leqslant n}$$

A aplicação μ_I é multilinear e alternada. Pela definição de potência exterior, existe uma única transformação linear $T_I\colon \bigwedge^n V \to \mathbb{K}$ tal que $T_I(v_1 \wedge \ldots \wedge v_n) = \mu_I(v_1, \ldots, v_n)$.
Seja $J = (j_1, \ldots, j_n)$ com $1 \leqslant j_1 < \ldots < j_n \leqslant m$. A monotonicidade implica que quando $J \neq I$ temos que algum j_t, $t = 1, \ldots, n$, deve ser diferente de todos os i_k, para todo $k = 1, \ldots, n$. Logo, $T_I(e_{j_1} \wedge \ldots \wedge e_{j_n}) = 0$, pois a matriz formada pelos coeficientes dos elementos da base terá uma coluna de zeros. É claro que $T_I(e_{i_1} \wedge \ldots \wedge e_{i_n}) = 1$, já que é o determinante da matriz identidade. Suponha que

$$\sum_{1 \leqslant j_1 < \ldots < j_n \leqslant m} c_{j_1 \ldots j_n} e_{j_1} \wedge \ldots \wedge e_{j_n} = 0.$$

Aplicando T_I, segue que $c_{i_1 \ldots i_n} = 0$. Portanto, o conjunto é linearmente independente.

□

Conhecendo-se a base, é interessante saber a dimensão da mesma. A ideia é escolher n elementos dos m disponíveis, que é a dimensão de V, ou seja, $\begin{pmatrix} m \\ n \end{pmatrix}$. Assim, está demonstrada a proposição abaixo.

Proposição 3.5.7. *Seja V um espaço vetorial sobre o corpo $\mathbb{K}$ tal que $dim(V) = m$, então $dim(\wedge^n V) = \begin{pmatrix} m \\ n \end{pmatrix}$.*

Exemplo 3.5.8. *Considere $V = \mathbb{R}^4$ e $\beta = \{x, y, z, w\}$ uma base de V. Seja $\alpha = x \wedge y + z \wedge w$. Então,*

$$\begin{aligned} \alpha \wedge \alpha &= (x \wedge y + z \wedge w) \wedge (x \wedge y + z \wedge w) \\ &= x \wedge y \wedge x \wedge y + x \wedge y \wedge z \wedge w + z \wedge w \wedge x \wedge y + z \wedge w \wedge z \wedge w \\ &= x \wedge y \wedge z \wedge w - x \wedge w \wedge z \wedge y \\ &= x \wedge y \wedge z \wedge w + x \wedge y \wedge z \wedge w \\ &= 2(x \wedge y \wedge z \wedge w) \end{aligned}$$

Observe que $\alpha \wedge \alpha \neq 0$. Isso mostra que α é uma potência exterior pura ($\alpha \neq u \wedge v$, para qualquer $u, v \in \mathbb{R}^4$).

4 REPRESENTAÇÃO DE GRUPOS

Em geral, é difícil entender um grupo conhecendo somente a sua operação sem antes realizar um trabalho árduo. Desse modo, dado um grupo, é interessante conseguir descrever seus elementos de maneira mais simples. Um modo de fazer isso, por exemplo, seria transformá-lo em um grupo de matrizes, pois o produto entre matrizes não é complicado e elas têm várias características interessantes que são de fácil compreensão.

Assim, a ideia da Teoria de Representação de Grupos é desenvolver uma teoria capaz de transformar os elementos de um grupo em matrizes, de modo que a operação do grupo corresponda ao produto de matrizes. E a maneira de fazer isso é por meio de um homomorfismo entre esses grupos.

Neste capítulo, escrito com base em Segal (2014), Pena (2014) e Fulton e Harris (1991), a representação de grupo será definida e exemplificada. Além disso, será demonstrado um dos resultados mais interessantes desse trabalho, o teorema 4.4.24, o qual alia as construções do capítulo anterior com a teoria de representações.

Serão considerados espaços vetoriais sobre o corpo dos números complexos $\mathbb{C}$, ainda que alguns dos conceitos e resultados também sejam válidos para um corpo qualquer.

4.1 REPRESENTAÇÕES

Com base na situação descrita acima, segue a seguinte definição:

Definição 4.1.1. *Sejam V um espaço vetorial de dimensão finita sobre $\mathbb{C}$, $GL(V)$ o grupo das transformações lineares inversíveis de V em V, e G um grupo. Diz-se que*

$$\rho : G \to GL(V)$$

é uma representação de G em V quando é um homomorfismo.

Simbolicamente,

$$\rho\colon G \to GL(V)$$
$$g \mapsto \rho(g)$$

tal que

$$\rho(gh) = \rho(g)\rho(h)$$

para todo $g,h \in G$.

O espaço V é denominado **representação** do grupo G e $dim(V)$ é denominado **grau** ou **dimensão** da representação.

Note que a definição não constrói um homomorfismo entre o grupo G e $GL_n(\mathbb{C})$, o grupo das matrizes invertíveis de ordem n que tem como entradas os números complexos.

Porém, existe um isomorfismo entre $GL(V)$ e $GL_n(\mathbb{C})$. De fato, seja V um espaço vetorial sobre $\mathbb{C}$ tal que $dim(V) = n$ e considere a aplicação φ definida da seguinte maneira:

$$\varphi\colon GL(V) \to GL_n(\mathbb{C})$$
$$T \mapsto [T]_\beta$$

para todo $T \in GL(V)$, sendo $\beta = \{v_1, \ldots, v_n\}$ uma base fixada de V e $[T]_\beta$ a matriz da transformação linear de T na base β.

Por resultados da Álgebra Linear, segue que φ é um homomorfismo:

$$\varphi(T_1 \circ T_2) = [T_1 \circ T_2]_\beta = [T_1]_\beta [T_2]_\beta = \varphi(T_1)\varphi(T_2).$$

Do modo como é definida a matriz de transformação linear, obtém-se a sobrejetividade da aplicação. Agora, sendo $[T_1]_\beta = [T_2]_\beta$, com $T_1, T_2 \in GL(V)$, tem-se $T_1(v_i) = T_2(v_i)$, para $i \in \{1, \ldots, n\}$. Supondo $v \in V$, segue que

$$v = \sum_{i=1}^{n} \alpha_i v_i.$$

Daí,

$$T_1(v) = \sum_{i=1}^{n} \alpha_i T_1(v_i) = \sum_{i=1}^{n} \alpha_i T_2(v_i) = T_2(v),$$

para todo $v \in V$. Logo, φ é injetora. Portanto, a aplicação é bijetora. Vem que φ é um isomor-

fismo.

Com base nesse raciocínio, é possível definir uma representação da seguinte maneira:

Definição 4.1.2. *Sejam $GL_n(\mathbb{C})$ o grupo das matrizes invertíveis de ordem n que tem como entradas os números complexos e G um grupo. Diz-se que $\rho : G \to GL_n(\mathbb{C})$ é uma representação de G quando é um homomorfismo.*

Informalmente, essa definição remete ao fato de que uma representação de um grupo é uma forma de escrevê-lo como um grupo de matrizes.

O conceito de representações de grupos está intimamente ligado com o de ação de grupos em espaços vetoriais. Com efeito, sendo V um espaço vetorial sobre $\mathbb{C}$ e G um grupo, dada $\rho : G \to GL(V)$ uma representação de G, é possível definir a seguinte ação de G em V:

$$\begin{aligned} \mu : G \times V &\to V \\ (g, v) &\mapsto \rho(g)(v) \end{aligned}$$

para todo $g \in G$ e $v \in V$.

Por outro lado, dada uma ação $\varphi : G \times V \to V$ de G em V, é possível definir uma representação de G em V, da seguinte maneira:

$$\begin{aligned} \rho : G &\to GL(V) \\ g &\mapsto \rho(g) = \varphi(g, \cdot) \end{aligned}$$

para todo $g \in G$, sendo

$$\varphi(g, \cdot) : V \to V$$

um operador linear com g fixado.

Seguem alguns exemplos de representações.

Exemplo 4.1.3. *Seja G um grupo e V um espaço vetorial sobre o corpo $\mathbb{C}$, tal que $dim(V) = n$. Considere a aplicação*

$$\begin{aligned} \rho : G &\to GL(V) \\ g &\mapsto \rho(g) = Id_V \end{aligned}$$

para todo $g \in G$.

Note que $\rho(g) = Id_V$ é a transformação identidade, ou seja,

$$\rho(g) = Id_V : V \to V$$
$$h \mapsto \rho(g)(h) = Id_V(h) = h$$

para todo $h \in V$.
Desse modo, podemos escrever que $\rho(g)(h) = h$.
Considerando $g_1, g_2 \in G$, segue que

$$\rho(g_1 g_2) = Id_V = Id_V \ \ Id_V = \rho(g_1)\rho(g_2),$$

ou seja, ρ é um homomorfismo. Logo, ρ é uma representação de G em V.
*Se $dim(V) = 1$, a representação é denominada **representação trivial** de G.*
Para que seja possível construir a representação trivial em sua forma matricial, é preciso fixar uma base para V. Feito isso, obtém-se

$$\rho : G \to GL_n(\mathbb{C})$$
$$g \mapsto \rho(g) = I_n$$

para todo $g \in G$, e sendo I_n a matriz identidade de ordem n.

A seguir, será apresentado um caso particular do exemplo anterior. Mas antes é necessário o seguinte resultado:

Proposição 4.1.4. *$GL(\mathbb{C})$ é isomorfo a $\mathbb{C} \setminus \{0\}$.*

Demonstração:
Para mostrar essa afirmação, é necessário definir uma aplicação $\varphi : GL(\mathbb{C}) \to \mathbb{C} \setminus \{0\}$ tal que φ seja isomorfismo. Considere a aplicação

$$\varphi : GL(\mathbb{C}) \to \mathbb{C} \setminus \{0\}$$
$$f \mapsto \varphi(f) = f(1)$$

para todo $f \in GL(\mathbb{C})$. Note que $f(1) = r \neq 0$, assim $f(1) \in \mathbb{C} \setminus \{0\}$. Suponha que isso não acontece, ou seja, $f(1) = 0$. Como f é um isomorfismo, então $f(0) = 0$. Desse modo, $f(1) = f(0)$, mas $1 \neq 0$, o que implica na não injetividade de f, contradizendo o fato de f ser um isomorfismo.
Agora, considerando $x \in \mathbb{C}$, tem-se que $f(x) = f(1 \cdot x) = f(1)f(x) = rx$. Isso será utilizado na demonstração de que φ é um isomorfismo.

Suponha $f, g \in GL(\mathbb{C})$, tais que $f(1) = r$ e $g(1) = s$, com $r, s \in \mathbb{C}$, então

$$\varphi(fg) = (fg)(1) = f(g(1)) = f(s) = rs = f(1)g(1) = \varphi(f)\varphi(g).$$

Logo, φ é homomorfismo.
Considerando $f \in Nu(\varphi)$, vem $\varphi(f) = 1$, ou seja, $f(1) = 1$. Daí, $f(x) = f(x \cdot 1) = xf(1) = x \cdot 1 = x$. Logo, $f = Id$. Portanto, φ é injetora.
Por último, dado $z \in \mathbb{C} \setminus \{0\}$, é necessário mostrar que existe $f \in GL(\mathbb{C})$ tal que $\varphi(f) = z$. Considerando $f\colon \mathbb{C} \to \mathbb{C}$ definida por $f(x) = zx$, para todo $x \in \mathbb{C}$, tem-se que $f \in GL(\mathbb{C})$, basta notar que f é bijetora, então, considerando $g\colon \mathbb{C} \to \mathbb{C}$ definida por $g(x) = z^{-1}x$, e sendo $x \in \mathbb{C}$, vem que $(f \circ g)(x) = f(g(x)) = f(z^{-1}x) = zz^{-1}x = x$. Por outro lado, $(g \circ f)(x) = g(f(x)) = g(zx) = z^{-1}zx = x$. Desse modo, $\varphi(f) = f(1) = z \cdot 1 = z$. Portanto, φ é sobrejetora.
Conclui-se que $GL(\mathbb{C})$ é isomorfo a $\mathbb{C} \setminus \{0\}$.

□

Exemplo 4.1.5. *Considere o espaço vetorial $\mathbb{C}$. Então, $GL(V) = GL(\mathbb{C}) = \mathbb{C} \setminus \{0\}$. Sendo G um grupo, é possível definir a seguinte aplicação:*

$$\begin{aligned} \rho\colon G &\to \mathbb{C} \setminus \{0\} \\ g &\mapsto \rho(g) = 1 \end{aligned}$$

para todo $g \in G$.
Considere $g_1, g_2 \in G$, então $\rho(g_1g_2) = 1 = \rho(g_1)\rho(g_2)$. Decorre que ρ é uma representação de G.

Exemplo 4.1.6. *Considere o grupo simétrico S_n e defina a seguinte aplicação*

$$\rho\colon S_n \to GL(\mathbb{C}) \cong \mathbb{C} \setminus \{0\}$$

dada por

$$\rho(g) = \begin{cases} 1, & \text{se } g \text{ é par} \\ -1, & \text{se } g \text{ é ímpar} \end{cases}$$

para todo $g \in S_n$.
Sejam $g_1, g_2 \in S_n$, podem acontecer três casos:

(i) *g_1 e g_2 são pares, então g_1g_2 é par. Assim, $\rho(g_1g_2) = 1 = 1 \cdot 1 = \rho(g_1)\rho(g_2)$.*

(ii) *g_1 e g_2 são ímpares, então g_1g_2 é par. Assim, $\rho(g_1g_2) = 1 = (-1) \cdot (-1) = \rho(g_1)\rho(g_2)$.*

(iii) g_1 *é par e* g_2 *é ímpar, então* g_1g_2 *é ímpar. Assim,* $\rho(g_1g_2) = -1 = 1 \cdot (-1) = \rho(g_1)\rho(g_2)$.

Segue que ρ *é uma representação de* S_n *de grau 1, denominada* ***representação sinal*** *de* S_n.

Exemplo 4.1.7. *Sejam G um grupo e* $\mathbb{C}$ *um corpo. Considere* $V = \mathbb{C}(G)$ *o espaço vetorial cuja base é G. Defina a seguinte aplicação*

$$\rho : G \to GL(V)$$
$$g \mapsto \rho(g)$$

onde $\rho(g) : V \to V$ *é definida por* $\rho(g)(h) = gh$, *para todo* $h \in G$, *já que G é base de V.*
Agora, dados $g_1, g_2 \in G$, *vem que*

$$\rho(g_1g_2)(h) = (g_1g_2)h = g_1(g_2h) = g_1\rho(g_2)(h) = \rho(g_1)(\rho(g_2)(h)) = (\rho(g_1)\rho(g_2))(h).$$

Conclui-se que ρ *é um homomorfismo. Logo,* ρ *é uma representação de G em V denominada* ***representação regular*** *(à esquerda) de G.*
A representação matricial associada em relação à base G possui zeros na diagonal e em cada uma de suas linhas (colunas) aparece apenas um elemento diferente de zero que é igual a 1.

Para fixar melhor o exemplo anterior, será apresentado um caso particular do mesmo.

Exemplo 4.1.8. *Considere* $G = S_3$. *Foi visto, no exemplo 2.10.4, que* S_3 *é gerado por apenas dois elementos* $y = \sigma_1$ *e* $x = \sigma_3$. *Desse modo,* $S_3 = \{e, x, xy = y^{-1}x, yx = xy^{-1}, y, y^{-1}\}$.
Considerando ρ *a representação regular (à esquerda) de* S_3, *tem-se*

$$\rho : S_3 \to GL(V)$$

definida por $\rho(g)(h) = gh$, *para* $g, h \in S_3$, *já que V tem como base* S_3.

O objetivo é encontrar a representação matricial associada em relação a base S_3. *Como* S_3 *é gerado somente por x e y, basta encontrar as matrizes que se associam com esses elementos. Desse modo,*

$$\rho(x)(e) = xe = x = 0e + 1x + 0xy + 0yx + 0y + 0y^{-1}$$
$$\rho(x)(x) = xx = x^2 = e = 1e + 0x + 0xy + 0yx + 0y + 0y^{-1}$$
$$\rho(x)(xy) = xxy = x^2y = y = 0e + 0x + 0xy + 0yx + 1y + 0y^{-1}$$
$$\rho(x)(yx) = xyx = xxy^{-1} = x^2y^{-1} = y^{-1} = 0e + 0x + 0xy + 0yx + 0y + 1y^{-1}$$
$$\rho(x)(y) = xy = 0e + 0x + 1xy + 0yx + 0y + 0y^{-1}$$
$$\rho(x)(y^{-1}) = xy^{-1} = yx = 0e + 0x + 0xy + 1yx + 0y + 0y^{-1}$$

A matriz associada é

$$X = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

Fazendo o mesmo raciocínio para o elemento y, segue que

$$\begin{aligned}
&\rho(y)(e) = ye = y = 0e + 0x + 0xy + 0yx + 1y + 0y^{-1} \\
&\rho(y)(x) = yx = 0e + 0x + 0xy + 1yx + 0y + 0y^{-1} \\
&\rho(y)(xy) = yxy = yy^{-1}x = x = 0e + 1x + 0xy + 0yx + 0y + 0y^{-1} \\
&\rho(y)(yx) = yyx = y^2x = y^{-1}x = xy = 0e + 0x + 1xy + 0yx + 0y + 0y^{-1} \\
&\rho(y)(y) = yy = y^2 = y^{-1} = 0e + 0x + 0xy + 0yx + 0y + 1y^{-1} \\
&\rho(y)(y^{-1}) = yy^{-1} = e = 1e + 0x + 0xy + 0yx + 0y + 0y^{-1}
\end{aligned}$$

A matriz associada é

$$Y = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

Agora, caso seja necessário encontrar a matriz associada ao elemento xy, não é necessário calcular $\rho(xy)(h)$, em todo $h \in S_3$, basta multiplicar as matrizes X e Y. Assim,

$$XY = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Isso quer dizer que

$$\begin{aligned}
\rho(xy)(e) &= xy \\
\rho(xy)(x) &= y^{-1} \\
\rho(xy)(xy) &= e \\
\rho(xy)(yx) &= y \\
\rho(xy)(y) &= yx \\
\rho(xy)(y^{-1}) &= x
\end{aligned}$$

Calculando $\rho(xy)(h)$, em todo $h \in S_3$, chega-se no mesmo resultado.

A representação regular é um exemplo do que denomina-se representação fiel.

Definição 4.1.9. *Seja G um grupo. Uma representação ρ de G é dita **fiel** quando $Nu(\rho) = \{e\}$, sendo e o elemento neutro de G.*

No caso dessa definição, o grupo G é isomorfo a um subgrupo de $GL(V)$. Sabendo que $Nu(\rho) \lhd G$, tem-se que se G é um grupo simples (grupo que admite como subgrupos normais somente os triviais), então toda representação não trivial é fiel.

Agora, segue um exemplo de representação não fiel.

Exemplo 4.1.10. *Sejam $G = \langle a \rangle$ um grupo cíclico, de ordem 6, gerado por a e $V = GL_1(\mathbb{C}) = \mathbb{C} \setminus \{0\}$. Defina a aplicação*

$$\begin{aligned}
\rho : G &\to GL_1(\mathbb{C}) \\
a &\mapsto \rho(a)
\end{aligned}$$

para todo $a \in G$, onde $\rho(a^k) = e^{\frac{2\pi ik}{3}}$.
Note que ρ está bem definida, pois $\rho(a^6) = e^{4\pi i} = \cos(4\pi) + i\sin(4\pi) = 1$. Também, ρ é uma representação, já que

$$\rho(a^k a^l) = \rho(a^{k+l}) = e^{\frac{2\pi i(k+l)}{3}} = e^{\frac{2\pi ik + 2\pi il}{3}} = e^{\frac{2\pi ik}{3}} e^{\frac{2\pi il}{3}} = \rho(a^k)\rho(a^l),$$

para todo $a^k, a^l \in G$.
Porém, $\rho(a^3) = e^{2\pi i} = \cos(2\pi) + i\sin(2\pi) = 1$.
Logo, $Nu(\rho) = \{a^6 = 1, a^3\} \neq \{1\}$.

Exemplo 4.1.11. *Sejam $G = \langle a \rangle$ um grupo cíclico, de ordem 2, gerado por a, e $V = \mathbb{C}^2$ um*

espaço vetorial sobre o corpo $\mathbb{C}$. Considere a representação regular de G em V dada por

$$\rho : G \to GL(\mathbb{C}^2)$$

tal que $\rho(g)(h) = gh$, para todo $g \in G$ e $h \in V$.

Como ρ é a representação regular, então G é uma base para V. Desse modo, para encontrar a representação matricial associada a G, basta fazer os cálculos nos elementos da base, para todo $g \in G$.

$$\rho(e)(e) = ee = e = 1e + 0a$$
$$\rho(e)(a) = ea = a = 0e + 1a$$

A matriz associada é

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Analogamente, para o elemento $a \in G$.

$$\rho(a)(e) = ae = a = 0e + 1a$$
$$\rho(a)(a) = aa = e = 1e + 0a$$

A matriz associada é

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Desse modo, a representação matricial será dada por

$$\rho : G \to GL_2(\mathbb{C})$$
$$g \mapsto \rho(g)$$

para todo $g \in G$, tal que $\rho(e) = I$ e $\rho(a) = A$.

Exemplo 4.1.12. *Sejam V um espaço vetorial sobre o corpo $\mathbb{C}$, tal que $dim(V) = n$ e $\beta = \{v_1, \ldots, v_n\}$ uma base para V. Considere G um subgrupo de S_n. Defina a aplicação*

$$\rho : G \to GL(V)$$

tal que $\rho(g)(v_i) = v_{g(i)}$, para todo $g \in G$ e $v_i \in \beta$, sendo $i \in \{1, \ldots, n\}$.

Sejam $g_1, g_2 \in G$, vem

$$\rho(g_1g_2)(v_i) = v_{(g_1g_2)(i)} = v_{(g_1(g_2(i)))} = \rho(g_1)(v_{g_2(i)}) = \rho(g_1)\rho(g_2)(v_i).$$

Daí, tem-se que ρ é um homomorfismo.
Logo, ρ é uma representação de G em V denominada ***representação permutação*** *de G.*

Para ilustrar o exemplo anterior, segue:

Exemplo 4.1.13. *Considere $\beta = \{v_1, v_2, v_3\}$ uma base para V. Defina a seguinte aplicação:*

$$\rho : S_3 \to GL(V)$$

tal que $\rho(g)(v_i) = v_{g(i)}$, para $g \in S_3$ e $v_i \in \beta$, com $i = 1,2,3$. Pelo exemplo 2.10.4, tem-se que S_3 é gerado por

$$x = \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad e \quad y = \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix},$$

então basta calcular $\rho(g)$ em g igual a x e y.
Desse modo,

$$\begin{aligned} \rho(x)(v_1) &= v_{x(1)} = v_1 = 1v_1 + 0v_2 + 0v_3 \\ \rho(x)(v_2) &= v_{x(2)} = v_3 = 0v_1 + 0v_2 + 1v_3 \\ \rho(x)(v_3) &= v_{x(3)} = v_2 = 0v_1 + 1v_2 + 0v_3 \end{aligned}$$

A matriz associada é

$$X = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

Analogamente, para y, obtém-se

$$\begin{aligned} \rho(y)(v_1) &= v_{y(1)} = v_2 = 0v_1 + 1v_2 + 0v_3 \\ \rho(y)(v_2) &= v_{y(2)} = v_3 = 0v_1 + 0v_2 + 1v_3 \\ \rho(y)(v_3) &= v_{y(3)} = v_1 = 1v_1 + 0v_2 + 0v_3 \end{aligned}$$

A matriz associada é

$$Y = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

Para calcular a matriz associada ao elemento xy, basta fazer:

$$XY = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

Isso significa que

$$\rho(xy)(v_1) = v_3$$
$$\rho(xy)(v_2) = v_2$$
$$\rho(xy)(v_3) = v_1$$

Calculando $\rho(xy)(v_i)$ em todo $v_i \in \beta$, chega-se no mesmo resultado.

Exemplo 4.1.14. *Seja $G = \langle a \rangle$ um grupo cíclico, de ordem n, gerado por a, isto é, $a^n = e$. Considere $w = e^{\frac{2\pi i}{n}} = cos(\frac{2\pi}{n}) + i\ \ sen(\frac{2\pi}{n})$. Definindo a aplicação*

$$\rho : G \to GL(\mathbb{C}) \cong \mathbb{C} \setminus \{0\}$$

tal que $\rho(a^i) = w^i$, para todo $a^i \in G$, sendo $i \in \{1, \ldots, n\}$.
Dados $a^i, a^j \in G$ tal que $i, j \in \{1, \ldots, n\}$ tem-se que

$$\rho(a^i a^j) = \rho(a^{i+j}) = w^{i+j} = w^i w^j = \rho(a^i)\rho(a^j)$$

. Logo, ρ é uma representação de G.

Exemplo 4.1.15. *Seja $G = D_4$ o grupo diedral de ordem 8. Foi visto no exemplo 2.1.12 que D_4 é gerado por $y = R_{\frac{\pi}{2}}$ e $x = M_1$. Podemos escrever $D_4 = \langle x, y : x^2 = e, y^4 = e, x^{-1}yx = y^{-1} \rangle$. Para definir uma representação de G, basta defini-la nos geradores. Então, seja ρ a representação de G definida como*

$$\rho : G \to GL_2(\mathbb{C})$$

tal que

$$\rho(x) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad e \quad \rho(y) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Outros exemplos serão apresentados ao decorrer desse trabalho. Por enquanto, perceba que nos exemplos em que foi construída a matriz associada à representação de G, sendo G um grupo, foi necessário considerar uma base para o espaço vetorial V. Então, uma pergunta que surge é: caso sejam consideradas duas bases para o espaço vetorial V, o que acontece com as representações matriciais de G nessas bases? Para discutir essa questão, serão necessários alguns conceitos prévios. Em seguida, será apresentada uma proposição que esclarece essa dúvida.

4.2 HOMOMORFISMO DE REPRESENTAÇÕES

Conhecendo as representações de grupos, é interessante definir uma função entre elas, do mesmo modo que existem funções entre grupos - homomorfismos, e funções entre espaços vetoriais - transformações lineares. Essa função é denominada homomorfismo (seguindo a notação de Pena (2014)), e a partir dela será possível encontrar o núcleo, a imagem, a aplicação inversa (caso exista), entre outros objetos associados à mesma.

Definição 4.2.1. *Sejam V e W espaços vetoriais sobre o corpo $\mathbb{C}$ e seja G um grupo. Considere ρ_V e ρ_W representações de G em V e W, respectivamente, dadas por*

$$\rho_V : G \to GL(V)$$
$$\rho_W : G \to GL(W).$$

Diz-se que a transformação linear $f : V \to W$ é um ***homomorfismo*** *entre ρ_V e ρ_W (**ou aplicação G-linear**) quando*

$$f \circ \rho_V(g) = \rho_W \circ f(g),$$

para todo $g \in G$, ou seja, tal que o diagrama

$$\begin{array}{ccc} V & \xrightarrow{\rho_V(g)} & V \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle f} \\ W & \xrightarrow[\rho_W(g)]{} & W \end{array}$$

comuta.

A definição de homomorfismo de representações, de certa forma, é análoga à definição de transformação linear, pois se f é uma transformação linear tal que $f\colon V \to W$, sendo V e W espaços vetoriais sobre o corpo $\mathbb{C}$, tem-se que

$$f(\alpha v) = \alpha f(v),$$

para todo $\alpha \in \mathbb{C}$ e $v \in V$, ou seja, é possível colocar os escalares "para fora" da transformação.

Agora, se f é um homomorfismo de representações tal que $f\colon V \to W$, sendo V e W espaços vetoriais sobre o corpo $\mathbb{C}$, então

$$f(\rho_V(g)(x)) = \rho_W(g)(f(x)),$$

para todo $g \in G$, e para todo $x \in V$, ou seja, a representação de G em V "sai" como a representação de G em W.

Sendo f um homomorfismo de representações, e supondo que f é um isomorfismo de espaços vetoriais V e W, ou seja, $f\colon V \to W$ é uma transformação linear bijetora, então existe uma transformação linear bijetora $f^{-1}\colon W \to V$, tal que $f \circ f^{-1} = Id_W$ e $f^{-1} \circ f = Id_V$.

A partir dessas observações, surge a seguinte questão: f^{-1} é um homomorfismo de representações? A resposta é sim e decorre diretamente do fato de que f é um homomorfismo.

Agora é possível definir isomorfismo de representações.

Definição 4.2.2. *Sejam V e W espaços vetoriais sobre o corpo $\mathbb{C}$ e seja G um grupo. Considere $\rho_V\colon G \to GL(V)$ e $\rho_W\colon G \to GL(W)$ representações de G em V e W, respectivamente. Diz-se que a transformação linear $f\colon V \to W$ é um **isomorfismo** entre ρ_V e ρ_W quando f é um homomorfismo das representações ρ_V e ρ_W e, f é um isomorfismo de V em W.*

Observação 4.2.3. *Quando existe um isomorfismo entre as representações ρ_V e ρ_W, diz-se que ρ_V é isomorfa a ρ_W.*

Exemplo 4.2.4. *Seja $G = \langle a \rangle$ um grupo cíclico, de ordem 2, gerado por a e considere a representação regular de G em $\mathbb{C}^2$:*

$$\rho_1\colon G \to GL_2(\mathbb{C})$$

tal que

$$\rho_1(e) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \ e \ \rho_1(a) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Considere a representação de G em $\mathbb{C}$*:*

$$\rho_2 \colon G \to GL_1(\mathbb{C}) = \mathbb{C} \setminus \{0\}$$

tal que

$$\rho_2(e) = 1 \;\; e \;\; \rho_2(a) = -1.$$

Seja a transformação linear $f \colon \mathbb{C}^2 \to \mathbb{C}$*, representada pela matriz* $(1 \;\; -1)$ *em relação às bases canônicas. Afirma-se que* f *é um homomorfismo entre* ρ_1 *e* ρ_2*. De fato, seja* $\begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{C}^2$*, então*

$$\begin{aligned} f\rho_1(a) \begin{pmatrix} x \\ y \end{pmatrix} &= \begin{pmatrix} 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \\ &= \begin{pmatrix} -1 & 1 \end{pmatrix} \begin{pmatrix} y \\ x \end{pmatrix} \\ &= (-1) \begin{pmatrix} 1 & -1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \\ &= \rho_2(a) f \begin{pmatrix} x \\ y \end{pmatrix} \end{aligned}$$

e

$$\begin{aligned} f\rho_1(e) \begin{pmatrix} x \\ y \end{pmatrix} &= \begin{pmatrix} 1 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \\ &= \begin{pmatrix} 1 & -1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \\ &= \rho_2(e) f \begin{pmatrix} x \\ y \end{pmatrix}. \end{aligned}$$

Definido o homomorfismo entre representações, retorna-se à dúvida que surgiu ao final da seção anterior: quando são consideradas diferentes bases de um espaço vetorial para a representação matricial de um grupo G, o que acontece?

Observação 4.2.5. *Primeiramente, considere P uma matriz invertível. A aplicação*

$$p^C \colon GL_n(\mathbb{C}) \to GL_n(\mathbb{C})$$

dada por

$$p^C(M) = P^{-1}MP,$$

para todo $M \in GL_n(\mathbb{C})$*, é um homomorfismo. De fato, se* $M,N \in GL_n(\mathbb{C})$*, então*

$$p^C(MN) = P^{-1}MNP = P^{-1}MPP^{-1}NP = p^C(M)p^C(N).$$

Considerando ρ *uma representação de G, vem que* $p^C \circ \rho$ *é um homomorfismo, já que a composição de homomorfismos é um homomorfismo.*

Decorre a seguinte definição.

Definição 4.2.6. *Sejam G um grupo e* ρ_1*,* ρ_2 *duas representações matriciais de G tais que*

$$\rho_1 \colon G \to GL_n(\mathbb{C})$$
$$\rho_2 \colon G \to GL_n(\mathbb{C}).$$

Diz-se que ρ_1 *e* ρ_2 *são* ***equivalentes*** *quando existe* $P \in GL_n(\mathbb{C})$ *tal que*

$$\rho_2 = p^C \circ \rho_1.$$

Tendo a definição de equivalência entre representações de um grupo G, afirma-se que duas representações matriciais de G definidas em bases diferentes de V são equivalentes.

Proposição 4.2.7. *Sejam G um grupo e V um espaço vetorial sobre o corpo* $\mathbb{C}$ *com* $dim(V) = n$*, tal que* $\alpha = \{u_1, \ldots, u_n\}$ *e* $\beta = \{v_1, \ldots, v_n\}$ *são bases de V. Se*

$$\rho^\alpha \colon G \to GL_n(\mathbb{C})$$
$$\rho^\beta \colon G \to GL_n(\mathbb{C})$$

são as representações matriciais associadas de G, então ρ^α *e* ρ^β *são equivalentes.*

Demonstração:
Para cada $g \in G$, existe uma transformação linear $\rho(g) \in GL(V)$. Escrevendo essa transformação com respeito a base α, obtém-se a matriz $\rho^\alpha(g)$. Analogamente, escrevendo essa transformação com respeito a base β, obtém-se a matriz $\rho^\beta(g)$. Considerando P a matriz de mudança de bases de α para β, segue que

$$\rho^\beta(g) = P^{-1}\rho^\alpha(g)P$$

para todo $g \in G$.
Utilizando a aplicação p^C definida na observação 4.2.5, tem-se

$$\rho^{\beta}(g) = P^{-1}\rho^{\alpha}(g)P = p^C(\rho^{\alpha}(g)) = p^C \circ \rho^{\alpha}(g).$$

Pela definição de representações equivalentes, segue que ρ^{α} e ρ^{β} são equivalentes.

□

A proposição a seguir mostra que os isomorfismos de representações são análogos a equivalência de matrizes.

Proposição 4.2.8. *Seja G um grupo e sejam V e W espaços vetoriais sobre o corpo* $\mathbb{C}$ *tais que* $dim(V) = dim(W) = n$. *Considere* $\rho_V : G \to GL(V)$ *e* $\rho_W : G \to GL(W)$ *representações de G em V e W, respectivamente. Sendo* $\beta_V = \{v_1, \ldots, v_n\}$ *uma base de V e* $\beta_W = \{w_1, \ldots, w_n\}$ *uma base de W, vem que*

$$\rho_V^{\beta_V} : G \to GL_n(C)$$
$$\rho_W^{\beta_W} : G \to GL_n(C)$$

são duas representações matriciais associadas a G, na base β_V *e na base* β_W. *Tem-se que* ρ_V *e* ρ_W *são isomorfas se, e somente se,* $\rho_V^{\beta_V}$ *e* $\rho_W^{\beta_W}$ *são equivalentes.*

Demonstração:
Para demonstração, ver Segal (2014).

□

4.3 SUB-REPRESENTAÇÕES

É sempre interessante definir estruturas menores que possuam propriedades semelhantes as de estruturas maiores com as quais se relacionam.

Sejam V um espaço vetorial sobre o corpo $\mathbb{C}$, W um subespaço vetorial de V e considere $\rho : G \to GL(V)$ uma representação de G em V. Suponha que $\rho(g)(W) \subseteq W$, para todo $g \in G$. Considere a aplicação $\rho(g)|_W : W \to W$.

Como essa restrição é um isomorfismo de W, então defini-se

$$\rho|_W : G \to GL(W)$$
$$g \mapsto \rho|_W(g)$$

para todo $g \in G$.

Definição 4.3.1. *Sejam V um espaço vetorial sobre o corpo $\mathbb{C}$ e W um subespaço vetorial de V. Considere G um grupo e ρ uma representação de G em V, tal que $\rho : G \to GL(V)$. Diz-se que W é uma* ***sub-representação*** *de V quando*

$$\rho(g)(x) \in W,$$

para todo $g \in G$ e para todo $x \in W$.

Exemplo 4.3.2. *Sejam $G = \langle a \rangle$ um grupo cíclico, de ordem 2, gerado por a, $V = \mathbb{C}^2$ um espaço vetorial sobre o corpo $\mathbb{C}$ e W_1 um subespaço vetorial de V, cuja base é $\{(1,1)\}$. Considere a representação regular de G em V*

$$\begin{aligned} \rho : G &\to GL_2(\mathbb{C}) \\ g &\mapsto \rho(g) \end{aligned}$$

para $g \in G$, tal que $\rho(e) = I$ e $\rho(a) = A$, sendo

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ e } A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Como $\{(1,1)\}$ é base de W_1, então W_1 é gerado pelo vetor $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$. Segue que,

$$\rho(e)\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix} \in W_1$$

$$\rho(a)\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix} \in W_1.$$

Logo, W_1 é sub-representação de V.

Na Álgebra Linear tem-se que o núcleo de uma transformação linear é subespaço vetorial do seu domínio e a imagem é subespaço vetorial do seu contradomínio. Isto acontece analogamente com os homomorfismos de representações e sub-representações.

Proposição 4.3.3. *Sejam V e W espaços vetoriais sobre o corpo $\mathbb{C}$ e seja G um grupo. Considere $\rho_V : G \to GL(V)$ e $\rho_W : G \to GL(W)$ representações de G em V e W, respectivamente. Se $f : V \to W$ é um homomorfismo entre ρ_V e ρ_W, então $Nu(f)$ é uma sub-representação de V e $Im(f)$ é uma sub-representação de W.*

Demonstração:
Sendo f um homomorfismo de V em W, tem-se que f é uma transformação linear. Desse modo, $Nu(f)$ é subespaço vetorial de V e $Im(f)$ é subespaço vetorial de W. Basta mostrar que se $g \in G$, então $\rho_V(g)(x) \in Nu(f)$, para todo $x \in Nu(f)$ e $\rho_W(g)(y) \in Im(f)$, para todo $y \in Im(f)$.
Considere $g \in G$ e $x \in Nu(f)$, então $f(x) = 0$. Pelo fato de f ser homomorfismo de V e W e $\rho_W(g)$ ser transformação linear,

$$f(\rho_V(g)(x)) = \rho_W(g)(f(x)) = \rho_W(g)(0) = 0$$

Segue que $\rho_V(g)(x) \in Nu(f)$.
Analogamente, sejam $g \in G$ e $y \in Im(f)$, então existe $v \in V$ tal que $f(v) = y$. Pelo fato de f ser homomorfismo de V e W,

$$f(\rho_V(g)(v)) = \rho_W(g)(f(v)) = \rho_W(g)(y)$$

Note que $f(\rho_V(g)(v)) \in Im(f)$. Logo, $\rho_W(g)(y) \in Im(f)$.

□

4.4 REPRESENTAÇÕES INDUZIDAS

Nesta seção é dado continuidade à apresentação de mais alguns exemplos de representações.

Exemplo 4.4.1. *Seja V um espaço vetorial sobre o corpo $\mathbb{C}$ tal que $dim(V) = n$ e considere V^* o espaço dual $V^* = L(V, \mathbb{C})$. Dada uma base $\{v_1, \ldots, v_n\}$ de V, tem-se que $\{T_1, \ldots, T_n\}$ é uma base de V^*, onde*

$$T_i(v_j) = \begin{cases} 1, & se \;\; i = j \\ 0, & se \;\; i \neq j \end{cases}$$

Seja $\rho\colon G \to GL(V)$ uma representação de G, defina a aplicação

$$\rho^*\colon G \to GL(V^*)$$
$$g \mapsto \rho^*(g)$$

para todo $g \in G$. Sendo

$$\rho^*(g)\colon V^* \to V^*$$
$$T \mapsto \rho^*(g)(T) = T\rho(g^{-1})$$

para todo $T \in V^*$.
Pelo fato de ρ ser uma representação de G, afirma-se que ρ^* também o é. Com efeito, sejam $g_1, g_2 \in G$ e $T \in V^*$,

$$\begin{aligned}\rho^*(g_1g_2)(T) &= T\rho((g_1g_2)^{-1}) \\ &= T\rho(g_2^{-1})\rho(g_1^{-1}) \\ &= \rho^*(g_1)(T\rho(g_2^{-1})) \\ &= \rho^*(g_1)\rho^*(g_2)(T)\end{aligned}$$

A representação ρ^* é denominada ***representação dual*** *de G.*

Para ilustrar uma representação dual, segue o exemplo abaixo.

Exemplo 4.4.2. *Seja V um espaço vetorial sobre o corpo $\mathbb{C}$ tal que $dim(V) = 3$ e $\{v_1, v_2, v_3\}$ base de V. Considere $\rho : S_3 \to GL(V)$ a representação do grupo S_3 definida por*

$$\rho(g)(v_i) = v_{g(i)},$$

para $i \in \{1,2,3\}$.
Para $y \in G$, sendo $y = \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, tem-se $y^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$. Calculando $\rho(y^{-1})$ nos elementos da base de V:

$$\begin{aligned}\rho(y^{-1})(v_1) &= v_{y^{-1}(1)} = v_3 = 0v_1 + 0v_2 + 1v_3 \\ \rho(y^{-1})(v_2) &= v_{y^{-1}(2)} = v_1 = 1v_1 + 0v_2 + 0v_3 \\ \rho(y^{-1})(v_3) &= v_{y^{-1}(3)} = v_2 = 0v_1 + 1v_2 + 0v_3\end{aligned}$$

A matriz associada é

$$Y = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

A representação dual de S_3 é

$$\rho^* : S_3 \to GL(V^*)$$

definida por $\rho^*(g)(T)(v) = T\rho(g^{-1})(v)$, para todo $g \in S_3$, $T \in V^*$ e $v \in V$.
O objetivo é encontrar a representação matricial. Como $\{v_1, v_2, v_3\}$ é base de V, então $\{T_1, T_2, T_3\}$

é base de V^*, sendo

$$T_i(v_j) = \begin{cases} 1, & se \;\; i = j \\ 0, & se \;\; i \neq j \end{cases}$$

para $i, j \in \{1,2,3\}$. Basta fazer os cálculos para os elementos da base. Assim,

$$\rho^*(y)(T_1)(v_1) = T_1\rho(y^{-1})(v_1) = T_1v_3 = 0$$
$$\rho^*(y)(T_1)(v_2) = T_1\rho(y^{-1})(v_2) = T_1v_1 = 1$$
$$\rho^*(y)(T_1)(v_3) = T_1\rho(y^{-1})(v_3) = T_1v_2 = 0$$

$$\rho^*(y)(T_1) = T_2 = 0T_1 + 1T_2 + 0T_3$$

$$\rho^*(y)(T_2)(v_1) = T_2\rho(y^{-1})(v_1) = T_2v_3 = 0$$
$$\rho^*(y)(T_2)(v_2) = T_2\rho(y^{-1})(v_2) = T_2v_1 = 0$$
$$\rho^*(y)(T_2)(v_3) = T_2\rho(y^{-1})(v_3) = T_2v_2 = 1$$

$$\rho^*(y)(T_2) = T_3 = 0T_1 + 0T_2 + 1T_3$$

$$\rho^*(y)(T_3)(v_1) = T_3\rho(y^{-1})(v_1) = T_3v_3 = 1$$
$$\rho^*(y)(T_3)(v_2) = T_3\rho(y^{-1})(v_2) = T_3v_1 = 0$$
$$\rho^*(y)(T_3)(v_3) = T_3\rho(y^{-1})(v_3) = T_3v_2 = 0$$

$$\rho^*(y)(T_3) = T_1 = 1T_1 + 0T_2 + 0T_3$$

A matriz associada a $\rho^*(y)$ é

$$Y^* = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

Note que $Y^* = Y^t$.

Antes de prosseguir com os exemplos, serão retomados conceitos sobre soma direta,

pois será necessário saber se podem ser obtidas representações de um grupo G a partir da soma direta de duas ou mais representações de G.

Definição 4.4.3. *Seja V um espaço vetorial sobre o corpo $\mathbb{C}$ e considere W_1 e W_2 dois subespaços vetoriais de V. Diz-se que V é a* ***soma direta*** *de W_1 e W_2, e denota-se por $W_1 \oplus W_2$, quando para todo $v \in V$, existem únicos $w_1 \in W_1$ e $w_2 \in W_2$ tais que $v = w_1 + w_2$.*

Proposição 4.4.4. *Seja V um espaço vetorial sobre o corpo $\mathbb{C}$ e considere W_1 e W_2 dois subespaços vetoriais de V. V é soma direta de W_1 e W_2 se, e somente se, $V = W_1 + W_2$ e $W_1 \cap W_2 = \{0\}$.*

Outra proposição importante é a que faz afirmações a respeito da dimensão e da base para a soma direta. Ela será útil na construção da representação matricial associada a um grupo G.

Proposição 4.4.5. *Seja V um espaço vetorial sobre o corpo $\mathbb{C}$ e considere W_1 e W_2 dois subespaços vetoriais de V. Se $dim(W_1) = n$ e $dim(W_2) = m$, $\beta_1 = \{w_1^1, \ldots, w_1^n\}$ e $\beta_2 = \{w_2^1, \ldots, w_2^m\}$ são bases para W_1 e W_2, respectivamente, então $dim(V) = dim(W_1) + dim(W_2) = n + m$ e $\beta = \{w_1^1, \ldots, w_1^n, w_2^1, \ldots, w_2^m\}$ é uma base para V.*

Voltando aos exemplos, o raciocínio a seguir apresenta que é possível obter representações de um grupo G a partir da soma direta de duas ou mais representações.

Exemplo 4.4.6. *Sejam V um espaço vetorial sobre o corpo $\mathbb{C}$ e considere W_1 e W_2 dois subespaços vetoriais de V, tais que $dim(W_1) = n$ e $dim(W_2) = m$. Sejam*

$$\rho_1 \colon G \to GL(W_1)$$
$$\rho_2 \colon G \to GL(W_2)$$

duas representações de G em W_1 e W_2, respectivamente.
Defina a seguinte aplicação

$$\rho_1 \oplus \rho_2 \colon G \to GL(W_1 \oplus W_2)$$
$$g \mapsto (\rho_1 \oplus \rho_2)(g)$$

para todo $g \in G$, tal que

$$(\rho_1 \oplus \rho_2)(g) \colon W_1 \oplus W_2 \to W_1 \oplus W_2$$
$$w_1 + w_2 \mapsto (\rho_1 \oplus \rho_2)(g)(w_1 + w_2) = \rho_1(g)(w_1) + \rho_2(g)(w_2)$$

para todo $w_1 \in W_1$ e $w_2 \in W_2$.
A aplicação $(\rho_1 \oplus \rho_2)(g) \in GL(W_1 \oplus W_2)$, para todo $g \in G$, ou seja, é uma transformação linear invertível.
Tem-se que $\rho_1 \oplus \rho_2$ é uma representação. De fato, sejam $g_1, g_2 \in G$, então

$$\begin{aligned}(\rho_1 \oplus \rho_2)(g_1g_2)(w_1+w_2) &= \rho_1(g_1g_2)(w_1) + \rho_2(g_1g_2)(w_2)\\ &= \rho_1(g_1)(\rho_1(g_2)(w_1)) + \rho_2(g_1)(\rho_2(g_2)(w_2))\\ &= (\rho_1 \oplus \rho_2)(g_1)(\rho_1(g_2)(w_1) + \rho_2(g_2)(w_2))\\ &= (\rho_1 \oplus \rho_2)(g_1)((\rho_1 \oplus \rho_2)(g_2)(w_1+w_2))\\ &= ((\rho_1 \oplus \rho_2)(g_1)(\rho_1 \oplus \rho_2)(g_2))(w_1+w_2)\end{aligned}$$

para todo $w_1 \in W_1$ e para todo $w_2 \in W_2$.
Para encontrar a representação matricial associada a G, considere $\beta_1 = \{w_1^1, \ldots, w_1^n\}$ e $\beta_2 = \{w_2^1, \ldots, w_2^m\}$ bases para W_1 e W_2. Tem-se que

$$\begin{aligned}\rho_1 &: G \to GL_n(\mathbb{C})\\ \rho_2 &: G \to GL_m(\mathbb{C})\end{aligned}$$

para todo $g \in G$, são representações matriciais de G em W_1 e W_2, respectivamente. Pelos resultados da proposição 4.4.5, segue que

$$\begin{aligned}\rho_1 \oplus \rho_2 &: G \to GL_{n+m}(\mathbb{C})\\ g &\mapsto (\rho_1 \oplus \rho_2)(g)\end{aligned}$$

para todo $g \in G$, é a representação matricial de G em $W_1 \oplus W_2$, dada por

$$(\rho_1 \oplus \rho_2)(g) = \begin{pmatrix} \rho_1(g) & 0 \\ 0 & \rho_2(g) \end{pmatrix}_{(m+n)\times(m+n)}$$

para $\rho_1 \in GL_n(\mathbb{C})$ e $\rho_2 \in GL_m(\mathbb{C})$.

Exemplo 4.4.7. *Seja V um espaço vetorial sobre o corpo $\mathbb{C}$ e considere G um grupo. Sendo $\rho : G \to GL(V)$ uma representação de G e W um subespaço vetorial de V, tal que $\rho(g)(w) \in W$, para todo $w \in W$ e $g \in G$, defina a seguinte aplicação*

$$\begin{aligned}\rho_W &: G \to GL(V/W)\\ g &\mapsto \rho_W(g)\end{aligned}$$

para todo $g \in G$, com

$$\begin{aligned} \rho_W(g)\colon V/W &\to V/W \\ v+W &\mapsto \rho_W(g)(v+W) = \rho(g)(v)+W \end{aligned}$$

para todo $v \in V$.
Como essa aplicação envolve espaços quocientes é necessário verificar se ela está bem definida. Suponha $\overline{v_1}, \overline{v_2} \in V/W$, tal que $\overline{v_1} = \overline{v_2}$, então $v_1 - v_2 \in W$. Assim,

$$\begin{aligned} \rho_W(g)(v_1+W) &= \rho(g)(v_1)+W \\ &= \rho(g)(v_2+(v_1-v_2))+W \\ &= \rho(g)(v_2)+\rho(g)(v_1-v_2))+W \\ &= \rho(g)(v_2)+W \\ &= \rho_W(g)(v_2+W) \end{aligned}$$

Segue que ρ_W está bem definida.
Como ρ é uma representação de G, tem-se que ρ_W também o é. De fato, sejam $g_1, g_2 \in G$ e $v+W \in V/W$, então

$$\begin{aligned} \rho_W(g_1g_2)(v+W) &= \rho(g_1g_2)(v)+W \\ &= \rho(g_1)(\rho(g_2)(v))+W \\ &= \rho_W(g_1)(\rho(g_2)(v)+W) \\ &= \rho_W(g_1)\rho_W(g_2)(v+W) \end{aligned}$$

Essa representação ρ_W é denominada ***representação quociente*** *de G.*

Considere o seguinte exemplo:

Exemplo 4.4.8. *Sejam $G = \langle a \rangle$ um grupo cíclico, de ordem 2, gerado por a, $V = \mathbb{C}^2$ um espaço vetorial sobre o corpo $\mathbb{C}$ e W_1 um subespaço vetorial de V. E considere $\rho\colon G \to GL_2(\mathbb{C})$ a representação do exemplo 4.3.2. Foi demonstrado que W_1 é uma sub-representação de V quando W_1 é gerado pelo vetor $\begin{pmatrix} 1 \\ 1 \end{pmatrix} \in V$. Dessa forma, o objetivo é tentar encontrar um subespaço vetorial W_2 de V de forma que $V = W_1 \oplus W_2$.*

Considere que W_2 é o espaço gerado por $\begin{pmatrix} 1 \\ -1 \end{pmatrix} \in V$. *Desse modo,*

$$\rho(e)\begin{pmatrix} 1 \\ -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 \\ -1 \end{pmatrix} = \begin{pmatrix} 1 \\ -1 \end{pmatrix} \in W_2$$

e

$$\rho(a)\begin{pmatrix} 1 \\ -1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ -1 \end{pmatrix} = \begin{pmatrix} -1 \\ 1 \end{pmatrix} = -\begin{pmatrix} 1 \\ -1 \end{pmatrix} \in W_2.$$

Então, W_2 é uma sub-representação de V.
Agora, é necessário verificar se $V = W_1 \oplus W_2$. Note que, $W_1 \cap W_2 = \emptyset$. Com efeito, suponha que existe $(x,y) \in W_1 \cap W_2$ diferente do nulo, então $(x,y) = (w,w)$ e $(x,y) = (w,-w)$, essa situação só é válida para $w = 0$. Além disso, segue diretamente que $dim(V) = 2 = 1+1 = dim(W_1) + dim(W_2)$.

Definição 4.4.9. *Sejam V um espaço vetorial sobre o corpo $\mathbb{C}$ e W_1 uma sub-representação de V. Diz-se que W_2, uma outra sub-representação V, é uma* ***sub-representação complementar*** *de W_1 quando $V = W_1 \oplus W_2$.*

Exemplo 4.4.10. *Sendo V uma representação de G e W uma sub-representação de V, tem-se que W nem sempre admite uma sub-representação complementar, considere, por exemplo a representação $\rho\colon GL_1(\mathbb{R}) \to GL_2(\mathbb{R})$, definida por*

$$\rho(g) = \begin{pmatrix} 1 & \log|g| \\ 0 & 1 \end{pmatrix},$$

para $g \in GL_1(\mathbb{R})$.

Observação 4.4.11. *Sabe-se que se um subespaço W de um espaço vetorial V tem um subespaço complementar (isto é, um subespaço $\tilde{W}$ tal que $V = W \oplus \tilde{W}$), então $V/W \cong \tilde{W}$. Com efeito, seja $\pi\colon V \to V/W$ a projeção canônica e considere $\pi|_{\tilde{W}}\colon \tilde{W} \to V/W$. É claro que $\pi|_{\tilde{W}}$ é um isomorfismo. No contexto de representações, se W admite um complemento $\tilde{W}$ (nem sempre admite, como pode ser visto no exemplo 4.4.10) que também satisfaz $\rho(g)\tilde{w} \in \tilde{W}$ quando $\tilde{w} \in \tilde{W}$, com $g \in G$, então a representação quociente pode ser identificada com a representação de G em $\tilde{W}$, pois $\pi|_{\tilde{W}}$ é um isomorfismo que respeita a ação de G.*
Essa observação será importante nos exemplos de representações do grupo linear geral.

Exemplo 4.4.12. *Sejam ρ_i, para $i \in \{1,\ldots,n\}$, representações de G. Considere $\rho\colon G \to$*

$GL(V^{\otimes n})$ definida por

$$\begin{aligned}\rho(g)(v_1 \otimes \ldots \otimes v_n) &= (\rho_1(g) \otimes \ldots \otimes \rho_n(g))(v_1 \otimes \ldots \otimes v_n) \\ &= \rho_1(g)(v_1) \otimes \ldots \otimes \rho_n(g)(v_n)\end{aligned}$$

para $g \in G$ e $v_i \in V$, $i \in \{1, \ldots, n\}$.
Note que ρ é homomorfismo. De fato, sejam $g_1, g_2 \in G$, então

$$\begin{aligned}\rho(g_1g_2)(v_1 \otimes \ldots \otimes v_n) &= (\rho_1(g_1g_2) \otimes \ldots \otimes \rho_n(g_1g_2))(v_1 \otimes \ldots \otimes v_n) \\ &= \rho_1(g_1g_2)(v_1) \otimes \ldots \otimes \rho_n(g_1g_2)(v_n) \\ &= \rho_1(g_1)\rho_1(g_2)(v_1) \otimes \ldots \otimes \rho_n(g_1)\rho_n(g_2)(v_n) \\ &= (\rho_1(g_1) \otimes \ldots \otimes \rho_n(g_1))(\rho_1(g_2)(v_1) \otimes \ldots \otimes \rho_n(g_2)(v_n)) \\ &= \rho(g_1)\rho(g_2)(v_1 \otimes \ldots \otimes v_n)\end{aligned}$$

Essa representação ρ é denominada representação ***produto tensorial****.*

Para determinar a representação matricial $\rho : G \to GL(V \otimes V)$, considere o seguinte exemplo.

Se V é um espaço vetorial com $dim(V) = 2$ e tem base igual a $\beta_1 = \{e_1, e_2\}$, então $dim(V \otimes V) = 4$, cuja base é $\beta_2 = \{e_1 \otimes e_1, e_1 \otimes e_2, e_2 \otimes e_1, e_2 \otimes e_2\}$. Sejam

$$\rho_1^{\beta_1}(g) = \begin{pmatrix} a & b \\ c & d \end{pmatrix} = A \;\; e \;\; \rho_2^{\beta_1}(g) = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = B$$

Calculando $\rho(g)$ nos elementos da base β_2, vem

$$\begin{aligned}\rho(g)(e_1 \otimes e_1) &= \rho_1(g)(e_1) \otimes \rho_2(g)(e_1) \\ &= (ae_1 + ce_2) \otimes (a'e_1 + c'e_2) \\ &= (ae_1 + ce_2) \otimes a'e_1 + (ae_1 + ce_2) \otimes c'e_2 \\ &= ae_1 \otimes a'e_1 + ce_2 \otimes a'e_1 + ae_1 \otimes c'e_2 + ce_2 \otimes c'e_2 \\ &= aa'e_1 \otimes e_1 + ac'e_1 \otimes e_2 + ca'e_2 \otimes e_1 + cc'e_2 \otimes e_2\end{aligned}$$

$$\begin{aligned}\rho(g)(e_1 \otimes e_2) &= \rho_1(g)(e_1) \otimes \rho_2(g)(e_2) \\ &= (ae_1 + ce_2) \otimes (b'e_1 + d'e_2) \\ &= ab'e_1 \otimes e_1 + ad'e_1 \otimes e_2 + cb'e_2 \otimes e_1 + cd'e_2 \otimes e_2\end{aligned}$$

$$\begin{aligned}\rho(g)(e_2 \otimes e_1) &= \rho_1(g)(e_2) \otimes \rho_2(g)(e_1) \\ &= (be_1 + de_2) \otimes (a'e_1 + c'e_2) \\ &= ba'e_1 \otimes e_2 + bc'e_1 \otimes e_2 + da'e_2 \otimes e_1 + dc'e_2 \otimes e_2\end{aligned}$$

$$\begin{aligned}\rho(g)(e_2 \otimes e_2) &= \rho_1(g)(e_2) \otimes \rho_2(g)(e_2) \\ &= (be_1 + de_2) \otimes (b'e_1 + d'e_2) \\ &= bb'e_1 \otimes e_1 + bd'e_1 \otimes e_2 + db'e_2 \otimes e_1 + dd'e_2 \otimes e_2\end{aligned}$$

Desse modo, a representação matricial de g dá-se

$$\begin{pmatrix} aa' & ab' & ba' & bb' \\ ac' & ad' & bc' & bd' \\ ca' & cb' & da' & db' \\ cc' & cd' & dc' & dd' \end{pmatrix} = \begin{pmatrix} aB & bB \\ cB & dB \end{pmatrix}$$

4.4.1 REPRESENTAÇÕES DO GRUPO LINEAR GERAL

Exemplo 4.4.13. *Sejam $\mathbb{C}$ um corpo e ρ_I uma aplicação tal que*

$$\begin{aligned}\rho_I \colon GL_n(\mathbb{C}) &\to GL(\mathbb{C}^n) \\ A &\mapsto \rho_I(A) = T_A\end{aligned}$$

para todo $A \in GL_n(\mathbb{C})$, sendo T_A a seguinte aplicação

$$\begin{aligned}\rho_I(A) = T_A \colon \mathbb{C}^n &\to \mathbb{C}^n \\ v &\mapsto \rho_I(A)(v) = T_A(v) = Av\end{aligned}$$

para todo $v \in \mathbb{C}^n$.
Tem-se que ρ_I é uma representação de $GL_n(\mathbb{C})$ denominada ***representação identidade****.*

Exemplo 4.4.14. *Sejam $\mathbb{C}$ um corpo e ρ uma aplicação tal que*

$$\begin{aligned}\rho \colon GL_n(\mathbb{C}) &\to GL(\mathbb{C}) \\ A &\mapsto \rho(A) = T_A\end{aligned}$$

para todo $A \in GL_n(\mathbb{C})$, sendo T_A a seguinte aplicação

$$\begin{aligned}\rho(A) = T_A \colon \mathbb{C} &\to \mathbb{C} \\ r &\mapsto \rho(A)(r) = T_A(r) = (\det(A))r\end{aligned}$$

para todo $r \in \mathbb{C}$.
Tem-se que ρ é uma representação de $GL_n(\mathbb{C})$ denominada ***representação determinante****.*

Ilustrando esse exemplo, segue:

Exemplo 4.4.15. *Considere o corpo dos números complexos $\mathbb{C}$ e ρ uma aplicação tal que*

$$\begin{aligned}\rho \colon GL_n(\mathbb{C}) &\to GL_1(\mathbb{C}) \\ A &\mapsto \rho(A) = \det(A)\end{aligned}$$

para todo $A \in GL_n(\mathbb{C})$. Se $n = 2$, tem-se

$$\rho\left(\begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix}\right) = x_1x_4 - x_2x_3.$$

Tem-se que a composição de representações também é uma representação. Então, segue um exemplo para ilustrar esse fato.

Exemplo 4.4.16. *Sejam ρ a representação de $GL_n(\mathbb{C})$ do exemplo anterior e $\varphi \colon GL_1(\mathbb{C}) \to GL_2(\mathbb{C})$ definida por*

$$\varphi(z) = \begin{pmatrix} 1 & \log|z| \\ 0 & 1 \end{pmatrix},$$

para $z \in GL_1(\mathbb{C}) \cong \mathbb{C} \setminus \{0\}$. Tem-se que a aplicação $\varphi \circ \rho \colon GL_n(\mathbb{C}) \to GL_2(\mathbb{C})$ dada por

$$\varphi \circ \rho(A) = \varphi(\det(A)) = \begin{pmatrix} 1 & \log|\det(A)| \\ 0 & 1 \end{pmatrix}$$

é uma representação de $GL_n(\mathbb{C})$.

Exemplo 4.4.17. *Seja V um espaço vetorial sobre o corpo $\mathbb{C}$ tal que $dim(V) = 2$. Considere*

$$\begin{aligned}\rho \colon G &\to GL(V \otimes V) \\ A &\mapsto T_A \otimes T_A\end{aligned}$$

para todo $A \in G$, onde $G = GL_2(\mathbb{C})$ e T_A a representação identidade, se $\{e_1, e_2\}$ é uma base de V, então a base $V \otimes V$ é $\{e_1 \otimes e_1, e_1 \otimes e_2, e_2 \otimes e_1, e_2 \otimes e_2\}$. A seguir, será construída a

representação matricial de $\rho(A)$. Calculando ρ nos elementos da base.

$$\begin{aligned}\rho(A)(e_1\otimes e_1) =& T_A(e_1)\otimes T_A(e_1)\\ =&(x_1e_1+x_3e_2)\otimes(x_1e_1+x_3e_2)\\ =&x_1^2e_1\otimes e_1+x_1x_3e_1\otimes e_2+x_3x_1e_2\otimes e_1+x_3^2e_2\otimes e_2\end{aligned}$$

$$\begin{aligned}\rho(A)(e_1\otimes e_2) =& T_A(e_1)\otimes T_A(e_2)\\ =&(x_1e_1+x_3e_2)\otimes(x_2e_1+x_4e_2)\\ =&x_1x_2e_1\otimes e_1+x_1x_4e_1\otimes e_2+x_3x_2e_2\otimes e_1+x_3x_4e_2\otimes e_2\end{aligned}$$

Analogamente, segue que

$$\begin{aligned}\rho(A)(e_2\otimes e_1) =& T_A(e_2)\otimes T_A(e_1)\\ =&x_2x_1e_1\otimes e_1+x_2x_3e_1\otimes e_2+x_4x_1e_2\otimes e_1+x_3x_4e_2\otimes e_2\end{aligned}$$

$$\begin{aligned}\rho(A)(e_1\otimes e_2) =& T_A(e_2)\otimes T_A(e_2)\\ =&x_2^2e_1\otimes e_1+x_2x_4e_1\otimes e_2+x_4x_2e_2\otimes e_1+x_4^2e_2\otimes e_2\end{aligned}$$

Desse modo, a representação matricial de A é dada por

$$\begin{pmatrix} x_1^2 & x_1x_2 & x_2x_1 & x_2^2\\ x_1x_3 & x_1x_4 & x_2x_3 & x_2x_4\\ x_3x_1 & x_3x_2 & x_4x_1 & x_4x_2\\ x_3^2 & x_3x_4 & x_4x_3 & x_4^2\end{pmatrix}=\begin{pmatrix} x_1A & x_2A\\ x_3A & x_4A\end{pmatrix}$$

Exemplo 4.4.18. *Com os dados do exemplo anterior, será determinada a representação matricial da potência simétrica. Sabe-se que $\{e_1^2,e_1e_2,e_2^2\}$ é uma base para $S^2(V)$. Assim, calculando ρ nos elementos da base, segue que:*

$$\begin{aligned}\rho_S(A)(e_1^2) =& Ae_1Ae_1\\ =&(x_1e_1+x_3e_2)(x_1e_1+x_3e_2)\\ =&x_1^2e_1^2+2x_1x_3e_1e_2+x_3^2e_2^2\end{aligned}$$

$$\begin{aligned}\rho_S(A)(e_1e_2) =& Ae_1Ae_2\\ =&(x_1e_1+x_3e_2)(x_2e_1+x_4e_2)\\ =&x_1x_2e_1^2+(x_1x_4+x_3x_2)e_1e_2+x_3x_4e_2^2\end{aligned}$$

$$\begin{aligned}\rho_S(A)(e_2^2) =& Ae_2Ae_2\\ =&(x_2e_1+x_4e_2)(x_2e_1+x_4e_2)\\ =&x_2^2e_1^2+2x_2x_4e_1e_2+x_4^2e_2^2\end{aligned}$$

Desse modo, A pode ser escrito como

$$\begin{pmatrix} x_1^2 & x_1x_2 & x_2^2 \\ 2x_1x_3 & x_1x_4+x_3x_2 & 2x_2x_4 \\ x_3^2 & x_3x_4 & x_4^2 \end{pmatrix}$$

Exemplo 4.4.19. *Na situação do exemplo 4.4.17, sabendo que* $\{e_1 \wedge e_2\}$ *é uma base para* $\bigwedge^2(V)$*, será determinada a representação matricial da potência exterior. Aplicando a* ρ_E *no elemento da base, segue que:*

$$\begin{aligned}\rho_E(A)(e_1 \wedge e_2) =& Ae_1 \wedge Ae_2\\ =&(x_1e_1+x_3e_2)(x_2e_1+x_4e_2)\\ =&x_1x_4e_1 \wedge e_2 + x_3x_2e_2 \wedge e_1\\ =&(x_1x_4-x_3x_2)e_1 \wedge e_2\\ =&(\det(A))e_1 \wedge e_2\end{aligned}$$

que é a representação determinante.

Seja V espaço vetorial sobre o corpo $\mathbb{C}$, sendo $\{e_1, e_2\}$ uma base para V. No exemplo 4.4.17, foi utilizada a base $\{e_1 \otimes e_1, e_1 \otimes e_2, e_2 \otimes e_1, e_2 \otimes e_2\}$ de $V \otimes V$. Porém, será escrita outra base para $V \otimes V$, já que ela é melhor adaptada a esse estudo:

$$\beta = \{e_1 \otimes e_1, e_2 \otimes e_2, e_1 \otimes e_2 + e_2 \otimes e_1, e_1 \otimes e_2 - e_2 \otimes e_1\}$$

É claro que β é uma base de $V \otimes V$. Considerando $\mathscr{S}$ o subespaço gerado pelos primeiros três elementos da base β e $\mathscr{E}$ o subespaço gerado pelo último elemento, seguem os seguintes resultados:

Lema 4.4.20. $\mathscr{S}$ *é o espaço gerado pelos vetores da forma* $v \otimes v$*, sendo* $v \in V$*.*

Demonstração:
O objetivo é mostrar que $\mathscr{S} = \langle \{v \otimes v \colon v \in V\} \rangle$.

Seja $v \in V$, então $v = \alpha_1 e_1 + \alpha_2 e_2$, com $\alpha_1, \alpha_2 \in \mathbb{C}$. Assim,

$$\begin{aligned} v \otimes v &= (\alpha_1 e_1 + \alpha_2 e_2) \otimes (\alpha_1 e_1 + \alpha_2 e_2) \\ &= \alpha_1^2 e_1 \otimes e_1 + \alpha_2^2 e_2 \otimes e_2 + \alpha_1 \alpha_2 (e_1 \otimes e_2 + e_2 \otimes e_1) \in \mathscr{S} \end{aligned}$$

De onde, $\langle \{ v \otimes v \colon v \in V \} \rangle \subset \mathscr{S}$.
Agora, será provado que $\mathscr{S} \subset \langle \{ v \otimes v \colon v \in V \} \rangle$. É claro que $e_1 \otimes e_1, e_2 \otimes e_2 \in \langle \{ v \otimes v \colon v \in V \} \rangle$. Como

$$e_1 \otimes e_2 + e_2 \otimes e_1 = (e_1 + e_2) \otimes (e_1 + e_2) - e_1 \otimes e_1 - e_2 \otimes e_2,$$

então $e_1 \otimes e_2 + e_2 \otimes e_1 \in \mathscr{S}$.

□

Lema 4.4.21. *$\mathscr{E}$ é o espaço gerado pelos vetores da forma $v_1 \otimes v_2 - v_2 \otimes v_1$, sendo $v_1, v_2 \in V$.*

Demonstração:
Note que o elemento que gera $\mathscr{E}$ é dessa forma. Por outro lado, considere $v_1, v_2 \in V$, sendo $v_1 = \alpha_1 e_1 + \alpha_2 e_2$ e $v_2 = \alpha_3 e_1 + \alpha_4 e_2$. Assim,

$$\begin{aligned} v_1 \otimes v_2 &= (\alpha_1 e_1 + \alpha_2 e_2) \otimes (\alpha_3 e_1 + \alpha_4 e_2) \\ &= \alpha_1 \alpha_3 e_1 \otimes e_1 + \alpha_1 \alpha_4 e_1 \otimes e_2 + \alpha_2 \alpha_3 e_2 \otimes e_1 + \alpha_2 \alpha_4 e_2 \otimes e_2 \end{aligned}$$

$$\begin{aligned} v_2 \otimes v_1 &= (\alpha_3 e_1 + \alpha_4 e_2) \otimes (\alpha_1 e_1 + \alpha_2 e_2) \\ &= \alpha_3 \alpha_1 e_1 \otimes e_1 + \alpha_3 \alpha_2 e_1 \otimes e_2 + \alpha_4 \alpha_1 e_2 \otimes e_1 + \alpha_4 \alpha_2 e_2 \otimes e_2 \end{aligned}$$

Segue que

$$v_1 \otimes v_2 - v_2 \otimes v_1 = (\alpha_1 \alpha_4 - \alpha_3 \alpha_2)(e_1 \otimes e_2 - e_2 \otimes e_1) \in \mathscr{E}.$$

□

Desses lemas decorre o seguinte resultado.

Lema 4.4.22. *$\mathscr{S}$ e $\mathscr{E}$ são invariantes pela representação de $GL_2(\mathbb{C})$ induzida em $V \otimes V$.*

Observe que $V \otimes V = \mathscr{S} \oplus \mathscr{E}$ é a soma direta de dois subespaços invariantes pela representação de $GL_2(\mathbb{C})$ em $V \otimes V$. $\mathscr{S}$ é o espaço pelo qual quocientamos $V \otimes V$ para definir a representação potência exterior, $V \otimes V / \mathscr{S} \cong \bigwedge^2(V)$. $\mathscr{E}$ é o espaço pelo qual quocientamos $V \otimes V$ para obter a representação potência simétrica, $V \otimes V / \mathscr{E} \cong S^2(V)$. Pela observação 4.4.11, tem-se o seguinte teorema:

Teorema 4.4.23. *(i) A representação potência exterior é isomorfa a sub-representação $\mathscr{E}$ da representação de $V \otimes V$.*

(ii) A representação potência simétrica é isomorfa a sub-representação $\mathscr{S}$ da representação de $V \otimes V$.

Sendo que $V \otimes V = \mathscr{S} \oplus \mathscr{E}$, segue que

Teorema 4.4.24. *A representação de $GL_2(\mathbb{C})$ em $V \otimes V$ é isomorfa à soma direta $S^2(V) \oplus \bigwedge^2(V)$.*

É possível fazer construções similares para qualquer n se $\mathbb{C}$ é um corpo de característica zero, isto é, verifica-se que as representações simétrica $S^n(V)$ e exterior $\bigwedge^n(V)$ são (isomorfas a) sub-representações de $V^{\otimes n}$. Porém, não é sempre verdade que $V^{\otimes n} \cong S^n(V) \oplus \bigwedge^n(V)$, simplesmente contando dimensões. Por exemplo, se $n = 3$ e $dim(V) = 5$, então

$$dim(V \otimes V \otimes V) = 125$$
$$dim(S^3(V) + \wedge^3 V) = \begin{pmatrix} 7 \\ 4 \end{pmatrix} + \begin{pmatrix} 5 \\ 3 \end{pmatrix} = 45$$

Note que as dimensões são diferentes. Isto leva à teoria de Módulos de Weyl, a qual estuda as representações de $GL_n(\mathbb{C})$ usando relações combinatórias do mesmo gênero, porém mais complexas que o produto simétrico e exterior.

4.5 TEOREMA DE MASCHKE E LEMA DE SCHUR

Nesta seção, serão discutidos alguns fatos básicos da teoria de representações de grupos.

A partir do exemplo 4.4.8, surge o seguinte questionamento: sejam V um espaço vetorial sobre o corpo $\mathbb{C}$ e W_1 uma sub-representação de V, então sempre existe uma outra sub-representação W_2 de V, tal que $V = W_1 \oplus W_2$? A resposta é afirmativa e vale para um caso geral, sendo demonstrada pelo Teorema de Maschke (com as hipóteses de que G um grupo finito e a característica do corpo - nesse caso $\mathbb{C}$ - não divide a ordem do grupo G). O subespaço W_2 que garante a validade dessa afirmação é denominado sub-representação complementar de W_1.

Para demonstrar o Teorema de Maschke é necessário o seguinte lema.

Lema 4.5.1. *Seja V um espaço vetorial sobre o corpo $\mathbb{C}$, e considere W um subespaço vetorial de V. Se $f\colon V \to W$ é uma transformação linear tal que $f(x) = x$, para todo $x \in W$, então $Nu(f) \subset V$ é uma sub-representação complementar de W, ou seja, $V = W \oplus Nu(f)$.*

Demonstração:
O objetivo é mostrar que a interseção entre W e $Nu(f)$ é somente o zero, e que a soma de suas dimensões resulta na dimensão de V.
Seja $x \in W \cap Nu(f)$, então $x \in Nu(f)$. Segue que $f(x) = 0$. Como $x \in W$, $f(x) = x$. Daí, $x = 0$. Portanto, $W \cap Nu(f) = \{0\}$.
Note que W é um subespaço vetorial de V, isto quer dizer que $W \subset V$, então f é sobrejetiva. Pelo teorema do Núcleo e da Imagem, segue que $dim(V) = dim(Nu(f)) + dim(Im(f)) = dim(Nu(f)) + dim(W)$.

□

A transformação linear f definida nesse lema é denominada projeção. Assim, seja V um espaço vetorial sobre o copo $\mathbb{C}$ e considere W_1 um subespaço de V. Seja W_2 o subespaço de V que é sub-espaço complementar de W_1. A transformação linear

$$\begin{aligned} \pi_{W_1} : V = W_1 \oplus W_2 &\to W_1 \\ (w_1, w_2) &\mapsto w_1 \end{aligned}$$

é uma **projeção** e o $Nu(\pi_{W_1}) = W_2$.

Abaixo, é possível observar um corolário que segue diretamente do lema 4.5.1 e da definição de projeção.

Corolário 4.5.2. *Seja V um espaço vetorial sobre o corpo $\mathbb{C}$, e considere W um subespaço vetorial de V. Sejam G um grupo, $\rho : G \to GL(V)$ uma representação de G e W uma sub-representação de V. Se $\pi : V \to W$ é uma projeção tal que π é homomorfismo entre V e W, então $Nu(\pi)$ é a representação complementar de W.*

Teorema 4.5.3. *(Teorema de Maschke) Sejam G um grupo finito, V um espaço vetorial sobre o corpo $\mathbb{C}$, cuja característica não divide a ordem de G. Se $\rho : G \to GL(V)$ é uma representação de G e W_1 uma sub-representação de V. Então, existe uma sub-representação complementar W_2 de W_1.*

Demonstração:
A ideia da demonstração é encontrar uma projeção G-linear $f : V \to W_1$, e utilizar o corolário anterior, obtendo que $Nu(f) = W_2$, tal que $V = W_1 \oplus W_2$.
Por resultado da Álgebra Linear, existe W_2 um subespaço complementar de W_1 de modo que $V = W_1 \oplus W_2$. A partir disso, defina a projeção $\pi : V = W_1 \oplus W_2 \to W_1$, sendo $W_2 = Nu(\pi)$. Como

não há garantia de que π seja uma aplicação G-linear, então considere a aplicação $f\colon V \to V$, definida por

$$f(x) = \frac{1}{o(G)} \sum_{g \in G} (\rho(g)\pi\rho(g^{-1})(x),$$

para todo $x \in V$. Afirma-se que f é uma projeção G-linear de V em W_1. É necessário demonstrar que:

(i) $Im(f) \subset W_1$

(ii) f é projeção

(iii) f é G-linear

Desse modo,

(i) Sejam $x \in V$ e $g \in G$, segue que $\rho(g^{-1})(x) \in V$. Aplicando π, tem-se que $\pi(\rho(g^{-1})(x) \in W_1$. Como W_1 é uma sub-representação de V, $\rho(g)(\pi(\rho(g^{-1})(x))) \in W_1$. Logo, $Im(f) \subset W_1$, ou seja, $f\colon V \to W_1 \subset V$.

(ii) Sejam $w \in W_1$ e $g \in G$. Como W_1 é sub-representação de V, então $\rho(g)(w) \in W_1$. Pelo fato de π ser projeção de V em W_1, tem-se $\pi(\rho(g)(w)) = \rho(g)(w)$. Então,

$$\begin{aligned} f(w) &= \frac{1}{o(G)} \sum_{g \in G} (\rho(g)\pi\rho(g^{-1}))(w) \\ &= \frac{1}{o(G)} \sum_{g \in G} (\rho(g)\rho(g^{-1}))(w) \\ &= \frac{1}{o(G)} \sum_{g \in G} (\rho(gg^{-1}))(w) \\ &= \frac{1}{o(G)} \sum_{g \in G} \rho(e)(w) \\ &= \frac{1}{o(G)} \sum_{g \in G} w \\ &= \frac{o(G)}{o(G)} w \\ &= w \end{aligned}$$

Logo, f é uma projeção de V em W.

(iii) Sejam $x \in V$ e $h \in G$, então

$$\begin{aligned} f(\rho(h)(x)) &= \frac{1}{o(G)} \sum_{g \in G} (\rho(g)\pi\rho(g^{-1})\rho(h))(w) \\ &= \frac{1}{o(G)} \sum_{g \in G} (\rho(g)\pi\rho(g^{-1}h))(w) \\ &= \frac{1}{o(G)} \sum_{g \in G} (\rho(hg)\pi\rho(g^{-1}))(w) \\ &= \rho(h) \left(\frac{1}{o(G)} \sum_{g \in G} (\rho(g)\pi\rho(g^{-1}))(w) \right) \\ &= \rho(h) f(x) \end{aligned}$$

Portanto, f é G-linear.

□

Observe que a representação φ dada no exemplo 4.4.16 não contradiz o teorema de Maschke, pois o grupo $GL_1(\mathbb{C})$ é infinito.

Pelo teorema de Maschke, se V contém uma sub-representação W_1, então é possível decompor V em uma soma direta de sub-representações. Caso V não possua sub-representações diferentes das triviais, define-se a representação irredutível.

Definição 4.5.4. *Seja V um espaço vetorial sobre o corpo $\mathbb{C}$ e considere G um grupo. Diz-se que $\rho : G \to GL(V)$ é uma **representação irredutível** de G quando V não possui sub-representações, a não ser as triviais ($\{0\}$ e V).*

Qualquer representação de dimensão 1 é irredutível.

Segue um corolário muito interessante do Teorema de Maschke.

Corolário 4.5.5. *Seja V um espaço vetorial sobre o corpo $\mathbb{C}$ e considere G um grupo. Se $\rho : G \to GL(V)$ é uma representação de G, então V pode ser escrito como uma soma direta de representações irredutíveis.*

Demonstração:
Seja V a representação de G tal que $dim(V) = n$. Se V é irredutível, está demonstrado o resultado. Se V não é irredutível, então V contém uma sub-representação W_1 diferente das triviais. Pelo Teorema de Maschke, existe uma sub-representação complementar W_2 de W_1, tal que $V = W_1 \oplus W_2$ e $dim(W_1), dim(W_2) < n$. Se W_1 de W_2 são irredutíveis, está demonstrado o

corolário. Caso contrário, irão existir sub-representações nos quais esses espaços podem ser decompostos. Como V tem dimensão finita, esse processo se repetirá finitamente até atingir o resultado.

□

Esse corolário afirma que toda representação pode ser construída por uma soma direta de sub-representações irredutíveis. Esse fato é semelhante à decomposição de um número natural em fatores primos. Desse modo, as representações irredutíveis, com um pensamento análogo, podem ser consideradas os números primos da teoria de representações.

Finalmente, será discutido o lema de Schur e dada uma aplicação do mesmo.

Teorema 4.5.6. *(Lema de Schur) Sejam V e W espaços vetoriais sobre o corpo $\mathbb{C}$ e considere G um grupo. Dadas $\rho_V : G \to GL(V)$ e $\rho_W : G \to GL(W)$ são representações irredutíveis de G, segue:*

(i) Se $f : V \to W$ é um homomorfismo de V e W, então ou f é um isomorfismo ou f é a aplicação nula.

(ii) Se $f : V \to V$ é um homomorfismo de V em V, onde V é um espaço vetorial sobre $\mathbb{C}$, então $f = \lambda I_V$, para $\lambda \in \mathbb{C}$.

Demonstração:

(i) Se f é a aplicação nula, está demonstrado o resultado. Suponha que f não é a aplicação nula. Sabe-se que $Nu(f) \subset V$, mas V é uma representação irredutível, então $Nu(f) = \{0\}$ ou $Nu(f) = V$. Como f não é a aplicação nula, existe $x \in V$ tal que $f(x) \neq 0$, logo, $Nu(f) = \{0\}$. Segue que f é injetora.
Por outro lado, $Im(f) \subset W$, mas W é uma representação irredutível, então $Im(f) = \{0\}$ ou $Im(f) = W$. Como f não é a aplicação nula, existe $x \in V$ tal que $f(x) \neq 0$, logo, $Im(f) = W$. Conclui-se que f é sobrejetora.
Portanto, f é bijetora. Decorre daí o isomorfismo.

(ii) Sendo $f : V \to V$ um homomorfismo de V em V, então f é uma transformação linear, então f possui pelo menos um autovalor $\lambda \in \mathbb{C}$. Defina a aplicação $f' = f - \lambda I_V$ tal que

$$f' : V \to V$$

Note que f' é um homomorfismo de V em V, pois

$$\begin{aligned} f'(\rho_V(g)(x)) &= f(\rho_V(g)(x)) - \lambda\rho_V(g)(x) \\ &= \rho_V(g)(f(x)) - \rho_V(g)(\lambda x) \\ &= \rho_V(g)(f(x) - \lambda x) \\ &= \rho_V(g)(f'(x)) \end{aligned}$$

para todo $g \in G$ e $x \in V$. Sendo λ um autovalor de f, vem que $Nu(f')$ tem pelo menos dimensão 1. Por (i), f' é a aplicação nula, ou seja, $f - \lambda I_V = 0$. Portanto, $f = \lambda I_V$.

□

A partir do Lema de Schur é possível caracterizar todas as representações irredutíveis de um grupo abeliano.

Proposição 4.5.7. *Seja V espaço vetorial sobre o corpo $\mathbb{C}$ e considere G um grupo abeliano. Se $\rho : G \to GL(V)$ é uma representação irredutível de G, então possui dimensão 1.*

Demonstração:
Considere $h \in G$. Então, $\rho(h) : V \to V$ é uma transformação linear. E mais, $\rho(h)$ é um homomorfismo de V e V. Com efeito,

$$\begin{aligned} \rho(h)(\rho(g)(x)) &= \rho(hg)(x) \\ &= \rho(gh)(x) \\ &= \rho(g)(\rho(h)(x)) \end{aligned}$$

para todo $g \in G$ e $x \in V$. Pelo Lema de Schur, $\rho(h) = \lambda_h I_V$, sendo $\lambda_h \in \mathbb{C}$. Para qualquer $h \in G$ tem-se que $\rho(h)(x) = \lambda_h x \in \langle x \rangle$. Sendo V uma representação irredutível e $\langle x \rangle$ sub-representação de V, conclui-se que $V = \langle x \rangle$, isto é, V tem dimensão 1.

□

5 CONCLUSÃO

Na Matemática, é interessante perceber como diversas teorias se relacionam. No caso desse trabalho, foi possível constatar interligações entre a Teoria de Grupos, Álgebra Multilinear e Teoria de Representações de Grupos.

Estabelecer analogias entre definições e resultados encontrados na Álgebra Multilinear e na Teoria de Representações, tornaram o desenvolvimento desse estudo mais prazeroso.

Desse modo, a assimilação de conceitos como produto tensorial, potência simétrica e potência exterior ficaram mais compreensíveis com a observação de suas representações. Bem como, o entendimento de homomorfismo de representações tornou-se mais simples quando associado à definição de transformação linear. A construção de diversos exemplos, com riqueza de detalhes também auxiliou na apreensão dos temas em estudo.

Além disso, esse trabalho proporcionou uma experiência significativa no desenvolvimento da habilidade de estudo e pesquisa científica.

REFERÊNCIAS

BASES of symmetric and exterior powers. Disponível em: http://math.stanford.edu/ conrad/diffgeomPage/handouts/symmwedgebasis.pdf. Acesso em: 20 ago. 2015, p. 1–5, s.d.

BUCHBAUM, G. C. R. A new construction in homological algebra. p. 4115–4119, 1994.

DOMINGUES, H. H.; IEZZI, G. **Álgebra Moderna**. 4. ed. São Paulo: Atual, 2003.

EGG, G. E. M. Contando as simetrias rotacionais dos poliedros regulares. p. 31–51, 2013.

FULTON, H.; HARRIS, J. **Representation Theory: A first course**. 1. ed. New York: Springer-Verlag, 1991.

GARCIA, A.; LEQUAIN, Y. **Elementos de álgebra**. 1. ed. Rio de Janeiro: Sociedade Brasileira de Matemática, 2003.

GREUB, W. H. **Multilinear Algebra**. 1. ed. New York: Springer-Verlag, 1967.

HEFEZ, A. **Elementos de aritmética**. 2. ed. Rio de Janeiro: SBM, 2011.

HUNGERFORD, T. W. **Algebra**. 1. ed. New York: Springer-Verlag, 1974.

PENA, F. X. Introdução ás representações de grupos finitos. Disponível em: http://www.sbm.org.br/docs/coloquios/SU3-09.pdf. Acesso em: 20 ago. 2015, p. 11–21, 2014.

SANO, M. A combinatorial description of the syzygies of certain weul modules. v. 31, p. 5115–5167, 2003.

SANO, M. Homotopies for the generalized bar complex associated to certain 3-rowed weyl modules. v. 34, p. 3056–3075, 2006.

SEGAL, E. Group representation theory. Disponível em: http://wwwf.imperial.ac.uk/ epsegal/repthy/GroupAcesso em: 15 out. 2015, p. 2–51, 2014.

TENSOR Algebras, Symmetric Algebras and Exterior Algebras. Disponível em: http://www.cis.upenn.edu/ cis610/diffgeom7.pdf. Acesso em: 30 mar. 2015, p. 585–619, s.d.

WUSSING, H. **The Genesis of the Abstract Group Concept: A Contribution to the History of the Origin of Abstract Group Theory**. New York: Dover Publications, 2007.