Universidade Federal de Campina Grande
Centro de Ciências e Tecnologia
Unidade Acadêmica de Matemática
Curso de Graduação em Matemática

Representações de Grupos Finitos e Graduações em Álgebras

por

Eduardo Pinto da Fonsêca [†]

sob orientação do

Prof. Dr. Diogo Diniz Pereira da Silva e Silva

Trabalho apresentado ao Curso de Graduação de Matemática da Universidade Federal de Campina Grande como requisito para a obtenção do título de Bacharel em matemática.

[†]Este trabalho contou com apoio financeiro do CNpq.

Representações de Grupos Finitos e Graduações em Álgebras

por

Eduardo Pinto da Fonsêca

Trabalho de conclusão de curso defendido e aprovado, em 21 de agosto de 2020, pela Comissão Examinadora constituída pelos professores:

Prof. Dr. Antônio Pereira Brandão Júnior
Examinador

Prof. Dr. Thyago Santos de Souza
Examinador

Prof. Dr. Diogo Diniz Pereira da Silva e Silva
Orientador

com nota igual a 8,0.

Agosto/2020

Agradecimentos

Agradeço a todos os amigos que fiz no departamento e fora dele. Em particular aos amigos que fiz quando buscava companhia na sala do PET-Matemática, são alguns deles: *Amanda de Araújo Queiroz, Bruna Alves da Silva Santos, Fábio Lima de Oliveira, Gabriel Pereira de Figueiredo, Isabella Tito de Oliveira Silva, Jonas Barros Lima de Medeiros, Leticia Dornellas Dias, Luis Filipe Ramos Campos da Silva, Matheus da Silva Nascimento, Otacília Meira de Freitas Neta, Pedro Henrique Alves Guedes e Rodrigo Marques Faustino da Silva* .
Também aos amigos do mestrado, como *Geisa Gama Oliveira*, *Ismael Sandro da Silva*, *etc.*

Esses amigos serviram como uma verdadeira família durante o período de minha graduação, me ajudando e me apoiando nos momentos que eu mais precisei, quando perdi familiares, quando perdia a confiança e o desespero batia, quando precisava ir na biblioteca, etc. Sem eles definitivamente eu não seria competente para chegar até aqui.

Claramente devo também muito a amigos mais antigos que me ajudaram, principalmente quando me mudei para uma nova cidade e não sabia e não conhecia absolutamente nada, o apoio e a amizade deles me fizeram suportar a solidão, tais como *Anderson, André Macedo, Eloíse Diniz, Marcos Vagner, Samara Cristina, Ranelson Santos, etc.*

Agradeço também a todos os professores, em particular a *Antônio Brandão*, que me ensinou muita Álgebra; *Diogo Diniz*, que me orientou e ficou mandando eu fazer as coisas; ao jovem professor *Marco Aurélio*, que é uma figuraça e me ensinou muitas coisas bacanas de Análise; entre outros professores.

Por fim, à minha família que acreditou em mim.

Dedicatória

A todos que confiaram em mim.

Resumo

Uma representação linear de um grupo G (finito) em um espaço vetorial V (de dimensão finita) sobre o corpo dos números complexos, é um homomorfismo de grupos ρ onde o domínio é o grupo G e o contradomínio é o grupo de automorfismos de V. Tais homomorfismos nos permitem estudar propriedades de G, uma vez que a teoria dos operadores lineares é rica em resultados. Isto pode ser visto, por exemplo, na utilização da Teoria de Representações de Grupos (finitos) para demonstrar o Teorema $p^a q^b$ de Burnside.

Para cada representação ρ definimos uma aplicação χ que associa ao elemento s do grupo o traço $\chi(s)$ da transformação ρ_s obtida quando avaliamos o elemento $s \in G$ pela representação ρ. Tal aplicação é chamada de *caracter* da representação, que, a princípio, parece não nos fornecer muita informação sobre a representação, mas a determina de forma única, a menos de isomorfismo.

Neste trabalho apresentamos um estudo sobre representações lineares de grupos finitos tendo como foco seu caracter. Nosso objetivo é mostrar a equivalência entre uma ação de G e uma G-graduação em uma álgebra associativa A, no caso em que G é um grupo abeliano finito, utilizando a representação de grupos como ferramenta.

Abstract

A linear representation of a group G in a finite dimensional vector space V, over the field of the complex numbers, is a group homomorphism ρ where the group G is the domain, and the group of automorphisms of V is the codomain. These homomorphisms allow us to study properties of the group G since the theory of linear operators is rich in results. This is seen, for example, in the proof of Burnside's p^aq^b-Theorem using the Theory of Representations of (finite) Groups.

For each representation ρ we define a function χ that associates to the element s of the group G the trace $\chi(s)$ of the linear transformation ρ_s that is obtained when we evaluate the element s of G by representation ρ. This function is called character of the representation. At first it does not seem to provide a lot of information about the representation, however it determines the representation uniquely up to isomorphism.

In this work we prove the basic results about linear representations of (finite) groups, focusing on its character. Our goal is to prove the duality between the action of G by automorphisms and a G-grading on an associative algebra A, when G is a finite abelian group, using results on representations of groups as a tool.

Conteúdo

Introdução

Uma representação linear de um grupo finito em um espaço vetorial equivale a uma ação do grupo no espaço vetorial. A teoria de representações lineares de grupos finitos e dos caracteres das representações teve inicio em 1986, com G. Frobenius, tal estudo tem grande aplicabilidade na PI-teoria, que é a subárea da *Teoria de Aneis* que estuda as PI-álgebras, principalmente quando se trata de identidades graduadas. Este trabalho está dividido em 3 capítulos. No primeiro capítulo apresentamos o conceito de grupos, juntamente com exemplos. Fixamos notações, expomos definições e resultados básicos sobre a teoria de grupos, como por exemplo: subgrupos, Teorema de Lagrange, grupos cíclicos, homomorfismos, ações e produto direto de grupos.

No capítulo 2 definimos e desenvolvemos a teoria de representações lineares de grupos finitos, e dos caracteres relacionados a essas representações. Ainda no capítulo 2 mostramos o importante resultado chamado Lema de Schur, e seus corolários, tais como a equivalência: representações são isomorfas se, e somente se, têm o mesmo caracter.

No capítulo 3 apresentamos os conceitos de álgebra de grupo, álgebras, graduações de álgebras por um grupo, ações de um grupo em uma álgebra e grupo dual. Terminando com o resultado principal, que consiste em mostrar a equivalência entre a ação de um grupo G em uma álgebra A e uma G-graduação de A, no caso em que G é um grupo abeliano finito.

Capítulo 1

Noções preliminares

Neste trabalho é presumido que o leitor tenha conhecimento das definições iniciais de *Álgebra Linear* tais como: combinação linear, vetores L.I. e L.D., base, dimensão, subespaço, transformações lineares e matrizes, *etc.* Embora tais conhecimentos, possivelmente, sejam sobre espaços vetoriais sobre o corpo dos números reais, os conceitos aqui trabalhados são os mesmos sobre o corpo dos números complexos (ou sobre qualquer outro corpo), que será o corpo base que usaremos. De toda forma, ainda assim, serão apresentadas definições e resultados sobre espaços vetoriais e transformações lineares que serão usados. Abordaremos neste capítulo inicial noções básicas sobre a *Teoria de Grupos* que serão necessárias no decorrer dos próximos capítulos do trabalho. Para um leitor que deseja um aprofundamento no assunto de Teoria de Grupos indicamos as referências [1], [3] e [4].

1.1 Grupos e subgrupos

Começamos com as definições de grupos e subgrupos e com os resultados básicos. Apresentaremos também exemplos para ilustrar tais conceitos que serão utilizados adiante.

1.1.1 Grupos

Definição 1.1 *Sendo G um conjunto não vazio e "$*$" uma operação binária em G, dizemos que o par $(G, *)$ é um grupo se:*

i) $*$ *é associativa, ou seja:* $(a * b) * c = a * (b * c)$, $\forall a, b, c \in G$,

ii) $*$ *tem elemento neutro, ou seja:* $\exists e \in G$; $x * e = e * x = x, \forall x \in G$,

iii) todo elemento de G *é inversível com respeito a* $*$, *ou seja:* $\forall x \in G, \exists y \in G$; $x * y = y * x = e$.

Observação 1.1 *Sejam e_1 e e_2 elementos neutros de $(G, *)$, pela definição temos $e_1 = e_1 * e_2 = e_2$, logo o elemento neutro de $(G, *)$ é único, e o denotaremos por "e". Para cada x em G, o inverso de x é único, de fato, tomemos x' e $x"$ em G tais que $x * x' = x' * x = e$ e $x * x" = x" * x = e$. Temos então:*

$$x * x" = e \Rightarrow x' * (x * x") = x' * e \Rightarrow (x' * x) * x" = x' \Rightarrow e * x" = x' \Rightarrow x" = x'.$$

Assim denotaremos por x^{-1} o (único) inverso de x. Além do mais, para $n \in \mathbb{Z}$ definimos:

$$x^n = \begin{cases} \underbrace{x * x * \cdots * x}_{n \text{ vezes}}, \text{ se } n > 0 \\ e, \text{ se } n = 0 \\ (x^{-1})^{-n}, \text{se } n < 0. \end{cases}$$

Por simplicidade denotaremos $(G, *)$ apenas por "G", onde a operação fica subentendida quando não houver risco de confusão, e $ab := a * b$. Em alguns casos usamos notação aditiva $a + b := a * b$ quando a operação $*$ for comutativa; além do mais, quando a operação $*$ for comutativa, diremos que G é um grupo **abeliano**. Definimos a ordem do grupo G como sendo a ordem do conjunto G (quantidade de elementos do conjunto G), denotamos a ordem do grupo G por $| G |$.

Proposição 1.2 *Seja G um grupo com elemento neutro "e". Para quaisquer m e n inteiros e $a, a_1, a_2, \ldots, a_k \in G$ temos:*

i) $(a^{-1})^{-1} = a$

ii) $(a_1 a_2 \cdots a_{k-1} a_k)^{-1} = a_k^{-1} a_{k-1}^{-1} \cdots a_2^{-1} a_1^{-1}$

iii) $(a^n)^{-1} = (a^{-1})^n = a^{-n}$

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

v) $(a^m)^n = a^{mn}$.

Prova.

i) O elemento $y = (a^{-1})^{-1} \in G$ é, por definição, o elemento que satisfaz

$$ya^{-1} = a^{-1}y = e$$

daí

$$ya^{-1} = e \Rightarrow (ya^{-1})a = ea \Rightarrow y(a^{-1}a) = a \Rightarrow y = a.$$

ii) Provemos por indução em k. Para $k = 2$, fazendo uma verificação direta temos:

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

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

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

Supondo verdade para algum $k \geq 2$, temos por hipótese:

$$(a_1 a_2 \cdots a_{k-1} a_k)^{-1} = a_k^{-1} a_{k-1}^{-1} \cdots a_2^{-1} a_1^{-1}$$

Daí, tendo em vista que a sentença é verdadeira para dois elementos temos:

$$\begin{aligned}(a_1 a_2 \cdots a_{k-1} a_k a_{k+1})^{-1} &= ((a_1 a_2 \cdots a_{k-1} a_k)a_{k+1})^{-1} \\ &= a_{k+1}^{-1}(a_1 a_2 \cdots a_{k-1} a_k)^{-1} \\ &= a_{k+1}^{-1}(a_k^{-1} a_{k-1}^{-1} \cdots a_2^{-1} a_1^{-1}) \\ &= a_{k+1}^{-1} a_k^{-1} a_{k-1}^{-1} \cdots a_2^{-1} a_1^{-1}.\end{aligned}$$

Validando assim a sentença para $k + 1$ e completando a indução.

iii) Para $n = 0$ o resultado é imediato: $(a^0)^{-1} = e^{-1} = e = (a^{-1})^0 = a^{-0}$.

Para $n > 0$ temos:

$$(a^n)^{-1} = (\underbrace{aa\cdots a}_{n \text{ vezes}})^{-1} \overset{ii)}{=} (a^{-1}\cdots a^{-1}a^{-1}) := (a^{-1})^n.$$

Como $n > 0$, então $-n < 0$ e daí

$$a^{-n} := (a^{-1})^{-(-n)} = (a^{-1})^n$$

logo $(a^n)^{-1} = (a^{-1})^n = a^{-n}$ para $n > 0$.

Para $n < 0$, temos $-n > 0$ e daí, como visto acima, temos $(b^{-n})^{-1} = b^{-(-n)}$ para qualquer $b \in G$. Lembrando que $a^n := (a^{-1})^{-n}$ temos:

$$(a^n)^{-1} = ((a^{-1})^{-n})^{-1} = (a^{-1})^{-(-n)} = (a^{-1})^n.$$

Por fim $(a^{-1})^n := \underbrace{(a^{-1})^{-1}(a^{-1})^{-1}\cdots(a^{-1})^{-1}}_{-n \text{ vezes}} \overset{i)}{=} aa\cdots a := a^{-n}$.

iv) Inicialmente vamos mostrar que $a^{1+m} = aa^m$ para todo inteiro m. Se $m \geq 0$ segue da definição que $aa^m = a^{1+m}$. Caso $m < 0$ então

$$aa^m = a(a^{-1})^{-m} = a(a^{-1})^{-m-1+1} = a(a^{-1}(a^{-1})^{-m-1}) = (aa^{-1})(a^{-1})^{(-m-1)} = a^{1+m}.$$

Ou seja, $aa^m = a^{1+m}$ para todo $m \in \mathbb{Z}$.

Faremos agora indução em n para provar o item no caso $n \geq 0$. Para $n = 0$ temos $a^{0+m} = a^m$ e $a^0a^m = ea^m = a^m$.

Suponha que para algum natural $k \geq 0$ valha $a^{k+m} = a^ka^m$ para todo $m \in \mathbb{Z}$. Então:

$$a^{(k+1)+m} = a^{k+(1+m)} = a^ka^{1+m} = a^kaa^m = a^{k+1}a^m.$$

Portanto $a^{n+m} = a^na^m$ sempre que $n \geq 0$.

Caso $n < 0$, então $-n > 0$ e daí

$$a^{n+m} = (a^{-1})^{-n-m} = (a^{-1})^{-n}(a^{-1})^{-m} = a^na^m.$$

v) Vamos mostrar por indução em n que para qualquer inteiro m a igualdade vale sempre que $n \geq 0$. Para $n = 0, 1$ é imediato. Supondo que para algum natural $k \geq 1$ temos $(a^m)^k = a^{mk}$ para todo $m \in \mathbb{Z}$, então

$$(a^m)^{k+1} \overset{iv)}{=} (a^m)^k(a^m)^1 = a^{mk}a^m = a^{mk+m} = a^{m(k+1)}$$

donde segue que $(a^m)^n = a^{mn}$ sempre que $n \geq 0$.

Caso $n < 0$, então $-n > 0$ e daí

$$(a^m)^n := ((a^m)^{-1})^{-n} \overset{iii)}{=} (a^{-m})^{-n} = a^{(-m)(-n)} = a^{mn}.$$

■

Observação 1.2 *As igualdades da proposição anterior em notação aditiva são escritas do seguinte modo:*

i) $-(-a) = a$

ii) $-(a + b) = (-b) + (-a)$

iii) $-(na) = n(-a) = (-n)a$

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

v) $n(ma) = (nm)a$.

Para a familiarização com a estrutura de um grupo, segue uma lista de exemplos. À medida que o trabalho for se desenvolvendo novos exemplos serão apresentados.

Exemplo 1 *São exemplos de grupo:*

i) $(\mathbb{Z}, +)$: *o conjunto dos números inteiros com a soma usual de inteiros forma um grupo abeliano onde o elemento neutro é o zero. Chamamos esse grupo de grupo aditivo dos inteiros.*

Note que $\mathbb{Z}$ *com a multiplicação usual não forma um grupo, pois o elemento* 2*, em particular, não é inversível, visto que o elemento neutro é o* 1 *e não existe um elemento* $m \in \mathbb{Z}$ *tal que* $m \cdot 2 = 1$*. Portanto* $(\mathbb{Z}, \cdot)$ ***não*** *é um grupo.*

Munindo $\mathbb{Z}$ *com a operação* $a * b = a + b + 1$*, temos:*

$$(a * b) * c = (a + b + 1) * c = a + b + 1 + c + 1 = a + b + c + 2$$

$$a * (b * c) = a * (b + c + 1) = a + b + c + 1 + 1 = a + b + c + 2$$

para quaisquer $a, b, c \in \mathbb{Z}$*, ou seja,* $*$ *é associativa. Ademais* $a*(-1) = (-1)*a = a$*, logo* -1 *é elemento neutro e* $a*(-a-2) = -1$*, como* $*$ *é comutativa* $a' = -a-2$ *é o inverso de* a *em* $(\mathbb{Z}, *)$*. Concluímos que* $(\mathbb{Z}, *)$ *é um grupo (abeliano) com elemento neutro* -1*.*

Esse exemplo ilustra a importância da operação. Sobre um mesmo conjunto podemos formar mais de um grupo.

ii) $(\mathbb{C}^*, \cdot)$ *: o conjunto dos números complexos não nulos com a multiplicação usual de números complexos forma um grupo abeliano com o 1 como elemento neutro.*

iii) $(C_n, \cdot)$ *: Fixado um inteiro positivo* n*, esse grupo consiste dos números complexos que satisfazem a equação* $z^n = 1$*, munido da multiplicação usual de números complexos. Note que* $1 \in C_n \neq \emptyset$*. Ademais dados* $a, b \in C_n$*, então* $a^n = 1 = b^n$*, daí* $(ab)^n = a^n b^n = 1 \cdot 1 = 1$*. Logo* $ab \in C_n$*, concluindo que a multiplicação é uma operação binária em* C_n*, claramente associativa e de elemento neutro* 1*. Ademais se* $a \in C_n$*, então o número complexo* a^{-1} *satisfaz* $(a^{-1})^n = \frac{1}{a^n} = \frac{1}{1} = 1$*, logo* $a^{-1} \in C_n$*, donde segue que* $\frac{1}{a}$ *é o inverso de* a *em* C_n *e portanto* C_n *é de fato um grupo.*

Para obtermos um melhor entendimento do conjunto C_n *veja que o polinômio* $p(x) = x^n - 1$ *tem no máximo* n *raízes distintas em* $\mathbb{C}$*, donde segue que* $| C_n | \leq n$*. Ademais tomando o número* $\omega = e^{\frac{2\pi i}{n}} = \cos(\frac{2\pi}{n}) + i sen(\frac{2\pi}{n})$*, onde* $i^2 = -1$*, temos:*

$$\omega^k = (e^{\frac{2\pi}{n} i})^k = e^{\frac{2k\pi}{n} i} = \cos(\frac{2k\pi}{n}) + i \cdot sen(\frac{2k\pi}{n}).$$

Donde segue que $\omega^n = 1$ *e portanto* $\omega \in C_n$*. Também é possível ver que as potências* $1, \omega, \omega^2, \ldots, \omega^{n-2}, \omega^{n-1}$ *são distintas, logo* $\{1, \omega, \ldots, \omega^{n-1}\}$ *é um subconjunto de* C_n *com* n *elementos. Portanto*

$$C_n := \{z \in \mathbb{C}^* \mid z^n = 1\} = \{1, \omega, \ldots, \omega^{n-1}\} = \{\omega^k \mid k = 0, 1, 2, \ldots, n-1\}.$$

Para $n = 2$ *sabemos que* $x^2 = 1$ *tem soluções* 1 *e* -1*, logo* $C_2 = \{1, -1\}$*.*

Para $n = 3$ *temos* $\omega = e^{\frac{2\pi}{3}} = \cos(\frac{2\pi}{3}) + i \cdot sen(\frac{2\pi}{3}) = -\frac{1}{2} + \frac{i\sqrt{3}}{2}$*, logo* $C_3 = \{1, -\frac{1}{2} + \frac{i\sqrt{3}}{2}, -\frac{1}{2} - \frac{i\sqrt{3}}{2}\}$*.*

Para $n = 4$ *temos* $C_4 = \{1, -1, i, -i\}$*.*

Observe que para cada $z \in C_n$ *temos* $\mid z \mid = 1$ *e não é difícil ver que*

$$\{z \in \mathbb{C}^*; \mid z \mid = 1\}$$

também é um grupo com a multiplicação de $\mathbb{C}$.

iv) $(M_{n\times m}(\mathbb{R}), +)$: *o conjunto* $M_{n\times m}(\mathbb{R})$, *das matrizes com* n *linhas e* m *colunas com coeficientes reais, munido com a operação de soma usual de matrizes, é um grupo. Da mesma forma, o conjunto* $M_{n\times m}(\mathbb{C})$ *das matrizes com entradas sobre os números complexos também é um grupo, munido com a soma usual de matrizes.*

Quando $m = n$, *representamos* $M_n(\mathbb{X}) := M_{n\times n}(\mathbb{X})$, *onde* $\mathbb{X} \in \{\mathbb{R}, \mathbb{C}\}$.

v) $(Gl_n(\mathbb{R}), \cdot)$: *o conjunto* $Gl_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) \mid detA \neq 0\}$, *munido da multiplicação usual de matrizes (que é associativa) é um grupo. De fato, note que* $I_n \in Gl_n(\mathbb{R}) \neq \emptyset$, *onde* I_n *é a matriz identidade de ordem* n. *Ademais sabemos que* $det(AB) = det(A)det(B)$ *e portanto temos* $det(AB) \neq 0$ *sempre que* $A, B \in Gl_n(\mathbb{R})$. *Como* $detA \neq 0$ *existe* $A^{-1} \in M_n(\mathbb{R})$ *tal que* $A^{-1}A = AA^{-1} = I_n$ *e* $detA^{-1} = (detA)^{-1} \neq 0$, *donde* $A^{-1} \in Gl_n(\mathbb{R})$ *é o elemento simétrico para* A *em* $Gl_n(\mathbb{R})$. *Portanto* $Gl_n(\mathbb{R})$ *é um grupo.*

Analogamente o conjunto $Gl_n(\mathbb{C})$ *também forma um grupo com a multiplicação de matrizes.*

Veja que, com a soma usual de matrizes, $Gl_n(\mathbb{R})$ *e* $Gl_n(\mathbb{C})$ ***não*** *são grupos, pois não são fechados para a operação.*

vi) $(Sl_n(\mathbb{R}), \cdot)$: *considere o conjunto* $Sl_n(\mathbb{R}) = \{A \in Gl_n(\mathbb{R}) \mid detA = 1\}$. *Tal conjunto, munido da multiplicação usual de matrizes, é um grupo (não abeliano para* $n \geq 2$ *) com elemento neutro* I_n, *pois note que dados* $A, B \in Sl_n(\mathbb{R})$ *temos* $det(AB) = det(A)det(B) = 1 \cdot 1 = 1$, *logo* $AB \in Sl_n(\mathbb{R})$, *concluindo que* $Sl_n(\mathbb{R})$ *é fechado à operação. Além do mais, como* $det(A) \neq 0$, *então* A *é inversível e* $det(A^{-1}) = det(A)^{-1} = 1^{-1} = 1$, *donde temos* $A^{-1} \in Sl_n(\mathbb{R})$, *concluindo que* $Sl_n(\mathbb{R})$ *é um grupo. Tal grupo é chamado de Grupo Especial Linear.*

Igualmente $Sl_n(\mathbb{C})$ *também é um grupo com a multiplicação de matrizes.*

vii) $(V,+)$: *Sendo* V *um espaço vetorial real, então* V *com sua soma de vetores forma um grupo abeliano onde o elemento neutro é o vetor nulo.*

viii) Grupos Diedrais D_3 *e* D_n*: Considere um triângulo equilátero* T *no plano* $\mathbb{R}^2$*, com centro na origem e vértices* v_1, v_2 *e* v_3 *respectivamente em sentido anti-horário. Note que algumas rotações do plano preservam o triângulo. Para ser mais exato, temos* 3 *rotações que preservam* T*. Ademais também temos 3 reflexões do plano,* S_1, S_2 *e* S_3*, determinadas pelas retas que contém a origem e cada um dos vértices, que preservam o triângulo. Tomemos* D_3 *como sendo o conjunto dessas rotações e reflexões que preservam o triângulo (6 ao total). Denotaremos a função que rotaciona o plano em* θ *radianos em sentido anti-horário por* R_θ*. Sendo* S_i *a reflexão determinada pela reta que passa pelo vértice* v_i *e pela origem,* $i = 1, 2, 3$*, temos:*

$$D_3 = \{R_0, R_{\frac{2\pi}{3}}, R_{\frac{4\pi}{3}}, S_1, S_2, S_3\}.$$

Note que fazer quaisquer dois desses movimentos seguidos não altera T*. Na verdade* D_3 *é fechado com respeito a composição de funções. A composição de funções é associativa. A rotação* R_0*, que é a função identidade em* $\mathbb{R}^2$*, é o elemento neutro para esta operação e todo elemento tem um inverso. Então* $(D_3, \circ)$ *é um grupo de elemento neutro* R_0*.*

Na verdade, a tabela da operação composição em D_3 *é*

$\circ$	R_0	$R_{\frac{2\pi}{3}}$	$R_{\frac{4\pi}{3}}$	S_1	S_2	S_3
R_0	R_0	$R_{\frac{2\pi}{3}}$	$R_{\frac{4\pi}{3}}$	S_1	S_2	S_3
$R_{\frac{2\pi}{3}}$	$R_{\frac{2\pi}{3}}$	$R_{\frac{4\pi}{3}}$	R_0	S_3	S_1	S_2
$R_{\frac{4\pi}{3}}$	$R_{\frac{4\pi}{3}}$	R_0	$R_{\frac{2\pi}{3}}$	S_2	S_3	S_1
S_1	S_1	S_2	S_3	R_0	$R_{\frac{2\pi}{3}}$	$R_{\frac{4\pi}{3}}$
S_2	S_2	S_3	S_1	$R_{\frac{4\pi}{3}}$	R_0	$R_{\frac{2\pi}{3}}$
S_3	S_3	S_1	S_2	$R_{\frac{2\pi}{3}}$	$R_{\frac{4\pi}{3}}$	R_0

Generalizando, temos

$$D_n = \{R_0, R_{\frac{2\pi}{n}}, R_{\frac{4\pi}{n}}, R_{\frac{6\pi}{n}}, \ldots, R_{\frac{(n-1)2\pi}{n}}, S_1, S_2, S_3, \ldots, S_n\}$$

sendo o grupo das rotações e reflexões do plano que preservam um polígono regular de n lados com centro na origem. Ele contém n rotações $R_{\frac{k2\pi}{n}}$, $k = 0, 1, \ldots, n-1$, *e n reflexões* S_j, $j = 1, 2, \ldots, n$. *Cada reflexão é em relação à reta determinada pela origem e por um dos seus vértices. Portanto* $\mid D_n \mid = 2n$. D_n, *munido com a composição de funções é um grupo de elemento neutro* R_0.

Sendo S uma reflexão fixa e R uma rotação qualquer, então

$$(R_{\frac{2\pi}{n}})^n = R_0, \quad S^2 = R_0, \quad SR_{\frac{2\pi}{n}}S = (R_{\frac{2\pi}{n}})^{-1}, \quad R = (R_{\frac{2\pi}{n}})^k \text{ para algum } k \in \mathbb{Z}_+.$$

Cada elemento de D_n *pode ser escrito de forma única como* $(R_{\frac{2\pi}{n}})^k$, $0 \leq k \leq n-1$, *se for uma rotação, ou na forma* $S \circ (R_{\frac{2\pi}{n}})^k$, $0 \leq k \leq n-1$, *se for uma reflexão. Observe que a partir da relação* $SR_{\frac{2\pi}{n}}S = (R_{\frac{2\pi}{n}})^{-1}$ *obtemos* $S(R_{\frac{2\pi}{n}})^k S = (R_{\frac{2\pi}{n}})^{-k}$.

1.1.2 Subgrupos

Definição 1.3 *Sendo G um grupo e H um subconjunto não vazio de G, se H for fechado em relação à operação de G e se sempre que* $x \in H$ *tivermos que* $x^{-1} \in H$, *então diremos que H é subgrupo de G.*

A próxima proposição nos dá caracterizações para um subgrupo.

Proposição 1.4 *Sendo G um grupo, supondo que* $\emptyset \neq H \subseteq G$, *são equivalentes:*

i) H *é subgrupo de* G.

ii) $xy^{-1} \in H \ \forall x, y \in H$.

iii) H *é um grupo com a restrição de* $*$ (*operação de* G).

Prova.

i) $\Rightarrow$ *ii)*

Tomemos $x, y \in H$. Como $y \in H$, então por hipótese temos $y^{-1} \in H$. Como ainda por hipótese H é fechado à operação, temos $xy^{-1} \in H$.

ii) $\Rightarrow$ *iii)*

Como H é não vazio, tomemos $x \in H$ e fazendo $y = x \in H$, temos por hipótese $xy^{-1} = xx^{-1} = e \in H$, onde e é o elemento neutro de G. Agora, tomando $y \in H$ e $x = e$ temos $xy^{-1} = ey^{-1} = y^{-1} \in H$, donde segue que H é fechado à inversos. Daí, para $x, y \in H$ temos $x(y^{-1})^{-1} = xy \in H$. Logo $*(H \times H) \subseteq H$. Então podemos restringir $*$ em H e tal restrição ainda será uma operação binária em H. Claramente ela continua associativa e ademais continuamos, em particular, com $he = eh = h$ para todo $h \in H$. Logo o elemento $e \in H$ também é elemento neutro para H, e como já vimos todo elemento de H tem inverso em H. Portanto H com a restrição de $*$ satisfaz os axiomas de grupo.

iii) $\Rightarrow$ i)

É imediato que H é um conjunto não vazio e fechado com respeito a $*$. Só nos resta mostrar que $x^{-1} \in H$ para qualquer $x \in H$. Para isso tomemos e_H o elemento neutro de H e e o elemento neutro de G. Como e_H é neutro em H, em particular, temos $e_H^2 = e_H$, donde:

$$e_H^2 = e_H \Rightarrow e_H^{-1} e_H = e_H^{-1} e_H^2 \Rightarrow e = e_H$$

ou seja, os elementos neutros de H e G coincidem e portanto o elemento simétrico que $x \in H$ tem em H é o mesmo simétrico em G, concluindo que $x^{-1} \in H$.

■

Exemplo 2 *São exemplos de subgrupos:*

i) $(\mathbb{Z}, +)$ *é subgrupo de* $(\mathbb{Q}, +)$*, que por sua vez é subgrupo de* $(\mathbb{R}, +)$*, que ainda é subgrupo de* $(\mathbb{C}, +)$*.*

ii) O grupo multiplicativo $\{1, -1\}$ *é subgrupo de* $C_4 = \{1, -1, i, -i\}$*, que por sua vez é subgrupo do grupo multiplicativo* $C_{12} = \{z \in \mathbb{C}^*; z^{12} = 1\}$*, sendo esse último um subgrupo do grupo multiplicativo* $\{z \in \mathbb{C}^*; \mid z \mid = 1\}$*.*

iii) $Sl_n(\mathbb{R})$ *é subgrupo de* $Gl_n(\mathbb{R})$*.*

iv) *Seja* $F(]0,1[;\mathbb{R})$ *o conjunto de todas as funções com domínio* $]0,1[$ *e contradomínio* $\mathbb{R}$. *Consideramos em* $F(]0,1[;\mathbb{R})$ *a operação usual de soma de funções* $(f,g) \mapsto f+g=h$ *definida por* $h(x)=f(x)+g(x)$ *para todo* $x \in]0,1[$, *temos que* $F(]0,1[;\mathbb{R})$ *é um grupo de elemento neutro* $x \mapsto 0$ (*função constante igual a* 0).

Sendo $C^1(]0,1[)$ *o subconjunto de* $F(]0,1[;\mathbb{R})$ *formado pelas funções deriváveis e com derivada contínua, temos então que* $(C^1(]0,1[),+)$ *é subgrupo de* $(F(]0,1[;\mathbb{R}),+)$, *visto que dados* $f,g \in C^1(]0,1[)$, *temos que* $f-g$ *é derivável,* $(f-g)'=f'-g'$, *como* f' *e* g' *são contínuas, então* $f'-g'$ *também é. Logo* $f-g=h \in C^1(]0,1[])$.

v) *Se* V *é um espaço vetorial real e* W *é subespaço de* V, *então* $(W,+)$ *é subgrupo de* $(V,+)$.

vi) $H = \left\{ \begin{pmatrix} cos(x) & sen(x) \\ -sen(x) & cos(x) \end{pmatrix} \mid x \in \mathbb{R} \right\}$ *é subgrupo de* $Sl_2(\mathbb{R})$. *Primeiramente note que*

$$det \begin{pmatrix} cos(x) & sen(x) \\ -sen(x) & cos(x) \end{pmatrix} = cos^2(x) + sen^2(x) = 1$$

ou seja, $H \subseteq Sl_2(\mathbb{R})$.

Tomando agora $A = \begin{pmatrix} cos(a) & sen(a) \\ -sen(a) & cos(a) \end{pmatrix}, B = \begin{pmatrix} cos(b) & sen(b) \\ -sen(b) & cos(b) \end{pmatrix} \in H$, *uma verificação simples mostra que* $B^{-1} = \begin{pmatrix} cos(b) & -sen(b) \\ sen(b) & cos(b) \end{pmatrix}$. *Lembrando que*

$$cos(a-b) = cos(a)cos(b)+sen(a)sen(b) \text{ e } sen(a-b) = sen(a)cos(b)-cos(a)sen(b)$$

temos:

$$\begin{aligned} AB^{-1} &= \begin{pmatrix} cos(a) & sen(a) \\ -sen(a) & cos(a) \end{pmatrix} \begin{pmatrix} cos(b) & -sen(b) \\ sen(b) & cos(b) \end{pmatrix} \\ &= \begin{pmatrix} cos(a)cos(b)+sen(a)sen(b) & -cos(a)sen(b)+sen(a)cos(b) \\ -sen(a)cos(b)+cos(a)sen(b) & sen(a)sen(b)+cos(a)cos(b) \end{pmatrix} \\ &= \begin{pmatrix} cos(a-b) & sen(a-b) \\ -sen(a-b) & cos(a-b) \end{pmatrix} \in H. \end{aligned}$$

vii) Seja G um grupo qualquer. Fixando $s \in G$, tomemos $H = \{s^n \in G \mid n \in \mathbb{Z}\}$. Dados $x, y \in H$ devem existir $n, m \in \mathbb{Z}$ tais que $x = s^n$ e $y = s^m$ e daí

$$xy^{-1} = s^n(s^m)^{-1} = s^n s^{-m} = s^{n-m} \in H$$

concluindo que H é um subgrupo. Chamamos H de subgrupo gerado por s. Não é difícil ver que se algum subgrupo L de G contem s como elemento, então $H \subseteq L$.

Observação 1.3 *A nomenclatura "subgrupo" faz jus à ideia intuitiva do que seria um subgrupo, que é literalmente uma parte de G que por si só é um grupo. Da demonstração da **Proposição 1.4** podemos notar que o elemento neutro de H coincide com o de G e que o inverso de $x \in H$ em H é o mesmo inverso que x tem em G. Claramente como os exemplos nos fazem suspeitar, se N é subgrupo de H e H é subgrupo de G, então N é subgrupo de G.*

Ademais note que tomando $H = \mathbb{R}^*$ e $G = \mathbb{R}$ temos que H é um grupo com a multiplicação usual e G é um grupo com a soma usual. Porém mesmo que $H \subseteq G$, H não é subgrupo de G e isso ocorreu devido à diferença nas operações, a operação em H não é a restrição da operação de G.

1.2 Classes laterais e Teorema de Lagrange

Um importante resultado na área de teoria de grupos e que será usado neste trabalho é o *Teorema de Lagrange* que diz que se H é subgrupo de um grupo finito G, então $\mid H \mid$ divide $\mid G \mid$. Para mostrar isso vamos desenvolver o assunto de classes laterais, que também será muito importante.

Definição 1.5 ***Classes laterais à esquerda**: Sejam G um grupo e H um subgrupo de G. Para $s \in G$ denotamos por sH o conjunto $\{st;\ t \in H\}$, e dizemos que sH é a classe lateral à esquerda de H que contém s. Dois elementos x e y de G são ditos congruentes módulo H se eles geram a mesma classe lateral à esquerda, isto é, $xH = yH$, escrevemos $x \equiv y$ (módulo H).*

O conjunto das (distintas) classes laterais de H é denotado por G/H e o número de elementos de G/H é dito ser o índice de H em G e é denotado por $(G : H)$.

Escolhendo um elemento em cada sH, formamos um subconjunto R de G chamado de sistema de representantes de G/H ou conjunto transversal. Cada $s \in G$ pode ser escrito de forma única como $s = rt$, onde $r \in R$ e $t \in H$.

Note que dados $x, y \in G$, então se $x^{-1}y \in H$, existe $h \in H$ tal que $x^{-1}y = h$ e daí $y = xh$, tomando então $\alpha \in yH$ temos $\alpha = yt$ para algum $t \in H$ e daí $\alpha = yt = (xh)t = x(ht)$. Como H é fechado para a operação, temos $ht \in H$ e portanto $\alpha \in xH$, concluindo que $yH \subseteq xH$. Observando que $x^{-1}y = h$ implica em $y^{-1}x = h^{-1} \in H$, temos de forma análoga $xH \subseteq yH$ e portanto $xH = yH$.

Reciprocamente, caso $xH = yH$, temos $x = xe \in xH = yH$, donde existe $t \in H$ tal que $x = yt$ e daí $y^{-1}x = t \in H$. Consequentemente também temos $x^{-1}y \in H$.

Vemos que $x \equiv y$ (módulo H) se, e somente se, $x^{-1}y \in H$.

Proposição 1.6 *Sejam G um grupo e H um subgrupo de G. Então:*

i) $G = \bigcup_{s \in G} sH$.

ii) *Para $x, y \in G$ tem-se: $xH = yH \Leftrightarrow x^{-1}y \in H \Leftrightarrow x \in yH \Leftrightarrow y \in xH$.*

iii) *Se $x, y \in G$ e $xH \neq yH$, então $xH \cap yH = \emptyset$.*

Prova.

i) Claramente $\bigcup_{s \in G} sH \subseteq G$ e para a inclusão contrária basta notar que como H é subgrupo de G, então $e \in H$ e portanto dado $s \in G$ temos $s = se \in sH \subseteq \bigcup_{s \in G} sH$.

ii) Segue do que foi dito logo após a definição de classe lateral.

iii) Suponha que $xH \cap yH \neq \emptyset$. Então tomando $\alpha \in xH \cap yH$, existem $t, h \in H$ tais que $yh = \alpha = xt$ e daí $x^{-1}y = th^{-1} \in H$, e pelo item anterior teríamos $xH = yH$, absurdo.

■

Concluímos que a coleção de elementos G/H (cada elemento é um subconjunto de G) é uma partição para G, particularmente, supondo G finito, então G/H também

é finito, denotemos $m = (G : H)$, sejam $H_1, H_2, \ldots, H_m \in G/H$ as distintas classes laterais à esquerda de H. Então G é a *união disjunta* delas:

$$G = H_1 \dot{\cup} H_2 \dot{\cup} \cdots \dot{\cup} H_m, \quad H_i \cap H_j = \emptyset \text{ sempre que } i \neq j.$$

Disso temos que se G for finito ocorre: $\mid G \mid = \mid H_1 \mid + \mid H_2 \mid + \cdots + \mid H_m \mid$.

Observação 1.4 *Lembrando que se X é um conjunto não vazio, uma relação " $\sim$ " em X é uma relação de equivalência se satisfaz*

i) $\sim$ *é reflexiva, isto é, $x \sim x$ para todo x em X.*

ii) $\sim$ *é simétrica, isto é, para $x, y \in X$ se $x \sim y$, então $y \sim x$.*

iii) $\sim$ *é transitiva, isto é, para $x, y, z \in X$ se $x \sim y$ e $y \sim z$, então $x \sim z$.*

Considerando, para cada $x \in X$, a classe de equivalência de x como sendo o conjunto $\overline{x} = \{t \in X \mid x \sim t\} \subseteq X$ (sempre não vazio desde que $\sim$ é uma relação de equivalência temos $x \in \overline{x}$), a coleção das distintas classes de equivalência é uma partição para X.

Reciprocamente, sendo $X \neq \emptyset$, suponha que $\{X_\lambda \mid \lambda \in \Lambda\}$ forme uma partição para X, pondo $x \sim y$ se, e somente se, x e y pertencem ao mesmo X_λ. Temos que " $\sim$ " é uma relação de equivalência.

Sendo G um grupo qualquer e H um subgrupo de G, então a partição de G dada pelas distintas classes laterais $\{H_\lambda \mid \lambda \in \Lambda\}$ é proveniente da relação em G dada por :

$$x \sim y \Leftrightarrow x^{-1}y \in H$$

para quaisquer $x, y \in G$. Ou uma das equivalências

$$x \sim y \Leftrightarrow x \equiv y \ (\textit{módulo } H)$$

$$x \sim y \Leftrightarrow xH = yH.$$

Note que de fato

(i) $\sim$ *é reflexiva, pois $x^{-1}x = e \in H$. Logo $x \sim x$ para todo $x \in G$.*

(ii) $\sim$ *é simétrica, pois se* $x^{-1}y \in H$, *então* $y^{-1}x = (x^{-1}y)^{-1} \in H$. *Logo se* $x \sim y$, *temos* $y \sim x$.

(iii) $\sim$ *é transitiva, pois se* $x^{-1}y \in H$ *e* $y^{-1}z \in H$, *então* $x^{-1}z = x^{-1}yy^{-1}z = (x^{-1}y)(y^{-1}z) \in H$. *Logo se* $x \sim y$ *e* $y \sim z$, *temos* $x \sim z$.

Agora, dado $\alpha \in \overline{x}$, *então* $x^{-1}\alpha \in H$ *e portanto* $\alpha = xt$ *para algum* $t \in H$, *donde temos* $\alpha \in xH$ *e daí* $\overline{x} \subseteq xH$. *Por outro lado, dado* $\alpha \in xH$, *então* $\alpha = xt$ *para algum* $t \in H$ *e consequentemente* $x^{-1}\alpha = t \in H$ *e* $\alpha \in \overline{x}$. *Portanto* $xH \subseteq \overline{x}$, *concluindo que* $\overline{x} = xH$.

Vamos agora mostrar que as classes laterais têm todas a mesma quantidade de elementos. Para isto, fixando $s \in G$, considere a aplicação:

$$\begin{aligned} \psi : H &\to sH \\ t &\mapsto \psi(t) = st \end{aligned}$$

ψ é claramente sobrejetiva e ademais, dados $t_1, t_2 \in H$ tais que $\psi(t_1) = \psi(t_2)$, então

$$st_1 = st_2 \Rightarrow s^{-1}st_1 = s^{-1}st_2 \Rightarrow t_1 = t_2$$

concluindo que ψ é injetora, e portanto é uma bijeção entre H e sH.

No caso em que H é finito, temos que sH é finito e tem a mesma quantidade de elementos de H, ou seja, $\mid sH \mid = \mid H \mid$.

Estamos prontos para enunciar o Teorema de Lagrange.

Teorema 1.7 *Sendo* G *um grupo finito e* H *um subgrupo de* G, *temos:*

$$\mid G \mid = (G : H) \mid H \mid$$

e portanto $\mid H \mid$ *divide* $\mid G \mid$.

Prova. Sejam $m = (G : H)$ e $H_1, H_2, \ldots, H_m$ as distintas classes laterais de H. Sabemos que $\mid G \mid = \mid H_1 \mid + \mid H_2 \mid + \cdots + \mid H_m \mid$ e que $\mid H \mid = \mid H_i \mid$ para todo

$i = 1, 2, ..., m$. Disso segue que:

$$\begin{aligned} \mid G \mid &= \mid H_1 \mid + \mid H_2 \mid + \cdots + \mid H_m \mid \\ &= \underbrace{\mid H \mid + \mid H \mid + \cdots + \mid H \mid}_{m \text{ parcelas}} \\ &= m \mid H \mid \\ &= (G : H) \mid H \mid \end{aligned}$$

Ademais $\dfrac{\mid G \mid}{\mid H \mid} = (G : H) = \mid G/H \mid \in \mathbb{N}$, donde segue que $\mid H \mid$ divide $\mid G \mid$. ■

1.3 Classes de conjugação

Outra maneira muito importante de particionar um grupo G é por meio das classes de conjugação que serão apresentadas a seguir.

Definição 1.8 *Sendo G um grupo, dado $x \in G$ definimos a classe de conjugação de x em G como sendo o conjunto $Cl_G(x) := \{txt^{-1}; t \in G\}$, e se $y \in Cl_G(x)$ denotamos $y \sim x$.*

Proposição 1.9 *A relação " $\sim$ " acima é de equivalência.*

Prova.

" $\sim$ " é *reflexiva*: basta tomarmos $t = e$, então $x = exe^{-1} = txt^{-1} \in Cl_G(x)$, ou seja, $x \sim x$.

$\sim$ é *simétrica*: Se $x \sim y$, então existe $t \in G$ tal que $x = tyt^{-1}$ e daí $t^{-1}xt = y$. Tomando $s = t^{-1} \in G$ temos $y = sxs^{-1} \in Cl_G(x)$, donde $y \sim x$.

$\sim$ é *transitiva*: Se $x \sim y$ e $y \sim z$, então existem $t_1, t_2 \in G$ tais que $x = t_1yt_1^{-1}$ e $y = t_2zt_2^{-1}$, donde segue que $x = t_1(t_2zt_2^{-1})t_1^{-1} = t_1t_2z(t_1t_2)^{-1}$. Tomando $t = t_1t_2$ temos $x = tzt^{-1} \in Cl_G(z)$, concluindo que $x \sim z$. ■

Portanto os conjuntos $Cl_G(x)$ particionam o conjunto G, isto é,

$i)$ $Cl_G(x) \cap Cl_G(y) = \emptyset$ ou $Cl_G(x) = Cl_G(y)$ $\forall x, y \in G$.

ii) $G = \cup_{x \in G} Cl_G(x)$.

Exemplo 3

i) Sendo G um grupo de elemento neutro "e", então para qualquer $t \in G$ temos $tet^{-1} = tt^{-1} = e$, donde segue que $Cl_G(e) = \{e\}$.

ii) Seja G um grupo abeliano. Então, dados quaisquer $x, t \in G$ temos $txt^{-1} = tt^{-1}x = x$, donde segue que $Cl_G(x) = \{x\}$, e portanto todas as classes de conjugação são unitárias.

Reciprocamente, suponha que G seja tal que toda classe de conjugação seja unitária. Então dados $x, y \in G$, temos $yxy^{-1} \in Cl_G(x) = \{x\}$. Logo $yxy^{-1} = x$ e operando com y na direita, em ambos os lados da igualdade, temos $yx = xy$. Logo G é abeliano.

iii) Considere o grupo multiplicativo $H = Sl_2(\mathbb{R}) = \{A \in M_2(\mathbb{R}) \mid det(A) = 1\}$. Tomemos $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in H$, mostremos que

$$Cl_H(A) = \left\{ \begin{pmatrix} 1-ac & a^2 \\ -c^2 & 1+ac \end{pmatrix} \mid a, c \in \mathbb{R}, a \neq 0 \text{ ou } c \neq 0 \right\}.$$

Inicialmente, tomando $Y \in Cl_H(A)$, existe $P \in H$ tal que $Y = PAP^{-1}$. Sendo $P = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, temos $ad - bc = 1$ e então não podemos ter a e c ambos nulos, ou seja, $a \neq 0$ ou $c \neq 0$, uma verificação direta mostra que $P^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$. Daí

$$\begin{aligned} Y = PAP^{-1} &= \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \\ &= \begin{pmatrix} a & a+b \\ c & c+d \end{pmatrix} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \\ &= \begin{pmatrix} ad-ac-bc & -ab+a^2+ab \\ cd-c^2-cd & -bc+ac+ad \end{pmatrix} \\ &= \begin{pmatrix} 1-ac & a^2 \\ -c^2 & 1+ac \end{pmatrix} \end{aligned}$$

Isso nos dá uma inclusão.

Para a outra inclusão, dados $a, c \in \mathbb{R}$ não ambos nulos, sempre podemos escolher $b, d \in \mathbb{R}$ tais que $ad - bc = 1$, pois se $a \neq 0$, fixando $b \in \mathbb{R}$ qualquer, tomemos $d = \frac{bc+1}{a}$ e portanto $ad - bc = 1$. Caso $c \neq 0$, então fixando $d \in \mathbb{R}$ qualquer, tomemos $b = \frac{ad-1}{c}$ e portanto $ad - bc = 1$. Logo basta tomar $P = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ que teremos $P \in H$ e a conta anterior mostra que $PAP^{-1} = \begin{pmatrix} 1 - ac & a^2 \\ -c^2 & 1 + ac \end{pmatrix} \in Cl_H(A)$.

1.4 Ações de grupos e homomorfismos de grupos

As definições a seguir serão essenciais para esse trabalho, tendo em vista que o objetivo geral é mostrar a relação estrita que há entre a ação de um grupo finito abeliano em uma álgebra e a graduação dessa mesma álgebra dada por esse mesmo grupo (definição essa que será dada posteriormente).

1.4.1 Ações de grupos

Definição 1.10 *Sejam G um grupo e X um conjunto não vazio. Definimos uma ação de G em X como sendo uma aplicação $\theta : G \times X \to X$, $(s, x) \mapsto \theta(s, x) = s \cdot x$, que satisfaz:*

i) $e \cdot x = x$, para todo $x \in X$.

ii) $(s_1 s_2) \cdot x = s_1 \cdot (s_2 \cdot x)$, para quaisquer $s_1, s_2 \in G$ e $x \in X$.

A ideia da definição acima é conseguir "*multiplicar*" os elementos de um conjunto X, não vazio, pelos elementos de G de tal forma que essa multiplicação seja compatível com a operação de G. O item *i)* do exemplo a seguir ilustra a ideia.

Exemplo 4 *São exemplos de ações de grupos:*

i) Seja V um espaço vetorial real, considere o grupo multiplicativo $\mathbb{R}^*$, sendo "$\cdot$"

a multiplicação por escalar em V. Então a aplicação $\theta : \mathbb{R}^* \times V \to V$ dada por $\theta(\lambda, v) = \lambda \cdot v$ é uma ação de $\mathbb{R}^*$ em V.

ii) Sendo G um grupo e X um conjunto não vazio, definindo $\theta_0 : G \times X \to X$ por $\theta_0(s, x) = x$ para quaisquer $s \in G$ e $x \in X$, então essa aplicação é uma ação e é chamada de ação trivial.

iii) Considere o grupo $(\mathbb{R}, +)$, o conjunto $\mathbb{R}^2$ e a aplicação $T : \mathbb{R} \times \mathbb{R}^2 \to \mathbb{R}^2$, $(t, (x, y)) \mapsto t \cdot (x, y) = (x + t, y + t)$. Temos:

1. $0 \cdot (x, y) = (x, y)$
2. $(t_1 + t_2) \cdot (x, y) = (x + t_1 + t_2, y + t_1 + t_2) = t_1 \cdot (x + t_2, y + t_2) = t_1 \cdot (t_2 \cdot (x, y))$, *para quaisquer $t_1, t_2 \in \mathbb{R}$.*

portanto T é uma ação.

iv) Seja G um grupo, tomando $X = G$ definamos a ação $\theta : G \times G \to G$ como sendo a conjugação: $(s, x) \mapsto \theta(s, x) = s \cdot x = sxs^{-1}$. Temos $e \cdot x = exe^{-1} = x$, ademais:

$$(s_1 s_2) \cdot x = s_1 s_2 x (s_1 s_2)^{-1} = s_1 s_2 x s_2^{-1} s_1^{-1} = s_1 (s_2 x s_2^{-1}) s_1^{-1} =$$
$$s_1 (s_2 \cdot x) s_1^{-1} = s_1 \cdot (s_2 \cdot x).$$

Outra ação que poderíamos definir é $s \cdot x = sx$, ou seja, literalmente mandar o par no produto dos elementos, pois já temos por definição $ex = x$ e $s(tx) = (st)x$.

v) Sejam G um grupo, H um subgrupo de G, X um conjunto não vazio e $\theta : G \times X \to X$ uma ação de G em X. A aplicação $\theta_H : H \times X \to X$, definida por $\theta_H(h, x) = \theta(h, x)$, é uma ação de H em X e dizemos que esta ação é a restrição de θ a H.

vi) Considerando o conjunto G das funções bijetoras de $\mathbb{R}$ em $\mathbb{R}$, dos resultados da teoria clássica de funções não é difícil ver que G com a composição de funções forma um grupo, com elemento neutro dado pela função identidade, $Id : \mathbb{R} \to \mathbb{R}$ dada por $Id(x) = x$ para todo $x \in \mathbb{R}$. Tomando então a aplicação

$$\theta : G \times \mathbb{R} \to \mathbb{R}$$
$$(f, x) \mapsto \theta(f, x) = f \cdot x = f(x)$$

temos:

1. $Id \cdot x := Id(x) = x$ *para todo* $x \in \mathbb{R}$.
2. $(f_1 \circ f_2) \cdot x := (f_1 \circ f_2)(x) = f_1(f_2(x)) = f_1 \cdot (f_2(x)) = f_1 \cdot (f_2 \cdot x)$ *para quaisquer* $f_1 f_2 \in G$ *e* $x \in \mathbb{R}$.

Daí temos que $(f, x) \mapsto f(x)$ *é uma ação de* $(G, \circ)$ *em* $X = \mathbb{R}$.

1.4.2 Homomorfismos de grupos

Sejam $(G_1, *_1)$ e $(G_2, *_2)$ grupos, podemos nos perguntar quais funções que têm como domínio o conjunto G_1 e contradomínio o conjunto G_2 são compatíveis com as estruturas de G_1 e G_2 como grupos, assim como temos transformações lineares entre espaços vetoriais, que são funções compatíveis com a soma vetorial e a multiplicação por escalar.

Definição 1.11 *Sejam* $(G_1, *_1)$ *e* $(G_2, *_2)$ *grupos, dizemos que uma aplicação* φ*:* $G_1 \to G_2$ *é um homomorfismo de grupos quando*

$$\varphi(x *_1 y) = \varphi(x) *_2 \varphi(y) \quad \forall x, y \in G_1.$$

Observação 1.5 *Se* G_1 *e* G_2 *são grupos, com* e_2 *o elemento neutro de* G_2*, então a aplicação* $x \mapsto e_2$ *é um homomorfismo, chamado homomorfismo trivial, donde*

$$HOM(G_1, G_2) = \{\varphi : G_1 \to G_2 \mid \varphi \text{ é homomorfismo de grupos}\} \neq \emptyset.$$

Exemplo 5 *São exemplos de homomorfismo de grupos:*

i) Sejam $\mathbb{R}_+^*$ *o grupo multiplicativo dos reais positivos (a operação é a multiplicação usual de números reais) e* $\mathbb{R}$ *o grupo aditivo dos reais (a operação é a soma usual de números reais). Considere a aplicação* $\varphi : \mathbb{R}_+^* \to \mathbb{R}$ *definida por* $\varphi(x) = lnx$*. Note que dados* $x, y \in \mathbb{R}_+^*$*, temos:*

$$\varphi(xy) = ln(xy) = lnx + lny = \varphi(x) + \varphi(y).$$

Então φ *é um homomorfismo de grupos.*

ii) *Sendo $M_n(\mathbb{C})$ o grupo das matrizes quadradas de ordem n com entradas complexas com a operação de soma usual e $\mathbb{C}$ o grupo aditivo dos complexos, dada $A = (a_{ij})_{n\times n} \in M_n(\mathbb{C})$, definamos a aplicação $Tr : M_n(\mathbb{C}) \to \mathbb{C}$ por $Tr(A) = \sum_{k=1}^{n} a_{kk}$. Daí, sendo $B = (b_{ij}) \in M_n(\mathbb{C})$, temos:*

$$Tr(A+B) = \sum_{k=1}^{n}(a_{kk}+b_{kk}) = \sum_{k=1}^{n} a_{kk} + \sum_{k=1}^{n} b_{kk} = Tr(A) + Tr(B).$$

Portanto tal aplicação, que chamamos de traço, é um homomorfismo de grupos.

iii) *Sendo $\mathbb{Z}$ o grupo aditivo dos inteiros, tomemos $\varphi : \mathbb{Z} \to \mathbb{Z}$ definida por $\varphi(x) = 2x$. então*

$$\varphi(n+m) = 2(n+m) = 2n + 2m = \varphi(n) + \varphi(m) \quad \forall n, m \in \mathbb{Z}.$$

Portanto φ é um homomorfismo de grupos.

iv) *A aplicação determinante $det : Gl_n(\mathbb{R}) \to \mathbb{R}^*$ é um homomorfismo de grupos entre os grupos multiplicativos $Gl_n(\mathbb{R})$ e $\mathbb{R}^*$*

v) *Sendo $\mathbb{Z}$ o grupo aditivo dos inteiros e G um grupo qualquer, fixando $a \in G$ a aplicação*

$$\varphi_a : \mathbb{Z} \to G$$
$$n \mapsto \varphi_a(n) = a^n$$

é um homomorfismo, pois $\varphi_a(n+m) = a^{n+m} = a^n a^m = \varphi_a(n)\varphi_a(m)$.

vi) *Sendo G um grupo qualquer, fixando $s \in G$ a aplicação*

$$\mathcal{I}_s : G \to G$$
$$x \mapsto \mathcal{I}_s(x) = sxs^{-1}$$

é um homomorfismo, pois dados $x, y \in G$, temos

$$\mathcal{I}_s(x)\mathcal{I}_s(y) = (sxs^{-1})(sys^{-1}) = sxys^{-1} = \mathcal{I}_s(xy).$$

vii) *Considerando os grupos multiplicativos $\mathbb{C}^*$ e $\mathbb{R}^*$, a aplicação*

$$N : \mathbb{C}^* \to \mathbb{R}^*$$
$$z = a + bi \mapsto N(z) = \mid z \mid = \sqrt{a^2 + b^2}$$

é um homomorfismo de grupos.

Proposição 1.12 *Sejam G_1 e G_2 grupos, e $\varphi : G_1 \to G_2$ um homomorfismo de grupos, e_1 e e_2 elementos neutros de G_1 e G_2, respectivamente. Valem as seguintes propriedades:*

i) $\varphi(e_1) = e_2$;

ii) $\varphi(x^{-1}) = \varphi(x)^{-1}$;

iii) $\varphi(x^n) = \varphi(x)^n$ *para todo* $n \in \mathbb{Z}$;

iv) O conjunto $\varphi(H_1) = \{\varphi(x) \in G_2 \mid x \in H_1\}$ *é um subgrupo de* G_2, *onde* H_1 *é um subgrupo de* G_1. *Em particular,* $\varphi(G_1)$ *é subgrupo de* G_2.

v) O conjunto $\varphi^{-1}(H_2) = \{x \in G_1 \mid \varphi(x) \in H_2\}$ *é um subgrupo de* G_1, *onde* H_2 *é um subgrupo de* G_2. *Em particular* $Ker\varphi = \varphi^{-1}\{e_2\}$ *é um subgrupo de* G_1.

Prova.

i) $\varphi(e_1) = \varphi(e_1e_1) = \varphi(e_1)\varphi(e_1) \Rightarrow \varphi(e_1)\varphi(e_1)^{-1} = (\varphi(e_1)\varphi(e_1))\varphi(e_1)^{-1} \Rightarrow e_2 = \varphi(e_1)$.

ii) $e_2 = \varphi(e_1) = \varphi(xx^{-1}) = \varphi(x)\varphi(x^{-1}) \Rightarrow \varphi(x)^{-1} = \varphi(x^{-1})$.

iii) Para $n = 0$,

$$\varphi(x)^0 = e_2 = \varphi(e_1) = \varphi(x^0).$$

Para $n \in \mathbb{N}_0$ provemos por indução. Se $n = 1$, então de fato temos $\varphi(x^1) = \varphi(x) = \varphi(x)^1$. Supondo verdade para $n = k \geqslant 1$, ou seja, $\varphi(x^k) = \varphi(x)^k$, temos

$$\varphi(x^{k+1}) = \varphi(x^k x) = \varphi(x^k)\varphi(x) = \varphi(x)^k\varphi(x) = \varphi(x)^{k+1}.$$

Se $n \in \mathbb{Z}^*_-$, então $-n \in \mathbb{N}_0$ e daí $\varphi(y^{-n}) = \varphi(y)^{-n}$. Assim

$$\varphi(x^n) := \varphi((x^{-1})^{-n}) = \varphi(x^{-1})^{-n} = (\varphi(x)^{-1})^{-n} := \varphi(x)^n.$$

iv) $\varphi(H_1) \subseteq G_2$ é não vazio já que $e_1 \in H_1$ e pelo item *i)* temos $e_2 = \varphi(e_1) \in \varphi(H_1)$. Tomando $y_1, y_2 \in \varphi(H_1)$, existem $x_1, x_2 \in H_1$ tais que $\varphi(x_1) = y_1$ e $\varphi(x_2) = y_2$ e daí pelo item *ii)* temos $\varphi(x_2^{-1}) = y_2^{-1}$. Como H_1 é subgrupo, então $x_1x_2^{-1} \in H_1$ e portanto $y_1y_2^{-1} = \varphi(x_1)\varphi(x_2^{-1}) = \varphi(x_1x_2^{-1}) \in \varphi(H_1)$.

v) Pelo item *i*) temos que $\varphi^{-1}(H_2) \neq \emptyset$, visto que $\varphi(e_1) = e_2 \in H_2$. Tomando $x, y \in \varphi^{-1}(H_2)$, então existem $s, t \in H_2$ tais que $\varphi(x) = s$ e $\varphi(y) = t$. Como H_2 é subgrupo, então $st^{-1} \in H_2$, daí

$$\varphi(xy^{-1}) = \varphi(x)\varphi(y)^{-1} = st^{-1} \in H_2$$

ou seja, $xy^{-1} \in \varphi^{-1}(H_2)$.

■

Definição 1.13 *Sejam G_1 e G_2 grupos. Dizemos que G_1 é isomorfo a G_2 caso exista um homomorfismo de grupos $\varphi : G_1 \to G_2$ bijetor, e denotamos $G_1 \simeq G_2$.*

Observação 1.6 *Dois grupos isomorfos têm as mesmas características algébricas, a estrutura é basicamente a mesma, a diferença é apenas os elementos. Vejamos um exemplo que ilustra bem isso. Considere os grupos $(\mathbb{R}^2, +)$, $(M_{2\times 1}(\mathbb{R}), +)$ e a aplicação:*

$$\begin{aligned} \varphi : \mathbb{R}^2 &\to M_{2\times 1}(\mathbb{R}) \\ (x, y) &\mapsto \varphi(x, y) = \begin{pmatrix} x \\ y \end{pmatrix}. \end{aligned}$$

Note que φ é claramente um isomorfismo, a soma $(a, b) + (x, y) = (a + x, b + y)$ corresponde à soma $\begin{pmatrix} a \\ b \end{pmatrix} + \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} a+x \\ b+y \end{pmatrix}$ e a estrutura algébrica é a mesma, existindo apenas uma diferença na forma de representar os pares de números reais. Então as vezes, por conveniência, identificamos grupos isomorfos como sendo o mesmo grupo.

Caso um homomorfismo de grupos $\varphi : G_1 \to G_2$ seja injetivo, comumente chamado de mergulho ou monomorfismo, então G_1 é isomorfo a $\varphi(G_1)$, e daí vemos o subgrupo $\varphi(G_1)$ como sendo uma "cópia" de G_1 dentro de G_2.

1.5 Produto direto de grupos

Uma pergunta natural de ocorrer quando se tem um grupo G é se existe um algum grupo G' tal que G seja subgrupo de G'. A resposta para essa pergunta é positiva,

e ainda mais, dados dois grupos G_1 e G_2, existe um grupo G tal que G_1 e G_2 são subgrupos de G, por mais distintas que sejam as operações de G_1 e G_2.

Definição 1.14 *Sejam G_1 e G_2 grupos. Considere o conjunto*

$$G_1 \times G_2 = \{(s_1, s_2) \mid s_1 \in G_1, s_2 \in G_2\}$$

vamos a definir a seguinte operação em $G_1 \times G_2$:

$$(s_1, s_2)(t_1, t_2) = (s_1 t_1, s_2 t_2).$$

Com esta operação, $G_1 \times G_2$ é um grupo, chamado produto direto dos grupos G_1 e G_2.

As justaposições no lado direito da igualdade acima representam as operações de G_1 e G_2 respectivamente. Se g_1 e g_2 forem as ordens de G_1 e G_2 respectivamente, então a ordem de $G_1 \times G_2$ é $g = g_1 g_2$. Ademais sendo e_1 e e_2 os elementos neutros de G_1 e G_2 respectivamente, então $e = (e_1, e_2)$ é o elemento neutro de $G_1 \times G_2$.

É comum identificar o subgrupo $G_1 \times \{e_2\} = \{(s, e_2) \mid s \in G_1\}$ de $G_1 \times G_2$ como sendo o grupo G_1. Note que a aplicação $\psi_1 : G_1 \to \{(s, e_2) \mid s \in G_1\}$, dada por $\psi_1(s) = (s, e_2)$, é um isomorfismo de grupos. De forma similar identificamos G_2 com $\{e_1\} \times G_2 = \{(e_1, t) \mid t \in G_2\}$.

Com essas identificações temos que cada elemento $s \in G_1 \times G_2$ é escrito de forma única como $s = s_1 s_2$, com $s_1 \in G_1$ e $s_2 \in G_2$. Ademais, os elementos de G_1 comutam com os de G_2.

Reciprocamente, se G é um grupo contendo G_1 e G_2 como subgrupos, suponha que as seguintes condições são satisfeitas:

i) Cada $s \in G$ pode ser escrito de forma única como $s = s_1 s_2$, com $s_1 \in G_1$ e $s_2 \in G_2$;

ii) Para todos $s_1 \in G_1$ e $s_2 \in G_2$ temos $s_1 s_2 = s_2 s_1$.

O produto de dois elementos $s = s_1 s_2$, $t = t_1 t_2 \in G$, onde $s_1, t_1 \in G_1$ e $s_2, t_2 \in G_2$, pode ser escrito como:

$$st = s_1 s_2 t_1 t_2 = (s_1 t_1)(s_2 t_2).$$

Tomando então a aplicação $\varphi(s) = \varphi(s_1 s_2) = (s_1, s_2)$ de G em $G_1 \times G_2$, temos um isomorfismo de grupos. De fato:

$$\varphi(s)\varphi(t) = (s_1, s_2)(t_1, t_2) = (s_1 t_1, s_2 t_2) = \varphi(st).$$

Dado $y = (s_1, s_2) \in G_1 \times G_2$, tomemos $x = s_1 s_2 \in G$, e desse modo $\varphi(x) = y$.

Supondo que $s, t \in G$ são tais que $\varphi(s) = \varphi(t)$, então $(s_1, s_2) = (t_1, t_2)$, donde $s_1 = t_1$ e $s_2 = t_2$, ou seja, $s = t$.

Neste caso dizemos que G é o produto direto de seus subgrupos G_1 e G_2 e identificamos G como sendo $G_1 \times G_2$.

Observação 1.7 *Sejam $(G_1, *_1), (G_2, *_2), \ldots, (G_n, *_n)$ grupos. Definimos o produto direto deles $(G_1 \times G_2 \times \cdots \times G_n, *)$ de forma análoga:*

$$(s_1, s_2, \ldots, s_n) * (t_1, t_2, \ldots, t_n) = (s_1 *_1 t_1, s_2 *_2 t_2, \ldots, s_n *_n t_n)$$

onde $(s_1, s_2, \ldots, s_n), (t_1, t_2, \ldots, t_n) \in G_1 \times G_2 \times \cdots \times G_n$.

Exemplo 6

i) Considerando o grupo multiplicativo $C_2 = \{1, -1\}$, o produto direto $K = C_2 \times C_2$ é chamado de grupo de Klein. Denotando $e = (1, 1), a = (1, -1), b = (-1, 1)$ e $c = (-1, -1)$, temos $ex = xe = x$ para todo $x \in K$, e ainda temos as relações:

$$ab = ba = c \qquad ac = ca = b \qquad bc = cb = a \qquad a^2 = b^2 = c^2 = e$$

Note que K não é isomorfo a $C_4 = \{1, -1, i, -i\}$, pois dado um homomorfismo $\varphi : K \to C_4$, como $x^2 = e$ para todo $x \in K$, então

$$(\varphi(x))^2 = \varphi(x^2) = \varphi(e) = 1$$

e daí $\varphi(x) = \pm 1$ para qualquer $x \in K$. Portanto φ não pode ser sobrejetora e consequentemente não pode ser bijetora.

1.5.1 Estendendo ações e homomorfismos de G_1 e G_2 para o produto direto $G_1 \times G_2$

Suponha que G_1 e G_2 são grupos, sejam X_1 e X_2 conjuntos não vazios, $\theta_1 : G_1 \times X_1 \to X_1$ e $\theta_2 : G_2 \times X_2 \to X_2$ ações de grupos. Tomando o grupo $G = G_1 \times G_2$ e o conjunto $X = X_1 \times X_2$, podemos definir uma ação θ de G em X da seguinte forma

$$\begin{aligned} \theta : G \times X &\to X \\ ((s_1, s_2), (x_1, x_2)) &\mapsto \theta((s_1, s_2), (x_1, x_2)) = (\theta_1(s_1, x_1), \theta_2(s_2, x_2)) \end{aligned}$$

(i) Sendo $e = (e_1, e_2) \in G$ e $x = (x_1, x_2) \in X$ qualquer, temos:

$$\theta(e, x) = (\theta_1(e_1, x_1), \theta_2(e_2, x_2)) = (x_1, x_2) = x.$$

(ii) Dados $s = (s_1, s_2), t = (t_1, t_2) \in G$, $x = (x_1, x_2) \in X$, arbitrários, (para não sobrecarregar os índices, usemos a notação " $\cdot$ " para θ, θ_1 e θ_2) temos:

$$\begin{aligned} s \cdot (t \cdot x) &= (s_1, s_2) \cdot [(t_1, t_2) \cdot (x_1, x_2)] \\ &= (s_1, s_2) \cdot (t_1 \cdot x_1, t_2 \cdot x_2) \\ &= (s_1 \cdot [t_1 \cdot x_1], s_2 \cdot [t_2 \cdot x_2]) \\ &= ([s_1 t_1] \cdot x_1, [s_2 t_2] \cdot x_2) \\ &= (st) \cdot x \end{aligned}$$

Portanto θ é de fato uma ação de G em X.

Podemos também relacionar produto direto com homomorfismos. Sejam G_1, G_2, H_1, H_2 grupos, $\varphi_1 : G_1 \to H_1$ e $\varphi_2 : G_2 \to H_2$ homomorfismos de grupos. Então

$$\begin{aligned} \varphi : G_1 \times G_2 &\to H_1 \times H_2 \\ (s_1, s_2) &\mapsto \varphi(s_1, s_2) = (\varphi_1(s_1), \varphi_2(s_2)) \end{aligned}$$

é um homomorfismo de grupos, pois dados $s = (s_1, s_2), t = (t_1, t_2) \in G_1 \times G_2$ temos:

$$\begin{aligned} \varphi(s_1 t_1, s_2 t_2) &= (\varphi_1(s_1 t_1), \varphi_2(s_2 t_2)) \\ &= (\varphi_1(s_1)\varphi_1(t_1), \varphi_2(s_2)\varphi_2(t_2)) \\ &= (\varphi_1(s_1), \varphi_2(s_2))(\varphi_1(t_1), \varphi_2(t_2)). \end{aligned}$$

Portanto $\varphi(st) = \varphi(s)\varphi(t)$, ou seja, de fato φ é um homomorfismo de grupos. Ademais, se φ_1 e φ_2 forem bijetoras, então φ também será e isso justifica o seguinte resultado

Proposição 1.15 *Se G_1, G_2, H_1 e H_2 são grupos tais que $G_1 \simeq H_1$ e $G_2 \simeq H_2$, então $G_1 \times G_2 \simeq H_1 \times H_2$.*

Essas ideias serão úteis para o objetivo desse trabalho.

1.5.2 Grupos cíclicos e decomposição de grupos abelianos finitos em produto direto de grupos cíclicos

Os grupos cíclicos são uma classe de grupos que têm uma estrutura bem simples. Podemos decompor grupos abelianos finitos em produto direto de grupos cíclicos, o que é muito útil como vimos na seção anterior, pois podemos estender ações e homomorfismos se soubermos o comportamento das aplicações nos fatores da decomposição.

Definição 1.16 *Dizemos que G é um grupo cíclico se existe algum elemento $\gamma \in G$ tal que*

$$\{\gamma^n \mid n \in \mathbb{Z}\} = G$$

ou seja, o subgrupo gerado por γ é G.

Definição 1.17 *Definimos a ordem $o(s)$ de $s \in G$ como sendo a ordem do subgrupo gerado por s, caso seja finito. Caso o subgrupo gerado por s seja infinto, pomos $o(s) = \infty$.*

Exemplo 7 *Exemplos de grupos que são e que não são cíclicos.*

i) O grupo $G = \{e\}$ com apenas um elemento é cíclico. Ademais $o(e) = 1$.

*ii) Para todo inteiro positivo n, temos que o grupo multiplicativo C_n das raízes n-ésimas complexas da unidade é cíclico. Basta notar que $\omega = e^{\frac{2\pi}{n}i}$ gera C_n, como foi visto no item iii) do **Exemplo 1**. Ademais temos $o(\omega) = n$. Consequentemente, existem grupos cíclicos finitos de todas as ordens.*

iii) *O grupo aditivo $\mathbb{Z}$ dos inteiros é cíclico, afinal, lembrando que estamos em notação aditiva, temos $n1 = n$ para qualquer $n \in \mathbb{Z}$. Logo o elemento 1 gera $\mathbb{Z}$ como grupo e $o(1) = \infty$.*

iv) *O grupo aditivo dos reais $\mathbb{R}$ não é cíclico, pois caso contrário, existindo um número real r tal que*

$$\{nr \mid n \in \mathbb{Z}\} = \mathbb{R}$$

então a função

$$f : \mathbb{Z} \to \mathbb{R}$$
$$n \mapsto f(n) = nr$$

seria sobrejetiva, o que é um absurdo, pois a não enumerabilidade dos reais é um resultado que nos diz que não existem funções de $\mathbb{Z}$ em $\mathbb{R}$ sobrejetivas.
Igualmente para qualquer grupo G, onde G é um conjunto não enumerável temos que G não pode ser um grupo cíclico. Em particular, para $n \geq 2$ inteiro e $\mathbb{X} = \mathbb{R}$ ou $\mathbb{X} = \mathbb{C}$, ***não são cíclicos*** *os grupos: $(\mathbb{X}, +), (\mathbb{X}^*, \cdot), (M_{m\times n}(\mathbb{X}), +), (Gl_n(\mathbb{X}), \cdot)$, $(Sl_n(\mathbb{X}), \cdot)$.*

v) *Sendo G um grupo finito com $\mid G \mid = p$, onde p é um número primo, então G é cíclico. De fato, desde que $\mid G \mid \geq 2$, podemos tomar algum elemento γ em G que não seja o elemento neutro. Tomemos então o subgrupo gerado por γ*

$$H = \{\gamma^n \mid n \in \mathbb{Z}\}.$$

Como G é finito, então H também é. Ademais como $\{e, \gamma\} \subseteq H$, então $\mid H \mid > 1$. Usando agora o Teorema de Lagrange, temos que $\mid H \mid$ divide $\mid G \mid = p$ e pelo fato de que p é primo e $\mid H \mid > 1$, temos $\mid H \mid = p$. Concluindo que $H = G$. Portanto G é cíclico e pode ser gerado por qualquer elemento que não seja o neutro.

vi) *O produto direto $G = \mathbb{Z} \times \mathbb{Z}$ do grupo aditivo $\mathbb{Z}$* ***não*** *é cíclico. De fato, suponha que exista $(a, b) \in G$ tal que $G = \{n(a, b) \mid n \in \mathbb{Z}\}$. Então em particular, devem existir inteiros não nulos m e k tais que*

$$(1, 0) = m(a, b) \qquad (0, 1) = k(a, b)$$

donde devemos ter $a = b = 0$ e portanto $G = \{(0, 0)\}$. Absurdo.

Em verdade todo grupo cíclico ou é isomorfo a C_n, para algum inteiro positivo n, ou é isomorfo a $\mathbb{Z}$, fato esse que veremos mais adiante.

Proposição 1.18 *Seja G um grupo. Se $s \in G$ tem ordem finita, então $o(s)$ é o menor número m tal que $s^m = e$. Ademais $s^m = e$ se, e somente se, $o(s)$ divide m. Caso $o(s) = \infty$, então $s^m = e$ se, e somente se, $m = 0$.*

Prova. Supondo que $o(s)$ seja finita, então o subgrupo $H = \{s^n \mid n \in \mathbb{Z}\}$ é finito. Sendo assim a função

$$\begin{aligned} \varphi_s : \mathbb{Z} &\to H \\ n &\mapsto \varphi_s(n) = s^n \end{aligned}$$

não pode ser injetiva, pois caso contrário teríamos H infinito, donde devem existir $n_1, n_2 \in \mathbb{Z}$ com $n_1 > n_2$ e $\varphi_s(n_1) = \varphi_s(n_2)$, ou seja,

$$s^{n_1} = s^{n_2} \Rightarrow s^{n_1 - n_2} = e.$$

Como $n_1 - n_2 > 0$, então o conjunto $\{n \in \mathbb{N}^* \mid s^n = e\}$ é não vazio, e pelo Principio da Boa Ordenação deve ter um elemento mínimo, digamos que k é tal elemento. Mostremos que

$$\{e, s, s^2, \ldots, s^{k-2}, s^{k-1}\} = H.$$

Pela definição de H temos $\{e, s, s^2, \ldots, s^{k-2}, s^{k-1}\} \subseteq H$. Tomando $x \in H$ arbitrário, então existe $n \in \mathbb{Z}$ tal que $x = s^n$. Pelo algorítimo da divisão dos inteiros, existem $q, r \in \mathbb{Z}$, unicamente determinados com $0 \leq r \leq k-1$, tais que $n = qk + r$, donde

$$x = s^n = s^{qk+r} = (s^k)^q s^r = e^q s^r = s^r \in \{e, s, s^2, \ldots, s^{k-2}, s^{k-1}\}$$

concluindo que $\{e, s, s^2, \ldots, s^{k-2}, s^{k-1}\} = H$.

Mostremos agora que em $\{e, s, s^2, \ldots, s^{k-2}, s^{k-1}\}$ não há repetição de elementos e daí $\mid \{e, s, s^2, \ldots, s^{k-2}, s^{k-1}\} \mid = k$. Suponha que $n_1, n_2 \in \mathbb{Z}$, com $0 \leq n_1 < n_2 \leq k-1$, sejam tais que $s^{n_1} = s^{n_2}$. Então $n_2 - n_1 \in \{e, s, s^2, \ldots, s^{k-2}, s^{k-1}\}$, mas $1 \leq n_2 - n_1 < k$, o que contraria a minimalidade de k. Consequentemente

$$o(s) = \mid H \mid = k = min\{n \in \mathbb{N}^* \mid s^n = e\}.$$

Tomando agora $m \in \mathbb{Z}$ tal que $s^m = e$, e dividindo m por $k = o(s)$, então existem $q, r \in \mathbb{Z}$, com $0 \leq r < k$, tais que $m = qk + r$. Suponha por absurdo que k não divida m, ou seja $r > 0$. Daí

$$e = s^m = s^{qk+r} = (s^k)^q s^r = e^q s^r = s^r$$

donde $r \in \{n \in \mathbb{N}^* \mid s^n = e\}$, mas $r < k = min\{n \in \mathbb{N}^* \mid s^n = e\}$, absurdo. Portanto k divide m. Reciprocamente, se $o(s) = k$ divide m, então existe $q \in \mathbb{Z}$ tal que $m = qk$ e daí $s^m = s^{qk} = (s^k)^q = e^q = e$.

Para o caso em que $o(s) = \infty$, supondo por absurdo que exista $m \neq 0$ tal que $s^m = e$, então note que $s^{-m} = (s^m)^{-1} = e^{-1} = e$. Como m ou $-m$ é positivo, temos que o conjunto $\{n \in \mathbb{N}^* \mid s^n = e\}$ é não vazio e portanto possui algum elemento mínimo k, donde

$$\{e, s, s^2, \ldots, s^{k-2}, s^{k-1}\} = \{s^n \mid n \in \mathbb{Z}\}$$

e assim $o(s)$ seria finito, absurdo. ■

Corolário 1.19 *Seja G um grupo finito de elemento neutro e. Dado $s \in G$, então*

$$s^{|G|} = e.$$

Prova. Dado $s \in G$ arbitrário, seja H o subgrupo gerado por s. Pelo Teorema de Lagrange temos que $o(s) =\mid H \mid$ divide $\mid G \mid$. Então pelo teorema anterior temos que

$$s^{|G|} = e$$

como queríamos demonstrar. ■

Veremos a seguir todos os grupos cíclicos a menos de isomorfismo.

Proposição 1.20 *Seja G um grupo cíclico gerado por γ. Então*

i) *G é abeliano.*

ii) *A aplicação $n \mapsto \gamma^n$ de $\mathbb{Z}$ em G é um homomorfismo de grupos sobrejetor.*

iii) *Suponha que G é finito com $\mid G \mid = k$. Dado um grupo H cíclico com $\mid H \mid = k$, então G é isomorfo a H. Consequentemente, todo grupo cíclico de ordem n é isomorfo ao grupo multiplicativo C_n.*

iv) Suponha que G é infinito. Dado um grupo H cíclico infinito, então G é isomorfo a H. Consequentemente, todo grupo cíclico infinito é isomorfo ao grupo aditivo $\mathbb{Z}$.

Prova.

i) Dados $s, t \in G$ arbitrários, existem $m, n \in \mathbb{Z}$ tais que $s = \gamma^n$ e $t = \gamma^m$, daí

$$st = \gamma^n\gamma^m = \gamma^{n+m} = \gamma^{m+n} = \gamma^m\gamma^n = ts.$$

ii) Sendo φ_γ tal aplicação, claramente φ_γ é sobrejetiva. Dados $m, n \in \mathbb{Z}$, temos:

$$\varphi_\gamma(n+m) = \gamma^{n+m} = \gamma^n\gamma^m = \varphi_\gamma(n)\varphi_\gamma(m).$$

iii) Sendo H cíclico, existe $\alpha \in H$ que gera H. Pela demonstração da **Proposição 1.18**, dado $x \in G$ existe um único inteiro m_x com $0 \leq m_x < k$ tal que $x = \gamma^{m_x}$. Fica então bem definida a aplicação

$$\begin{aligned} \varphi : G &\to H \\ x \mapsto \varphi(x) &= \varphi(\gamma^{m_x}) = \alpha^{m_x} \end{aligned}$$

Dados $x, y \in G$, seja r o resto da divisão de m_x+m_y por k. Então $m_x+m_y = qk+r$ para inteiros q, r, com $0 \leq r < k$. Daí

$$xy = \gamma^{m_x}\gamma^{m_y} = \gamma^{m_x+m_y} = \gamma^{qk+r} = (\gamma^k)^q\gamma^r = \gamma^r$$

ou seja, $r = m_{xy}$. Ademais

$$\alpha^{m_x+m_y} = \alpha^{qk+r} = \alpha^r = \alpha^{m_{xy}}$$

e portanto

$$\varphi(xy) = \varphi(\gamma^{m_x+m_y}) = \varphi(\gamma^{m_{xy}}) = \alpha^{m_{xy}} = \alpha^{m_x+m_y} = \alpha^{m_x}\alpha^{m_y} = \varphi(x)\varphi(y).$$

Logo φ é um homomorfismo de grupos. É fácil ver que φ é sobrejetivo, e daí, como G e H são conjuntos finitos de mesma ordem, então segue que φ é bijetora, concluindo que φ é um isomorfismo de grupos.

iv) Pela **Proposição 1.18**, caso $o(s) = \infty$, temos:

$$s^n = s^m \iff s^{n-m} = e \iff n - m = 0 \iff n = m.$$

Portanto dado $x \in G$ existe um único inteiro m_x tal que $x = \gamma^{m_x}$. Podemos então reescrever G como sendo $G = \{\gamma^{m_x} \mid x \in G\}$, onde para $x, y \in G$ temos:

$$m_x = m_y \iff x = y$$

Sendo α o elemento que gera H, fica bem definida a aplicação

$$\begin{aligned} \varphi : G &\to H \\ \gamma^{m_x} &\mapsto \varphi(\gamma^{m_x}) = \alpha^{m_x} \end{aligned}$$

e temos que φ é um homomorfismo sobrejetivo de grupos. Basta mostrarmos que φ é injetiva. Tomando $x, y \in G$ tais que $\varphi(x) = \varphi(y)$, então

$$\varphi(x) = \varphi(y) \Longrightarrow \alpha^{m_x - m_y} = \alpha^0 \Longrightarrow m_x = m_y \Longrightarrow x = y.$$

■

Proposição 1.21 *Seja G um grupo abeliano finito. Então G é isomorfo a um produto direto de grupos cíclicos cujas ordens são potências de primos.*

Prova. Uma demonstração pode ser encontrada na página 93 de [7], Proposição III.4.6.

■

1.6 Grupos simétricos e alternados

Uma classe de grupos muito importante são os grupos de permutações, ou grupos simétricos, que de certa forma representam todos os grupos. Associado aos seus elementos tem o que chamamos de *sinal* da permutação, que tem relação com o que veremos no Capítulo 2. Vejamos então a sua definição, mas antes relembremos alguns resultados sobre funções bijetoras de um conjunto em si mesmo.

Observação 1.8 *Sejam X um conjunto não vazio, $f : X \to X$, $g : X \to X$ e $h : X \to X$ funções bijetoras quaisquer. Da teoria clássica de funções temos:*

(i) $f \circ g : X \to X$ *ainda é uma bijeção.*

(ii) f *é inversível com inversa* $f^{-1} : X \to X$.

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

(iv) a bijeção $Id : X \to X$, *dada por* $Id(x) = x$ *para todo* $x \in X$, *é tal que* $Id \circ g = g \circ Id = g$ *e* $f \circ f^{-1} = f^{-1} \circ f = Id$.

1.6.1 Grupos simétricos

Definição 1.22 *Seja* X *um conjunto não vazio. Considerando o conjunto* S_X *formado pelas funções bijetoras de* X *em* X, *temos que* S_X, *munido da composição usual de funções, é um grupo. Chamamos tal grupo de Grupo Simétrico sobre* X.

Observação 1.9 *Se* X *é finito e tem* n *elementos, digamos* $X = \{x_1, x_2, \ldots, x_n\}$, *para construir uma bijeção* $f : X \to X$ *(ou permutação), inicialmente, para escolher a imagem do elemento* x_1, *temos* n *opções, a saber qualquer, elemento de* $X = \{x_1, x_2, \ldots, x_n\}$. *Após escolher a imagem, digamos* $f(x_1) = x_{i_1}$, *para escolher a imagem de* x_2 *temos agora apenas* $n-1$ *possibilidades, a saber,* $\{x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n\}$, *pois para que* f *seja injetiva não podemos escolher o* $x_{i_1} = f(x_1)$ *para ser imagem de* x_2. *Em seguida para escolher a imagem do* x_3 *temos agora apenas* $n-3$ *escolhas. Seguindo esse raciocínio, usando o principio multiplicativo fundamental da contagem, temos* $n! = n \cdot (n-1) \cdot \ldots \cdot 3 \cdot 2 \cdot 1$ *possibilidades de construção para a função* f, *donde temos que* $\mid S_X \mid = n!$.

Observação 1.10 *Sendo* n *um inteiro positivo, quando temos* $X = I_n = \{1, 2, ..., n\}$ *denotamos* S_{I_n} *apenas por* S_n. *Cada elemento* $\sigma \in S_n$ *é representado da seguinte forma*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n-1 & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n-1) & \sigma(n) \end{pmatrix}.$$

Por exemplo, considere em S_4 *a permutação que satisfaz* $\sigma(1) = 4$, $\sigma(2) = 2$, $\sigma(3) = 1$ *e* $\sigma(4) = 3$. *Temos*

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

Com essa notação, dados $\sigma, \phi \in S_n$ temos:

$$\sigma \circ \phi = \sigma\phi = \begin{pmatrix} 1 & 2 & 3 & \cdots & n-1 & n \\ \sigma(\phi(1)) & \sigma(\phi(2)) & \sigma(\phi(3)) & \cdots & \sigma(\phi(n-1)) & \sigma(\phi(n)) \end{pmatrix}.$$

Por exemplo:

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

Observação 1.11 *Sendo G um grupo e X um conjunto não vazio, há uma estreita relação entre as ações de G em X e os homomorfismo de G em S_X.*

Suponha que $\varphi : G \to S_X$ seja um homomorfismo de grupos. Então pelo item i) da ***Proposição 1.12****, temos $\varphi(e) = Id$, onde e é o elemento neutro de G e Id é a permutação identidade. Ademais para $s \in G$, denotando $\varphi_s := \varphi(s)$, temos que φ_s é uma permutação em X, e sendo $s, t \in G$ temos $\varphi_s \circ \varphi_t = \varphi_{st}$.*

Definamos a aplicação

$$\begin{aligned} \theta : G \times X &\to X \\ (s, x) &\mapsto \theta(s, x) = s \cdot x := \varphi_s(x) \end{aligned}$$

Temos:

(i) $e \cdot x = \varphi_e(x) = Id(x) = x$ *para todo* $x \in X$*;*

(ii) $s \cdot (t \cdot x) = \varphi_s(\varphi_t(x)) = (\varphi_s \circ \varphi_t)(x) = \varphi_{st}(x) = (st) \cdot x$ *para quaisquer* $s, t \in G$ *e* $x \in X$*;*

donde concluímos que θ é uma ação de G em X.

Reciprocamente, suponha que $\theta : G \times X \to X$, $\theta(s, x) = s \cdot x$, seja uma ação de G em X. Fixando $s \in G$, definamos a função $\varphi_s : X \to X$ dada por $\varphi_s(x) = s \cdot x$. Mostremos que φ_s é bijetora. Inicialmente, mostremos a sobrejetividade. De fato, dado

$y \in X$, considerando os elemento $s^{-1} \cdot y \in X$, então $\varphi_s(s^{-1} \cdot y) = s \cdot (s^{-1} \cdot y) = e \cdot y = y$. Logo φ_s é sobrejetiva. Supondo agora que $x, y \in X$ são tais que $\varphi_s(x) = \varphi_s(y)$, temos:

$$\varphi_s(x) = \varphi_s(y) \Rightarrow s \cdot x = s \cdot y \Rightarrow s^{-1} \cdot (s \cdot x) = s^{-1} \cdot (s \cdot y) \Rightarrow e \cdot x = e \cdot y \Rightarrow x = y$$

ou seja, φ_s é injetiva, e daí $\varphi_s \in S_X$. Tomando $t \in G$, considerando as funções $\varphi_t, \varphi_{st} \in S_X$ dadas por $\varphi_t(x) = t \cdot x$ e $\varphi_{st}(x) = (st) \cdot x$, temos:

$$\varphi_{st}(x) = (st) \cdot x = s \cdot (t \cdot x) = \varphi_s(\varphi_t(x)) = (\varphi_s \circ \varphi_t)(x)$$

ou seja, $\varphi_{st} = \varphi_s \varphi_t$, e portanto a aplicação

$$\begin{aligned} \varphi : G &\to S_X \\ s &\mapsto \varphi(s) = \varphi_s \end{aligned}$$

é um homomorfismo de grupos.

1.6.2 Sinal de permutação e grupo alternado

Uma característica muito importante dos elementos de S_n é a que vamos definir a seguir. Colocamos nesta subseção as definições e resultados como estão apresentadas em [1].

Definição 1.23 *Seja $I_n = \{1, 2, \ldots, n\}$, com $n \geq 2$, e seja $\mathcal{P}_2(n)$ o conjunto de todos os subconjuntos com dois elementos de I_n. Dado $\sigma \in S_n$, defina o sinal de σ como sendo*

$$sign(\sigma) = \prod_{\{i,j\} \in \mathcal{P}_2(n)} \frac{\sigma(j) - \sigma(i)}{j - i} = \prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i}$$

Observação 1.12 *Note que quando $\{i, j\}$ corre sobre todo o conjunto $\mathcal{P}_2(n)$, tem-se que $\{\sigma(i), \sigma(j)\}$ também corre sobre todo o conjunto $\mathcal{P}_2(n)$. Logo, $\prod_{1 \leq i < j \leq n} (\sigma(j) - \sigma(i))$ e $\prod_{1 \leq i < j \leq n} (j - i)$ têm exatamente os mesmos fatores, a menos de ordem e sinal, donde segue que $sign(\sigma) = \pm 1$.*

Isso separa as permutações em dois tipos, que definiremos agora.

Definição 1.24 *Dizemos que $\sigma \in S_n$ é uma permutação par se $sign(\sigma) = 1$, e que σ é ímpar se $sign(\sigma) = -1$.*

Exemplo 8 *São exemplos de permutações e sinais:*

i) $Id \in S_n$ *é par.*

ii) *Considere* $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \in S_3$. *Temos:*

$$sign(\sigma) = \frac{\sigma(2) - \sigma(1)}{2-1} \cdot \frac{\sigma(3) - \sigma(1)}{3-1} \cdot \frac{\sigma(3) - \sigma(2)}{3-2} = \frac{1 \cdot (-1) \cdot (-2)}{1 \cdot 2 \cdot 1} = 1$$

e assim σ é par.

iii) *Considere* $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n-1 & n \\ 2 & 1 & 3 & 4 & \ldots & n-1 & n \end{pmatrix} \in S_n$. *Temos que a expressão de $sign(\sigma)$ pode ser dada por*

$$\left(\frac{\sigma(2) - \sigma(1)}{2-1}\right) \left(\prod_{2<j\leq n} \frac{\sigma(j) - \sigma(1)}{j-1}\right) \left(\prod_{2<j\leq n} \frac{\sigma(j) - \sigma(2)}{j-2}\right) \left(\prod_{2<i<j\leq n} \frac{\sigma(j) - \sigma(i)}{j-i}\right)$$

Observe que se $\{i, j\} \cap \{1, 2\} = \emptyset$, então $\frac{\sigma(j) - \sigma(i)}{j-i} = \frac{j-i}{j-i} = 1$. Se $2 < j \leq n$, então $\sigma(j) = j > 2$ e daí

$$\frac{\sigma(j) - \sigma(1)}{j-1} = \frac{\sigma(j) - 2}{j-1} > 0 \qquad e \qquad \frac{\sigma(j) - \sigma(2)}{j-2} = \frac{\sigma(j) - 1}{j-2} > 0$$

Logo $sign(\sigma) = -1$ e portanto σ é ímpar.

Como $sign(\sigma)$ é sempre um elemento de $C_2 = \{1, -1\}$, é natural se perguntar se $sign : S_n \to C_2$ é um homomorfismo de grupos. A resposta é positiva.

Proposição 1.25 *Dado um inteiro positivo n, considerando o grupo S_n e o grupo multiplicativo $C_2 = \{1, -1\}$, temos que a aplicação*

$$\begin{aligned} sign : S_n &\to C_2 \\ \sigma &\mapsto sign(\sigma) \end{aligned}$$

é um homomorfismo de grupos.

Prova. Dados $\sigma, \psi \in S_n$, temos:

$$\begin{aligned} sign(\sigma\psi) &= \prod_{\{i,j\}\in\mathcal{P}_2(n)} \frac{(\sigma\psi)(j)-(\sigma\psi)(i)}{j-i} \\ &= \prod_{\{i,j\}\in\mathcal{P}_2(n)} \frac{\sigma(\psi(j))-\sigma(\psi(i))}{j-i} \cdot \frac{\psi(j)-\psi(i)}{\psi(j)-\psi(i)} \\ &= \left(\prod_{\{i,j\}\in\mathcal{P}_2(n)} \frac{\sigma(\psi(j))-\sigma(\psi(i))}{\psi(j)-\psi(i)}\right)\left(\prod_{\{i,j\}\in\mathcal{P}_2(n)} \frac{\psi(j)-\psi(i)}{j-i}\right) \end{aligned}$$

Quando $\{i,j\}$ corre sobre todo o conjunto $\mathcal{P}_2(n)$, observa-se que $\{\psi(i),\psi(j)\}$ também corre sobre todo o conjunto $\mathcal{P}_2(n)$. Logo

$$\prod_{\{i,j\}\in\mathcal{P}_2(n)} \frac{\sigma(\psi(j))-\sigma(\psi(i))}{\psi(j)-\psi(i)} = \prod_{\{i,j\}\in\mathcal{P}_2(n)} \frac{\sigma(j)-\sigma(i)}{j-i} = sing(\sigma)$$

e assim $sign(\sigma\psi) = sign(\sigma)sign(\psi)$. ■

Corolário 1.26 *O conjunto* $A_n = \{\sigma \in S_n \mid sign(\sigma) = 1\}$ *é um subgrupo de* S_n.

Prova. Note que $A_n = Ker(sign) = sign^{-1}(\{1\})$. Então pelo item v) da **Proposição 1.12**, segue que A_n é um subgrupo de S_n. ■

Definição 1.27 *O subgrupo* $A_n = \{\sigma \in S_n \mid sign(\sigma) = 1\}$ *é chamado de grupo alternado de grau* n.

Esse grupo tem $\frac{n!}{2}$ elementos.

Capítulo 2

Teoria de representações de grupos e caracteres

Adiante precisaremos do conceito de espaços vetoriais sobre o corpo $\mathbb{C}$ dos números complexos, que é a mesma definição de espaço vetorial real visto em qualquer disciplina de Álgebra Linear 1. A diferença é que os escalares usados agora são números complexos, em vez de números reais apenas. Os resultados gerais ainda são válidos. Para um leitor que queira se aprofundar em álgebra linear, como por exemplo o estudo sobre espaços vetoriais sobre outros corpos indicamos a referência [6]. A teoria aqui desenvolvida sobre representações lineares de grupos tem como referência [8]. Neste capítulo iniciamos uma breve discussão à respeito de operadores lineares sobre um espaço vetorial e sobre matrizes. Apresentamos a definição de representações lineares (juntamente com exemplos, em particular, a representação regular), soma direta e produto tensorial de representações, representações irredutíveis, caracter da representação, Lema de Schur, ortogonalidade e representações induzidas.

2.1 Representações lineares de um grupo

2.1.1 Espaços vetoriais complexos e seus grupos de automorfismos.

Definição 2.1 *Sejam V um conjunto não vazio e aplicações $+ : V \times V \to V$ e $\cdot : \mathbb{C} \times V \to V$ que satisfazem as propriedades: com respeito a $+$ temos:*

$A_1)$ $u + (v + w) = (u + v) + w \quad \forall u, v, w \in V$;

$A_2)$ $u + v = v + u \quad \forall u, v \in V$;

$A_3)$ $\exists 0 \in V$; $v + 0 = v \quad \forall v \in V$;

$A_4)$ $\forall v \in V$, $\exists\ (-v) \in V$; $v + (-v) = 0$.

Em respeito a $\cdot$:

$M_1)$ $z_1 \cdot (z_2 \cdot v) = (z_1 z_2) \cdot v \quad \forall z_1, z_2 \in \mathbb{C}; v \in V$;

$M_2)$ $(z_1 + z_2) \cdot v = z_1 \cdot v + z_2 \cdot v \quad \forall z_1, z_2 \in \mathbb{C}; v \in V$;

$M_3)$ $z \cdot (u + v) = z \cdot u + z \cdot v \quad \forall z \in \mathbb{C}; u, v \in V$;

$M_4)$ $1 \cdot v = v \quad \forall v \in V$.

Dizemos então que V é um espaço vetorial sobre o corpo dos números complexos.

Chamamos a operação " $\cdot$ " de *multiplicação por escalar*, e geralmente denotamos $z \cdot v$ apenas por zv, para $z \in \mathbb{C}$ e $v \in V$.

Observação 2.1 *A menos de menção contrária, os espaços vetoriais aqui tratados serão sempre sobre o corpo dos números complexos, e V denotará um espaço vetorial de dimensão finita. A definição de dimensão de um espaço vetorial sobre o corpo $\mathbb{C}$ é a mesma de espaços vetoriais reais, e valem as mesmas propriedades.*

Observação 2.2 *Lembrando que ligado a essa estrutura, há funções que chamamos de operadores lineares sobre V, que são funções $T : V \to V$ que satisfazem*

$$T(u+v) = T(u) + T(v) \qquad\qquad T(\lambda v) = \lambda v$$

para quaisquer $u, v \in V$ e $\lambda \in \mathbb{C}$. Essas duas igualdades são equivalentes a $T(\lambda v + u) = \lambda T(v) + T(u)$.

Dentre essas funções podemos destacar as que são bijetoras, que chamamos de automorfismos do espaço vetorial V. Tomemos então $GL(V)$ como sendo o conjunto dos operadores lineares bijetores sobre V.

Veja que se T e S são elementos de $GL(V)$, então da teoria clássica de funções temos que $T \circ S$ é bijetora. Ademais,

$$T \circ S(u+v) = T(S(u+v)) = T(S(u) + S(v)) = T \circ S(u) + T \circ S(v)$$

$$T \circ S(\lambda v) = T(S(\lambda v)) = T(\lambda S(v)) = \lambda T(S(v)) = \lambda T \circ S(v)$$

para quaisquer $u, v \in V$ e $\lambda \in \mathbb{C}$. Logo $T \circ S \in GL(V)$. Note que $Id_V \in GL(V)$, onde $Id_V(v) = v \ \forall v \in V$, e $Id_V \circ T = T \circ Id_V = T$. Provemos que T^{-1} é ainda um elemento de $GL(V)$.

Dados $\alpha, \beta \in V$, como T é sobrejetora, existem α' e β' em V tais que $\alpha = T(\alpha')$ e $\beta = T(\beta')$. Segue que $\alpha' = T^{-1}(\alpha)$ e $\beta' = T^{-1}(\beta)$, e daí, sendo λ um número complexo temos:

$$\begin{aligned} T^{-1}(\lambda\alpha + \beta) &= T^{-1}(\lambda T(\alpha') + T(\beta')) \\ &= T^{-1}(T(\lambda\alpha' + \beta')) \\ &= \lambda\alpha' + \beta' \\ &= \lambda T^{-1}(\alpha) + T^{-1}(\beta). \end{aligned}$$

Logo T^{-1} é um elemento de $GL(V)$ desde que T também seja. Portanto $(GL(V), \circ)$ é um grupo.

Os operadores lineares sobre o espaço V, com $dimV = n$, têm estreita relação com as matrizes quadradas de ordem n, em particular os operadores lineares inversíveis (bijetores) têm estreita relação com as matrizes inversíveis. Isso nos dá uma caracterização do grupo $GL(V)$.

Considerando o grupo multiplicativo $Gl_n(\mathbb{C})$, seja V um espaço vetorial de dimensão n. Fixando $\beta = \{\beta_1, \beta_2, ..., \beta_n\}$ uma base de V, para T em $GL(V)$ definimos a matriz $[T]_\beta = (a_{ij})_{n\times n}$, com a_{ij} definidos pelas equações

$$T(\beta_j) = \sum_{i=1}^{n} a_{ij}\beta_j = a_{1j}\beta_1 + a_{2j}\beta_2 + ... + a_{nj}\beta_n$$

para cada $j = 1, 2, ..., n$. Em outras palavras, a_{ij} é a i-ésima coordenada do vetor $T(\beta_j)$ na base β. Sabemos que $[T]_\beta$ é inversível desde que $T \in GL(V)$. Ademais temos $[T \circ S]_\beta = [T]_\beta[S]_\beta$, $[T^{-1}]_\beta = [T]_\beta^{-1}$, $[S]_\beta = [T]_\beta \Leftrightarrow S = T$, e dada $A \in Gl_n(\mathbb{C})$, existe $U \in GL(V)$ tal que $[U]_\beta = A$. Portanto a aplicação

$$\begin{aligned} \varphi : GL(V) &\to Gl_n(\mathbb{C}) \\ T &\mapsto \varphi(T) = [T]_\beta \end{aligned}$$

é um homomorfismo de grupos bijetor, logo $GL(V) \simeq Gl_n(\mathbb{C})$. Quando β for a base canônica, se houver, ou alguma base fixada, representaremos $[T]_\beta$ apenas por $[T]$.

O fato de que $GL(V) \simeq Gl_n(\mathbb{C})$ nos permite, quando conveniente, considerar os operadores lineares bijetores como matrizes inversíveis.

2.1.2 Representações lineares de grupos finitos

A teoria desenvolvida a respeito de operadores lineares é rica em resultados, e então, se pudermos aproximar um grupo G desses operadores lineares, poderemos utilizar esses resultados para poder extrair informações a respeito do grupo G. Isso motiva a definição adiante.

Definição 2.2 *Sejam G um grupo finito e V um espaço vetorial de dimensão finita, $dimV = n$. Então se $\rho : G \to GL(V)$ é um homomorfismo de grupos, dizemos que ρ é uma representação linear de G em V de grau n. Quando não houver risco de confusão diremos apenas que V é uma representação de G.*

Se $\rho : G \to GL(V)$ é uma representação de G, então para cada $s \in G$, temos um automorfismo $\rho(s)$ do espaço vetorial V. Em particular, pela **Proposição 1.12**, temos $\rho(e) = Id_V$. Por simplicidade de notação denotaremos $\rho_s := \rho(s)$. Fixada

$\beta = \{\beta_1, \ldots, \beta_n\}$ base de V, então temos a matriz $R_s = [\rho_s]_\beta = (r(s)_{ij})_{n\times n}$, e daí temos:

$$det(R_s) \neq 0 \qquad R_{st} = R_s R_t \qquad r(st)_{ij} = \sum_{k=1}^{n} r(s)_{ik} r(t)_{kj} \qquad \forall s, t \in G.$$

Reciprocamente, dadas matrizes $R_s = (r(s)_{ij})_{n\times n}$, $s \in G$, satisfazendo as identidades anteriores, então há uma representação ρ de G satisfazendo $[\rho(s)]_\beta = R_s$. Basta tomar $\rho(s) = T$, onde $[T]_\beta = R_s$, e daí temos uma representação em forma de matrizes.

Exemplo 9 *São exemplos de representações de grupos:*

i) Dados um grupo G finito e V um espaço vetorial, tomando $\rho_0 : G \to GL(V)$ definida por $\rho_0(s) = Id_V$ $\forall s \in G$, temos então que ρ_0 é uma representação de G em V. Chamamos tal representação de representação trivial.

ii) Seja $C_4 = \{1, -1, i, -i\}$ o grupo multiplicativo das raízes complexas da equação $x^4 - 1 = 0$. Definindo $\rho_s(x, y) = (x, sy)$ para cada $s \in C_4$, então $\rho : C_4 \to GL(\mathbb{C}^2)$, definida por $\rho(s) = \rho_s$, é uma representação de grau 2 de C_4 (pode ser verificado de forma direta que de fato é uma representação), que em representação matricial temos:

$$[\rho(1)] = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad [\rho(-1)] = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$
$$[\rho(i)] = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, \quad [\rho(-i)] = \begin{pmatrix} 1 & 0 \\ 0 & -i \end{pmatrix}.$$

iii) Seja $G = \{e, a, b, c\}$ o grupo de Klein ($ab = ba = c, ac = ca = b, bc = cb = a, a^2 = b^2 = c^2 = e$). Tomando $\rho_e(x, y) = (x, y)$, $\rho_a(x, y) = (-x, y)$, $\rho_b(x, y) = (x, -y)$ e $\rho_c(x, y) = (-x, -y)$, temos uma representação de grau 2 de G em $\mathbb{C}^2$ (também pode ser verificado de forma direta), que em forma matricial temos:

$$[\rho(e)] = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad [\rho(a)] = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix},$$
$$[\rho(b)] = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad [\rho(c)] = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Se tomássemos $\rho_e(z) = \rho_b(z) = z$ *e* $\rho_a(z) = \rho_c(z) = -z$ *para todo* $z \in \mathbb{C}$, *teríamos uma representação de grau 1 de* G *em* $\mathbb{C}$.

iv) Tomando o grupo aditivo $\mathbb{Z}_3 = \{\overline{0}, \overline{1}, \overline{2}\}$ *e* $\omega = e^{\frac{2\pi i}{3}} = -\frac{1}{2} + \frac{i\sqrt{3}}{2}$, *pondo* $\rho_{\overline{a}}(z) = \omega^a z$, $z \in \mathbb{C}$, *então temos uma representação de* $\mathbb{Z}_3$ *de grau 1, pois claramente* $\rho_{\overline{a}}$ *é linear e sendo* r *o resto da divisão de* $a+b$ *por 3, então temos* $\overline{a}+\overline{b} = \overline{a+b} = \overline{r}$ *e* $\omega^{a+b} = \omega^{3q+r} = \omega^{3q}\omega^r = \omega^r$ *para algum* $q \in \mathbb{Z}$, *donde* $\rho_{\overline{a}}(\rho_{\overline{b}}(z)) = \rho_{\overline{a}+\overline{b}}(z)$, *e tomando* $b = 3 - a$, *temos* $\rho_{\overline{a}}(\rho_{\overline{b}}(z)) = \rho_{\overline{b}}(\rho_{\overline{a}}(z)) = \rho_{\overline{0}}(z) = \omega^0 z = 1z = z$.

Tal exemplo pode ser generalizado para qualquer $\mathbb{Z}_n$, *pondo* $\omega = e^{\frac{2\pi i}{n}}$ *e* $\rho_{\overline{a}}(z) = \omega^a z$.

v) Considerando o grupo S_n, *então para cada* $\sigma \in S_n$, *definindo a transformação linear* $\rho_\sigma : \mathbb{C} \to \mathbb{C}$, *dada por* $\rho_\sigma(z) = sign(\sigma)z$, *temos que* $\rho : S_n \to GL(\mathbb{C})$ *dada por* $\rho(\sigma) = \rho_\sigma$, *é uma representação de* S_n, *afinal*

$$\rho_\sigma(\rho_\psi(z)) = sign(\sigma)sign(\psi)z = sign(\sigma\psi)z = \rho_{\sigma\psi}(z)$$

para quaisquer $\sigma, \psi \in S_n$ *e* $z \in \mathbb{C}$.

vi) Considerando o grupo aditivo $\mathbb{Z}$, *para cada* $n \in \mathbb{Z}$ *definamos o operador linear* ρ_n *do espaço vetorial* $\mathbb{C}^2$ *como sendo* $\rho_n(x, y) = (x + ny, y)$, *que em representação matricial é*

$$[\rho_n] = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}.$$

Como $det[\rho_n] = 1 \neq 0$, *temos que* $\rho_n \in GL(\mathbb{C}^2)$, *já que* $[\rho_n] \in Gl_2(\mathbb{C})$.

Note que dados $m, n \in \mathbb{Z}$ *temos:*

$$[\rho_n][\rho_m] = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & n+m \\ 0 & 1 \end{pmatrix} = [\rho_{n+m}].$$

Portanto se definirmos $\rho : \mathbb{Z} \to GL(\mathbb{C}^2)$ *como sendo* $\rho(n) = \rho_n$ *para todo* $n \in \mathbb{Z}$, *temos que* ρ *é uma representação de* $\mathbb{Z}$. *Como* $GL(\mathbb{C}^2) \simeq Gl_2(\mathbb{C})$, *poderíamos representar* ρ *diretamente como*

$$\rho : \mathbb{Z} \to Gl_2(\mathbb{C})$$
$$n \mapsto \rho(n) = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}.$$

Definição 2.3 *Sejam ρ e ρ' duas representações do mesmo grupo G em espaços vetoriais V e V', respectivamente. Dizemos que ρ e ρ' são isomorfas (ou similares) se existir um isomorfismo $\tau : V \to V'$ de espaços vetoriais satisfazendo a identidade:*

$$\tau \circ \rho(s) = \rho'(s) \circ \tau \qquad \forall s \in G.$$

Em outras palavras, sendo R_s e R'_s as representações matriciais de ρ e ρ', respectivamente, existe uma matriz inversível P satisfazendo

$$P \cdot R_s = R'_s \cdot P \quad \forall s \in G$$

ou equivalentemente, $R'_s = P \cdot R_s \cdot P^{-1}$, onde essa matriz P é a matriz da transformação τ, fixadas bases dos espaços. Este isomorfismo nos permite fazer a identificação de $x \in V$ por $\tau(x) \in V'$. Como V e V' têm a mesma dimensão, então ρ e ρ' têm o mesmo grau. Caso ρ e ρ' não sejam isomorfas, dizemos que elas são não isomorfas.

Observação 2.3 *Duas representações isomorfas admitem uma mesma representação matricial. De fato, suponha ρ e ρ' representações de G nas condições da definição anterior. Sendo $\beta = \{v_1, v_2, \cdots, v_n\}$ uma base de V, então $\beta' = \tau(\beta) = \{\tau(v_1), \tau(v_2), \cdots, \tau(v_n)\}$ é uma base de V'. Note que a coordenada j de $\tau(v_j)$ na base β' é 1 e as demais são 0, e daí a matriz P da transformação τ da base β para base β' é a matriz identidade $n \times n$. Logo*

$$R_s = R'_s \quad \forall s \in G.$$

Em particular, R_s e R'_s têm o mesmo traço (soma dos elementos da diagonal principal da matriz). A importância deste fato ficará clara mais adiante.

Um caso particular de representação de um grupo G que será importante para neste trabalho é o que vem a seguir.

2.2 Representação regular

Definição 2.4 *Seja $n =\mid G \mid$ a ordem de G. Tomando V com $dimV = n$ ($V = \mathbb{C}^n$, por exemplo) podemos indexar uma base de V usando G como o conjunto de índices,*

digamos que $\beta = \{v_t \in V;\ t \in G\} = (v_t)_{t\in G}$ *seja uma base indexada. Pelo teorema fundamental da álgebra linear, definindo a imagem dos vetores de uma base, então existe, e é única, a transformação linear que satisfaz as escolhas das imagens feitas. Para cada* $s \in G$*, definamos* ρ_s *na base* β *por*

$$\rho_s(v_t) = v_{st}. \tag{2.1}$$

A representação definida em (2.1) *é chamada de Representação Regular, e o grau desta representação é a ordem do grupo* G*.*

Note que dado um vetor $v_{t_0} \in \beta$, tomando $v_{s^{-1}t_0} \in \beta$ temos $\rho_s(v_{s^{-1}t_0}) = v_{t_0}$. Logo $\rho_s(\beta) = \beta$, e daí temos $\rho_s \in GL(V)$, pois leva uma base de V em uma base de V, fica então definida a representação $\rho : G \to GL(V)$ com $\rho(s) = \rho_s$.

Note que na situação da definição acima temos $v_s = \rho_s(v_e)$ para todo $s \in G$, donde as imagens de v_e formam uma base para V. Reciprocamente, seja W uma representação linear de G, digamos $\rho' : G \to GL(W)$, tal que haja um vetor $w \in W$ onde os vetores $(\rho'_s(w))_{s\in G}$ formem uma base para W. Então W é uma representação isomorfa a V. De fato, tomemos $\tau : V \to W$ definida em β por $\tau(v_s) = \rho'_s(w)$. Temos que τ leva base em base, logo é um isomorfismo de espaços vetoriais, e para $v_t \in \beta$ temos:

$$\tau(\rho_s(v_t)) = \tau(v_{st}) = \rho'_{st}(w) = \rho'_s(\rho'_t(w)) = \rho'_s(\tau(v_t)).$$

Como temos $\tau(\rho_s(v_t)) = \rho'_s(\tau(v_t))$ para todo vetor v_t da base β, então

$$\tau(\rho_s(v)) = \rho'_s(\tau(v)) \quad \forall v \in V.$$

Mais geralmente, suponha que G tem uma ação sobre um conjunto finito X. Seja V um espaço vetorial com base $\beta = (v_x)_{x\in X}$ indexada por X. Para cada $s \in G$ tomemos ρ_s definida na base β por

$$\rho_s(v_x) = v_{sx}.$$

Temos então uma representação linear de G, que é chamada de *representação de permutação associada a* X. A representação regular seria o caso particular onde tomamos

$X = G$ e tomamos a segunda ação do item $iv)$ do **Exemplo 4** de ações de grupos $(\theta(s,x) = sx)$.

A seguir discutimos um pouco mais sobre relações entre representações de grupos e ações por esse mesmo grupo. Dada uma representação $\rho : G \to GL(V)$ de um grupo G, definindo a aplicação

$$\theta : G \times V \to V$$
$$(s,v) \mapsto s \cdot v = \rho_s(v)$$

temos as seguintes propriedades:

$i)$ $e \cdot v = \rho_e(v) = Id_V(v) = v$;

$ii)$ $s \cdot (t \cdot v) = \rho_s(\rho_t(v)) = (\rho_s \circ \rho_t)(v) = \rho_{st}(v) = (st) \cdot v$.

para quaisquer $s, t \in G$ e $v \in V$. Logo θ define uma ação de G em V.

Reciprocamente, seja $\theta' : G \times V \to V$ uma ação de G em V, satisfazendo $s \cdot (cv + u) = c(s \cdot v) + s \cdot u$ para quaisquer $v, u \in V$, $c \in \mathbb{C}$ e $s \in G$. Fixado $s \in G$, definimos a aplicação $\rho'_s : V \to V$ por $\rho'_s(v) = s \cdot v$. Então ρ'_s é linear e note que

$$\rho'_s(v) = \rho'_s(u) \Rightarrow s \cdot v = s \cdot u \Rightarrow s^{-1} \cdot (s \cdot v) = s^{-1} \cdot (s \cdot u) \Rightarrow v = u.$$

Logo ρ'_s é injetora e, como V tem dimensão finita, isso acarreta em $\rho'_s \in GL(V)$. Ademais,

$$\rho'_s(\rho'_t(v)) = s \cdot (t \cdot v) = (st) \cdot v = \rho'_{st}(v)$$

e portanto podemos definir a representação de G em V:

$$\rho' : G \to GL(V)$$
$$s \mapsto \rho'(s) = \rho'_s.$$

Definição 2.5 *Sendo V uma representação de um grupo finito G, dizemos que um subespaço W de V é uma sub-representação de V se W é invariante por G, isto é, se $\rho_s(w) \in W$ para quaisquer $s \in G$ e $w \in W$.*

Nesse caso, a restrição ρ_s^W de ρ_s a W é um automorfismo de W, donde temos a representação:

$$\rho^W : G \to GL(W)$$
$$s \mapsto \rho^W(s) = \rho_s^W$$

de G em W. Diremos que ρ^W é uma sub-representação de ρ.

Observação 2.4 *Sendo W um subespaço de V, dizemos que um subespaço W' de V é um complemento para W em V se $W \oplus W' = V$ ($W + W' = V$ e $W \cap W' = \{0\}$). Para cada decomposição de V dessa forma, está associada de forma biunívoca uma projeção linear de V em W, isto é, uma transformação linear p de V em V tal que $p(w) = w$, para todo $w \in W$, e $p(V) \subseteq W$.*

Observação 2.5 *Antes de prosseguirmos, dado um conjunto $X = \{x_1, x_2..., x_g\}$, com $g =\mid G \mid$ elementos, podemos indexá-los por elementos de G, ou seja, $X = \{x_1, x_2..., x_g\} = \{x_t; t \in G\}$, e denotaremos $\sum_{t\in G} x_t$ como sendo a soma:*

$$\sum_{t\in G} x_t := \sum_{i=1}^{g} x_i = x_1 + x_2 + ... + x_g.$$

Caso formos somar uma família $(x_t)_{t\in G}$ constante (digamos $x_t = x_0$), então $\sum_{t\in G} x_t = gx_0$. Claramente estamos supondo que há uma soma definida com tais elementos.

Daqui em diante tal notação será muito usada, principalmente porque quando dada uma representação ρ de G, como denotamos $\rho(t) = \rho_t$, temos naturalmente $\rho(G) = \{\rho_t; t \in G\}$. Caso fôssemos enumerar os elementos de G da forma $G = \{t_1, t_2, ..., t_g\}$, teríamos:

$$\sum_{t\in G} \rho_t := \sum_{i=1}^{g} \rho_{t_i} = \rho_{t_1} + \rho_{t_2} + ... + \rho_{t_g}.$$

Proposição 2.6 *Seja $\rho : G \to GL(V)$ uma representação linear de G em V e seja W um subespaço de V invariante por G. Então há um complemento W^0 de W que é invariante por G.*

Prova. Seja W' um complemento arbitrário para W em V, e p a projeção associada de V em W. Definamos:

$$p^0 = \frac{1}{g}\sum_{t\in G} \rho_t p \rho_t^{-1}, \quad g = \mid G \mid .$$

Como W é G invariante, temos $\rho_t^{-1}(v) = \rho_{t^{-1}}(v) \in W$ para todo v em W. Ademais como $p(w) = w$ para todo $w \in W$, em particular para $w = \rho_{t^{-1}}(v)$, temos:

$$\rho_t(p(\rho_{t^{-1}}(v))) = \rho_t(\rho_{t^{-1}}(v)) = v, \ \ \forall v \in W, t \in G.$$

Portanto

$$p^0(v) = \frac{1}{g}\sum_{t\in G} \rho_t p \rho_t^{-1}(v) = \frac{1}{g}\sum_{t\in G} v = \frac{1}{g} g v = v, \ \ \forall v \in W.$$

Ademais, como $p(\rho_{t^{-1}}(x)) \in W$ para qualquer $x \in V$, temos que $\rho_t(p(\rho_{t^{-1}}(x))) \in W$ para todo $x \in V$, visto que W é G-invariante. Portanto p^0 é uma projeção de V em W, que corresponde a um complemento $W^0 = Ker(p^0)$ de W em V, ou seja, $V = W \oplus W^0$. Mostremos agora que W^0 é invariante por G. De fato, dado $s \in G$, computemos $\rho_s p^0 \rho_s^{-1}$:

$$\rho_s p^0 \rho_s^{-1} = \rho_s(\frac{1}{g}\sum_{t\in G} \rho_t p \rho_t^{-1})\rho_s^{-1} = \frac{1}{g}\sum_{t\in G} \rho_s \rho_t p \rho_t^{-1} \rho_s^{-1} = \frac{1}{g}\sum_{t\in G} \rho_{st} p \rho_{st}^{-1} = p^0.$$

Portanto $\rho_s p^0 = p^0 \rho_s$ para todo s em G. Dado $v \in W^0$ temos, por definição, $p^0(v) = 0$ e assim $p^0(\rho_s(v)) = \rho_s(p^0(v)) = 0$, e isso mostra que $\rho_s(v) \in W^0$ para quaisquer s em G e v em W^0, finalizando a demonstração. ■

Continuando sob as hipóteses do teorema anterior e sob as mesmas notações, dado $v \in V$, temos $v = w + w^0$ com $w \in W$ e $w^0 \in W^0$, ou seja, w e w^0 são suas projeções em W e W^0, respectivamente. Pela linearidade de ρ_s, com $s \in G$, temos $\rho_s(v) = \rho_s(w) + \rho_s(w^0)$ e pelo fato de que W e W^0 são invariantes por G, temos $\rho_s(w) \in W$ e $\rho_s(w^0) \in W^0$, ou seja, $\rho_s(w)$ e $\rho_s(w^0)$ são as projeções de $\rho_s(v)$. Segue que as sub-representações W e W^0 determinam a representação V. Sejam R_s e R_s^0 as representações matriciais de W e W^0, respectivamente. Temos a representação matricial em blocos de V da seguinte forma:

$$\begin{pmatrix} R_s & 0 \\ 0 & R_s^0 \end{pmatrix}$$

Assim, dizemos que a representação V é a soma das representações W e W^0.

Definição 2.7 *Seja $\rho : G \to GL(V)$ uma representação linear de G. Dizemos que ρ é irredutível se $V \neq 0$ e nenhum subespaço próprio não nulo de V é invariante por G.*

Intuitivamente, isso significa que não podemos mais "*quebrar*" a representação V em sub-representações de *grau* menor. De acordo com o teorema anterior, V não pode ser decomposto como soma direta de dois subespaços invariantes por G, a não ser a decomposição trivial $V = 0 \oplus V$.

As representações irredutíveis são usadas para construir outras representações, assim como os números primos são usados para construir os números inteiros, ou seja, decompor uma representação em representações irredutíveis tem a mesma importância da decomposição de inteiros em números primos.

Proposição 2.8 *Toda representação é a soma direta de representações irredutíveis.*

Prova. Seja V uma representação linear de G. Se $dimV = 0$, o resultado segue, já que V será a soma direta de uma família vazia de representações irredutíveis. Prosseguindo por indução, sendo $dimV \geq 1$, vamos supor que o resultado é valido para todas as representações com grau menor que V. Caso V seja uma representação irredutível, não há o que provar; caso contrário, há uma sub-representação V' de V com

$$0 < dimV' < dimV.$$

Pelo teorema anterior, há uma sub-representação V'' de V tal que $V = V' \oplus V''$. Nessas condições temos $dimV'' = dimV - dimV'$, ou seja,

$$0 < dimV'' < dimV.$$

Por indução V' e V'' são somas diretas de sub-representações irredutíveis, concluindo que $V = V' \oplus V''$ é soma direta de sub representações irredutíveis. ■

2.3 Soma direta e produto tensorial de representações de um mesmo grupo

Em *álgebra linear* temos a noção de *soma* e *produto* de espaços vetoriais. Naturalmente nos perguntamos como adaptar esses conceitos para representações de G, que é o que faremos a seguir.

2.3.1 Soma direta de representações de um mesmo grupo G

Sejam espaços vetoriais U e W sobre o corpo dos números complexos, com $dimU = n$ e $dimW = m$. Inicialmente, tomando o conjunto $V = U \times W$, munimos V com as seguintes operações:

$$\lambda(u, w) = (\lambda u, \lambda w), \qquad (u_1, w_1) + (u_2, w_2) = (u_1 + u_2, w_1 + w_2).$$

Temos que V se torna um $\mathbb{C}$-espaço vetorial que denotaremos $V = U \oplus W$. Ademais, sendo $\beta = \{\alpha_1, \alpha_2, \cdots, \alpha_n\}$ e $\beta' = \{\omega_1, \omega_2, \cdots, \omega_m\}$ bases de U e W, respectivamente, então $\{(\alpha_1, 0), (\alpha_2, 0), \cdots, (\alpha_n, 0), (0, \omega_1), (0, \omega_2), \cdots, (0, \omega_m)\}$ é base de V. Logo $dimV = dimU + dimW$. No caso onde U e W são subespaços de um mesmo espaço vetorial e $U \cap W = 0$, então V é isomorfo à soma direta usual de U e W. Dependendo da situação podemos fazer as seguintes identificações: $u = (u, 0)$ e $w = (0, w)$, onde naturalmente se estende $u + w = (u, 0) + (0, w) = (u, w)$.

Definição 2.9 *Sendo $\rho^1 : G \to GL(U)$ e $\rho^2 : G \to GL(W)$ representações de G, então podemos definir a representação $\rho = \rho^1 \oplus \rho^2$ de G em $V = U \oplus W$ da seguinte forma: dado $v \in V$ temos $v = (u, w)$, com $u \in U$ e $w \in W$, e definimos para cada $s \in G$, $\rho_s(v) = (\rho^1_s(u), \rho^2_s(w))$.*

Note que dados $v_1 = (u_1, w_1)$, $v_2 = (u_2, w_2) \in V$ e $\lambda \in \mathbb{C}$, temos:

$$\begin{aligned}
\rho_s(\lambda v_1 + v_2) &= \rho_s(\lambda(u_1, w_1) + (u_2, w_2)) \\
&= \rho_s(\lambda u_1 + u_2, \lambda w_1 + w_2) \\
&= (\rho_s^1(\lambda u_1 + u_2), \rho_s^2(\lambda w_1 + w_2)) \\
&= (\lambda\rho_s^1(u_1) + \rho_s^1(u_2), \lambda\rho_s^2(w_1) + \rho_s^2(w_2)) \\
&= \lambda(\rho_s^1(u_1), \rho_s^2(w_1)) + (\rho_s^1(u_2), \rho_s^2(w_2)) \\
&= \lambda\rho_s(v_1) + \rho_s(v_2).
\end{aligned}$$

Logo ρ_s é um operador linear de V. Suponha agora que $v = (u, w) \in V = U \oplus W$ é tal que $\rho_s(v) = (0, 0)$. Então, $\rho_s^1(u) = 0$ e $\rho_s^2(w) = 0$. Mas como ρ_s^1 e ρ_s^2 são injetoras, temos $u = 0$ e $w = 0$, e daí temos $v = 0$, concluindo que ρ_s é injetiva. Como V tem dimensão finita, temos então que ρ_s é um isomorfismo de V em V.

Pondo $\rho(s) = \rho_s$, temos $\rho(st) = \rho(s) \circ \rho(t)$ para quaisquer $s, t \in G$. De fato,

$$\begin{aligned}
\rho_{st}(u, w) &= (\rho_{st}^1(u), \rho_{st}^2(w)) \\
&= (\rho_s^1(\rho_t^1(u)), \rho_s^2(\rho_t^2(w))) \\
&= \rho_s(\rho_t^1(u), \rho_t^2(w)) \\
&= \rho_s(\rho_t(u, w)).
\end{aligned}$$

Portanto temos uma representação de G em V.

2.3.2 Produto tensorial de representações de um mesmo grupo G

Igualmente ao que fizemos para a soma direta, faremos para o produto tensorial.

Definição 2.10 *Um espaço vetorial V, com uma aplicação $(u, w) \mapsto u \cdot w$ de $U \times W$ em V, é dito um produto tensorial de U e W se as duas seguintes condições são satisfeitas:*

i) $u \cdot w$ é linear em ambas as variáveis u e w.

ii) Se $\{u_1, u_2, ..., u_n\}$ *é uma base de* U *e* $\{w_1, w_2, ..., w_m\}$ *é uma base para* W*, então* $\{u_i \cdot w_j \mid i = 1, 2, .., n \text{ e } j = 1, 2, ..., m\}$ *é uma base para* V*.*

Nesse caso denotamos $V = U \otimes W$, e V é único a menos de isomorfismo. Ademais temos a relação $dimV = dimU \cdot dimW$.

Podemos tomar, por exemplo, $V = M_{n\times m}(\mathbb{C})$ com a aplicação que mapeia o par (u, w) na matriz $\sum_{i=1}^{n}\sum_{j=1}^{m} x_i y_j E_{ij}$, onde:

$$u = \sum_{k=1}^{n} x_k u_k, \qquad w = \sum_{k=1}^{m} y_k w_k \qquad x_k, y_k \in \mathbb{C}$$

$E_{ij} = (a_{pq}) \in M_{n\times m}(\mathbb{C})$ é definida por $a_{pq} = 1$ se $p = i$, $j = q$, e $a_{pq} = 0$ caso contrário. Podemos denotar também $a_{pq} = \delta_{ip} \cdot \delta_{jq}$, onde δ_{lk} denota o delta de Kronecker ($\delta_{lk} = 1$ se $l = k$, $\delta_{lk} = 0$ caso $l \neq k$).

Agora sejam $\rho^1 : G \to GL(U)$ e $\rho^2 : G \to GL(W)$ duas representações lineares de G. Para $s \in G$ definamos $\rho_s \in GL(U \otimes W)$ da seguinte forma:

$$\rho_s(u_i \cdot w_j) = \rho_s^1(u_i) \cdot \rho_s^2(w_j)$$

para u_i na base fixada de U e w_j na base fixada de W. Dado $v \in V = U \otimes W$, existem escalares $\lambda_{ij} \in \mathbb{C}$ unicamente determinados tais que

$$v = \sum_{i=1}^{n}\sum_{j=1}^{m} \lambda_{ij} u_i \cdot w_j.$$

Definamos então:

$$\rho_s(v) := \sum_{i=1}^{n}\sum_{j=1}^{m} \lambda_{ij}\rho_s(u_i \cdot w_j) = \sum_{i=1}^{n}\sum_{j=1}^{m} \lambda_{ij}\rho_s^1(u_i) \cdot \rho_s^2(w_j).$$

Dessa forma é claro que, em particular, temos $\rho_s(u \cdot w) = \rho_s^1(u) \cdot \rho_s^2(w)$ para quaisquer $u \in U$ e $w \in W$.

Denotamos:

$$\rho_s = \rho_s^1 \otimes \rho_s^2.$$

Isso define uma representação linear de G em $U \otimes W$.

Definição 2.11 *Dadas representações $\rho^1 : G \to GL(U)$ e $\rho^2 : G \to GL(W)$ de G, chamamos a representação $\rho = \rho^1 \otimes \rho^2 : G \to GL(U \otimes W)$ definida acima de produto tensorial das representações ρ^1 e ρ^2 do grupo G.*

Esta representação tem uma representação matricial dada da seguinte forma: sendo $\{u_1, u_2, ..., u_n\}$ base de U e $\{w_1, w_2, ..., w_m\}$ base de W, e $r^1_{ij}(s), r^2_{ij}(s)$ as representações matriciais de ρ^1 e ρ^2 respectivamente, então temos:

$$\rho^1_s(u_{j_1}) = \sum_{i_1=1}^{n} r^1_{i_1 j_1}(s) u_{i_1}, \quad \rho^2_s(w_{j_2}) = \sum_{i_2=1}^{n} r^2_{i_2 j_2}(s) w_{i_2}.$$

Daí segue que

$$\rho_s(u_{j_1} \cdot w_{j_2}) = \sum_{i_1=1}^{n} \sum_{i_2=1}^{m} r^1_{i_1 j_1}(s) r^2_{i_2 j_2}(s) u_{i_1} \cdot w_{i_2}.$$

2.4 Caracter de uma representação, Lema de Schur e relações de ortogonalidade.

2.4.1 Caracter

Nesta seção introduziremos uma aplicação chamada de *caracter*, que é definida com base em uma representação. Embora não aparente, essa aplicação caracteriza a representação completamente a menos de isomorfismo, isto é, duas representações são isomorfas se, e somente se, têm o mesmo caracter.

Relembremos o que é o traço de uma matriz.

Observação 2.6 *Como vimos no **Capítulo 1**, o traço de uma matriz $A = (a_{ij}) \in M_n(\mathbb{C})$ é dado por $Tr(A) = \sum_{k=1}^{n} a_{kk}$, isto é, a soma dos elementos da diagonal principal de A. Temos $Tr(AB) = Tr(BA)$ para $A, B \in M_n(\mathbb{C})$, e daí, se $D, E \in M_n(\mathbb{C})$ são tais que existe uma matriz inversível P satisfazendo $E = PDP^{-1}$, ou seja, D e E são matrizes conjugadas, fazendo $A = DP^{-1}$ e $B = P$ temos:*

$$Tr(D) = Tr(DP^{-1}P) = Tr(AB) = Tr(BA) = Tr(PDP^{-1}) = Tr(E)$$

concluindo que matrizes conjugadas têm o mesmo traço.

Seja T um operador linear sobre V. Tomando α e β bases de V, temos a seguinte relação:

$$[T]_\alpha = [I]_\alpha^\beta [T]_\beta ([I]_\alpha^\beta)^{-1}$$

onde $[I]_\alpha^\beta$ denota a matriz de mudança de base de β para α. Assim $Tr([T]_\alpha) = Tr([T]_\beta)$. Note também que $Tr([T]_\alpha)$ coincide com a soma dos autovalores de T, visto que o polinômio característico de T se decompõe por completo sobre $\mathbb{C}$ e assim T é triangulável. Ademais se $\lambda \in \mathbb{C}^*$ é um autovalor de T, então existe $v \in V$ não nulo tal que $T(v) = \lambda v$, e daí

$$T(v) = \lambda v \Rightarrow T^{-1}(T(v)) = T^{-1}(\lambda v) \Rightarrow v = \lambda T^{-1}(v) \Rightarrow T^{-1}(v) = \lambda^{-1} v.$$

Assim λ^{-1} é autovalor de T^{-1}. Caso T seja invertível, sendo $\lambda_1, \lambda_2, ..., \lambda_n$ os autovalores de T (todo complexos, já que $\mathbb{C}$ é algebricamente fechado e eles são não nulos, pois como T é injetora não admite 0 como autovalor). Temos:

$$Tr(T) = \sum_{k=1}^{n} \lambda_k \qquad Tr(T^{-1}) = \sum_{k=1}^{n} \lambda_k^{-1}.$$

Definição 2.12 *Seja T um operador linear sobre V. Definimos o traço $Tr(T)$ da aplicação T como sendo o traço da matriz de T em qualquer base de V.*

Seja $\rho : G \to GL(V)$ uma representação linear de G. Para cada $s \in G$, definimos $\chi_\rho(s) = Tr(\rho_s)$, e assim temos uma função $\chi_\rho : G \to \mathbb{C}$ que satisfaz $\chi_\rho(st) = \chi_\rho(ts)$.

Definição 2.13 *Dada uma representação linear $\rho : G \to GL(V)$ de G, chamaremos de caracter da representação a função:*

$$\begin{aligned} \chi_\rho : G &\to \mathbb{C} \\ s &\mapsto \chi_\rho(s) = Tr(\rho_s). \end{aligned}$$

Denotaremos χ_ρ apenas por χ quando estiver pré-determinada a representação ρ e não houver risco de confusão.

Exemplo 10 *Exemplos de caracteres.*

i) Seja ρ_0 a representação trivial (item i) do ***Exemplo 9*** *de representações, $\rho_0(s) = Id_V$ para todo $s \in G$). Então $\chi(s) = dimV$ para todo $s \in G$;*

ii) O caracter da representação do item ii) do ***Exemplo 9*** *de representações é dado por:*

$$\chi(1) = 2, \qquad \chi(-1) = 0, \qquad \chi(i) = 1 + i, \qquad \chi(-i) = 1 - i$$

iii) Caracter do primeiro exemplo do item iii) do ***Exemplo 9*** *de representações:*

$$\chi(e) = 2, \qquad \chi(a) = 0, \qquad \chi(b) = 0, \qquad \chi(c) = -2.$$

Caracter do segundo exemplo do item iii) do ***Exemplo 9*** *de representações:*

$$\chi(e) = 1, \qquad \chi(a) = -1, \qquad \chi(b) = 1, \qquad \chi(c) = -1.$$

iv) Caracter do exemplo do item iv) do ***Exemplo 9*** *de representações:*

$$\chi(\overline{0}) = 1, \qquad \chi(\overline{1}) = -\frac{1}{2} + i\frac{\sqrt{3}}{2}, \qquad \chi(\overline{2}) = -\frac{1}{2} - i\frac{\sqrt{3}}{2}.$$

De agora em diante $\overline{z}$ representará o complexo conjugado do número complexo z ($\overline{a + bi} = a - bi$; $a, b \in \mathbb{R}, i^2 = -1$).

Proposição 2.14 *Se χ é o caracter de uma representação $\rho : G \to GL(V)$ de grau n, para quaisquer $s, t \in G$ temos:*

i) $\chi(e) = n$;

ii) $\chi(s^{-1}) = \overline{\chi(s)}$;

iii) $\chi(tst^{-1}) = \chi(s)$.

Prova.

i) Como $\rho(e) = Id_V$, temos $[\rho(e)] = I_n$. Segue então que $\chi(e) = Tr(I_n) = n$.

ii) Como G tem ordem finita, segue que $\rho(G)$ é um subgrupo finito de $Gl_n(\mathbb{C})$. Daí para todo $s \in G$, temos que $\rho_s \in \rho(G)$ tem ordem finita, donde, existe $m \in \mathbb{N}$ tal que $[\rho_s]^m = I_n$. Seja $\lambda \in \mathbb{C}$ um autovalor de ρ_s (ρ_s terá seus n autovalores em $\mathbb{C}$ pois $\mathbb{C}$ é algebricamente fechado). Sendo v um autovetor associado a λ, não é difícil ver que $\rho_s^m(v) = \lambda^m v$. Mas como ρ_s^m é a transformação identidade, temos:

$$v = \lambda^m v \Rightarrow (1 - \lambda^m)v = 0 \stackrel{v \neq 0}{\Longrightarrow} 1 = \lambda^m$$

e então $\lambda^m = 1$, assim

$$\mid \lambda^m \mid = \mid \lambda \mid^m = 1 \Rightarrow \mid \lambda \mid = 1 \Rightarrow \mid \lambda \mid^2 = 1 \Rightarrow \lambda\overline{\lambda} = 1 \Rightarrow \overline{\lambda} = \lambda^{-1}.$$

Sendo então $\lambda_1, \lambda_2, ..., \lambda_n$ os autovalores de ρ_s, então

$$\overline{\chi(s)} = \overline{Tr(\rho_s)} = \overline{\sum_{k=1}^{n} \lambda_k} = \sum_{k=1}^{n} \overline{\lambda_k} = \sum_{k=1}^{n} \lambda_k^{-1} = Tr(\rho_s^{-1}) = \chi(s^{-1}).$$

iii) Segue direto da **Observação 2.6**.

■

Proposição 2.15 *Sejam $\rho^1 : G \to GL(V_1)$ e $\rho^2 : G \to GL(V_2)$ duas representações lineares de G, com caracteres χ_1 e χ_2 respectivamente. Temos:*

i) o caracter χ da representação soma direta $V_1 \oplus V_2$ é igual a $\chi_1 + \chi_2$;

ii) o caracter ψ da representação produto tensorial $V_1 \otimes V_2$ é igual a $\chi_1 \cdot \chi_2$.

Prova. Tomemos ρ^1 e ρ^2 em forma matricial: R_s^1, R_s^2. A forma matricial da representação $V_1 \oplus V_2$ é

$$R_s = \begin{pmatrix} R_s^1 & 0 \\ 0 & R_s^2 \end{pmatrix}.$$

Daí $Tr(R_s) = Tr(R_s^1) + Tr(R_s^2)$, isto é, $\chi(s) = \chi_1(s) + \chi_2(s)$.

Para *ii*), continuando com a notação usada após a **Definição 2.11**, temos:

$$\chi_1(s) = \sum_{i_1} r_{i_1 i_1}(s), \quad \chi_2(s) = \sum_{i_2} r_{i_2 i_2}(s)$$

$$\psi(s) = \sum_{i_1, i_2} r_{i_1 i_1}(s) r_{i_2 i_2}(s) = (\sum_{i_1} r_{i_1 i_1}(s))(\sum_{i_2} r_{i_2 i_2}(s)) = \chi_1(s)\chi_2(s).$$

■

2.4.2 Lema de Schur

Para podermos caracterizar as representações apenas pelo caracter associado a elas, usaremos o resultado a seguir juntamente com seus corolários.

Proposição 2.16 (*Lema de Schur*): *Sejam* $\rho^1 : G \to GL(V_1)$ *e* $\rho^2 : G \to GL(V_2)$ *duas representações irredutíveis de* G *e* T *uma transformação linear de* V_1 *em* V_2 *tal que* $\rho^2_s \circ T = T \circ \rho^1_s$ *para todo* $s \in G$. *Então:*

i) Se ρ^1 *e* ρ^2 *são não isomorfas, então* $T = 0$;

ii) Se $V_1 = V_2 = V$ *e* $\rho^1 = \rho^2$, *então* T *é um múltiplo escalar da transformação identidade.*

Prova.

i) Se mostramos que $T \neq 0$ implica que T é um isomorfismo, então estará provado o item, já que T seria um isomorfismo de espaços vetoriais de V_1 em V_2 satisfazendo $\rho^2_s \circ T = T \circ \rho^1_s$, o que contradiria o fato de ρ^1 e ρ^2 serem não isomorfas. Portanto, suponha $T \neq 0$ e tome W_1 como seu núcleo. Para $w \in W_1$, temos

$$T(\rho^1_s(w)) = \rho^2_s(T(w)) = \rho^2_s(0) = 0$$

ou seja, $\rho^1_s(w) \in W_1$ para todo $w \in W_1$, donde W_1 é invariante por G. Desde que V_1 é irredutível, então $W_1 = 0$ ou $W_1 = V_1$. Como $T \neq 0$, não podemos ter $W_1 = V_1$, então $W_1 = 0$, ou seja, T é injetiva. Seja agora $W_2 = T(V_1)$ a imagem de T. Tomando $w \in W_2$, então $w = T(v)$ para algum $v \in V_1$, donde

$$\rho^2_s(w) = \rho^2_s(T(v)) = T(\rho^1_s(v)) \in W_2$$

ou seja, $\rho^2_s(w) \in W_2$ para todo $w \in W_2$, donde concluímos que W_2 é G-invariante. Como por hipótese V_2 é uma representação irredutível, temos $W_2 = 0$ ou $W_2 = V_2$. Mas supomos que $T \neq 0$, então $W_2 = V_2$, ou seja, T é sobrejetiva, concluindo que T é um isomorfismo.

ii) Suponha que $V_1 = V_2 = V$ e $\rho^1 = \rho^2$. Como $\mathbb{C}$ é algebricamente fechado T tem auto valor complexo, chamemos um tal autovalor de λ. Tomando agora a transformação linear $T' := T - \lambda Id_V$, então

$$\begin{aligned}
\rho_s^2 \circ T' &= \rho_s^2 \circ (T - \lambda Id_V) \\
&= \rho_s^2 \circ T - \rho_s^2 \circ \lambda Id_V \\
&= T \circ \rho_s^1 - \lambda \rho_s^2 \\
&= T \circ \rho_s^1 - \lambda \rho_s^1 \\
&= (T - \lambda Id_V) \circ \rho_s^1 \\
&= T' \circ \rho_s^1.
\end{aligned}$$

Analogamente ao que fizemos no item *i)*, mostramos que o núcleo W' da transformação T' é invariante por G, ou seja, $W' = 0$ ou $W' = V$. Mas, como λ é autovalor de T, então existe $w \in V$ não nulo tal que $T(w) = \lambda w$, ou seja, $T'(w) = 0$, donde segue que $w \in W' \neq 0$, concluindo que $W' = V$ e portanto $T' = 0$, seguindo assim o resultado $T = \lambda Id_V$.

■

Denotemos $g =\mid G \mid$ e $TS = T \circ S$ para transformações, ou seja, a justaposição de transformações denota a composição.

Corolário 2.17 *Sejam $\rho^1 : G \to GL(V_1)$, $\rho^2 : G \to GL(V_2)$ representações irredutíveis de G e $T : V_1 \to V_2$ uma transformação linear. Considere*

$$T^0 = \frac{1}{g} \sum_{t \in G} [(\rho_t^2)^{-1} T \rho_t^1].$$

Daí temos:

i) Se ρ^1 e ρ^2 são não isomorfas, então $T^0 = 0$;

ii) Se $V_1 = V_2$ e $\rho^1 = \rho^2$, então $T^0 = \lambda Id_V$, com $\lambda = \dfrac{1}{dim V_1} Tr(T)$.

Prova. Inicialmente computemos $(\rho_s^2)^{-1}T^0\rho_s^1$:

$$\begin{aligned}(\rho_s^2)^{-1}T^0\rho_s^1 &= (\rho_s^2)^{-1}(\frac{1}{g}\sum_{t\in G}[(\rho_t^2)^{-1}T\rho_t^1])\rho_s^1\\ &= \frac{1}{g}\sum_{t\in G}[(\rho_s^2)^{-1}(\rho_t^2)^{-1}T\rho_t^1\rho_s^1]\\ &= \frac{1}{g}\sum_{t\in G}[(\rho_{ts}^2)^{-1}T\rho_{ts}^1]\\ &= \frac{1}{g}\sum_{r\in G}[(\rho_r^2)^{-1}T\rho_r^1]\\ &= T^0.\end{aligned}$$

Então temos $T^0\circ\rho_s^1 = \rho_s^2\circ T^0$, e tendo isso em vista provemos os itens.

i) Como $T^0\circ\rho_s^1 = \rho_s^2\circ T^0$, basta aplicar a **Proposição 2.16** em T^0 e daí temos $T^0 = 0$.

ii) Aplicando a **Proposição 2.16** novamente, temos $T^0 = \lambda Id_{V_1}$. Então, temos $\lambda Id_{V_1} = T^0 = \frac{1}{g}\sum_{t\in G}[(\rho_t^2)^{-1}T\rho_t^1]$, e daí

$$Tr(\lambda Id_{V_1}) = Tr(T^0) = Tr(\frac{1}{g}\sum_{t\in G}[(\rho_t^2)^{-1}T\rho_t^1])$$

$$Tr(\lambda Id_{V_1}) = Tr(T^0) = Tr(\frac{1}{g}\sum_{t\in G}[(\rho_t^1)^{-1}T\rho_t^1])$$

$$\lambda Tr(Id_{V_1}) = Tr(T^0) = \frac{1}{g}\sum_{t\in G}[Tr((\rho_t^1)^{-1}T\rho_t^1)]$$

$$\lambda\cdot dimV_1 = Tr(T^0) = \frac{1}{g}\sum_{t\in G}Tr(T)$$

$$\lambda\cdot dimV_1 = Tr(T^0) = \frac{1}{g}(gTr(T)) = Tr(T).$$

Daí temos $\lambda = \dfrac{1}{dimV_1}Tr(T)$. ■

Note que nos cálculos usamos o fato de que $Tr(Id_{V_1})$ é o traço da matriz unidade de ordem $dimV_1\times dimV_1$ que resulta na soma $1+1+...+1$ com "$dimV_1$" parcelas, o que

resulta em $dimV_1$, e que $Tr((\rho_t^1)^{-1}T\rho_t^1) = Tr(T)$, pois as matrizes das transformações serão matrizes conjugadas, e logo terão o mesmo traço.

Vamos agora analisar o **Corolário 2.17** com as representações em forma matricial. Ponha ρ^1 e ρ^2 em forma matricial:

$$\rho^1 = (r_{i_1j_1}(t)), \qquad \rho^2 = (\ddot{\mathrm{r}}_{i_2j_2}(t)) \qquad t \in G.$$

Se a transformação T for representada pela matriz $(x_{i_2i_1})$ e digamos que T^0 seja representada por $(x^0_{i_2i_1})$, pela definição de T^0 temos:

$$x^0_{i_2i_1} = \frac{1}{g}\sum_{t,j_1,j_2} \ddot{\mathrm{r}}_{i_2j_2}(t^{-1})x_{j_2j_1}r_{j_1i_1}(t) = \sum_{j_1,j_2}\left(x_{j_2j_1}\frac{1}{g}\sum_{t\in G}\ddot{\mathrm{r}}_{i_2j_2}(t^{-1})r_{j_1i_1}(t)\right)$$

Observe que o último membro é uma combinação linear dos elementos $x_{j_2j_1}$, que no caso i) sempre se anula, não importando os valores escolhidos para as entradas $x_{j_2j_1}$. Fixando um $x_{j_2j_1}$, atribuindo a essa entrada o valor 1 e às demais entradas o valor 0, no caso i) obtemos:

Corolário 2.18 *No caso i) do **Corolário 2.17**, com $r_{i_1j_1}(s)$ e $\ddot{r}_{i_2j_2}(s)$ as formas matriciais das representações ρ^1 e ρ^2, respectivamente, temos:*

$$\frac{1}{g}\sum_{t\in G}[\ddot{r}_{i_2j_2}(t^{-1})r_{j_1i_1}(t)] = 0$$

para i_1, i_2, j_1 e j_2 arbitrários.

Vamos agora considerar o caso ii) do **Corolário 2.17** de modo análogo ao que fizemos acima no caso i). Temos $T^0 = \lambda I$ ($I = Id_V$). Se denotarmos por δ_{pq} o delta de Kronecker, então temos $x^0_{i_2i_1} = \lambda\delta_{i_2i_1}$, com $\lambda = \frac{1}{n}Tr(T)$ e $n = dimV_1$, como $n\lambda = \sum_k x_{kk} = \sum_{j_1}\sum_{j_2}\delta_{j_2j_1}x_{j_2j_1}$, temos então $\lambda = \frac{1}{n}\sum_{j_2,j_1}\delta_{j_2j_1}x_{j_2j_1}$, ou seja,

$$\frac{1}{g}\sum_{t,j_1,j_2}\ddot{\mathrm{r}}_{i_2j_2}(t^{-1})x_{j_2j_1}r_{j_1i_1}(t) = \frac{1}{n}\sum_{j_1,j_2}\delta_{i_2i_1}\delta_{j_2j_1}x_{j_2j_1}.$$

Note que a igualdade acima vale para quaisquer $x_{j_2j_1}$, e portanto os coeficientes em cada um dos membros da igualdade são iguais. Deste modo temos o seguinte corolário

Corolário 2.19 *No caso ii) temos:*

$$\frac{1}{g}\sum_{t\in G} \ddot{r}_{i_2j_2}(t^{-1})r_{j_1i_1}(t) = \frac{1}{n}\delta_{i_2i_1}\delta_{j_1j_2}$$

que resulta em $\frac{1}{n}$ *se* $i_1 = i_2$ *e* $j_1 = j_2$, *e* 0 *caso contrário.*

2.4.3 Relações de ortogonalidade

Para prosseguirmos com a análise dos corolários provados na seção **2.4.2** , recordemos que se X é um conjunto não vazio, então o conjunto $F(X;\mathbb{C})$ de todas as funções de X em $\mathbb{C}$, munido com a soma $(f+h)(x) := f(x) + h(x)$, para $f, g \in F(X;\mathbb{C})$, e com a multiplicação por escalar $(\lambda f)(x) := \lambda f(x)$ para $\lambda \in \mathbb{C}$, é um espaço vetorial sobre o corpo dos complexos. Tomando então particularmente $X = G$, vamos definir:

$$\begin{aligned} <,>: F(G;\mathbb{C}) \times F(G;\mathbb{C}) &\to \mathbb{C} \\ (f,h) &\mapsto < f,h >= \frac{1}{g}\sum_{t\in G} f(t^{-1})\cdot h(t) \end{aligned}$$

lembrando que $g =\mid G \mid$. Vamos mostrar que $< f,h >=< h,f >$. De fato, a medida que t^{-1} percorre G, t percorre igualmente. Podemos então reindexar $s = t^{-1}$ e consequentemente $s^{-1} = t$, com $s \in G$. Daí

$$< f,h >= \frac{1}{g}\sum_{t\in G} f(t^{-1})\cdot h(t) = \frac{1}{g}\sum_{s\in G} f(s)\cdot h(s^{-1}) = \frac{1}{g}\sum_{s\in G} h(s^{-1})\cdot f(s) =< h,f > .$$

Ademais, dados $f_1, f_2, h \in F(G;\mathbb{C})$ e $\lambda \in \mathbb{C}$ temos:

$$\begin{aligned} < f_1 + \lambda f_2, h > &= \frac{1}{g}\sum_{t\in G}(f_1 + \lambda f_2)(t^{-1})\cdot h(t) \\ &= \frac{1}{g}\sum_{t\in G} f_1(t^{-1})\cdot h(t) + \frac{\lambda}{g}\sum_{t\in G} f_2(t^{-1})\cdot h(t) \\ &=< f_1,h > +\lambda < f_2,h > . \end{aligned}$$

Daí $< f,h >$ é linear em f e em h. Dizemos então que $<,>$ é uma forma bilinear simétrica, e com essa notação o **Corolário 2.18** pode ser escrito como:

$$< \ddot{\mathrm{r}}_{i_2j_2}, r_{j_1i_1} >= 0.$$

Já o **Corolário 2.19** fica

$$< \ddot{\mathrm{r}}_{i_2j_2}, r_{j_1i_1} >= \frac{1}{n}\delta_{i_2i_1}\delta_{j_2j_1}.$$

Essas características de formas bilineares simétricas vistas logo acima lembram muito produto interno, mas ainda não é, já que não satisfaz $< f, h >= \overline{< h, f >}$, pois tomando $f : G \to \mathbb{C}$ como sendo a função constante $f(x) = 1$ e a função $h : G \to \mathbb{C}$ como sendo a função constante $h(x) = i$, temos

$$< f, h >= \frac{1}{g}\sum_{t\in G} f(t^{-1}) \cdot h(t) = \frac{1}{g}\sum_{t\in G} i = i$$

enquanto que

$$\overline{< h, f >} = \overline{\frac{1}{g}\sum_{t\in G} h(t^{-1}) \cdot f(t)} = \overline{\frac{1}{g}\sum_{t\in G} i} = \bar{i} = -i.$$

Vamos construir um produto interno em $F(G;\mathbb{C})$ para podermos então falar em ortogonalidade. Primeiramente vamos definir formalmente o que é um produto interno em um espaço vetorial complexo.

Definição 2.20 *Sendo V um espaço vetorial sobre o corpo $\mathbb{C}$ dos números complexos, dizemos que uma aplicação $(\ |\ ) : V \times V \to \mathbb{C}$ é um produto interno se para todos $u, v, w \in V$ e $\lambda \in \mathbb{C}$ valem:*

i) $(u + v \mid w) = (u \mid w) + (v \mid w)$;

ii) $(\lambda v \mid w) = \lambda(v \mid w)$;

iii) $(v \mid w) = \overline{(w \mid v)}$;

iv) $(v \mid v) \in \mathbb{R}^*_+$ *sempre que* $v \neq 0$, *ou seja,* $(v \mid v) > 0$ *para todo* $v \neq 0$.

É importante salientar que $i), ii)$ e $iii)$ implicam em

$$(w \mid \lambda u + v) = \overline{\lambda}(w \mid u) + (w \mid v).$$

É também importante notar que $i)$ e $ii)$ são satisfeitas se, e somente se, vale a igualdade

$$(\lambda u + v \mid w) = \lambda(u \mid w) + (v \mid w) \qquad \forall u, v, w \in V, \lambda \in \mathbb{C}.$$

Definamos então para $V = F(G;\mathbb{C})$ a aplicação:

$$\begin{aligned}(\mid) : F(G;\mathbb{C}) \times F(G;\mathbb{C}) &\to \mathbb{C} \\ (f,h) &\mapsto (f \mid h) = \frac{1}{g}\sum_{t\in G} f(t)\cdot\overline{h(t)}\end{aligned}$$

Dados $f_1, f_2, f, h \in F(G;\mathbb{C})$ e $\lambda \in \mathbb{C}$ temos:

$$\begin{aligned}(\lambda f_1 + f_2 \mid h) &= \frac{1}{g}\sum_{t\in G}(\lambda f_1 + f_2)(t)\cdot\overline{h(t)} \\ &= \frac{1}{g}\sum_{t\in G}([\lambda f_1(t) + f_2(t)]\cdot\overline{h(t)} \\ &= \frac{\lambda}{g}\sum_{t\in G} f_1(t)\cdot\overline{h(t)} + \frac{1}{g}\sum_{t\in G} f_2(t)\cdot\overline{h(t)} \\ &= \lambda(f_1 \mid h) + (f_2 \mid h).\end{aligned}$$

Portanto as condições $i)$ e $ii)$ de produto interno são satisfeitas. Ademais para condição $iii)$ temos:

$$(f \mid h) = \frac{1}{g}\sum_{t\in G} f(t)\cdot\overline{h(t)} = \overline{\frac{1}{g}\sum_{t\in G}\overline{f(t)}h(t)} = \overline{\frac{1}{g}\sum_{t\in G} h(t)\overline{f(t)}} = \overline{(h \mid f)}.$$

Por fim, para o item $iv)$

$$(f \mid f) = \frac{1}{g}\sum_{t\in G} f(t)\cdot\overline{f(t)} = \frac{1}{g}\sum_{t\in G} \mid f(t) \mid^2 \geq 0$$

e a soma resulta em 0 se, e somente se, $f(t) = 0$ para todo $t \in G$, ou seja, $f = 0$. Portanto $(f \mid h)$ define um produto interno em $F(G;\mathbb{C})$ e naturalmente definimos que f é ortogonal a h se $(f \mid h) = 0$.

Se definirmos a função $\tilde{h}(t) = \overline{h(t^{-1})}$ para $h \in F(G;\mathbb{C})$, temos $(f \mid h) =< f, \tilde{h} >$. Note que se χ é o caracter de uma representação, então $\tilde{\chi} = \chi$. Logo $(f \mid \chi) =< f, \chi >$. Então, em se tratando de caracter de representação, podemos usar tanto $(\mid)$ quanto $< , >$.

Observação 2.7 *Sejam V um espaço vetorial sobre $\mathbb{C}$ de dimensão finita e $\rho : G \to GL(V)$ uma representação linear de G. Suponha que V esteja munido de um produto interno $(\mid)$. Suponha ainda que tal produto interno seja invariante por G, isto é, $(\rho_s(v) \mid \rho_s(u)) = (v \mid u)$ para quaisquer $u, v \in V$. Podemos sempre reduzir para esse*

caso trocando $(v \mid u)$ *por* $\sum_{t\in G}(\rho_t(v) \mid \rho_t(u))$. *De fato, suponha que* $(\ \mid\ )$ *seja um produto interno em* V, *definamos então a aplicação:*

$$\begin{aligned}(\ \mid\ )_2 : V \times V &\to V \\ (v,u) &\mapsto (v \mid u)_2 = \sum_{t\in G}(\rho_t(v) \mid \rho_t(u)).\end{aligned}$$

Então, dados $u, v, w \in V$ *e* $\lambda \in \mathbb{C}$, *temos:*

$$\begin{aligned}(\lambda u + v \mid w)_2 &= \sum_{t\in G}(\rho_t(\lambda u + v) \mid \rho_t(w)) \\ &= \sum_{t\in G}(\lambda\rho_t(u) + \rho_t(v) \mid \rho_t(w)) \\ &= \sum_{t\in G}[(\lambda\rho_t(u) \mid \rho_t(w)) + (\rho_t(v) \mid \rho_t(w))] \\ &= \lambda\sum_{t\in G}(\rho_t(u) \mid \rho_t(w)) + \sum_{t\in G}(\rho_t(v) \mid \rho_t(w)) \\ &= \lambda(u \mid w)_2 + (v \mid w)_2\end{aligned}$$

donde $(\ \mid\ )_2$ *satisfaz os itens i) e ii) da* ***Definição 2.20*** *de produto interno. Ademais*

$$\begin{aligned}(v,w)_2 &= \sum_{t\in G}(\rho_t(v) \mid \rho_t(w)) \\ &= \sum_{t\in G}\overline{(\rho_t(w) \mid \rho_t(v))} \\ &= \overline{\sum_{t\in G}(\rho_t(w) \mid \rho_t(v))} \\ &= \overline{(w \mid v)_2}.\end{aligned}$$

Por fim, para mostrar que $(\ \mid\ )_2$ *é um produto interno, tomemos* $v \neq 0$. *Como* ρ_t *é injetora para todo* $t \in G$, *temos* $\rho_t(v) \neq 0$, *e daí* $(\rho_t(v) \mid \rho_t(v)) > 0$. *Portanto*

$$(v \mid v)_2 = \sum_{t\in G}(\rho_t(v) \mid \rho_t(v)) > 0.$$

Fixado $s \in G$ *e tomando* $u, v \in V$, *temos:*

$$(\rho_s(v) \mid \rho_s(u)) = \sum_{t\in G}(\rho_t(\rho_s(v)) \mid \rho_t(\rho_s(u))) = \sum_{t\in G}(\rho_{ts}(v) \mid \rho_{ts}(u)).$$

Como a aplicação $t \mapsto ts$ *é uma bijeção em* G, *podemos reindexar* ts *por* $h \in G$, *ou seja*

$$(\rho_s(v) \mid \rho_s(u)) = \sum_{h\in G}(\rho_h(v) \mid \rho_h(u)) = (v,u)_2.$$

Daí concluímos que $(\ |\ )_2$ *é um produto interno em* V *que é invariante por* G.

Note que a invariância do produto interno $(v \mid u)$ *significa que se* (v_i) *é uma base ortonormal de* V, *então a matriz de* ρ_s *com respeito a essa base é uma matriz unitária. Lembrando que dizemos que uma matriz* $A = (a_{ij})_{n\times n}$ *é unitária se* A *é inversível e* $A \cdot \overline{A^t} = I_n$. *Em particular, temos* $r_{ij}(t) = \overline{r_{ji}(t^{-1})}$, *onde* $r_{ij}(t)$ *é a representação matricial de* ρ.

Proposição 2.21 .

i) Se χ *é o caracter de uma representação irredutível, então* $(\chi \mid \chi) = 1$, *ou seja,* χ *tem norma* 1;

ii) Se χ *e* χ' *são os caracteres de duas representações irredutíveis não isomorfas, então* $(\chi \mid \chi') = 0$, *ou seja,* χ *e* χ' *são ortogonais.*

Prova.

i) Seja ρ a representação com caracter χ dada na forma de matriz $\rho_t = (r_{ij}(t))$. Como na **Observação 2.7**, temos $\overline{r_{ij}(t)} = r_{ji}(t^{-1})$ e $\chi(t) = \sum_k r_{kk}(t)$. então

$$\begin{aligned}
(\chi \mid \chi) &= \frac{1}{g}\sum_{t\in G} \chi(t)\overline{\chi(t)} \\
&= \frac{1}{g}\sum_{t\in G}\left(\left(\sum_i r_{ii}(t)\right)\left(\overline{\sum_j r_{jj}(t)}\right)\right) \\
&= \frac{1}{g}\sum_{t\in G}\left(\left(\sum_i r_{ii}(t)\right)\left(\sum_j \overline{r_{jj}(t)}\right)\right) \\
&= \frac{1}{g}\sum_{t\in G}\left(\left(\sum_i r_{ii}(t)\right)\left(\sum_j r_{jj}(t^{-1})\right)\right) \\
&= \frac{1}{g}\sum_{t\in G}\sum_i\sum_j r_{ii}(t)r_{jj}(t^{-1}) \\
&= \sum_{i,j}\left(\frac{1}{g}\sum_{t\in G} r_{ii}(t)r_{jj}(t^{-1})\right) \\
&= \sum_{i,j} < r_{ii}(t), r_{jj}(t) >.
\end{aligned}$$

De acordo com o **Corolário 2.19** temos $< r_{ii}, r_{jj} >= \frac{\delta_{ij}}{n}$, onde n é o grau de ρ. Então

$$(\chi \mid \chi) = \sum_{i,j} \frac{\delta_{ij}}{n} = \frac{n}{n} = 1.$$

ii) Sejam ρ^1 e ρ^2 as representações de G que têm caracteres χ e χ', respectivamente, com representações matriciais $\rho^1 = (r_{i_1 j_1}(t))$ e $\rho^2 = (\ddot{\mathrm{r}}_{i_2 j_2}(t))$. Ainda supondo as bases como no item anterior, temos $\overline{r_{i_1 j_1}(t)} = r_{j_1 i_1}(t^{-1})$. Ademais por definição, temos $\chi(t) = \sum_{k_1} r_{k_1 k_1}(t)$ e $\chi'(t) = \sum_{k_2} \ddot{\mathrm{r}}_{k_2 k_2}(t)$. Então juntamente com o **Corolário 2.18**, temos:

$$\begin{aligned}
(\chi' \mid \chi) &= \frac{1}{g} \sum_{t \in G} \chi'(t) \overline{\chi(t)} \\
&= \frac{1}{g} \sum_{t \in G} \left(\sum_{k_2} \ddot{\mathrm{r}}_{k_2 k_2}(t) \right) \left(\overline{\sum_{k_1} r_{k_1 k_1}(t)} \right) \\
&= \frac{1}{g} \sum_{t \in G} \sum_{k_2} \sum_{k_1} \ddot{\mathrm{r}}_{k_2 k_2}(t) r_{k_1 k_1}(t^{-1}) \\
&= \sum_{k_2} \sum_{k_1} \left(\frac{1}{g} \sum_{t \in G} \ddot{\mathrm{r}}_{k_2 k_2}(t) r_{k_1 k_1}(t^{-1}) \right).
\end{aligned}$$

Daí $(\chi' \mid \chi) = \sum_{k_2} \sum_{k_1} < \ddot{\mathrm{r}}_{k_2 k_2}, r_{k_1 k_1} >= \sum_{k_2} \sum_{k_1} 0 = 0.$

■

Uma consequência dessa proposição é que os caracteres das representações irredutíveis formam um conjunto ortonormal no espaço $F(G; \mathbb{C})$.

Proposição 2.22 *Considere V uma representação linear de G com caracter ϕ, supondo que V se decompõe como soma direta de representações irredutíveis:*

$$V = W_1 \oplus W_2 \oplus ... \oplus W_k.$$

Então, se W é uma representação de G irredutível com caracter χ, o número de representações W_i isomorfas a W é igual a $(\phi \mid \chi) =< \phi, \chi >$.

Prova. Seja χ_i o caracter de W_i. Pela **Proposição 2.15**, temos

$$\phi = \chi_1 + \chi_2 + ... + \chi_k$$

e daí

$$(\phi \mid \chi) = (\chi_1 \mid \chi) + (\chi_2 \mid \chi) + ... + (\chi_k \mid \chi).$$

Pelo resultado anterior, (χ_i, χ) resulta em 1 ou 0, dependo se W é ou não isomorfa a W_i para $i = 1, 2, \ldots, k$, o que completa a demonstração. ■

Corolário 2.23 *O número de W_i's isomorfas a W não depende da decomposição.*

Observação 2.8 *Temos então uma unicidade na decomposição, o número de parcelas não muda, e também não muda o número de parcelas isomorfas entre si, como se fosse uma decomposição em números primos dos inteiros. Dizemos que W_i aparece $(\phi \mid \chi_i)$ vezes em V.*

Corolário 2.24 *Duas representações com mesmo caracter são isomorfas.*

Prova. Se V e V' são representações com mesmo caracter ϕ, e supondo que as decomposições em representações irredutíveis de V e V' são

$$V = W_1 \oplus W_2 \oplus ... \oplus W_k$$

$$V' = W_1' \oplus W_2' \oplus ... \oplus W_l'$$

então se, χ_i é o caracter de W_i, tanto o número de representações W_j' em V', quanto o número de representações W_j em V isomorfas a W_i, é igual a $(\phi \mid \chi_i)$, donde segue que $k \leq l$.

Sendo agora χ_i' o caracter de W_i', tanto o número de representações W_j em V, quanto o número de representações W_j' em V' isomorfas a W_i', é igual a $(\phi \mid \chi_i')$, donde segue que $l \leq k$.

Temos então $k = l$. Ademais, como os números de parcelas isomorfas são iguais, a menos de uma reordenação, podemos, sem perda de generalidade, assumir que W_i é isomorfa a W_i', para $i = 1, 2, \ldots, k$.

Sendo então $\rho^i : G \to GL(W_i)$ as representações dos W_i's induzidas por restrição da representação ρ de V, sejam também $(\rho')^i : G \to GL(W_i')$ as representações dos

(W_i')'s induzidas por restrição da representação ρ' de V'. Podemos então estender cada ρ_s^i como um operador de V pondo $\rho_s^i(v) = \rho_s^i(w_i)$, onde

$$v = w_1 + w_2 + \cdots + w_k, \quad w_j \in W_j \;\; j = 1, 2, \ldots, k.$$

Estendemos os $(\rho')_s^i$ como operadores em V' de forma análoga. Ademais temos que a representação ρ será a soma direta das sub-representações ρ^i, assim como ρ' será a soma direta das sub-representações $(\rho')^i$.

Para cada i de 1 a k, existem isomorfismos $\tau_i : W_i \to W_i'$ tais que $\tau_i \circ \rho_s^i = (\rho')_s^i \circ \tau_i$. Definindo agora $\tau : V \to V'$ como sendo

$$\tau = \tau_1 + \tau_2 + \cdots + \tau_k$$

mostremos que τ é sobrejetiva. Já que $dimV = dimV'$, pois $dimW_i = dimW_i'$, teremos que τ será um isomorfismo entre V e V'. De fato, dado $v' \in V'$, existem únicos $w_j' \in W_j'$, $j = 1, 2, ..., k$, tais que

$$v' = w_1' + w_2' + \cdots + w_k'.$$

Ademais, para cada w_j', existe $w_j \in W_j$ tal que $\tau_j(w_j) = w_j'$. Tomando $v \in V$ por definição

$$v = w_1 + w_2 + \cdots + w_k$$

temos

$$\begin{aligned} \tau(v) &= \tau_1(w_1) + \cdots + \tau_k(w_k) \\ &= w_1' + w_2' + \cdots + w_k' \\ &= v'. \end{aligned}$$

Logo $\tau : V \to V'$ é um isomorfismo de espaços vetoriais.

Mostremos agora que $\tau \circ \rho_s = \rho_s' \circ \tau$ para todo $s \in G$. De fato, tomando $v \in V$, existem $w_i \in W_i$, $i = 1, 2, \ldots, k$, tais que

$$v = w_1 + w_2 + \cdots + w_k$$

e daí

$$\begin{aligned}\tau(\rho_s(v)) &= \tau(\rho_s^1(w_1) + \rho_s^2(w_2) + \cdots + \rho_s^k(w_k)) \\ &:= \tau_1(\rho_s^1(w_1)) + \tau_2(\rho_s^2(w_2)) + \cdots + \tau_k(\rho_s^k(w_k)) \\ &= (\rho'_s)^1(\tau_1(w_1)) + (\rho'_s)^2(\tau_2(w_2)) + \cdots + (\rho'_s)^k(\tau_k(w_k)) \\ &= \rho'_s(\tau_1(w_1) + \tau_2(w_2) + \cdots + \tau_k(w_k)) \\ &= \rho'_s(\tau(v))\end{aligned}$$

concluindo que de fato $\tau \circ \rho_s = \rho'_s \circ \tau$ para todo $s \in G$. Portanto V e V' são isomorfas. ■

Tendo em vista esses resultados, sendo V uma representação de G, então

$$V = m_1W_1 \oplus m_2W_2 \oplus ... \oplus m_hW_h$$

para $m_i \in \mathbb{N}$ e W_i representações irredutíveis. Sendo ϕ o caracter da representação V e χ_i o caracter de W_i, então

$$\phi = m_1\chi_1 + m_2\chi_2 + ... + m_h\chi_h.$$

Ademais, temos $m_i = (\phi \mid \chi_i)$ e $(\chi_i \mid \chi_j) = \delta_{ij}$, visto que $\{\chi_1, \chi_2, ..., \chi_h\}$ é um conjunto ortonormal. Portanto

$$\begin{aligned}(\phi \mid \phi) &= (\sum_{i=1}^{h} m_i\chi_i \mid \sum_{j=1}^{h} m_j\chi_j) \\ &= \sum_{i=1}^{h} m_i(\chi_i \mid \sum_{j=1}^{h} m_j\chi_j) \\ &= \sum_{i=1}^{h} m_i \left[\sum_{j=1}^{h} m_j(\chi_i \mid \chi_j)\right] \\ &= \sum_{i,j} m_im_j(\chi_i \mid \chi_j) \\ &= \sum_{i,j} m_im_j\delta_{ij} \\ &= \sum_{k=1}^{h} m_k^2.\end{aligned}$$

Proposição 2.25 *Seja $V \neq 0$ uma representação de G com caracter ϕ. Então $(\phi \mid \phi)$ é um número inteiro positivo e é igual a 1 se, e somente se, V é uma representação irredutível.*

Prova. Como $(\phi \mid \phi) = \sum m_k^2$, é claro que $(\phi \mid \phi)$ resulta em um inteiro positivo. Ademais, se $(\phi \mid \phi) = \sum_{k=1}^{h} m_k^2 = 1$, então $m_i = 1$ para algum i e $m_j = 0$ para $j \neq i$, donde $V = W_i$, concluindo que V é irredutível. Reciprocamente, caso V seja irredutível, então $V = W_i$ para algum i e consequentemente $\phi = \chi_i$, daí $(\phi \mid \phi) = (\chi_i \mid \chi_i) = \delta_{ii} = 1$. ■

Observação 2.9 *Temos agora dois potentes resultados:*

i) Duas representações são isomorfas se, e somente se, têm o mesmo caracter.

ii) Uma representação de caracter χ é irredutível se, e somente, $(\chi \mid \chi) = 1$.

Busquemos então resolver a seguinte questão: "quantas representações irredutíveis de G existem a menos de isomorfismo?". Para isso estudemos a representação regular e as classes de conjugação de G.

Seja R a representação regular de G, isto é, R é um $\mathbb{C}$ espaço vetorial com uma base $\{v_t \in R; t \in G\}$ tal que $\rho_s(v_t) = v_{st}$. Sendo "e" o elemento neutro de G, como de costume, note que:

$$st = t \Leftrightarrow stt^{-1} = tt^{-1} \Leftrightarrow s = e.$$

Concluímos então que para $s \neq e$, ρ_s não fixa nenhum vetor da base. Na verdade longe disso, leva cada vetor da base em uma imagem que é L.I. com ele. Portanto a matriz de ρ_s nessa base tem diagonal nula, donde, sendo r_G o caracter da representação regular, temos $r_G(s) = 0$ para $s \neq e$.

Já para $s = e$, já vimos que, independente da representação,

$$r_G(e) = dimR = g = \mid G \mid .$$

Esses breves comentários servem como justificativa para a seguinte proposição.

Proposição 2.26 *Seja R a representação regular do grupo finito G de elemento neutro "e". Digamos que r_G seja o caracter de R e $g = \mid G \mid = dimR$. Temos:*

$$r_G(e) = g$$

$$r_G(s) = 0 \ \ \forall s \in G, s \neq e.$$

Corolário 2.27 *Seja W uma representação irredutível de G de grau $m = dimW$, com caracter χ. Então W apare m vezes na decomposição da representação regular.*

Prova. Basta calcularmos $(r_G \mid \chi)$, lembrando que várias parcelas serão nulas e $\chi(e) = m$.

$$(r_G \mid \chi) = \frac{1}{g}\sum_{t\in G} r_G(t)\overline{\chi(t)} = \frac{1}{g} r_G(e)\overline{\chi(e)} = \frac{gm}{g} = m.$$

■

Corolário 2.28 *O número de representações irredutíveis não isomorfas é finito e não superior a $g =\mid G \mid$.*

Prova. Pois caso contrário, supondo que haja pelo menos $g+1$ representações irredutíveis não isomorfas, digamos $W_1, W_2, .., W_{g+1}$, cada W_i um com grau $n_i = dimW_i \geq 1$, então, como $W_1 \oplus W_2 \oplus ... \oplus W_{g+1}$ é um subespaço de R, temos:

$$\begin{aligned} g &= dimR \\ &\geq dim(W_1 \oplus W_2 \oplus ... \oplus W_{g+1}) \\ &= dimW_1 + dimW_2 + ... + dimW_{g+1} \\ &\geq 1 + 1 + ... + 1 \quad (g+1 \text{ parcelas}) \\ &\geq g + 1 \end{aligned}$$

ou seja, $g \geq g + 1$, absurdo! ■

Observação 2.10 *Como sabemos que o número de caracteres irredutíveis é finito, a partir de agora identificaremos $\{\chi_1, \chi_2, \ldots, \chi_h\}$ como sendo uma lista completa e sem redundância dos caracteres irredutíveis de G. Denotaremos o grau de χ_i por n_i e W_i será uma representação irredutível de caracter χ_i.*

Corolário 2.29 *:*

i) Os graus n_i's satisfazem $\sum_{i=1}^{h} n_i^2 = g.$

ii) Para $s \neq e$ *temos* $\sum_{i=1}^{h} n_i \chi_i(s) = 0$.

Prova. Para justificar o item i) note que $R = n_1 W_1 \oplus n_2 W_2 \oplus ... \oplus n_h W_h$, donde $r_G = n_1\chi_1 + n_2\chi_2 + ... + n_h\chi_h$. Avaliando em $s = e$, temos $g = r_G(e) = \sum_{i=1}^{h} n_i \chi_i(e) = \sum_{i=1}^{h} n_i^2$.

Para o item ii) basta tomar $s \neq e$, e daí $0 = r_G(s) = \sum_{i=1}^{h} n_i \chi_i(s)$. ■

Sabemos agora que o número de representações irredutíveis é finito, e não superior a $g = \mid G \mid$. Procuremos agora descobrir com mais exatidão quanto é esse valor.

Definição 2.30 *Dizemos que* $f \in F(G;\mathbb{C})$ *é uma função de classe sobre* G *se*

$$f(st) = f(ts)$$

para todos $s, t \in G$.

Essa nomenclatura faz jus ao fato de que f é constante sobre o conjunto $Cl_G(x)$, visto que dado $x_0 \in Cl_G(x)$, existe $t \in G$ tal que $x_0 = txt^{-1}$. Tomando $s = xt^{-1}$ temos

$$f(x) = f(xt^{-1}t) = f(st) = f(ts) = f(txt^{-1}) = f(x_0).$$

Ademais, considerando o conjunto

$$H := \{f \in F(G;\mathbb{C});\ f \text{ é função de classe sobre } G\ \}$$

temos que H é subespaço vetorial de $F(G;\mathbb{C})$. De fato, dados $f_1, f_2 \in F(G;\mathbb{C})$, $\lambda \in \mathbb{C}$, temos:

$$(\lambda f_1 + f_2)(st) = \lambda f_1(st) + f_2(st) = \lambda f_1(ts) + f_2(ts) = (\lambda f_1 + f_2)(ts)$$

donde $\lambda f_1 + f_2 = f \in H$.

Note que $\chi_i \in H$, para $i = 1, 2, ..., h$, e que $\{\chi_1, \chi_2, ..., \chi_h\}$ é um conjunto ortonormal em H.

Proposição 2.31 *Sejam f uma função de classe sobre G e $\rho : G \to GL(V)$ uma representação de G de grau n e caracter χ. Definamos o operador linear ρ_f sobre V pela expressão:*

$$\rho_f := \sum_{t \in G} f(t)\rho_t.$$

Se V é irredutível, então $\rho_f = \lambda Id_V$, onde $\lambda = \frac{1}{n}\sum_{t \in G} f(t)\chi(t)$.

Prova. Computemos $\rho_s \rho_f \rho_{s^{-1}}$ para $s \in G$:

$$\begin{aligned}
\rho_s \rho_f \rho_{s^{-1}} &= \rho_s \left(\sum_{t \in G} f(t)\rho_t \right) \rho_{s^{-1}} \\
&= \sum_{t \in G} f(t)\rho_s \rho_t \rho_{s^{-1}} \\
&= \sum_{t \in G} f(t)\rho_{sts^{-1}} \\
&= \sum_{t \in G} f(sts^{-1})\rho_{sts^{-1}} \\
&= \sum_{u \in G} f(u)\rho_u \\
&= \rho_f.
\end{aligned}$$

Sendo assim $\rho_f \circ \rho_s = \rho_s \circ \rho_f$, e pelo **Corolário 2.17**, temos $\rho_f = \lambda Id_V$. Como $Tr(\lambda Id_V) = n\lambda$ e $Tr(\rho_f) = \sum_{t \in G} f(t)Tr(\rho_t) = \sum_{t \in G} f(t)\chi(t)$, temos $\lambda = \frac{1}{n}\sum_{t \in G} f(t)\chi(t)$. ■

Tomando $\chi^*(t) = \overline{\chi(t)}$, então a respeito da proposição anterior, temos:

$$\lambda = \frac{1}{n}\sum_{t \in G} f(t)\chi(t) = \frac{|\, G \,|}{n}(f \mid \chi^*).$$

Proposição 2.32 *Os caracteres $\chi_1, \chi_2, ..., \chi_h$ formam uma base ortonormal de H.*

Prova. Nos resta apenas mostrar que geram H, e para isso é suficiente mostrar que todo elemento de H que é ortogonal aos χ_i^*'s é zero. Dado $f \in H$ tal que por hipótese f seja ortogonal a χ_i^*. Para cada representação ρ de G tomemos $\rho_f = \sum_{t \in G} f(t)\rho_t$. Caso ρ seja uma representação irredutível de caracter χ_j, pela proposição anterior temos $\rho_f = \lambda Id_V$, onde $\lambda = \frac{g}{n}(f \mid \chi_j^*) = 0$. Logo $\rho_f = 0$. Pela decomposição em

soma direta de representações irredutíveis, concluímos que em todo caso $\rho_f = 0$. Em particular, para ρ sendo a representação regular R de G, aplicando ρ_f no vetor da base v_e temos:

$$0 = \rho_f(v_e) = \sum_{t \in G} f(t)\rho_t(v_e) = \sum_{t \in G} f(t)v_t.$$

Assim temos uma combinação linear dos vetores da base de R dando 0 e como eles são L.I., então os escalares da combinação são todos nulos, ou seja, $f(t) = 0$ para todo $t \in G$, donde concluímos que $f = 0$. ■

Observação 2.11 *Sejam $Cl_1, Cl_2, ..., Cl_k$ todas as distintas classes de conjugação de G. Como já vimos, se f é uma função de classe, então f é constante sobre cada Cl_i. Reciprocamente, supondo que f seja constante sobre cada Cl_i, então dados $s, t \in G$ temos:*

$$f(st) = f(stss^{-1}) = f(ts)$$

donde vemos que f é uma função de classe. Portanto ser uma função de classe é equivalente a ser constante sobre as classes de conjugação de G. Para criarmos então funções desse tipo basta escolhermos escalares $\lambda_i \in \mathbb{C}$ arbitrários. Para cada $i = 1, 2, ...k$, definamos a função f_i com domínio G como sendo $f_i(x_j) = \delta_{ij}$ para $x_j \in Cl_j$. Dessa forma sendo f uma função de classe que assume o valor λ_i na classe Cl_i, temos:

$$f = \lambda_1 f_1 + \lambda_2 f_2 + ... + \lambda_k f_k.$$

Logo $\{f_1, f_2, ..., f_k\}$ gera H. Ademais suponha que

$$\lambda_1 f_1 + \lambda_2 f_2 + ... + \lambda_k f_k = 0.$$

Tomando $x_j \in Cl_j$ temos:

$$0 = \lambda_1 f_1(x_j) + \lambda_2 f_2(x_j) + ... + \lambda_k f_k(x_j) = \lambda_j$$

donde segue que $\{f_1, f_2, ..., f_k\}$ é L.I. e portanto uma base para H. Assim $dim H = k$. Mas por outro lado, $\{\chi_1, \chi_2, ..., \chi_h\}$ forma uma base ortonormal para H, e essa observação justifica a proposição seguinte.

Proposição 2.33 *O número de representações irredutíveis de G, a menos de isomorfismo, é igual ao número das distintas classes de conjugação de G. Isto é, o número de classes de isomorfismos das representações irredutíveis de G é igual o número de classes de conjugação de G.*

2.5 Decomposição canônica de uma representação

Vimos que dada uma representação V de G, então V pode ser decomposto como soma direta de representações irredutíveis, porém essa decomposição não é única (é única apenas a menos de isomorfismo). Vejamos agora uma decomposição de V que é de fato única.

Dada uma representação linear $\rho : G \to GL(V)$, podemos decompor V como sendo soma direta de representações U_i irredutíveis:

$$V = U_1 \oplus U_2 \oplus ... \oplus U_m.$$

Sejam $W_1, W_2, ..., W_h$ as representações irredutíveis (não isomorfas) de G, cada W_i com grau $n_i = dim W_i$ e caracter χ_i. Para j fixo, agrupemos todas as representações U_i que são isomorfas a W_j, digamos $U_{j_1}, U_{j_2}, ..., U_{j_k}$, e denotemos V_j como sendo a sub-representação $U_{j_1} \oplus U_{j_2} \oplus ... \oplus U_{j_k}$ de G. Então claramente temos:

$$V = V_1 \oplus V_2 \oplus ... \oplus V_h.$$

Tal decomposição é chamada de *decomposição canônica.*

Proposição 2.34 .

i) A decomposição $V = V_1 \oplus V_2 \oplus ... \oplus V_h$ não depende da escolha inicial dos U_i's.

ii) A projeção p_i de V em V_i associada a essa decomposição é:

$$p_i = \frac{n_i}{g} \sum_{t \in G} \overline{\chi_i(t)} \rho_t.$$

Prova. Basta mostrar o item *ii*), pois o item *i*) é consequência deste. Seja

$$q_i = \frac{n_i}{g} \sum_{t \in G} \overline{\chi_i(t)} \rho_t.$$

A **Proposição 2.31** mostra que a restrição de q_i a uma representação irredutível W de caracter χ e de grau n é um operador múltiplo escalar da identidade, com escalar igual a $\frac{n_i}{n}(\chi_i \mid \chi)$, que é 0, se $\chi \neq \chi_i$, e 1, caso $\chi = \chi_i$. Em outras palavras, q_i é a identidade em uma representação isomorfa a W_i, e é 0 nas outras. Pela definição de V_i, isto já mostra que q_i é projeção. ■

Foquemos agora em subgrupos, produtos diretos e representações induzidas.

Observação 2.12 *Relembrando que dizemos que um grupo G é abeliano caso $st = ts$ para quaisquer $s, t \in G$. Desse modo, as classes de conjugações dos elementos de G são todas unitárias, e toda função sobre G é uma função de classe.*

Proposição 2.35 *São equivalentes:*

i) *G é um grupo abeliano.*

ii) *Todas as representações irredutíveis de G têm grau 1.*

Prova. Sendo g a ordem de G e $n_1, n_2, ..., n_h$ os graus das representações irredutíveis de G, sabemos que h é a quantidade de classes de conjugação distintas de G. Porém como G é abeliano, então $txt^{-1} = xtt^{-1} = x$, ou seja, as classes de conjugação são todas unitárias, donde $h = g$. Daí, temos:

$$\sum_{i=1}^{g} n_i^2 = g, \quad n_i \geq 1$$

i) $\Rightarrow$ *ii)*

Suponha por absurdo que haja pelo menos um n_j maior que 1. Daí:

$$\begin{aligned} n_j^2 > 1 &\Rightarrow n_1^2 + ... + n_j^2 + ... + n_g^2 > n_1^2 + ... + n_{j-1}^2 + 1 + n_{j+1}^2 + ... + n_g^2 \\ &\Rightarrow \sum_{i=1}^{g} n_i^2 > 1 + 1 + ... + 1 \quad (g \text{ parcelas iguais a } 1) \\ &\Rightarrow g > g, \end{aligned}$$

absurdo. Portanto $n_i = 1$ para $i = 1, 2, ..., h$.

ii) $\Rightarrow$ *i)*

Caso tenhamos $n_i = 1$ para todo i, então $g = \sum_{i=1}^{h} n_i^2 = \sum_{i=1}^{h} 1^2 = h$, donde deve haver tantas classes de conjugação quanto elementos de G. Sendo esse o caso, não pode haver uma classe de conjugação com mais de um elemento. Daí temos que, como $st = stss^{-1}$ está na classe de conjugação de ts, devemos ter $st = ts$.

■

Corolário 2.36 *Sejam G um grupo finito qualquer e A um subgrupo abeliano de G, sendo $a =\mid A \mid$ e $g =\mid G \mid$. Então cada representação irredutível de G tem grau não superior ao inteiro*[1] *positivo* $\frac{g}{a}$.

Prova. Sendo $\rho : G \to GL(V)$ uma representação irredutível de G, a restrição de ρ a A define uma representação $\rho^A : A \to GL(V)$ de A. Seja $W \subseteq V$ uma sub-representação irredutível de ρ^A. Pela proposição anterior, como A é abeliano, então $dim W = 1$. Seja V' o subespaço de V gerado pelas imagens $\rho_s(W) = \{\rho_s(x); x \in W\}$ de W, s variando em G, isto é,

$$V' = \sum_{s \in G} \rho_s(W).$$

É claro que V' é invariante por G. Como ρ é irredutível, então $V' = V$. Mas para $s \in G$ e $t \in A$, temos:

$$\rho_{st}(W) = \rho_s(\rho_t(W)) = \rho_s(\rho_t^A(W)) = \rho_s(W)$$

e então, se $s, s' \in G$ são tais que existe $t \in A$ com $s = s't$, devemos ter $\rho_s(W) = \rho_{s'}(W)$, donde segue que o número de espaços $\rho_s(W)$ distintos é não superior à quantidade das classes laterais $sA = \{st \mid t \in A\}$, com s em G. Tal quantidade é justamente o índice de A em G, que vale $\frac{g}{a} = \frac{\mid G \mid}{\mid A \mid}$. Note que $dim \rho_s(W) = 1$, e daí

$$V = V' = \sum_{s \in G} \rho_s(W)$$

[1] O valor $\frac{g}{a}$ é chamado de índice de A em G e pelo Teorema de Lagrange, **Proposição 1.7**, é sempre um número inteiro.

sendo T um conjunto de representantes de A/G temos:

$$\begin{aligned} dimV &= dim\left(\sum_{s\in G}\rho_s(W)\right) \\ &\leqslant \sum_{s\in T} dim\rho_s(W) \\ &\leqslant \sum_{i=1}^{g/a} 1 \\ &\leqslant \frac{g}{a}. \end{aligned}$$

■

Tendo em vista a **Definição 1.14** dada na **Seção 1.5** no Capítulo 1 de produto direto de grupos, um questionamento natural de surgir é sobre como estender, se possível, uma representação para $G_1 \times G_2$ a partir de uma representação de G_1 e outra de G_2. É esta a construção que faremos a seguir.

Definição 2.37 *Sejam $\rho^1 : G_1 \to GL(V_1)$ e $\rho^2 : G_2 \to GL(V_2)$ representações lineares de G_1 e G_2, respectivamente. Definimos uma representação linear $\rho = \rho^1 \otimes \rho^2$ de $G_1 \times G_2$ em $V_1 \otimes V_2$ (**Definição 2.3.2**) pondo, para cada $s = (s_1, s_2) \in G_1 \times G_2$, as imagens*

$$\rho_s(u_i \cdot w_j) := \rho^1_{s_1}(u_i) \cdot \rho^2_{s_2}(w_j)$$

onde $\{u_i\}$ e $\{w_j\}$ são bases de V_1 e V_2, respectivamente.

Estendemos por linearidade para elementos $\sum_{i,j} \lambda_{ij} u_i \cdot w_j$ de $V_1 \otimes V_2$ ($\lambda_{ij} \in \mathbb{C}$) como:

$$\rho_{(s_1,s_2)}(\sum_{i,j} \lambda_{ij} u_i \cdot w_j) = \sum_{i,j} \lambda_{ij} \rho^1_{s_1}(u_i) \cdot \rho^2_{s_2}(w_j).$$

Em particular temos:

$$\rho_s(x_1 \cdot x_2) = \big((\rho^1 \otimes \rho^2)(s_1, s_2)\big)(x_1 \cdot x_2) = \rho^1_{s_1}(x_1) \cdot \rho^2_{s_2}(x_2) \qquad \forall x_1 \in V_1, x_2 \in V_2.$$

Essa representação é chamada de produto tensorial de ρ^1 e ρ^2, e sendo χ_1 e χ_2 os caracteres de ρ^1 e ρ^2, respectivamente, então o caracter χ do produto tensorial $\rho^1 \otimes \rho^2$ de ρ^1 e ρ^2 é dado por:

$$\chi(s_1, s_2) = \chi_1(s_1)\chi_2(s_2).$$

Observação 2.13 *Quando G_1 e G_2 são iguais ao mesmo grupo G , a representação $\rho^1 \otimes \rho^2$ definida acima é uma representação de $G \times G$ (consistindo dos elementos (s_1, s_2), com $s_1, s_2 \in G$). Esta é uma representação diferente da representação dada pelos elementos na forma (s, s), com $s \in G$, que é a representação de G na* ***Definição 2.11****, denotada também por $\rho^1 \otimes \rho^2$. Como a notação é a mesma, é importante distinguir essas duas representações. Assim, uma é uma representação de $G \times G$ em $V_1 \otimes V_2$ e a outra é uma representação de G em $V_1 \otimes V_2$.*

Proposição 2.38 .

i) Se ρ^1 e ρ^2 são irredutíveis, $\rho^1 \otimes \rho^2$ é uma representação irredutível de $G_1 \times G_2$.

ii) Cada representação irredutível de $G_1 \times G_2$ é isomorfa a uma representação $\rho^1 \otimes \rho^2$, onde ρ^1 e ρ^2 são representações irredutíveis de G_1 e G_2, respectivamente.

Prova.

i) Lembrando que uma representação é irredutível se, e somente, se seu caracter tem norma 1 (isto é, $(\chi \mid \chi) = 1$), então se ρ^1, ρ^2 e $\rho^1 \otimes \rho^2$ tem caracteres χ_1, χ_2 e χ respectivamente, temos:

$$(\chi_1 \mid \chi_1) = \frac{1}{g_1} \sum_{s_1 \in G_1} \mid \chi_1(s_1) \mid^2 = 1$$

$$(\chi_2 \mid \chi_2) = \frac{1}{g_2} \sum_{s_2 \in G_2} \mid \chi_2(s_2) \mid^2 = 1$$

onde g_1 e g_2 são as ordem de G_1 e G_2 respectivamente. Multiplicando essas duas equações temos:

$$(\chi \mid \chi) = \frac{1}{g_1 g_2} \sum_{s_1, s_2} \mid \chi(s_1, s_2) \mid^2 = 1.$$

ii) Sabemos que os caracteres irredutíveis de $G_1 \times G_2$ formam uma base para o espaço das funções de classe sobre $G_1 \times G_2$. Mostremos então que os caracteres $\chi_1(s_1)\chi_2(s_2)$ de $G_1 \times G_2$ geram o espaço das funções de classe de $G_1 \times G_2$. Para isto é suficiente mostrar que toda função f de classe sobre $G_1 \times G_2$ que é ortogonal

aos caracteres na forma $\chi_1(s_1)\chi_2(s_2)$ é nula.

Suponha então que f seja uma função dessa. Então:

$$\sum_{s_1,s_2} f(s_1,s_2)\overline{\chi_1(s_1)\chi_2(s_2)} = 0. \tag{2.2}$$

Fixando χ_2 e pondo $f'(s_1) = \sum_{s_2 \in G_2} f(s_1,s_2)\overline{\chi_2(s_2)}$, temos que f' é uma função de classe sobre G_1. De fato:

$$\begin{aligned} f'(s_1t_1) &= \sum_{s_2\in G_2} f(s_1t_1,s_2)\overline{\chi_2(s_2)} \\ &= \sum_{s_2\in G_2} f\left[(s_1,s_2)(t_1,e_2)\right]\overline{\chi_2(s_2)} \\ &= \sum_{s_2\in G_2} f\left[(t_1,e_2)(s_1,s_2)\right]\overline{\chi_2(s_2)} \\ &= \sum_{s_2\in G_2} f(t_1s_1,s_2)\overline{\chi_2(s_2)} \\ &= f'(t_1s_1). \end{aligned}$$

Portanto, de (2.2) temos:

$$0 = \sum_{s_1,s_2} f(s_1,s_2)\overline{\chi_1(s_1)\chi_2(s_2)} = \sum_{s_1} f'(s_1)\overline{\chi_1(s_1)},$$

para todo caracter irredutível χ_1 de G_1. Logo $f' = 0$. Agora, fixando $s_1 \in G_1$, vamos definir a função sobre G_2 dada por $f_{s_1}(s_2) = f(s_1,s_2)$. Note que f_{s_1} é uma função de classe sobre G_2. Ademais

$$(f_{s_1} \mid \chi_2) = \frac{1}{g_2}\sum_{s_2} f(s_1,s_2)\overline{\chi_2(s_2)} = \frac{1}{g_2}f'(s_1) = 0.$$

Como χ_2 foi tomado de forma arbitrária, segue que $(f_{s_1} \mid \chi_2) = 0$ para todo caracter χ_2 irredutível de G_2, donde $f_{s_1} = 0$, ou seja, $f(s_1,s_2) = 0$.

■

Sendo assim, o estudo sobre as representações de $G_1 \times G_2$ fica reduzido ao estudo de representações de G_1 e de G_2.

2.6 Representações induzidas

Definição 2.39 ***Representação induzida:***
Sejam $\rho : G \to GL(V)$ uma representação linear do grupo G, ρ_H sua restrição a um subgrupo H de G. Sendo W uma sub-representação de ρ_H, isto é, um subespaço de V estável por H, denotemos por $\theta : H \to GL(W)$ tal representação de H em W. Dado $s \in G$, o subespaço $\rho_s(W)$ depende somente da classe lateral sH, visto que $\rho_t(W) = W$ para todo $t \in H$, e então $\rho_{st}(W) = \rho_s(\rho_t(W)) = \rho_s(W)$. Se σ é uma classe lateral à esquerda de H, podemos definir o subespaço W_σ como sendo $\rho_s(W)$ para qualquer $s \in \sigma$. Ademais dado $s' \in G$, sendo σ' a classe lateral do elemento $s's \in G$, então $\rho_{s'}(W_\sigma) = W_{\sigma'}$, com $s \in \sigma$. Dessa forma o subespaço

$$\sum_{\sigma \in G/H} W_\sigma \leqslant V$$

é uma sub-representação de V. Dizemos que a representação ρ de G é induzida pela representação θ de H em W se V é igual à soma direta de W_σ, $\sigma \in G/H$, isto é, $V = \bigoplus_{\sigma \in G/H} W_\sigma$. Podemos reescrever isso dando as seguintes condições:

i) Cada $v \in V$ pode ser escrito de forma única como $\sum_{\sigma \in G/H} v_\sigma$, com $v_\sigma \in W_\sigma$ para cada $\sigma \in G/H$.

ii) Se R é um sistema de representantes de G/H, o espaço vetorial V é a soma direta de $\rho_r(W)$, com $r \in R$. Em particular, temos $dim V = \sum_{r \in R} dim \rho_r(W) = \sum_{r \in R} dim W = (G : H) \cdot dim W$.

Exemplo 11 *São exemplos de representações induzidas:*

i) Sendo V a representação regular de G, o espaço V tem uma base $\{v_s;\ s \in G\}$ tal que $\rho_s(v_t) = v_{st}$ para todos $s, t \in G$. Seja W o subespaço de V com base $\{v_t;\ t \in H\}$, e a representação θ de H em W é a representação regular de H. Temos então que ρ é induzida por θ, pois dado $v \in V$ existem escalares $\lambda_s \in \mathbb{C}$ tais que $v = \sum_{s \in G} \lambda_s v_s$. Agrupando os vetores $\lambda_s v_s$ tais que seus índices pertencem à mesma classe lateral σ de H, denotemos a soma deles por v_σ e teremos então

$v = \sum_{\sigma \in G/H} v_\sigma$, *donde* $V = \sum_{\sigma \in G/H} W_\sigma$. *Como* $\sum_{\sigma \in G/H} dim W_\sigma = (G : H) \cdot \mid H \mid = \mid G \mid = dim V$, *temos que a soma* $V = \sum_{\sigma \in G/H} W_\sigma$ *é direta.*

ii) *Note que se* σ *é uma classe lateral de* H, *então* $s\sigma = \{st;\, t \in \sigma\}$ *é também uma classe lateral de* H. *Supondo que* V *tenha uma base* $\{v_\sigma;\, \sigma \in G/H\}$, *definamos a representação* ρ *de* G *em* V *pondo* $\rho_s(v_\sigma) = v_{s\sigma}$. *Obtemos a representação de permutação associada a* G/H. *O vetor* v_H *correspondente à classe lateral* H *de* H *é invariante por* H, *isto é,* $\rho_t(v_H) = v_H$ *para todo* $t \in H$. *A representação de* H *no subespaço gerado por* v_H *é a representação trivial de* H. *É claro que essa representação induz a representação* ρ *de* G *em* V.

iii) *Se* $\rho^1 : G \to GL(V_1)$ *é induzida por* $\theta^1 : H \to GL(W_1)$ *e* $\rho^2 : G \to GL(V_2)$ *é induzida por* $\theta^2 : H \to GL(W_2)$, *onde* W_i *é subespaço de* V_i *para* $i = 1, 2$, *então* $\rho^1 \oplus \rho^2 : G \to GL(V_1 \oplus V_2)$ *é induzida por* $\theta^1 \oplus \theta^2 : H \to GL(W_1 \oplus W_2)$. *De fato, como* ρ^1 *é induzida por* θ^1, *então*

$$V_1 = \bigoplus_{\sigma \in G/H} (W_1)_\sigma.$$

Analogamente, como ρ^2 *é induzida por* θ^2, *então*

$$V_2 = \bigoplus_{\sigma \in G/H} (W_2)_\sigma.$$

Tomando o subespaço $W = W_1 \oplus W_2$ *de* $V_1 \oplus V_2$, *temos que*

$$\rho^1_t(W_1) \oplus \rho^2_t(W_2) = \theta^1_t(W_1) \oplus \theta^2_t(W_2) = W_1 \oplus W_2 \quad \forall t \in H.$$

Logo, W *é invariante por* H *e podemos considerar a restrição* $\theta^1 \oplus \theta^2 : H \to GL(W_1 \oplus W_2)$. *Dado* $s \in \sigma$, *então*

$$W_\sigma = (\rho^1 \oplus \rho^2)_s(W) = \rho^1_s(W_1) \oplus \rho^2_s(W_2) = (W_1)_\sigma \oplus (W_2)_\sigma$$

e portanto

$$\begin{aligned} V_1 \oplus V_2 &= \left(\bigoplus_{\sigma \in G/H} (W_1)_\sigma \right) \oplus \left(\bigoplus_{\sigma \in G/H} (W_2)_\sigma \right) \\ &= \bigoplus_{\sigma \in G/H} ((W_1)_\sigma \oplus (W_2)_\sigma) \\ &= \bigoplus_{\sigma \in G/H} W_\sigma. \end{aligned}$$

iv) Suponha que a representação ρ' de G em V' é induzida pela representação θ' de H em W'. Se W_1 é um subespaço de W' estável por H, o subespaço $V = \sum_{r\in R} \rho_r(W_1)$ de V' é estável por G, onde R é um sistema de representantes das classes laterais de H em G. A representação de G em V é induzida pela representação de H em W_1. De fato, dados $s \in G$ e $r \in R$, como $sr \in G$, então $sr = r't$, com $r' \in R$ e $t \in H$, e como W_1 é estável por H, então $\rho_t(W_1) = \theta'_t(W_1) = W_1$. Daí temos:

$$\rho_s(\rho_r(W_1)) = \rho_{sr}(W_1) = \rho_{r't}(W_1) = \rho_{r'}(W_1) \subseteq V$$

e portanto

$$\rho_s(V) = \left(\sum_{r\in R} \rho_s(\rho_r(W_1))\right) \subseteq V$$

ou seja, V é estável por G. Ademais, como W_1 é subespaço de W', então $\rho_r(W_1)$ é subespaço de $\rho_r(W')$. Tendo isso em vista, como por hipótese V' é induzida por W', então a soma $\sum_{r\in R} \rho_r(W')$ é direta, e temos então que a soma $\sum_{r\in R} \rho_r(W_1)$ também é uma soma direta.

Lema 2.1 *Suponha que a representação ρ de G em V seja induzida pela representação θ de H em W. Seja $\rho' : G \to GL(V')$ uma representação de G e seja $f : W \to V'$ uma transformação linear tal que $f(\theta_t(w)) = \rho'_t(f(w))$ para todos $t \in H$ e $w \in W$. Então existe, e é única, a transformação linear $F : V \to V'$ que estende f e que satisfaz $F \circ \rho_s = \rho'_s \circ F$ para todo $s \in G$.*

Prova.

Unicidade.

Suponha que F satisfaz as condições do enunciado do lema. Se $v \in \rho_s(W)$, temos $\rho_s^{-1}(v) \in W$, donde

$$F(v) = F(\rho_s(\rho_s^{-1}(v))) = \rho'_s(F(\rho_s^{-1}(v))) = \rho'_s(f(\rho_s^{-1}(v))).$$

Essa fórmula determina F de modo único em $\rho_s(W)$, e como por hipótese ρ é induzida por θ, temos que V é soma direta dos subespaços $\rho_s(W)$, $s \in G$, e isso determina F de forma única em todo V.

Existência.

Inicialmente, sendo $s \in G$, $t \in H$ e $v \in \rho_s(W)$, então $v = \rho_s(w)$ para algum $w \in W$. Temos:

$$\begin{aligned}
\rho'_{st}(f(\rho_{st}^{-1}(v))) &= \rho'_s(\rho'_t(f(\rho_t^{-1}(\rho_s^{-1}(\rho_s(w)))))) \\
&= \rho'_s(\rho'_t(f(\rho_t^{-1}(w)))) \\
&= \rho'_s(\rho'_t(f(\theta_{t^{-1}}(w)))) \\
&= \rho'_s(\rho'_t(\rho'_{t^{-1}}(f(w)))) \\
&= \rho'_s(f(w)) \\
&= \rho'_s(f(\rho_s^{-1}(\rho_s(w)))) \\
&= \rho'_s(f(\rho_s^{-1}(v))).
\end{aligned}$$

Daí segue que é constante a expressão $\rho'_{s'}(f(\rho_{s'}^{-1}(v)))$, com $v \in \rho_s(W)$ e quando s' corre em σ, onde σ é a classe lateral de s. Além do mais, $\rho_s(W) = \rho_{s'}(W)$.

Dado $v \in W_\sigma$, escolhendo $s \in \sigma$, definamos $F(v)$ pela formula $F(v) = \rho'_s(f(\rho_s^{-1}(v)))$. Como vimos anteriormente, essa expressão dá o mesmo resultado seja qual for a escolha do $s \in \sigma$, e portanto F está bem definida. Como V é a soma direta dos W_σ, então temos de fato uma transformação com domínio V. Dado $v \in V$, temos $v = \sum_{r \in R} v_r$, com R sendo um conjunto transversal de representantes de G/H, $v_r \in W_\sigma$ onde σ é a classe rH. Além do mais, note que $\rho_s(v_r) \in W_{srH}$, e

então temos $F(\rho_s(v_r)) = \rho'_{sr}(f(\rho_{(sr)^{-1}}(\rho_s(v_r))) = \rho'_s(\rho'_r(f(\rho_r^{-1}(v_r))))$. Daí

$$\begin{aligned}
\rho'_s(F(v)) &= \rho'_s\left(F\left(\sum_{r\in R} v_r\right)\right) \\
&= \rho'_s\left(\sum_{r\in R} F(v_r)\right) \\
&= \rho'_s\left(\sum_{r\in R} \rho'_r(f(\rho_r^{-1}(v_r)))\right) \\
&= \sum_{r\in R} \rho'_s(\rho'_r(f(\rho_r^{-1}(v_r)))) \\
&= \sum_{r\in R} F(\rho_s(v_r)) \\
&= F\left(\rho_s\left(\sum_{r\in R} v_r\right)\right) \\
&= F(\rho_s(v)).
\end{aligned}$$

Vemos então que $\rho'_s \circ F = F \circ \rho_s$ para todo $s \in G$.

■

Proposição 2.40 *Sejam G um grupo e H subgrupo de G. Dada θ representação linear de H em W, existe, e é única, a menos de isomorfismo, uma representação linear $\rho : G \to GL(V)$ que é induzida por θ.*

Prova.

Existência: pelo item *iii*) dos exemplos de representações induzidas, vemos que podemos assumir que θ é irredutível. Neste caso, tomemos $\rho' : G \to GL(V')$ como sendo a representação regular de G e seja W' o subespaço de V' com base $\{v_t; t \in H\}$. Vimos que W' é estável por H. Sendo θ' a representação de H em W', então θ' é a representação regular de H. Como θ é irredutível, então θ é isomorfa a uma sub-representação de θ', e digamos que W_1 é uma sub-representação de W' que é isomorfa a θ. Pelo item *i*) dos exemplos de representações induzidas, temos que ρ' é induzida por θ'. Tomando $V := \sum_{r\in R} \rho'_r(W_1)$, temos pelo item *iv*) dos exemplos de representações induzidas que V é estável por G. Chamemos de ρ a representação de G em V. Então

ainda pelo mesmo item *iv*), a representação ρ é induzida pela representação de H em W_1 (lembrando que θ é isomorfa à representação de H em W_1).

Unicidade (a menos de isomorfismo): sejam $\rho : G \to GL(V)$ e $\rho' : G \to GL(V')$ duas representações induzidas pela representação θ. Considerando a aplicação f como sendo a inclusão de W em V', vemos, pelo **Lema 2.1**, que existe uma transformação linear $F : V \to V'$ que é a identidade em W e satisfaz $F \circ \rho_s = \rho'_s \circ F$ para todo $s \in G$, restando apenas que F seja um isomorfismo de espaços vetoriais para completar a prova do teorema. Note que $F(V)$ contém todos os $\rho'_s(W)$, e é igual a V'. Desde que V e V' têm a mesma dimensão $(G : H) \cdot dim W$, temos então que F é um isomorfismo de espaços vetoriais, o que prova o teorema.

■

Caracter de uma representação induzida.

Suponha que a representação ρ de G em V é induzida pela representação θ de H em W e sejam χ_ρ e χ_θ os caracteres de ρ e de θ, respectivamente. Como θ determina ρ, a menos de isomorfismo, estamos aptos a calcular χ_ρ em função de χ_θ, e o teorema a seguir nos mostra como fazer isso.

Proposição 2.41 *Sejam h a ordem de H e R um conjunto transversal de representantes de G/H. Para cada $u \in G$, temos:*

$$\chi_\rho(u) = \sum_{\substack{r \in R \\ r^{-1}ur \in H}} \chi_\theta(r^{-1}ur) = \frac{1}{h} \sum_{\substack{s \in G \\ s^{-1}us \in H}} \chi_\theta(s^{-1}us).$$

(em particular, $\chi_\rho(u)$ é uma combinação linear de valores de χ_θ na intersecção de H com as classe de conjugação de u em G)

Prova. O espaço V é a soma direta dos $\rho_r(W)$, com $r \in R$. Além disso, ρ_u permuta os $\rho_r(W)$ entre si. Mais precisamente, se escrevermos ur na forma $r_u t$, com $r_u \in R$ e $t \in H$, vemos que ρ_u manda $\rho_r(W)$ em $\rho_{r_u}(W)$. Para determinar $\chi_\rho(u) = Tr_V(\rho_u)$ podemos usar uma base de V que é a união de bases dos $\rho_r(W)$. Os índices r tais que $r \neq r_u$ dão zero nos termos da diagonal, nos outros dão o traço de ρ_u em $\rho_r(W)$. Obtemos então

$$\chi_\rho(u) = \sum_{r \in R_u} Tr_{\rho_r(W)}(\rho_{u,r}),$$

onde R_u denota o conjunto dos $r \in R$ tais que $r = r_u$ e $\rho_{u,r}$ é a restrição de ρ_u a $\rho_r(W)$. Observe que $r \in R_u$ se, e somente se, ur pode ser escrito como rt com $t \in H$, isto é, $r^{-1}ur \in H$.

Resta computar $Tr_{\rho_r(W)}(\rho_{u,r})$ para $r \in R_u$. Para fazer isso, note que ρ_r define um isomorfismo de W em $\rho_r(W)$, e que temos

$$\rho_r \circ \theta_t = \rho_{u,r} \circ \rho_r, \text{ com } t = r^{-1}ur \in H.$$

Daí segue que o traço de $\rho_{u,r}$ é igual ao do θ_t, isto é, $\chi_\theta(t) = \chi_\theta(r^{-1}ur)$. Obtemos então

$$\chi_\rho(u) = \sum_{r \in R_u} \chi_\theta(r^{-1}ur).$$

A segunda fórmula dada para $\chi_\theta(u)$ no enunciado segue da primeira, notando que todos os elementos $s \in G$ na classe lateral rH ($r \in R_u$) satisfazem $\chi_\theta(s^{-1}us) = \chi_\theta(r^{-1}ur)$. ■

Capítulo 3

Álgebras, graduações e o resultado principal

Neste capítulo introduziremos a noção de *Álgebra de Grupo*, que servirá como uma extensão de G para um espaço vetorial. Bem como introduziremos a noção de uma álgebra sobre o corpo dos complexos, graduações em álgebras e ações de grupos em uma álgebra. Finalizando com o resultado principal a respeito da equivalência entre a graduação e a ação de um grupo abeliano finito em uma álgebra. Para o estudos mais aprofundados indicamos a referência [5].

3.1 Álgebras e graduações de álgebras por um grupo

3.1.1 Álgebra de Grupo

Denotamos por $\mathbb{C}[G]$, a álgebra de G sobre $\mathbb{C}$, como sendo o conjunto formado pelos símbolos da forma $f = \sum_{s\in G} z_s s$, onde $z_s \in \mathbb{C}$. Definiremos que dois símbolos $f = \sum_{s\in G} z_s s$ e $f' = \sum_{s\in G} z'_s s$ em $\mathbb{C}[G]$ são iguais se, e somente se, $z_s = z'_s$ para todo $s \in G$. Denotaremos por "0" o símbolo $\sum_{s\in G} 0s$. Ademais, para $t \in G$ faremos a identificação

$t = \sum_{s\in G} z_s s$, onde $z_s = 0$ para $s \neq t$, e $z_t = 1$. Dessa forma temos $G \subset \mathbb{C}[G]$. Definiremos uma soma em $\mathbb{C}[G]$ e uma multiplicação por um escalar $\lambda \in \mathbb{C}$ da seguinte maneira: dados $f = \sum_{s\in G} z_s s$, $f' = \sum_{s\in G} z'_s s \in \mathbb{C}[G]$ tomaremos

$$f + f' := \sum_{s\in G} (z_s + z'_s)s$$
$$\lambda f := \sum_{s\in G} (\lambda z_s)s.$$

Desta maneira, sendo $f = \sum_{s\in G} z_s s$, $f' = \sum_{s\in G} z'_s s$, $f'' = \sum_{s\in G} z''_s s \in \mathbb{C}[G]$ e $\lambda, \lambda' \in \mathbb{C}$, temos que:

A_1) " $+$ " é associativa:

$$\begin{aligned}(f + f') + f'' &= \sum (z_s + z'_s)s + \sum z''_s s \\ &= \sum ((z_s + z'_s) + z''_s)s \\ &= \sum (z_s + (z'_s + z''_s))s \\ &= \sum z_s s + \sum (z'_s + z''_s)s \\ &= f + (f' + f'').\end{aligned}$$

A_2) " $+$ " é comutativa:

$$f + f' = \sum (z_s + z'_s)s = \sum (z'_s + z_s)s = f' + f.$$

A_3) " $+$ " possui elemento neutro, a saber, o elemento "0" de $\mathbb{C}[G]$:

$$0 + f = \sum 0s + \sum z_s s = \sum (0 + z_s)s = \sum z_s s = f.$$

A_4) Todo elemento de $\mathbb{C}[G]$ possui inverso com respeito a " $+$ ":

$$f + (-f) = \sum z_s s + \sum (-z_s)s = \sum 0s = 0.$$

Ademais, com respeito à multiplicação por escalar temos:

M_1) A multiplicação por escalar satisfaz $\lambda(\lambda' f) = (\lambda\lambda')f$:

$$\lambda(\lambda' f) = \lambda \sum (\lambda' z_s)s = (\lambda\lambda') \sum z_s s = (\lambda\lambda')f.$$

M_2) A multiplicacção por escalar satisfaz $(\lambda + \lambda')f = \lambda f + \lambda' f$:

$$\begin{aligned}(\lambda + \lambda')f &= (\lambda + \lambda')\sum z_s s \\ &= \sum(\lambda + \lambda')z_s s \\ &= \sum(\lambda z_s + \lambda' z_s)s \\ &= \sum \lambda z_s s + \sum \lambda' z_s s \\ &= \lambda \sum z_s s + \lambda' \sum z_s s \\ &= \lambda f + \lambda' f.\end{aligned}$$

M_3) A multiplicação por escalar satisfaz $\lambda(f + f') = \lambda f + \lambda f'$:

$$\begin{aligned}\lambda(f + f') &= \lambda \sum(z_s + z'_s)s \\ &= \sum \lambda(z_s + z'_s)s \\ &= \sum(\lambda z_s + \lambda z'_s)s \\ &= \sum(\lambda z_s)s + \sum(\lambda z'_s)s \\ &= \lambda \sum z_s s + \lambda \sum z'_s s \\ &= \lambda f + \lambda f'.\end{aligned}$$

M_4) A multiplicação por escalar satisfaz $1f = f$:

$$1f = \sum(1z_s)s = \sum z_s s = f.$$

Dessa forma temos que $\mathbb{C}[G]$ é um espaço vetorial sobre o corpo dos complexos. Lembrando que $G \subset \mathbb{C}[G]$, claramente G é um conjunto gerador para $\mathbb{C}[G]$. Ademais G é $L.I.$, pois tomando escalares $\lambda_s \in \mathbb{C}$ tais que $\sum_{s\in G} \lambda_s s = 0 = \sum_{s\in G} 0s$, pela definição de igualdade de símbolos temos $\lambda_s = 0$ para todo $s \in G$. Portanto G é base para $\mathbb{C}[G]$, e daí $dim\mathbb{C}[G] =\mid G \mid$.

Definiremos agora uma multiplicação " $*$ " entre os elementos de $\mathbb{C}[G]$. Primeiramente, sendo $t \in G$, $z'_t \in \mathbb{C}$ e $f = \sum_{s\in G} z_s s$, definiremos a multiplicação " $*$ " como sendo:

$$(z'_t t) * f = (z'_t t) * \left(\sum_{s\in G} z_s s\right) := \sum_{s\in G}(z'_t z_s)(ts).$$

Então, para $f' = \sum_{t\in G} z'_t t$, definimos:

$$f' * f := \sum_{t\in G} ((z'_t t) * f).$$

Dessa forma, para $s, t \in G \subset \mathbb{C}[G]$ temos $ts = t*s$, ou seja, "$*$" *estende* a multiplicação de G e satisfaz:

i) $f * (f' + f'') = f * f' + f * f'' \qquad \forall f, f', f'' \in \mathbb{C}[G].$

ii) $(f' + f'') * f = f' * f + f'' * f \qquad \forall f, f', f'' \in \mathbb{C}[G].$

Consequentemente, temos $f * (f_1 + f_2 + \cdots + f_n) = f * f_1 + f * f_2 + \cdots + f * f_n$ e $(f_1 + \cdots + f_n) * f = f_1 * f + \cdots + f_n * f$ para $f, f_i \in \mathbb{C}[G]$.

iii) $(f * f') * f'' = f * (f' * f'') \qquad \forall f, f', f'' \in \mathbb{C}[G].$

iv) $\lambda(f * f') = (\lambda f) * f' = f * (\lambda f') \qquad \forall f, f' \in \mathbb{C}[G]; \lambda \in \mathbb{C}.$

Prova. Tomando $f = \sum_{s\in G} z_s s$, $f' = \sum_{t\in G} z'_t t$, $f'' = \sum_{h\in G} z''_h h \in \mathbb{C}[G]$ e $\lambda \in \mathbb{C}$.

i) Primeiramente, calculando $(z_s s) * (f' + f'')$:

$$\begin{aligned}
(z_s s) * (f' + f'') &= (z_s s) * \sum_{t\in G} (z'_t + z''_t)t \\
&= \sum_{t\in G} (z_s(z'_t + z''_t))(st) \\
&= \sum_{t\in G} (z_s z'_t + z_s z''_t)(st) \\
&= \sum_{t\in G} z_s z'_t(st) + \sum_{t\in G} z_s z''_t(st) \\
&= (z_s s) * \sum_{t\in G} z'_t t + (z_s s) * \sum_{t\in G} z''_t t \\
&= (z_s s) * f' + (z_s s) * f''.
\end{aligned}$$

Portanto

$$\begin{aligned} f*(f'+f'') &= \sum_{s\in G}((z_s s)*(f'+f'')) \\ &= \sum_{s\in G}((z_s s)*f' + (z_s s)*f'') \\ &= \sum_{s\in G}(z_s s)*f' + \sum_{s\in G}(z_s s)*f'' \\ &= f*f' + f*f''. \end{aligned}$$

ii) Basta notar que $\left(\sum_{t\in G} z_t t\right)*(z_s s) = \sum_{t\in G}(z_t z_s)(ts)$ e então a demonstração será análoga.

iii) Por um lado temos:

$$\begin{aligned} (f*f')*f'' &= \left(\sum_{s\in G}(z_s s)*f\right)*f'' \\ &= \left(\sum_{s\in G}\sum_{t\in G}(z_s z'_t)(st)\right)*\left(\sum_{h\in G} z''_h h\right) \\ &\overset{ii)}{=} \sum_{s\in G}\sum_{t\in G}\left([(z_s z'_t)(st)]*\sum_{h\in G} z''_h h\right) \\ &= \sum_{s\in G}\sum_{t\in G}\sum_{h\in G}(z_s z'_t z''_h)(sth). \end{aligned}$$

Por outro lado temos:

$$\begin{aligned} f*(f'*f'') &= f*\left(\sum_{t\in G}(z_t t)*f''\right) \\ &= \left(\sum_{s\in G} z_s s\right)*\left(\sum_{t\in G}\sum_{h\in G}(z'_t z''_h)(th)\right) \\ &\overset{i)}{=} \sum_{t\in G}\sum_{h\in G}\left(\left(\sum_{s\in G} z_s s\right)*(z'_t z''_h(th))\right) \\ &= \sum_{t\in G}\sum_{h\in G}\sum_{s\in G}(z_s z'_t z''_h)(sth) \\ &= \sum_{s\in G}\sum_{t\in G}\sum_{h\in G}(z_s z'_t z''_h)(sth). \end{aligned}$$

Portanto, $f*(f'*f'') = (f*f')*f''$.

iv) Basta notar que se $e \in G$ é o elemento neutro do grupo, então

$$f * (\lambda e) = \left(\sum_{s\in G} z_s s\right) * (\lambda e) = \sum_{s\in G}(z_s s) * (\lambda e) = \sum_{s\in G}(\lambda z_s)s = \lambda f$$

ou seja, $\lambda f = f * (\lambda e)$. Analogamente mostramos que $\lambda f = (\lambda e) * f$. Daí

$$\lambda(f * f') = (\lambda e) * (f * f') \overset{iii)}{=} ((\lambda e) * f) * f' = (\lambda f) * f'$$

$$(\lambda f) * f' = (f * (\lambda e)) * f' \overset{iii)}{=} f * ((\lambda e) * f') = f * (\lambda f').$$

■

Observação 3.1 *Em particular, $\mathbb{C}[G]$ forma um anel com unidade com a soma e multiplicação definidas nesse capítulo, a saber, a unidade é o elemento neutro $e \in G$. Dessa forma, denotaremos $f * f'$ apenas por ff'. Não é difícil ver que $\mathbb{C}[G]$ será um anel comutativo se, e somente se, G for um grupo abeliano.*

Observação 3.2 *Tomando para cada $t \in G$ a aplicação $\rho_t : \mathbb{C}[G] \to \mathbb{C}[G]$ definida por $\rho_t(f) = t * f$, então $\rho_t \in GL(\mathbb{C}[G])$ e a aplicação $\rho(t) = \rho_t$ de G em $GL(\mathbb{C}[G])$ é a representação regular de G.*

Observação 3.3 *Sendo $\mathbb{K}$ um corpo qualquer, podemos definir a álgebra de G sobre $\mathbb{K}$ de forma análoga, como sendo o conjunto $\mathbb{K}[G]$ dos símbolos na forma $\sum_{s\in G} a_s s$, com $a_s \in \mathbb{K}$. As propriedades apresentadas até aqui sobre $\mathbb{C}[G]$ se mantém no caso $\mathbb{K}[G]$, pois todas as propriedades necessárias aos $z_s \in \mathbb{C}$ os $a_s \in \mathbb{K}$ também têm.*

Observação 3.4 *Sejam G um grupo finito e $\rho : G \to GL(V)$ uma representação linear de G. Para cada $s \in G$ e $v \in V$, denotemos $sv := \rho_s(v)$. Podemos estender para $\mathbb{C}[G]$ pondo $fv = \sum_{s\in G} z_s sv$, para $f = \sum_{s\in G} z_s s \in \mathbb{C}[G]$. Em outras palavras, estamos criando uma "multiplicação por escalar" com os escalares sendo os elementos $f \in \mathbb{C}[G]$:*

$$V \ni fv := \sum_{s\in G} z_s \cdot \rho_s(v) \ .$$

Note que se $f, f' \in \mathbb{C}[G]$ e $v, u \in V$, então:

i) $f(v+u) = fu + fv$

ii) $(f+f')v = fv + f'v$

iii) $f(f'v) = (ff')v$

iv) $ev = v$, *onde* $e \in G$ *é o elemento neutro.*

Consequentemente, temos também

v) $0v = 0$ *e* $f0 = 0$

vi) $f(\lambda v) = (\lambda f)v = \lambda fv$

pois $\lambda v = \lambda ev = (\lambda e)v$, *e daí* $f(\lambda v) = f((\lambda e)v) = (f(\lambda e))v = ((\lambda e)f) = (\lambda f)v = \lambda(fv)$.
Reciprocamente, dada uma "multiplicação por escalar" em V *por elementos de* $\mathbb{C}[G]$ *cumprindo as 4 primeiras propriedades anteriores, então, definindo para cada* $s \in G$ *a função* ρ_s *de* V *em* V *dada por* $\rho_s(v) = sv$, *temos que* $\rho(s) = \rho_s$ *é uma representação linear de* G *em* V.

3.1.2 Álgebras

Definiremos agora o conceito de uma $\mathbb{C}$-*álgebra*, que será necessário mais adiante e que também justifica a nomenclatura de "*Álgebra de* G *sobre* $\mathbb{C}$" dada a $\mathbb{C}[G]$.

Definição 3.1 *Sejam* A *um espaço vetorial sobre* $\mathbb{C}$ *e* $*$ *uma operação em* A. *Dizemos que o par* $(A, *)$ *é uma* $\mathbb{C}$*-álgebra se* $*$ *satisfaz:*

i) $a*(b+c) = a*b + a*c$

ii) $(a+b)*c = a*c + b*c$

iii) $\lambda(a*b) = (\lambda a)*b = a*(\lambda b)$

para todos $a, b, c \in A$ *e* $\lambda \in \mathbb{C}$.

Nesse caso, denotamos $a * b$ apenas por ab e $(A, *)$ apenas por A. Definimos a dimensão $dimA$ da álgebra A como sendo a dimensão de A como espaço vetorial e dizemos que $\beta \subseteq A$ é uma base para a álgebra A se β é base de A com espaço vetorial. Dizemos ainda que:

i) A é uma *álgebra associativa* se $*$ é associativa, isto é $(ab)c = a(bc)$ para quaisquer $a, b, c \in A$.

ii) A é uma *álgebra unitária* (ou *álgebra com unidade*) se $*$ possui elemento neutro, isto é, se existe algum vetor $u \in A$ tal que $ua = au = a$ para todo $a \in A$. Nesse caso, dizemos que u *é a unidade de* A. Em certos casos convém denotar u por $1 = 1_A \in A$.

iii) A é uma *álgebra comutativa* se $*$ é comutativa, isto é, $ab = ba$ para quaisquer $a, b \in A$.

Observação 3.5 *Sendo β uma base de A, então qualquer aplicação $*' : \beta \times \beta \to A$ pode ser estendida em uma aplicação $* : A \times A \to A$ bilinear, isto é, $w * v$ é linear em w e em v, ou seja, $a * (b + \lambda c) = (a * b) + \lambda(a * c)$ e $(a + \lambda c) * b = (a * b) + \lambda(c * b)$ para quaisquer $a, b, c \in A$ e $\lambda \in \mathbb{C}$. Portanto, basta definir as imagens em A das multiplicações $a * b$ com $(a, b) \in \beta \times \beta$ que existirá, e será única, a multiplicação em A que satisfaz a definição de álgebra e estende a escolha de multiplicação feita em $\beta \times \beta$.*

Observação 3.6 *Sendo $\mathbb{K}$ um corpo, podemos definir de forma análoga uma $\mathbb{K}$-álgebra como sendo um espaço vetorial A sobre o corpo $\mathbb{K}$ munido de uma aplicação bilinear $* : A \times A \to A$.*

Exemplo 12 *São exemplos de $\mathbb{C}$-álgebras:*

i) $(M_n(\mathbb{C}), \cdot)$: *o espaço vetorial $M_n(\mathbb{C})$ das matrizes quadradas de ordem n com entradas complexas, munido da multiplicação usual de matrizes, é uma álgebra associativa e unitária (porém não comutativa para $n \geq 2$).*

ii) $(\mathbb{C}[x], \cdot) >$ *o espaço vetorial $\mathbb{C}[x]$ dos polinômios com coeficientes complexos, munido da multiplicação usual de polinômios, é uma álgebra associativa, comutativa e unitária.*

iii) *Considere o espaço vetorial* $\mathbb{C}^2$ *munido da multiplicação* $(x_1, y_1)(x_2, y_2) = (x_1y_2, 0)$. *Então para* $u = (x, y), v = (a, b), w = (z, t) \in \mathbb{C}^2$ *e* $\lambda \in \mathbb{C}$, *temos:*

$$u(v + w) = (x, y)(a + z, b + t) = (xb + xt, 0) = (xb, 0) + (xt, 0) = uv + uw$$

$$(u + v)w = (xt + at, 0) = (xt, 0) + (at, 0) = uw + vw$$

$$\lambda(uv) = \lambda(xb, 0) = ((\lambda x)b, 0) = (\lambda u)v = (x(\lambda b), 0) = u(\lambda v).$$

Portanto $\mathbb{C}^2$ *com essa multiplicação é uma álgebra, porém não é comutativa, pois* $(1, 1)(1, 0) = (0, 0)$ *e* $(1, 0)(1, 1) = (1, 0)$.
Não possui unidade, pois $(x, y)(0, 1) = (0, 1) \Rightarrow (x, 0) = (0, 1)$, *ou seja,* $1 = 0$, *o que é um absurdo. Portanto não existe nenhum vetor* $1_{\mathbb{C}^2} \in \mathbb{C}^2$ *tal que* $1_{\mathbb{C}^2}(0, 1) = (0, 1)$. *Por fim, esta álgebra não é associativa, pois* $[(1, 0)(1, 1)](0, 1) = (1, 0)$ *e* $(1, 0)[(1, 1)(0, 1)] = (0, 0)$.

iv) *Sendo* G *um grupo finito, então* $\mathbb{C}[G]$ *é uma álgebra associativa, unitária, com dimensão* $\mid G \mid$, *e caso* G *seja abeliano, então* $\mathbb{C}[G]$ *é comutativa.*

v) *Considere o espaço vetorial* $L = M_n(\mathbb{C})$. *Sendo "*$\cdot$*" o produto usual de matrizes, definamos em* L *a operação* $A * B = A \cdot B - B \cdot A$. *Dadas* $A, B, C \in L$, *temos:*

$$\begin{aligned}(A + B) * C &= (A + B) \cdot C - C \cdot (A + B) \\ &= A \cdot C + B \cdot C - C \cdot A - C \cdot B \\ &= A \cdot C - C \cdot A + B \cdot C - C \cdot B \\ &= A * C + B * C.\end{aligned}$$

Note que $C * D = -D * C$ *para quaisquer* $C, D \in L$, *e então*

$$\begin{aligned}C * (A + B) &= -(A + B) * C \\ &= -(A * C + B * C) \\ &= -A * C - B * C \\ &= C * A + C * B.\end{aligned}$$

Dado agora $\lambda \in \mathbb{C}$,

$$\lambda(A * B) = \lambda(A \cdot B - B \cdot A) = \lambda A \cdot B - \lambda B \cdot A = (\lambda A) \cdot B - B \cdot (\lambda A) = (\lambda A) * B.$$

Por outro lado,

$$\lambda(A * B) = \lambda(-B * A) = -(\lambda(B * A)) = -((\lambda B) * A) = A * (\lambda B).$$

Portanto $(L, *)$ *é uma álgebra, claramente não comutativa. Ademais, também não é associativa.*

vi) Considerando no espaço vetorial $\mathbb{C}^n$ *a multiplicação* $(a_1, a_2, \ldots, a_n)(b_1, b_2, \ldots, b_n) = (a_1b_1, a_2b_2, \ldots, a_nb_n)$*, então* $\mathbb{C}^n$ *é uma álgebra comutativa com unidade.*

Definição 3.2 *Sejam* A *uma álgebra e* B *um subespaço vetorial de* A*. Dizemos que:*

i) B *é uma subálgebra de* A *se* $bc \in B$ *para quaisquer* $b, c \in B$*, ou seja,* B *é um subespaço vetorial fechado à multiplicação. Nesse caso,* B *com as restrições das operações é uma álgebra.*

ii) B *é um ideal à esquerda de* A *se* $ab \in B$ *para quaisquer* $a \in A$ *e* $b \in B$*, e é um ideal à direita de* A *se* $ba \in B$ *para quaisquer* $a \in A$ *e* $b \in B$*.* B *é dito um ideal bilateral de* A *se é simultaneamente ideal à esquerda e à direta. Em outras palavras, um ideal* B *é um subespaço vetorial com a propriedade de absorver multiplicações quando um dos fatores estiver em* B *(dependendo do lado). Note que todo ideal é uma subálgebra.*

Exemplo 13 *Exemplos e contraexemplos a respeito da definição anterior:*

i) Em $M_n(\mathbb{C})$*, com* $n \geq 2$*, note que* $B = \{Y \in M_n(\mathbb{C}) \mid detY = 0\}$ *tem a propriedade que, dados* $X \in M_n(\mathbb{C})$ *e* $Y \in B$*, então* $XY, YX \in B$*. Porém* B *não é um ideal nem uma subálgebra, pois* B *não é um subespaço vetorial. Tomando agora* $B' = \{Y \in M_n(\mathbb{C}) \mid Y \text{ é diagonal }\}$*, temos que* B' *é uma subálgebra, porém não é um ideal. Já*

$$B'' = \{Y \in M_n(\mathbb{C}) \mid Y \text{ tem apenas possivelmente a primeira coluna não nula }\}$$

é um ideal à esquerda de $M_n(\mathbb{C})$*.*
$M_n(\mathbb{C})$ *não possui ideais bilaterais, a não ser o próprio* $M_n(\mathbb{C})$ *e* $\{0_{n\times n}\}$*.*

ii) *Fixado $n \in \mathbb{N}$, tomando $P_n(\mathbb{C})$ como sendo o conjunto dos polinômios que não possuem grau superior a n, então $P_n(\mathbb{C})$ é um subespaço vetorial de $\mathbb{C}[x]$, porém não é uma subálgebra, pois não é fechado ao produto. Tomando agora $B = \{p \in \mathbb{C}[x] \mid p(1) \neq 0\}$, então B é fechado com respeito ao produto, porém não é uma subálgebra, pois não um é subespaço vetorial. Já tomando*

$$B' = \{p \in \mathbb{C}[x] \mid p(1) = 0\}$$

temos então que B' é um ideal bilateral de $\mathbb{C}[x]$, e consequentemente uma subálgebra.

iii) *Seja G um grupo finito de elemento neutro e. Tomando $B = \{\lambda e \mid \lambda \in \mathbb{C}\} = span_{\mathbb{C}}\{e\}$, o subespaço gerado por e, temos que B é uma subálgebra de $\mathbb{C}[G]$. Caso G tenha pelo menos 2 elementos, então B não é um ideal.*

iv) *Considerando a álgebra $L = M_n(\mathbb{C})$ com produto $A * B = AB - BA$, considere o subconjunto $sl_n(\mathbb{C})$ de L formado pelas matrizes com traço zero. Facilmente vemos que $sl_n(\mathbb{C})$ é um subespaço vetorial de L, pois $Tr(\lambda A + B) = \lambda Tr(A) + Tr(B)$ e daí, se $A, B \in sl_n(\mathbb{C})$, então $\lambda A + B \in sl_n(\mathbb{C})$.*
Ademais, lembrando que $Tr(AB) = Tr(BA)$, então

$$Tr(A * B) = Tr(AB - BA) = Tr(AB) - Tr(BA) = Tr(AB) - Tr(AB) = 0.$$

Segue que $A * B \in sl_n(\mathbb{C})$ para quaisquer $A, B \in L$, donde temos que $sl_n(\mathbb{C})$ é um ideal bilateral da álgebra $(L, *)$.

Definição 3.3 *Sejam $(A_1, *_1)$ e $(A_2, *_2)$ álgebras. Dizemos que uma aplicação $\varphi : A_1 \to A_2$ é um homomorfismo de álgebras quando φ é uma transformação linear entre os espaços vetoriais A_1 e A_2 e satisfaz $\varphi(a *_1 b) = \varphi(a) *_2 \varphi(b)$ para quaisquer $a, b \in A_1$. Caso φ seja bijetora, então dizemos que φ é um isomorfismo de álgebras.*

Note que se φ é bijetora, então φ^{-1} ainda é um isomorfismo de álgebras, pois já vimos no capítulo anterior que φ^{-1} continua sendo uma transformação linear. Agora note que dados $x, y \in A_2$, existem $a, b \in A_1$ tais que $x = \varphi(a)$ e $y = \varphi(b)$, o que equivale a $a = \varphi^{-1}(x)$ e $b = \varphi^{-1}(y)$. Então

$$\varphi^{-1}(xy) = \varphi^{-1}(\varphi(a)\varphi(b)) = \varphi^{-1}(\varphi(ab)) = ab = \varphi^{-1}(x)\varphi^{-1}(y).$$

Em particular, tomando $A = A_1 = A_2$, dizemos que um isomorfismo de álgebras de A em A é um automorfismo. Claramente o conjunto $Aut(A)$ dos automorfismos de A como álgebra é subconjunto do conjunto $GL(A)$ dos automorfismos de A somente como espaço vetorial. Note que se φ e ψ são automorfismos de A como álgebra, então temos para quaisquer $a, b \in A$:

$$\varphi(\psi(ab)) = \varphi(\psi(a)\psi(b)) = \varphi(\psi(a))\varphi(\psi(b)).$$

Portanto $\varphi \circ \psi$ é também um isomorfismo de álgebras (de modo geral, a composição de isomorfismos de álgebras ainda é um isomorfismo de álgebras), ou seja, $\varphi \circ \psi \in Aut(A)$. Como já observado, se $\psi \in Aut(A)$, então $\psi^{-1} \in Aut(A)$, e disso concluímos que

$$\varphi, \psi \in Aut(A) \Rightarrow \varphi \circ \psi^{-1} \in Aut(A).$$

Como $Id_A \in Aut(A) \neq \emptyset$, temos que $Aut(A)$ é subgrupo de $GL(A)$, e daí segue que, em particular, $Aut(A)$ é também um grupo. Assim, podemos olhar para as representações $\rho : G \to GL(A)$ tais que $\rho(G) \subseteq Aut(A)$. Caso isso aconteça, podemos considerar o homomorfismo de grupos $\rho : G \to Aut(A)$.

Definição 3.4 *Vamos definir uma ação de um grupo G em uma álgebra A como sendo uma ação de G sobre o conjunto A que satisfaça também:*

i) $s \cdot (\lambda a + b) = \lambda s \cdot a + s \cdot b$

ii) $s \cdot (ab) = (s \cdot a)(s \cdot b)$

para quaisquer $s \in G$, $a, b \in A$ e $\lambda \in \mathbb{C}$.

Note que dada uma ação $\cdot : G \times A \to A$, de G na álgebra A, definimos para cada $s \in G$ a aplicação

$$\rho_s : A \to A$$
$$a \mapsto \rho_s(a) = s \cdot a$$

Como $\rho_s(\rho_{s^{-1}}(a)) = s \cdot (s^{-1} \cdot a) = a$ e $\rho_{s^{-1}}(\rho_s(a)) = a$, temos que cada aplicação ρ_s admite uma inversa e portanto é bijetora. Ademais, como $t \cdot (s \cdot a) = (ts) \cdot a$

temos $\rho_t\rho_s = \rho_{ts}$, donde a aplicação $\rho : G \to GL(A)$, definida por $\rho(s) = \rho_s$, é um homomorfismo de grupos. Ademais, como

$$\rho_s(ab) = s \cdot (ab) = (s \cdot a)(s \cdot b) = \rho_s(a)\rho_s(b),$$

temos $\rho_s \in Aut(A)$. Com tudo isso temos que

$$\rho : G \to Aut(A)$$
$$s \mapsto \rho(s) = \rho_s$$

é um homomorfismo de grupos.

Reciprocamente, dado um homomorfismo $\rho : G \to Aut(A)$, definindo $s{\cdot}a := \rho_s(a)$, temos que $\cdot : G \times A \to A$ é uma ação de G na álgebra A.

3.1.3 Graduação de uma álgebra por um grupo

Para prosseguirmos com o intuito desse trabalho, vamos definir o que é uma graduação de uma álgebra A por um grupo G, que consiste em decompor a álgebra A em uma soma direta de subespaços de uma forma compatível com a operação do grupo G.

Observação 3.7 *Seja A uma álgebra, para $\emptyset \neq B, C \subseteq A$. Definimos de forma intuitiva o conjunto $BC = \{bc \mid \ b \in B \ e \ c \in C\}$.*

Definição 3.5 *Sejam A uma álgebra e G um grupo qualquer. Dizemos que A é G-graduada se A pode ser escrita como a soma de subespaços $A = \bigoplus_{s \in G} A^{(s)}$ tais que para quaisquer $s, t \in G$ tem-se $A^{(s)}A^{(t)} \subseteq A^{(st)}$. Os subespaços $A^{(s)}$ são chamados de componentes homogêneas de A, e um elemento não nulo $a \in A$ é dito homogêneo (ou homogêneo de grau s) se $a \in A^{(s)}$.*

Note que a definição não exige que G seja finito. Note também que da definição temos que qualquer $a \in A$ pode ser escrito de forma única como uma *soma finita* $a = \sum_{s \in G} a_s$, com $a_s \in A^{(s)}$ para todo $s \in G$. A soma ser finita, mesmo com os índices das parcelas podendo ser possivelmente infinitos, quer dizer que apenas uma quantidade finita desses a_s são não nulos, ou seja, estamos completando com zeros as parcelas referentes aos $A^{(s)}$ que na prática não apareceriam na decomposição de $a \in A$.

Se $B \subseteq A$ é um subespaço, dizemos que B é um *subespaço graduado* se $B = \bigoplus_{s\in G}\big(B \cap A^{(s)}\big)$, em outras palavras, B é graduado se qualquer $b = \sum_{s\in G} b_s \in B$, com $b_s \in A_{(s)}$, então $b_s \in B$ para todo $s \in G$. De forma similar definimos subálgebra graduada e ideal graduado. Note que se B é uma subálgebra (ou um ideal) graduado, então por si só B é uma álgebra graduada, bastando tomar $B^{(s)} := B \cap A^{(s)}$.

Note também que se H é um subgrupo de G é claro que $B := \bigoplus_{h\in H} A^{(h)}$ é uma subálgebra graduada de A. Em particular, sendo $e \in G$ o elemento neutro de G, então, tomando $H = \{e\}$, temos que $A^{(e)}$ é uma subálgebra de A.

Exemplo 14 *São exemplos de álgebras graduadas:*

i) *Qualquer álgebra A pode ser graduada por qualquer grupo G tomando $A^{(e)} = A$ e $A^{(s)} = \{0\}$, para $s \neq e$. Claramente temos $A^{(s)}A^{(t)} \subseteq A^{(st)}$ para quaisquer $s, t \in G$.*

ii) *Considere o grupo $(\mathbb{Z}, +)$, Então $A = \mathbb{C}[x]$ é uma álgebra $\mathbb{Z}$-graduada. De fato, para $n < 0$ tome $A^{(n)} = \{0\}$, para $n = 0$ tome $A^{(0)} = span_{\mathbb{C}}\{1\} = \mathbb{C}$, e para $n > 0$ tome $A^{(n)} = span_{\mathbb{C}}\{x^n\}$. Daí $\mathbb{C}[x] = \bigoplus_{n\in\mathbb{Z}} A^{(n)}$, e ademais é conhecido que $A^{(n)}A^{(m)} = A^{(n+m)}$.*

iii) *Sendo G um grupo finito, a álgebra $A = \mathbb{C}[G]$ é naturalmente G-graduada. De fato, tomando para cada $s \in G$ o subespaço $A^{(s)} = span_{\mathbb{C}}\{s\} = \{\lambda s \mid \lambda \in \mathbb{C}\}$, temos $A = \bigoplus_{s\in G} A^{(s)}$ e $A^{(s)}A^{(t)} = A^{(st)}$.*

iv) *Seja $G = \{e, a, b, c\} \simeq C_2 \times C_2$ o grupo de Klein. Então $A = M_2(\mathbb{C})$ é uma álgebra G-graduada. De fato, tomemos (lembrando que para $v \in V$ fixo estamos denotando por $span_{\mathbb{C}}\{v\} = \{\lambda v \mid \lambda \in \mathbb{C}\}$ o subespaço gerado por $\{v\}$):*

$$A^{(e)} = span_{\mathbb{C}}\left\{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right\}, \quad A^{(a)} = span_{\mathbb{C}}\left\{\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\right\}$$

$$A^{(b)} = span_{\mathbb{C}}\left\{\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right\}, \quad A^{(c)} = span_{\mathbb{C}}\left\{\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\right\}.$$

Por uma verificação direta vemos que $A = A^{(e)} \oplus A^{(a)} \oplus A^{(b)} \oplus A^{(c)}$ e que, para quaisquer $s, t \in G$, temos $A^{(s)}A^{(t)} = A^{(st)}$.

Observação 3.8 *Sendo* $\mathbb{Z}_2 = \{\overline{0}, \overline{1}\}$, *com a operação* $+$ *dada por:*

$$\overline{0}+\overline{0}=\overline{0} \qquad \overline{0}+\overline{1}=\overline{1}+\overline{0}=\overline{1} \qquad \overline{1}+\overline{1}=\overline{0}$$

então $(\mathbb{Z}_2, +)$ *é um grupo, isomorfo a* $(C_2, \cdot)$. *Se* A *é uma álgebra* $\mathbb{Z}_2$*-graduada, então dizemos que* A *é uma superálgebra.*

3.2 Resultado principal

Antes de prosseguirmos, no caso em que G é um grupo abeliano (comutativo) finito, vamos construir sobre o conjunto dos caracteres irredutíveis uma estrutura de grupo, isomorfa a G. Portanto, a partir daqui G será sempre abeliano.

Se G é um grupo abeliano finito, digamos que $\mid G \mid = g$, então vimos que a quantidade de caracteres irredutíveis distintos é igual a $g = \mid G \mid$. Sejam $\chi_1, \chi_2, ..., \chi_g$ os caracteres distintos de G, denotemos $\widehat{G} = \{\chi_1, \chi_2, \cdots, \chi_g\}$.

Observação 3.9 *Lembrando que todas as representações irredutíveis de* G *têm grau* 1, *então se* ρ *é uma representação irredutível de* G, *em sua forma matricial, temos que* $[\rho(s)]$ *é uma matriz* 1×1. *Logo podemos considerar* $\rho(s) \in \mathbb{C}^*$, *ou seja,* ρ *é um homomorfismo de* G *no grupo multiplicativo* $\mathbb{C}^*$. *Daí, se* χ *é o caracter* (*irredutível*) *de* ρ, *temos* $\chi(s) = \rho(s)$ *para* $s \in G$.

Note que se ρ^1 e ρ^2 são representações irredutíveis de G em V_1 e em V_2, respectivamente, de caracteres χ' e χ'', então $dimV_1 = dimV_2 = 1$. Daí $\rho^1 : G \to \mathbb{C}^*$ e $\rho^2 : G \to \mathbb{C}^*$. Considerando a representação $\rho = \rho^1 \otimes \rho^2$ de G em $V_1 \otimes V_2$ (**Definição 2.11**), como

$$dimV_1 \otimes V_2 = dimV_1 \cdot dimV_2 = 1$$

então ρ é irredutível e seu caracter irredutível χ satisfaz $\chi(s) = \chi'(s)\chi''(s)$.

Definindo em $\widehat{G} = \{\chi_1, \cdots, \chi_g\}$ a operação $(\chi_i, \chi_j) \mapsto \chi_i\chi_j = \chi$, com $\chi : G \to \mathbb{C}^*$ definido pela expressão $\chi(s) = \chi_i(s)\chi_j(s)$, temos então que essa operação está bem definida, pois pelo que foi visto acima temos que, de fato, $\chi \in \widehat{G}$.

$$\chi = \chi_i\chi_j : G \to \mathbb{C}^*$$
$$s \mapsto \chi(s) = (\chi_i\chi_j)(s) = \chi_i(s)\chi_j(s).$$

Ademais, o caracter da representação trivial ($\rho_0(s) = 1$ para todo $s \in G$) é elemento neutro para essa operação e claramente a operação é associativa e comutativa. Para verificarmos que todo caracter é inversível, veja que dada uma representação $\rho : G \to \mathbb{C}^*$, definindo a aplicação $\rho' : G \to \mathbb{C}^*$ por $\rho'(s) = (\rho(s))^{-1}$, então dados $s, t \in G$ temos:

$$\rho'(st) = \rho(st)^{-1} = (\rho(s)\rho(t))^{-1} = \rho(s)^{-1}\rho(t)^{-1} = \rho'(s)\rho(t)'.$$

Portanto ρ' é uma representação linear de G e seu caracter (que coincide com ρ') é o inverso do caracter de ρ na operação em $\widehat{G}$. Logo, temos que $\widehat{G} = \{\chi_1, \cdots, \chi_g\}$ é um grupo abeliano.

Definição 3.6 *Seja G um grupo abeliano finito. Chamamos o grupo $\widehat{G} = \{\chi_1, \ldots, \chi_g\}$ de grupo dual de G.*

Mostremos que G e $\widehat{G}$ são grupos isomorfos. Inicialmente, consideremos que G é cíclico. Lembrando que, pelo item *i*) da **Proposição 1.20**, temos que G é de fato abeliano.

Lema 3.1 *Se G é cíclico e finito, então G e $\widehat{G}$ são isomorfos.*

Prova. Como G é finito e $\mid \widehat{G} \mid = \mid G \mid$, pelo item *iii*) da **Proposição 1.20**, para que $G \simeq \widehat{G}$ é necessário e suficiente que $\widehat{G}$ seja cíclico.

Seja $g = \mid G \mid$ e γ um gerador de G. Cada elemento $s \in G$ pode ser identificado de forma única como $s = \gamma^m$, com $0 \leq m < g$. Tomando $\omega = e^{\frac{2\pi}{g}i} \in \mathbb{C}$, definamos a aplicação:

$$\chi : G \to \mathbb{C}^*$$
$$\gamma^m \mapsto \chi(\gamma^m) = \omega^m$$

Temos então $\chi \in \widehat{G}$. Dado $\psi \in \hat{G}$ arbitrário, tomando $s \in G$, pelo **Corolário 1.19**, temos $s^g = e$, onde e é o elemento neutro de G, e daí

$$\psi(s)^g = \psi(s^g) = \psi(e) = 1$$

donde $\psi(s)$ pertence ao grupo multiplicativo $C_g = \{z \in \mathbb{C}^* \mid z^g = 1\}$, que é gerado por ω. Desta forma segue que existe k tal que $\psi(\gamma) = \omega^k$, e daí

$$\psi(\gamma^m) = \psi(\gamma)^m = (\omega^k)^m = (\omega^m)^k = \chi(\gamma^m)^k$$

ou seja, $\psi = \chi^k$. Portanto $\widehat{G}$ é cíclico gerado por χ. ■

Lema 3.2 *Se H_1 e H_2 são grupos abelianos finitos, há um isomorfismo*

$$\widehat{H_1 \times H_2} \simeq \widehat{H_1} \times \widehat{H_2}.$$

Prova. Sejam χ um caracter de $H_1 \times H_2$, e_1 elemento neutro de H_1 e e_2 elemento neutro de H_2. Identifiquemos os subgrupos $H_1 \times \{e_2\}$ e $\{e_1\} \times H_2$ como H_1 e H_2, respectivamente. Sejam χ_1 e χ_2 as restrições de χ a H_1 e H_2, respectivamente, isto é,

$$\chi_1(s) = \chi(s, e_2) \qquad \chi_2(t) = \chi(e_1, t) \quad \forall s \in H_1, t \in H_2.$$

Deste modo temos que χ_1 e χ_2 são caracteres e

$$\chi(s,t) = \chi((s,e_2)(e_1,t)) = \chi(s,e_2)\chi(e_1,t) = \chi_1(s)\chi_2(t).$$

Consideremos então a aplicação:

$$\begin{aligned} \varphi : \widehat{H_1 \times H_2} &\to \widehat{H_1} \times \widehat{H_2} \\ \chi &\mapsto \varphi(\chi) = (\chi_1, \chi_2) \end{aligned}$$

Claramente

$$\varphi(\chi) = \varphi(\chi') \Rightarrow \chi = \chi'$$

donde segue que φ é injetiva e consequentemente bijetora, pois $\widehat{H_1 \times H_2}$ e $\widehat{H_1} \times \widehat{H_2}$ tem a mesma quantidade de elementos. Dados $\chi, \chi' \in \widehat{H_1 \times H_2}$, temos $\chi_1\chi_1' \in \widehat{H_1}$ e $\chi_2\chi_2' \in \widehat{H_2}$. Ademais

$$(\chi\chi')(s,t) := \chi(s,t)\chi'(s,t) = \chi_1(s)\chi_2(t)\chi_1'(s)\chi_2'(t) = (\chi_1(s)\chi_1'(s))(\chi_2(t)\chi_2'(t))$$

donde segue da definição de φ que $(\chi\chi')_1 = \chi_1\chi_1'$ e $(\chi\chi')_2 = \chi_2\chi_2'$. Portanto

$$\varphi(\chi\chi') = \varphi(\chi)\varphi(\chi')$$

concluindo que φ é um homomorfismo bijetor. ■

Para uma quantidade $k \in \mathbb{N}$ qualquer ainda temos $\widehat{H} \simeq \widehat{H_1} \times \widehat{H_2} \times \cdots \widehat{H_k}$, onde $H = H_1 \times H_2 \times \cdots \times H_k$. Basta tomar χ_j como sendo a restrição de $\chi \in H$ à H_j e definir $\varphi(\chi) = (\chi_1, \chi_2, \ldots, \chi_k)$.

Proposição 3.7 *Seja G um grupo abeliano finito. Então $G \simeq \widehat{G}$.*

Prova. Pela **Proposição 1.21**, existem $H_1, H_2, \ldots, H_k$ grupos cíclicos tais que

$$G \simeq H_1 \times H_2 \times \cdots \times H_k.$$

Como os H_j, $j = 1, 2, \ldots, k$, são abelianos e finitos, aplicando o **Lema 3.2** temos:

$$\widehat{G} \simeq \widehat{H_1} \times \widehat{H_2} \times \cdots \widehat{H_k}.$$

Aplicando agora o **Lema 3.1** nos H_j, já que são cíclicos e finitos, temos $\widehat{H_j} \simeq H_j$. Portanto pela **Proposição 1.15**, temos:

$$\widehat{H_1} \times \widehat{H_2} \times \cdots \widehat{H_k} \simeq H_1 \times H_2 \times \cdots H_k.$$

Finalmente concluímos que

$$\widehat{G} \simeq \widehat{H_1} \times \widehat{H_2} \times \cdots \widehat{H_k} \simeq H_1 \times H_2 \times \cdots H_k \simeq G$$

como queríamos provar. ■

Tomemos agora por hipótese global que A é uma $\mathbb{C}$-álgebra associativa e que G é um subgrupo abeliano finito de $Aut(A)$, digamos que $\mid G \mid = g$. Para $s \in G$ e $a \in A$, denotemos $a^s := s(a)$. Estenderemos de forma natural para $f = \sum_{s \in G} z_s s \in \mathbb{C}[G]$ como

$$a^f := \sum_{s \in G} z_s s(a) = \sum_{s \in G} z_s a^s \in A.$$

Definamos então em A uma multiplicação por escalar, onde os escalares são elementos de $\mathbb{C}[G]$, da forma $f \cdot a = a^f$, $a \in A, f \in \mathbb{C}[G]$, como na **Observação 3.4**.

Denotemos por 1 a unidade de $\mathbb{C}[G]$, que corresponde justamente à função identidade de A. Pondo os itens da **Observação 3.4** em nossa notação, para $a, b \in A$ e $f, f' \in \mathbb{C}[G]$ temos :

i) $(a+b)^f = a^f + b^f$

ii) $a^{f+f'} = a^f + a^{f'}$

iii) $(a^f)^{f'} = a^{f'f}$

iv) $a^1 = a$

v) $a^0 = 0$ e $0^f = 0$

vi) $(\lambda a)^f = a^{\lambda f} = \lambda a^f$.

Ademais, como $G \subseteq Aut(A)$, temos $s(ab) = s(a)s(b)$ para todos $a, b \in A$,$s \in G$, isto é, $(ab)^s = a^s b^s$ para $s \in G$.

Sejam $\chi_1, \chi_2, \ldots, \chi_g$ os caracteres irredutíveis de G. Definamos em $\mathbb{C}[G]$ os elementos:

$$f_1 = \frac{1}{g}\sum_{t\in G}\chi_1(t^{-1})t, \quad f_2 = \frac{1}{g}\sum_{t\in G}\chi_2(t^{-1})t, \quad \cdots, \quad f_g = \frac{1}{g}\sum_{t\in G}\chi_g(t^{-1})t.$$

Como $G \subseteq Aut(A)$, então cada $s \in G$ ainda é uma transformação linear do espaço vetorial A, daí temos que cada f_i é uma transformação linear do espaço vetorial A.

Dado $s \in G$, fixemos i com $1 \leq i \leq g$. Lembrando que cada χ_i é um homomorfismo visto que G é abeliano, temos em $\mathbb{C}[G]$:

$$\begin{aligned}
sf_i &= s\left(\frac{1}{g}\sum_{t\in G}\chi_i(t^{-1})t\right)\\
&= \frac{1}{g}\sum_{t\in G}\chi_i(t^{-1})st\\
&= \frac{1}{g}\sum_{t\in G}\chi_i(t^{-1}s^{-1}s)st\\
&= \frac{1}{g}\sum_{t\in G}\chi_i(t^{-1}s^{-1})\chi_i(s)st\\
&= \chi_i(s)\left(\frac{1}{g}\sum_{t\in G}\chi_i((st)^{-1})st\right)\\
&= \chi_i(s)\left(\frac{1}{g}\sum_{u\in G}\chi_i(u^{-1})u\right)\\
&= \chi_i(s)f_i.
\end{aligned}$$

Portanto, para qualquer $s \in G$, temos $sf_i = f_i s = \chi_i(s)f_i$. Tomando então f_i e f_j

temos

$$\begin{aligned} f_j f_i &= \left(\sum_{s\in G} \chi_j(s^{-1})s\right) f_i \\ &= \sum_{s\in G} \chi_j(s^{-1})(sf_i) \\ &= \sum_{s\in G} \chi_j(s^{-1})\chi_i(s)f_i \\ &= \left(\sum_{s\in G} \chi_j(s^{-1})\chi_i(s)\right) f_i \\ &=< \chi_j, \chi_i > f_i \\ &= \delta_{ij} f_i \end{aligned}$$

onde δ_{ij} é o delta de Kronecker, ou seja, $f_i^2 = f_i$ e $f_j f_i = 0$ para $i \neq j$. Podemos então deduzir que $\{f_1, f_2 \ldots, f_g\}$ é L.I. De fato, suponha que $\lambda_1, \lambda_2, \ldots, \lambda_g \in \mathbb{C}$ são tais que

$$\lambda_1 f_1 + \lambda_2 f_2 + \cdots + \lambda_g f_g = 0.$$

Fixando i e multiplicando por f_i ambos os lados da igualdade, teremos $\lambda_i f_i = 0$. Daí $\lambda_i = 0$ e portando $\{f_1, f_2 \ldots, f_g\}$ é L.I.

Ademais, sendo r_G o caracter da representação regular de G, pela **Proposição 2.26** temos que $r_G(1) = g$ e $r_G(s) = 0$ para $s \neq 1$, onde $1 \in G \subseteq \mathbb{C}[G]$ é o elemento neutro. Ademais, $r_G = \chi_1 + \chi_2 + \cdots + \chi_g$, já que todos os χ_i são representações de grau $n_i = 1$. Temos

$$\begin{aligned} f_1 + f_2 + \cdots + f_g &= \left(\frac{1}{g}\sum_{t\in G} \chi_1(t^{-1})t\right) + \left(\frac{1}{g}\sum_{t\in G} \chi_2(t^{-1})t\right) + \cdots + \left(\frac{1}{g}\sum_{t\in G} \chi_g(t^{-1})t\right) \\ &= \frac{1}{g}\sum_{t\in G} (\chi_1(t^{-1}) + \chi_2(t^{-1}) + \cdots + \chi_g(t^{-1}))t \\ &= \frac{1}{g}\sum_{t\in G} r_G(t^{-1})t \\ &= \frac{1}{g} r_G(1)1 \\ &= 1. \end{aligned}$$

Concluímos então que $f_1, \ldots, f_g$ são projeções. Portanto há uma decomposição em soma direta do espaço vetorial A associada a essas aplicações.

Para cada i definamos:

$$A^{(\chi_i)} = \{a \in A \mid a^s = \chi_i(s)a \ \forall s \in G\}.$$

Primeiramente, note que $0 \in A^{(\chi_i)} \neq \emptyset$. Tomando $a, b \in A^{(\chi_i)}$ e $\lambda \in \mathbb{C}$, e sendo $s \in G$ arbitrário, temos

$$(\lambda a + b)^s = (\lambda a)^s + b^s = \lambda a^s + b^s = \lambda\chi_i(s)a + \chi_i(s)b = \chi_i(s)(\lambda a + b)$$

donde $\lambda a + b \in A^{(\chi_i)}$. Temos então que $A^{(\chi_i)}$ é um subespaço de A. Ademais, dado $a \in A$ qualquer, então $a^{f_i} \in A^{(\chi_i)}$, pois tomando $s \in G$ arbitrário, temos

$$(a^{f_i})^s = a^{sf_i} = a^{\chi_i(s)f_i} = \chi_i(s)a^{f_i}$$

donde, de fato, temos $a^{f_i} \in A^{(\chi_i)}$ para todo $a \in A$. Logo, a imagem da projeção f_i está contida em $A^{(\chi_i)}$. Tomemos agora $b \in A^{(\chi_i)}$. Pela definição de $A^{(\chi_i)}$ temos $b^t = \chi_i(t)b$ para todo $t \in G$, e daí

$$\begin{aligned}
b^{f_i} &= b^{\frac{1}{g}\sum \chi_i(t^{-1})t} \\
&= \frac{1}{g}\left(\sum_{t\in G} b^{\chi_i(t^{-1})t}\right) \\
&= \frac{1}{g}\left(\sum_{t\in G} \chi_i(t^{-1})b^t\right) \\
&= \frac{1}{g}\left(\sum_{t\in G} \chi_i(t^{-1})\chi_i(t)b\right) \\
&= \frac{1}{g}\left(\sum_{t\in G} \chi_i(t^{-1}t)\right) b \\
&= \frac{1}{g} gb \\
&= b.
\end{aligned}$$

Portanto $b = b^{f_i}$ está na imagem de f_i, concluindo que $A^{(\chi_i)}$ é a imagem da projeção f_i, ou seja,

$$A = \bigoplus_{i=1}^{g} A^{(\chi_i)} = \bigoplus_{\chi\in\widehat{G}} A^{(\chi)}.$$

Mostremos que essa decomposição é uma $\widehat{G}$-graduação. De fato, dados $a \in A^{(\chi)}$ e $b \in A^{(\psi)}$, então $a^s = \chi(s)a$ e $b^s = \psi(s)b$ para todo $s \in G$. Daí

$$(ab)^s = a^s b^s = (\chi(s)a)(\psi(s)b) = (\chi(s)\psi(s))(ab) = [(\chi\psi)(s)](ab)$$

donde $ab \in A^{(\chi\psi)}$, ou seja,

$$A^{(\chi)}A^{(\psi)} \subseteq A^{(\chi\psi)} \quad \forall \chi, \psi \in \widehat{G}.$$

Portanto, com a ação natural de G em A dada por $s \cdot a = s(a)$, temos uma $\widehat{G}$-graduação em A. Como $\widehat{G} \simeq G$, podemos considerar uma G-graduação.

Para um caso mais geral, seja G um grupo abeliano finito qualquer agindo sobre a álgebra A. Como para cada $s \in G$ temos que a aplicação $a \mapsto s \cdot a$ define um automorfismo da álgebra A, podemos considerar que cada elemento de G é um automorfismo da álgebra A, relacionando s a $a \mapsto s \cdot a$. Dessa forma, podemos considerar $G \subseteq Aut(A)$ e, de forma mais geral, para qualquer grupo abeliano finto G agindo sobre a álgebra A, temos uma graduação de A por $\widehat{G}$ e consequentemente por G.

Por exemplo, caso $G = \{1, \varphi\} \simeq C_2$ (grupo cíclico de ordem 2), temos 2 caracteres irredutíveis, a saber, o caracter χ_0 da representação trivial e o caracter da representação sinal, o que satisfaz $\chi_1(1) = 1$ e $\chi_1(\varphi) = -1$. Temos então

$$A^0 := A^{(\chi_0)} = \{a \in A \mid \varphi(a) = a\}, \quad A^1 := A^{(\chi_1)} = \{a \in A \mid \varphi(a) = -a\}.$$

Então temos que $A = A^0 \oplus A^1$ é uma graduação para A. Com essa graduação temos que A é uma superálgebra.

Tomemos agora $A = \bigoplus_{s \in G} A^{(s)}$ uma G-graduação para A. Então, para cada $a \in A$, existem únicos $a_s \in A$ tais que $a = \sum_{s \in G} a_s$. Vamos definir uma ação de $\widehat{G}$ em A pondo

$$\chi \cdot a := \sum_{s \in G} \chi(s) a_s.$$

Isso determina de fato uma ação, pois dados $a = \sum a_s, b = \sum b_s \in A$, $\lambda \in \mathbb{C}$, $\chi, \psi \in \widehat{G}$ e $\chi_0 \in \widehat{G}$ o caracter trivial, temos:

$$\chi_0 \cdot a = \sum_{s \in G} \chi_0(s) a_s = \sum_{s \in G} a_s = a.$$

Como $\psi \cdot a = \sum_{s \in G} \psi(s) a_s$, note que $\psi(s)a_s \in A^{(s)}$, e portanto $\psi(s)a_s$ é a componente de $\psi \cdot a$ referente a $A^{(s)}$. Logo

$$\chi \cdot (\psi \cdot a) = \chi \cdot \left(\sum_{s \in G} \psi(s) a_s \right) = \sum_{s \in G} \chi(s)\psi(s) a_s = (\chi\psi) \cdot a.$$

Como $\lambda a_s + b_s$ é a componente de $\lambda a + b$ referente a $A^{(s)}$, temos:

$$\chi \cdot (\lambda a + b) = \sum_{s \in G} \chi(s)(\lambda a_s + b_s) = \lambda \sum_{s \in G} \chi(s) a_s + \sum_{s \in G} \chi(s) b_s = \lambda \chi \cdot a_s + \chi \cdot b.$$

Ademais, para $a = \sum a_s$ e $b = \sum b_t$, como $a_s b_t \in A^{(st)}$, temos $\chi \cdot (a_s b_t) = \chi(st) a_s b_t$. Também temos que χ é um homomorfismo, ou seja, $\chi(st) a_s b_t = (\chi(s) a_s)(\chi(s) b_t)$, donde temos

$$\chi \cdot (a_s b_t) = (\chi(s) a_s)(\chi_t(s) b_t).$$

Portanto, usando a já provada linearidade de " $\cdot$ ", temos

$$\begin{aligned}
\chi \cdot (ab) &= \chi \cdot \left(\left(\sum_{s \in G} a_s \right) \left(\sum_{t \in G} b_t \right) \right) \\
&= \chi \cdot \left(\sum_{s \in G} \sum_{t \in G} a_s b_t \right) \\
&= \sum_{s \in G} \sum_{t \in G} \chi \cdot (a_s b_t) \\
&= \sum_{s \in G} \sum_{t \in G} (\chi(s) a_s)(\chi_t(s) b_t) \\
&= \left(\sum_{s \in G} \chi(s) a_s \right) \left(\sum_{t \in G} \chi(t) b_t \right) \\
&= (\chi \cdot a)(\chi \cdot b)
\end{aligned}$$

concluindo que $\chi \cdot a = \sum \chi(s) a_s$ é de fato uma ação de $\widehat{G}$ na álgebra A. Como $\widehat{G}$ é isomorfo G, podemos considerar que isso é uma ação de G sobre A.

Tendo em vista essa reciprocidade, estamos prontos para anunciar o resultado

Teorema 3.8 *Sejam G um grupo abeliano finito e A uma $\mathbb{C}$-álgebra. Então, qualquer G-graduação da álgebra A define uma $\widehat{G}$-ação na álgebra A por automorfismos e vice-versa. Nessa situação, um subespaço $V \subseteq A$ é um subespaço graduado de A se, e somente se, V é invariante pela $\widehat{G}$-ação. Um elemento $a \in A$ é homogêneo na graduação se, e somente se, é autovetor para qualquer $\chi \in \widehat{G}$.*

Prova. Nos resta apenas mostrar a segunda afirmação e a terceira afirmação. Para a $\widehat{G}$-ação definida anteriormente, se $V = \bigoplus_{s \in G} V^{(s)}$ é um subespaço graduado de A, então $\chi \cdot V^{(s)} \subseteq V^{(s)}$ para todo $\chi \in \widehat{G}$ e $s \in G$.

Suponha agora que V é um subespaço de A invariante pela $\widehat{G}$-ação. Se V não é um subespaço graduado, então existe $v = v_{s_1} + v_{s_2} + \cdots + v_{s_k} \in V$, com $s_1, s_2, \ldots, s_k \in G$ distintos, onde $v_{s_1}, v_{s_2}, \ldots, v_{s_k} \notin V$. Tomando $\chi \in \widehat{G}$ tal que $\chi(s_1) = \lambda$ e $\chi(s_2) = \mu$, com $\lambda \neq \mu$ (a prova da existência desse caracter pode ser encontrada em [2], página 7, **Corollary 3.4**), então

$$u = \lambda v - \chi \cdot v = (\lambda - \mu)v_{s_2} + \cdots \in V.$$

Aplicando o mesmo procedimento a u, e assim por diante,Com o procedimento, chegamos a um múltiplo escalar não nulo de algum v_{s_j} que pertence a V, e daí v_{s_j} pertence a V, uma contradição. Esta contradição mostra que qualquer subespaço de A invariante pela $\widehat{G}$-ação é graduado. Em particular, se $dimV = 1$, temos a propriedade mencionada sobre os elementos homogêneos e os $\widehat{G}$-autovetores. ■

Bibliografia

[1] A. P. Brandão Júnior, *Notas de Aula da Disciplina Álgebra I*, Universidade Federal de Campina Grande, Unidade Acadêmica de Matemática, 2020. Não publicado.

[2] K. Conrad, *Character of abelian finite groups*, acessado em 06/08/2020 em <https://kconrad.math.uconn.edu/blurbs/grouptheory/charthy.pdf>.

[3] J. B. Fraleigh,*A First Course in Abstract Algebra*, Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont. 1967.

[4] A. García, Y. Lequain, *Álgebra: uma introdução*, Monografías de Matemática, 39. Instituto de Matemática Pura e Aplicada (IMPA), Rio de Janeiro, 1983.

[5] A. Giambruno, M. Zaicev, *Polynomial Identities and Asymptotic Methods*, Mathematical Surveys and Monographs 122, American Mathematical Society, Providence, RI, 2005.

[6] K. Hoffman, R. Kunze, *Linear Algebra*, Prentice-Hall Mathematics Series Prentice-Hall, Inc., Englewood Cliffs, N.J. 1961.

[7] F. C. P. Milies, *Anéis e Módulos*, Publicações do Instituto de Matemática e Estatística da Universidade de São Paulo, São Paulo, 1972.

[8] J. P. Serre, *Linear Representations of Finite Groups*, translated from the second French edition by Leonard L. Scott. Graduate Texts in Mathematics, Vol. 42. Springer-Verlag, New York-Heidelberg, 1977.