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

Teorema $p^a q^b$ de Burnside

por

Bruna Emanuelly Pereira Lucena

sob orientação do

Prof. Dr. Diogo Diniz Pereira da Silva e Silva

Campina Grande - PB
abril, 2015

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

Bruna Emanuelly Pereira Lucena

Teorema p^aq^b de Burnside

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

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

Campina Grande - PB, abril de 2015
Curso de Matemática, modalidade Bacharelado

Teorema p^aq^b de Burnside

Bruna Emanuelly Pereira Lucena

Trabalho de conclusão de curso defendido e aprovado em 13 de abril de 2015, pela Comissão Examinadora constituída pelos professores:

Prof. Ma. Josefa Itailma da Rocha
Examinadora

Prof. Dr. Antônio Pereira Brandão Júnior
Coorientador

com nota igual a:

Dedicatória

À minha mãe Élita e à memória de minha avó Davina, meu amigo Juarez e meu primo Yan.

Agradecimentos

No caminho da sabedoria te ensinei e pelas veredas da retidão te fiz andar (Provérbios; 4:11). Sou grata a Deus por seu infinito amor, por ter me dado saúde e força para chegar até aqui, por estar ao meu lado em qualquer situação, e mesmo diante das dificuldades não me deixar cair.

A esta Universidade, seu corpo docente, direção e administração. Em especial a Unidade Acadêmica de Matemática, por proporcionar um ambiente tão agradável, composto por professores e funcionários que realmente tornam este lugar a nossa segunda casa.

Aos meus orientadores Diogo Diniz e Antônio Brandão, por todo conhecimento transmitido, e em particular ao professor Brandão, não somente pela orientação nesse trabalho, mas por todo aprendizado durante o curso, de fato, um professor singular.

Ao grupo PET Conexões de Saberes Matemática e Estatística por esses quatro anos de aprendizado e rica experiência, serei eternamente grata.

Ao meu tutor Luiz Antônio, que foi quem me guiou e orientou nessa jornada, sempre disposto a me ajudar, mesmo quando não era sua atribuição. Fica um exemplo a ser seguido e uma amizade infindável.

Agradeço à minha família, em especial minha mãe Élita, um dos meus maiores exemplos, a pessoa responsável por eu estar aqui, que me ensinou o caminho certo a seguir, e a minha avó Davina (*in memoriam*), sem dúvida o meu maior incentivo para estudar, um presente na minha vida e na de todos que puderam conviver com sua presença.

Ao meu namorado Geovany, tão presente em minha vida, primeiramente como um grande amigo, e agora, como a pessoa com a qual eu hei de dividir essa vitória e todas as outras que estão por vir.

A todos os meus amigos e colegas, por todos os dias compartilhados, os momentos de felicidade e de tristeza, os dias e noites de estudo, não é exagero falar de finais de semana e feriados. Em especial Juarez Brito (*in memoriam*), com o qual gostaria de dividir esse momento, que tantas boas lembranças nos deixou, a lembrança de um grande amigo que se faz presente em nossos corações todos os dias.

Mesmo não citando todos os nomes, o meu obrigada a todos que direta ou indiretamente participaram dessa caminhada.

Consagre à Deus tudo que você faz e os seus planos serão bem sucedidos (Provérbios; 16:3).

Obrigada!

Resumo

O Teorema $p^a q^b$ de Burnside é um importante teorema na teoria de grupos e diz que grupos com tal ordem são solúveis. Esse teorema foi provado em 1904 pelo matemático inglês William Burnside (1852 – 1927), e a sua demonstração foi feita utilizando a teoria de Caracteres de um grupo, tema que se configura dentro da teoria das representações de um grupo. Apenas no final da década de 60 houve uma demonstração sem o uso dessa teoria. A teoria das representações busca caracterizar as formas que um grupo pode agir em um espaço vetorial e os efeitos dessas ações, isto é, através de um homomorfismo aplicar um grupo no conjunto das transformações lineares inversíveis de um espaço vetorial. Também podemos ver essas transformações como matrizes e utilizar toda a teoria da álgebra linear.

Abstract

The $p^a q^b$ Burnside Theorem is an important Theorem in theory of groups, which says that groups of such order are soluble. This theorem was proved in 1904 by the english mathematician Willian Burnside (1852 - 1927), and its demonstration was made using the Theory of Characters of Groups, a theme categorized in the Theory of Representation Groups. Only in the 60'th decade a demonstration was made without using this theory. The theory of representations aims to characterize the ways in which a groups may act in a vectorial space and the effects of these actions , that is, using a homomorfism, map a group in the set of the inversible linear transformations of a vectorial space. One can also see these linear transformation as matrices and in that point of view, utilize the whole theory of linear algebra.

Introdução

Nascido em 02 de julho de 1852 na cidade de Paddington, Londres, William Burnside foi um importante matemático em diversas áreas. Sua primeira publicação sobre a Teoria de Grupos Finitos foi em 1893. Em 1896 G. Frobenius começou a desenvolver a Teoria das Representações de um Grupo e a Teoria dos Caracteres. Burnside, vendo a relevência dos trabalhos de Frobenius, começou a usar esta teoria, e em 1904 publicou um de seus resultados mais importantes que diz que todo grupo de ordem $p^a q^b$, com p e q primos, é solúvel. Apesar de haver outra forma de demonstrar esse Teorema, o principal objetivo deste trabalho é demonstrá-lo fazendo uso da Teoria dos Caracteres.

Este trabalho consiste de 4 capítulos. No primeiro vamos expor definições e resultados preliminares que usaremos posteriormente, bem como indicaremos a notação utilizada no decorrer do texto. Esses resultados referem-se a grupos, álgebra linear e inteiros algébricos. No segundo capítulo, estudaremos a Teoria das Representações, com uma seção em especial para as representações irredutíveis. Essa teoria pode ser vista como o estudo das formas com que um grupo pode agir em em um espaço vetorial e as consequências dessas ações, e como o objetivo principal do trabalho não é falar apenas da Teoria das Representações, restringiremos apenas a grupos finitos e espaços vetoriais de dimensão finita.

No terceiro capítulo estudaremos a Teoria dos Caracteres, que, como já citada, foi desenvolvida inicialmente por Frobenius. Definiremos primeiramente o caracter de uma representação e em seguida estudamos a decomposição do caracter da representação regular, e por último o número de caracteres irredutíveis de um grupo finito. Dentre os resultados apresentados nesse capítulo, vale destacar o Lema de Schur e as relações de ortogonalidade.

No quarto capítulo, finalmente demonstramos o Teorema $p^a q^b$ de Burnside, assim como todos os resultados necessários preliminares. Um deles, também devido a Burnside, diz que se num grupo G o número de conjugados de algum elemento $g \neq 1$ é potência de um primo, então G não pode ser simples.

Capítulo 1

Preliminares

Neste capítulo apresentaremos alguns conceitos e resultados sobre grupos e álgebra linear que serão necessários para o estudo da Teoria de Representações e para o principal objetivo deste trabalho. Durante o texto, é assumido que o leitor possua um conhecimento dos conceitos mais básicos de Grupos e Álgebra Linear.

Para um leitor interessado numa leitura mais detalhada, indicamos as referências [1], [2], [3], [5] e [6] nas quais podem ser encontradas as demonstrações dos resultados aqui enunciados.

1.1 Grupos

Definição 1. Dizemos que um conjunto não vazio G, munido de uma operação binária

$$\begin{aligned} \cdot : G \times G &\longrightarrow G \\ (x, y) &\longmapsto xy \end{aligned}$$

é um grupo se satisfaz as seguintes condições:

1. Associatividade: $(xy)z = x(yz)$, para quaisquer $x, y, z \in G$.

2. Existência de elemento neutro: existe $e \in G$ tal que $xe = x = ex$, para todo $x \in G$.

3. Existência de elemento simétrico: para cada $x \in G$, existe $x^{-1} \in G$ tal que $xx^{-1} = x^{-1}x = e$.

No decorrer do texto vamos nos referir apenas a grupos finitos e a notação utilizada será a multiplicativa. Vamos usar o símbolo $|G|$ para denotar a ordem (número de elementos) de G.

São fatos conhecidos a unicidade do elemento neutro e do simétrico de cada elemento. Observe que $(x^{-1})^{-1} = x$ para todo $x \in G$.

Definição 2. Um grupo G é dito abeliano se $ab = ba$ para todo $a, b \in G$.

Definição 3. Dados dois elementos x, y de um grupo G, o comutador de x e y é definido como sendo o elemento $[x, y] = x^{-1}y^{-1}xy \in G$.

Definição 4. Para $g \in G$ e $n \in \mathbb{Z}$ definimos a potência de g como:

$$g^n = \begin{cases} e \quad , & \text{se} \quad n = 0, \\ \underbrace{g \cdot g \cdot \ldots \cdot g}_{n \text{ vezes}}, & \text{se} \quad n > 0, \\ (g^{-1})^{|n|}, & \text{se} \quad n < 0. \end{cases}$$

Propriedades básicas:

1. $(a^n)^{-1} = (a^{-1})^n = a^{-n}$
2. $a^{n+m} = a^n a^m$
3. $(a^n)^m = a^{nm}$

Definição 5. Sejam G um grupo e $\emptyset \neq S \subset G$. Dizemos que S é um subgrupo de G se valem

1. $xy \in S$, $\forall x, y \in S$.
2. $x^{-1} \in S$, $\forall x \in S$

Notação: $S \leqslant G$

Exemplo 1. *Para $a \in G$, consideremos o subconjunto $\langle a \rangle = \{a^n; n \in \mathbb{Z}\}$ de G. Temos que $\langle a \rangle$ é um subgrupo de G, chamado de subgrupo gerado por a. Ademais, dizemos que a tem ordem finita se existe $n \in \mathbb{N}$ tal que $a^n = e$. Neste caso, definimos a ordem de a, denotada por $o(a)$ como sendo*

$$o(a) = min\{n \in \mathbb{N}; a^n = e\}$$

Se não existe $n \in \mathbb{N}$ tal que $a^n = e$ dizemos que a tem ordem infinita e denotamos por $o(a) = \infty$.

Observe que se $o(a)$ é infinita, então $|\langle a \rangle|$ é infinita. Por outro lado, se $o(a)$ é finita igual a k, então $\langle a \rangle = \{e, a, a^2, \ldots, a^{k-1}\}$ e $|\langle a \rangle| = o(a)$.

Exemplo 2. *Sejam G um grupo, H um subgrupo de G e $a \in G$. Definimos o conjugado de H por a, denotado por H^a ou $a^{-1}Ha$, como sendo*

$$H^a = \{h^a; h \in H\} = \{a^{-1}ha; h \in H\}.$$

Temos que H^a é um subgrupo de G

.

Definição 6. Definimos o normalizador de H em G, denotado por $N_G(H)$, como sendo $N_G(H) = \{x \in G; H^x = H\}$.

Temos que $N_G(H)$ é um subgrupo de G e que $H \subseteq N_G(H)$.

Exemplo 3. *Sejam G um grupo, $a \in G$ e S um subconjunto não vazio de G. Definimos o centralizador de a em G, denotado por $C_G(a)$, e o centralizador de S em G, denotado por $C_G(S)$, como sendo*

$$C_G(a) = \{x \in G; xa = ax\} \quad e \quad C_G(S) = \{x \in G; xs = sx, \forall s \in S\} \ .$$

Temos que esses subconjuntos são subgrupos de G e que:

1. $b \in C_G(a) \Leftrightarrow ba = ab \Leftrightarrow a \in C_G(b)$.
2. $C_G(S) = \bigcap_{s \in S} C_G(s)$.

Definição 7. O subgrupo $C_G(G) = \{x \in G; xg = gx, \forall g \in G\}$ é chamado de centro de G e é denotado por $Z(G)$. É fácil ver que G é abeliano se, e somente se $Z(G) = G$.

Observação 1. *Se G é um grupo com $|G| = p^n$, com p primo e $n \in \mathbb{N}$, é um fato conhecido que $Z(G) \neq \{e\}$.*

Definição 8. Sejam G um grupo, H um subgrupo de G e $g \in G$. Definimos:

1. A classe lateral à direita de H contendo g, denotada por Hg, como sendo $Hg = \{hg; h \in H\}$.
2. A classe lateral à esquerda de H contendo g, denotada por gH, como sendo $gH = \{gh; h \in H\}$.

Observe que $g \in gH$ e $g \in Hg$. Além disso, podemos ter $Hg \neq gH$, no entanto, num grupo abeliano a igualdade claramente é válida.

Observação 2. *Sejam G um grupo, $a, b, g \in G$ e $H \leq G$ temos*

1. $Ha = Hb \Leftrightarrow ab^{-1} \in H$.
2. $aH = bH \Leftrightarrow a^{-1}b \in H$.
3. *O número de distintas classes laterais à direita de H em G é igual ao número de distintas classes laterais à esquerda de H em G. Este número é chamado índice de H em G e denotado por $|G : H|$.*
4. *Observa-se facilmente que as aplicações*

$$\begin{array}{rcl} \psi_1 : H & \longrightarrow & Hg \\ h & \longmapsto & \psi_1(h) = hg \end{array} \quad e \quad \begin{array}{rcl} \psi_2 : H & \longrightarrow & gH \\ h & \longmapsto & \psi_2(h) = gh \end{array}$$

são bijeções. Segue então que $|Hg| = |H| = |gH|$.

Teorema 1 (Lagrange). *Sejam G um grupo finito e H um subgrupo de G. Então, $|G| = |G : H||H|$ e consequentemente $|H|$ divide $|G|$.*

Definição 9. Sejam G um grupo e $N \leqslant G$. Dizemos que N é um subgrupo normal de G se $gN = Ng$, para todo $g \in G$.
Notação: $N \trianglelefteq G$.

Sendo G um grupo qualquer, é fácil ver que G e $\{e\}$ são subgrupos normais de G . No caso em que G e $\{e\}$ são os únicos subgrupos normais de G, dizemos que G é um grupo **simples**.

Sejam G um grupo e $N \trianglelefteq G$. Sabemos que $Ng = gN$ para todo $g \in G$, assim podemos falar de classe lateral sem nos preocupar com direita ou esquerda. Denotemos por $\frac{G}{N}$ o grupo de todas as classes laterais de N em G, isto é, $\frac{G}{N} = \{gN; g \in G\}$. Definamos a seguinte operação

$$\begin{array}{rcl} \cdot : \dfrac{G}{N} \times \dfrac{G}{N} & \longrightarrow & \dfrac{G}{N} \\ (aN, bN) & \longmapsto & (aN)(bN) = abN \end{array}$$

Primeiramente, observemos que essa operação está bem definida. Com efeito, se $a, b, a_1, b_1 \in G$ são tais que $aN = a_1N$ e $bN = b_1N$, então $a^{-1}a_1 \in N$ e $b^{-1}b_1 \in N$. Segue da normalidade de N que $(ab)^{-1}a_1b_1 \in N$ e assim $abN = a_1b_1N$.

Não é difícil ver que $\frac{G}{N}$, munido dessa operação é um grupo, chamado de grupo quociente de G por N. O elemento neutro de $\frac{G}{N}$ é a classe $eN = N$ e se $g \in G$, o inverso de gN em $\frac{G}{N}$ é $g^{-1}N$.

Teorema 2 (1° Teorema de Sylow). *Seja G um grupo finito de ordem $p^n m$, onde p é um primo, $n \geq 1$ e p não divide m. Se $k \in \{1, 2, \ldots, n\}$, então G possui pelo menos um subgrupo de ordem p^k. Ademais, se $k < n$ e H é um subgrupo de G de ordem p^k, então existe algum subgrupo N de G tal que $H \trianglelefteq N$ e $|N| = p^{k+1}$.*

Sendo G um grupo finito e p um divisor primo da ordem de G, esse teorema nos diz que se p^k divide a ordem de G, então G deve possuir pelo menos um subgrupo de ordem p^k. Particularmente, G deve possuir algum subgrupo com ordem igual à maior potência de p que divide $|G|$.

Considere p^n a maior potência de p que divide $|G|$ (isto é, $\frac{|G|}{p^n}$ não é múltipo de p). Um subgrupo de G de ordem p^n é chamado de S_p-subgrupo ou p-subgrupo de Sylow de G.

Definição 10. Definimos a classe de conjugação de um elemento a num grupo G como sendo

$$Cl_G(a) = \{xax^{-1}; x \in G\}.$$

E, para $a, b \in G$, valem:

1. $Cl_G(e) = \{e\}$
2. $Cl_G(a) = \{a\} \Leftrightarrow a \in Z(G)$.
3. $Cl_G(a) \cap Cl_G(b) \neq \{e\} \Leftrightarrow Cl_G(a) \neq Cl_G(b)$.
4. $G = \bigcup_{a \in G} Cl_G(a)$.
5. $\{b^{-1}yb; y \in C_G(a)\} = C_G(a)$.
6. Sendo $c_a = |Cl_G(a)|$, temos que $c_a = \frac{|G|}{|C_G(a)|}$

Definição 11. Sejam G e G_1 grupos. Dizemos que a aplicação $\varphi : G \to G_1$ é um homomorfismo de grupos se $\varphi(xy) = \varphi(x)\varphi(y)$ para quaisquer $x, y \in G$.

Propriedades básicas:

1. $\varphi(e) = e_1$, onde e denota o elemento neutro de G e e_1 denota o elemento neutro de G_1.
2. $\varphi(a^{-1}) = \varphi(a)^{-1}$ para todo $a \in G$.
3. $\varphi(a^n) = \varphi(a)^n$ para quaisquer $a \in G$ e $n \in \mathbb{Z}$.

Sendo G e G_1 grupos e $\varphi : G \longrightarrow G_1$ um homomorfismo, definimos o núcleo e a imagem de φ, denotados por $ker\varphi$ e $Im\varphi$, como sendo

$$ker\varphi = \{x \in G; \varphi(x) = e_1\} \quad \text{e} \quad Im\varphi = \{\varphi(x); x \in G\}$$

onde e_1 denota o elemento neutro de G_1.

Definição 12. Definimos um isomorfismo como sendo um homomorfismo bijetivo.

Sejam G e G_1 grupos. Se existe um isomorfismo $\varphi : G \longrightarrow G_1$, dizemos que G é isomorfo a G_1, e denotamos $G \simeq G_1$. Observe que dados $y_1, y_2 \in G_1$, existem $x_1, x_2 \in G$ tais que $\varphi(x_1) = y_1$ e $\varphi(x_2) = y_2$. Logo,

$$\varphi^{-1}(y_1y_2) = \varphi^{-1}(\varphi(x_1)\varphi(x_2)) = \varphi^{-1}(\varphi(x_1x_2)) = x_1x_2 = \varphi^{-1}(y_1)\varphi^{-1}(y_2)$$

e assim, φ^{-1} é também um isomorfismo, já que também é bijetora. Podemos então dizer que G e G_1 são grupos isomorfos.

Definição 13. Um grupo G diz-se solúvel se contém uma cadeia de subgrupos:

$$\{e\} = G_0 \subseteq G_1 \subseteq ... \subseteq G_n = G,$$

tal que cada G_{i-1} é normal em G_i e o grupo quociente $\frac{G_i}{G_{i-1}}$ é abeliano para $1 \leq i \leq n$.

Uma cadeia de subgrupos de G com esta propriedade chama-se uma **série subnormal abeliana** e os quocientes respectivos chamam-se os fatores da série.

Definição 14. Seja G um grupo e S um subconjunto de G. Definimos o subgrupo de G gerado por S, denotado por $\langle S\rangle$, como sendo a interseção de todos os subgrupos de G que contém S.

Observação 3. *Sendo G um grupo e S um subconjunto não vazio de G, temos:*

$$\langle S\rangle = \{x_1 \cdots x_n; n \in \mathbb{N},\ x_i \in S \cup S^{-1}\}$$

onde $S^{-1} = \{s^{-1}; s \in S\}$.

Sendo G um grupo e H um subgrupo de G. Se $H = \langle S\rangle$, dizemos que S gera H ou que S é um conjunto gerador de H. Particularmente, se $\langle S\rangle = G$, dizemos que S gera G ou que S é um conjunto gerador de G.

Dizemos que H é finitamente gerado se H possui algum conjunto gerador finito, ou seja, se existe S finito tal que $H = \langle S\rangle$.

Sendo $S = \{x_1, x_2, \ldots, x_n\}$, costuma-se denotar $\langle S\rangle$ simplesmente por $\langle x_1, x_2, \ldots, x_n\rangle$.

Definição 15. Dados dois subconjuntos H e K de um grupo G, denotaremos por $[H, K]$ o subgrupo de G gerado pelo conjunto $\{[h, k]; h \in H, k \in K\}$. Em particular, o grupo $G' = [G, G]$ chama-se **subgrupo comutador** ou **subgrupo derivado de** G.

Indutivamente, podemos definir agora uma sequência de subgrupos da seguinte forma:

$$\begin{aligned} G^{(0)} &= G \\ G^{(1)} &= G' \\ G^{(2)} &= (G^{(1)})' = G'' \\ &\vdots \\ G^{(n)} &= (G^{(n-1)})' \end{aligned}$$

O subgrupo $G^{(n)}$ acima chama-se **o n-ésimo grupo derivado de** G e a sequência

$$G = G^{(0)} \supseteq G^{(1)} \supseteq \ldots \supseteq G^{(n)} \supseteq \ldots$$

chama-se a **sequência derivada de** G.

Lema 1. *Seja H um subgrupo normal de um grupo G. Então o grupo quociente $\frac{G}{H}$ é abeliano se, e somente se, $G' \subseteq H$.*

Demonstração. Sejam $x, y \in G$ e denotemos por $\bar{x}$, $\bar{y}$ suas classes em $\frac{G}{H}$, respectivamente. Veja que $\overline{xy} = \overline{yx}$ se, e somente se, $(yx)^{-1}(xy) \in H$, ou seja, se, e somente se $[x, y] \in H$, para todo $x, y \in G$. Equivalentemente, $G' \subseteq H$. □

Teorema 3. *Um grupo G é solúvel se, e somente se, existe $n \in \mathbb{N}$ tal que $G^{(n)} = \{1\}$.*

Demonstração. Inicialmente, vamos supor que existe $n \in \mathbb{N}$ tal que $G^{(n)} = \{1\}$.
Claramente,

$$G = G^{(0)} \supseteq G^{(1)} \supseteq G^{(2)} \supseteq \ldots \supseteq G^{(n)} = \{1\}$$

é uma série subnormal abeliana para G.

Reciprocamente, suponhamos que G contém uma série subnormal abeliana

$$G_0 \supseteq G_1 \supseteq \ldots \supseteq G_n = \{1\}.$$

Como todo quociente $\frac{G_i}{G_{i-1}}$, com $0 \leq i \leq n-1$, é abeliano, segue do lema acima, argumentando por indução, que $G^{(i)} \subset G_i$, com $1 \leq i \leq n$. Assim, obtemos que $G^{(n)} = \{1\}$. □

Proposição 1. *Se $N \trianglelefteq G$, com N e $\frac{G}{N}$ solúveis, então G é solúvel.*

Demonstração. Pode ser consultada em [3], página 275. □

1.2 Álgebra Linear

Os espaços vetoriais citados no decorrer do texto serão complexos e todos de dimensão finita.

Denotaremos por $M_{m\times n}(\mathbb{C})$ e $M_n(\mathbb{C})$ os conjuntos das matrizes com entradas complexas de ordem m por n e de ordem $n \times n$, respectivamente, $GL_n(\mathbb{C})$ o conjunto das matrizes inversíveis de $M_n(\mathbb{C})$ e I_n a matriz identidade de ordem n.

Definição 16. O traço de uma matriz quadrada $A = (a_{ij})_{n\times n}$ é definido como $\sum_{i=1}^{n} a_{ii}$ e denotado por $Tr(A)$.
Valem as seguintes propriedades:

1. $Tr(A+B) = Tr(A) + Tr(B)$
2. $Tr(kA) = kTr(A)$
3. $Tr(AB) = Tr(BA)$

Definição 17. Dizemos que duas matrizes $n \times n$ A e B são semelhantes se existe uma matriz $n \times n$ inversível P tal que $A = P^{-1}BP$.

Observação 4. *Sejam A e A' duas matrizes semelhantes, isto é, existe R inversível tal que $A' = RAR^{-1}$. Temos que:*

$$\begin{aligned} Tr(A') &= Tr(RAR^{-1}) \\ &= Tr[(R(AR^{-1})] \\ &= Tr[(AR^{-1})R] \\ &= Tr[A(R^{-1}R)] \\ &= Tr(AI) \\ &= Tr(A) \end{aligned}$$

Proposição 2. *Toda matriz quadrada é semelhante a uma matriz triangular sobre* $\mathbb{C}$.

Definição 18. Uma transformação linear de um espaço vetorial V para um espaço vetorial W é uma aplicação $T : V \longrightarrow W$ tal que

$$T(\alpha u + \beta v) = \alpha T(u) + \beta T(v),$$

para quaisquer $u, v \in V$ e $\alpha, \beta \in \mathbb{C}$.

Seja $T : V \longrightarrow W$ uma transformação linear de V em W. Sejam $\beta = \{v_1, v_2, \ldots, v_n\}$ uma base de V e $\gamma = \{u_1, u_2, \ldots, u_m\}$ uma base de W. Como $T(v_1), T(v_2), \ldots, T(v_n)$ são elemntos de W, podemos escrever:

$$\begin{array}{ccccccccc} T(v_1) & = & a_{11}u_1 & + & a_{21}u_2 & + & \ldots & + & a_{m1}u_m \\ T(v_2) & = & a_{12}u_1 & + & a_{22}u_2 & + & \ldots & + & a_{m2}u_m \\ \vdots & & \vdots & & \vdots & & \vdots & & \vdots \\ T(v_n) & = & a_{1n}u_1 & + & a_{2n}u_2 & + & \ldots & + & a_{mn}u_m \end{array}$$

A representação matricial de T em relação às bases β e γ é definida como

$$[T]_\gamma^\beta = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & \ldots & \vdots \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{pmatrix}$$

O caso particular em que $V = W$ e $\beta = \gamma$ é definido da mesma forma, e denotamos a representação matricial de $T : V \longrightarrow V$ com relação à base β por $[T]_\beta$.

Definição 19. Sejam $S, T : V \longrightarrow W$ transformações lineares, definimos:

1. $S + T : V \longrightarrow W$ por $(S + T)(v) = S(v) + T(v)$, para todo $v \in V$.
2. $\lambda S : V \longrightarrow W$ por $(\lambda S)(v) = \lambda S(v)$, para todo $v \in V$ e $\lambda \in \mathbb{C}$.

Se β e β' são bases de V e W, respectivamente, então

1. $[S + T]_{\beta'}^{\beta} = [S]_{\beta'}^{\beta} + [T]_{\beta'}^{\beta}$.
2. $[\lambda T]_{\beta'}^{\beta} = \lambda [T]_{\beta'}^{\beta}$, para qualquer $\lambda \in \mathbb{C}$.
3. Seja $I : V \longrightarrow V$ o operador identidade de V, ou seja, $I(v) = v$, para todo $v \in V$. Temos que $[I]_\beta = I_n$, onde $n = dim V$.

Sejam $T : U \longrightarrow V$ e $S : V \longrightarrow W$ transformações lineares entre espaços vetoriais de dimensão finita e sejam β, $\beta^{'}$, $\beta^{''}$ bases de U, V e W, respectivamente. Então

$$[S \circ T]_{\beta''}^{\beta} = [S]_{\beta''}^{\beta'}[T]_{\beta'}^{\beta} \ .$$

Proposição 3. *Sejam $T : V \longrightarrow V$ uma transformação linear e β, $\beta^{'}$ bases do espaço vetorial V. Então, $[T]_{\beta'}$ e $[T]_{\beta}$ são semelhantes, isto é, existe P inversível, tal que $[T]_{\beta'} = P[T]_{\beta}P^{-1}$.*

Observação 5. *Todas as matrizes do mesmo operador T definido em um espaço de dimensão finita, independente da base escolhida tem o mesmo traço.*

Definição 20. Sejam V um espaço vetorial de dimensão n e β uma base de V. Definimos o traço do operador $T : V \longrightarrow V$, como sendo:

$$Tr(T) = Tr([T]_{\beta}) \ .$$

Definição 21. Seja $T : V \longrightarrow V$ uma aplicação definida por $T(v) = \lambda v$, para algum $\lambda \in \mathbb{C}$ e para todo $v \in V$, ou seja, $T = \lambda I$, onde I é operador identidade de V. Dizemos que T é uma de homotetia de raio λ.

Definição 22. Sejam V e W subspaços vetoriais sobre $\mathbb{C}$. Dizemos que uma transformação linear $T : V \longrightarrow W$ é um isomorfismo se T é injetora e sobrejetora.

Se $T : V \longrightarrow W$ é um isomorfismo, então $T^{-1} : W \longrightarrow V$ também é.
Denotamos por $GL(V)$ o conjunto dos operadores lineares bijetivos de V.

Observação 6. *Sendo V um espaço vetorial, temos que*

1. *$GL_n(\mathbb{C})$, munido do produto de matrizes, é um grupo.*

2. *$GL(V)$, munido da composição de funções, é um grupo.*

Sendo n a dimensão de V , fixada uma base β de V, seja $[T]_{\beta}$ a forma matricial da transformação T com respeito à base β. A aplicação

$$\begin{array}{rcl} f : GL(V) & \longrightarrow & GL_n(\mathbb{C}) \\ T & \longmapsto & [T]_{\beta} \end{array}$$

é um isomorfismo.

Definição 23. Seja $T : V \longrightarrow W$ uma transformação linear. Definimos

1. A imagem de T como sendo

$$Im(T) = \{T(x) \in W; w \in V\}.$$

2. O núcleo de T como sendo

$$Ker(T) = \{x \in V; T(x) = 0_W\}.$$

É fácil ver que $Im(T)$ é subespaço de W e $Ker(T)$ é subespaço de V.

Definição 24. Sejam V um espaço vetorial e $T : V \longrightarrow V$ um operador linear. Dizemos que $\lambda \in \mathbb{C}$ é um autovalor de T se existe $v \neq 0_V$ tal que $T(v) = \lambda v$. Neste caso, dizemos que v é um autovetor de T, associado ao autovalor λ.

Definição 25. Sejam $T : V \longrightarrow V$ um operador linear e β uma base de V. Definimos o polinômio característico do operador T por

$$p(x) = det([T]_\beta - xI)$$

.

Definição 26. O polinômio minimal de um operador linear $T : V \longrightarrow V$ é o ponimômio mônico $m_T(x)$ (ou seja, o termo do coeficiente de maior grau é igual a 1) de menor grau tal que $m_T(T) = 0$.

Observação 7. *Sendo $A \in M_n(\mathbb{C})$ uma matriz, definimos o polinômio minimal, o polinômio característico e os autovalores de A como sendo o polinômio minimal, o polinômio característico e os autovalores de um operador que tem A como uma representação matricial.*

Observação 8.

1. *Os autovalores de uma matriz diagonal são os elementos da diagonal.*

2. *Suponhamos que $\lambda_1, \ldots, \lambda_n$ são autovalores de A, então $Tr(A) = \sum_{i=1}^{n} \lambda_i$.*

3. *Duas matrizes quadradas semelhantes têm os mesmos autovalores, contando com sua multiplicidade.*

4. *Os autovalores de um operador linear são exatamente as raízes do seu polinômio característico.*

5. *Se $T : V \longrightarrow V$ é um operador linear inversível, e $\lambda_1, \lambda_2, \ldots, \lambda_n$ são os autovalores de T, então $\lambda_i \neq 0$, para todo $i = 1, \ldots, n$ e $\lambda_1^{-1}, \lambda_2^{-1}, \ldots, \lambda_n^{-1}$ são autovalores de T^{-1}.*

6. *Os elementos da diagonal de uma matriz triangular são exatamente os seus autovalores.*

7. *Se $T : V \longrightarrow V$ é um operador linear, então existe β base de V tal que $[T]_\beta$ é triangular.*

8. *Se T é um operador tal que existe $m \in \mathbb{N}$ satisfazendo $T^m = I$, então os autovalores de T tem módulo 1.*

9. *Se um polinômio anula o operador T, então este polinômio é divisível pelo minimal de T.*

Definição 27. Um produto interno num espaço vetorial V é uma aplicação

$$\begin{array}{rcl} \langle\ ,\ \rangle : V \times V & \longrightarrow & \mathbb{C} \\ (u, v) & \longmapsto & \langle u, v \rangle \end{array}$$

tal que para quaisquer $u, v, w \in V$ e $\lambda \in \mathbb{C}$ valem:

1. $\langle u, v \rangle = \overline{\langle v, u \rangle}$
2. $\langle u + v, w \rangle = \langle u, w \rangle + \langle v, w \rangle$
3. $\langle \lambda u, v \rangle = \lambda \langle u, v \rangle$
4. $\langle u, u \rangle \in \mathbb{R}$ e $\langle u, u \rangle > 0$ se $u \neq 0_V$.

Como consequência desses axiomas decorre que $\langle u, v + w \rangle = \langle u, v \rangle + \langle u, w \rangle$ e $\langle u, \lambda v \rangle = \bar{\lambda} \langle u, v \rangle$, para quaisquer $u, v \in V$ e $\lambda \in \mathbb{C}$.

Definição 28. Seja V um espaço vetorial com produto interno.

1. Dados os vetores $u, v \in V$, dizemos que u e v são ortogonais se $\langle u, v \rangle = 0$.
   Notação: $u \perp v$.

2. Dizemos que um subconjunto S não vazio de V é ortogonal se quaisquer dois vetores de V, distintos, são ortogonais.

É um fato conhecido que se V é um espaço com produto interno, então todo conjunto ortogonal de vetores não nulos de V é linearmente independente.

Definição 29. Seja S um subconjunto de um espaço vetorial V. O subespaço vetorial de V gerado por S é definido como o conjunto de todas as combinações lineares

$$\alpha_1 v_1 + \alpha_2 v_2 + \ldots + \alpha_n v_n \ ,$$

de vetores $v_1, v_2, \ldots, v_m \in S$.
Notação: $\langle S \rangle$.

Definição 30. Seja S um subconjunto não vazio de um espaço V com produto interno. O complemento ortogonal de S (denotado por $S^{\perp}$) é o conjunto dos vetores de V que são ortogonais a todos os vetores de S, isto é,

$$S^{\perp} = \{v \in V; v \perp w, \forall w \in S\}$$

Teorema 4. *Seja V um espaço vetorial com produto interno. Então:*

1. *$S^{\perp}$ é subespaço de V, para cada subconjunto não vazio S de V.*
2. *$V = W \oplus W^{\perp}$, para cada subespaço W de V.*

Observação 9. *Sejam V um espaço vetorial e S um subconjunto de V. Se $v \in V$ é ortogonal aos vetores $x_1, x_2, \ldots, x_m$ de S, então v é ortogonal a qualquer combinação linear $\sum \alpha_i x_i$, pois:*

$$\langle v, \sum \alpha_i x_i \rangle = \sum \alpha_i \langle v, x_i \rangle = 0 \ .$$

Daí, resulta que $S^{\perp} = \langle S \rangle^{\perp}$. Além disso, $S^{\perp} = \{0_V\} \Leftrightarrow \langle S \rangle = V$.

1.3 Inteiros Algébricos

Um polinômio sobre algum anel com unidade é chamado **mônico** quando o coeficiente do termo de maior grau é 1.

Definição 31. Consideremos o anel $\mathbb{C}$ e o subanel $\mathbb{Z}$ de $\mathbb{C}$. Diremos que o elemento $\alpha \in \mathbb{C}$ é **inteiro algébrico** se existir um polinômio mônico $f(x)$ com coeficientes inteiros tal que $f(\alpha) = 0$.

Exemplo 4. *As raízes da unidade são inteiros algébricos, pois são raízes do polinômio $p(x) = x^2 + 1$, por exemplo, i. Outro exemplo é o número $\frac{5+\sqrt{5}}{2}$, que é raiz do polinômio $q(x) = x^2 - 5x + 5$.*

Denotemos por $I_{\mathbb{C}}(\mathbb{Z})$ o conjunto dos elementos de $\mathbb{C}$ que são inteiros algébricos. Temos que $I_{\mathbb{C}}(\mathbb{Z})$ é um subanel de $\mathbb{C}$, ou seja, é fechado à adição e à multiplicação, que contém $\mathbb{Z}$ (a demonstração pode ser consultada em [2], capítulo 1, página 11).

Um resultado clássico, é que $\mathbb{Q} \cap I_{\mathbb{C}}(\mathbb{Z}) = \mathbb{Z}$, em outras palavras, os únicos racionais que são inteiros algébricos são os inteiros (esse resultado também pode ser encontrado em [2], capítulo 1, página 12).

Lema 2. *Se $w_1, \ldots, w_n \in \mathbb{C}$ são raízes da unidade, não todas iguais, e $\gamma = \dfrac{w_1 + \ldots + w_n}{n}$ é um inteiro algébrico, então $\gamma = 0$.*

Capítulo 2

Representações Lineares de Grupos Finitos

A Teoria de Representações busca caracterizar as formas como um grupo pode agir em um espaço vetorial e os efeitos dessas ações. Neste texto, G denotará um grupo finito, V denotará um espaço vetorial de dimensão finita sobre o corpo dos complexos $\mathbb{C}$ e a dimensão de V será denotada por $dim(V)$. O grupo dos isomorfismos de V em V, chamado de grupo linear de V, será denotado por $GL(V)$.

2.1 Representações Lineares

Definição 32. Seja G um grupo finito. Uma representação de G em V é um homomorfismo

$$\begin{array}{rcl} \rho : G & \longrightarrow & GL(V) \\ s & \longmapsto & \rho_s \ . \end{array}$$

Assim, $\rho_{st} = \rho_s \rho_t$, para quaisquer $s, t \in G$. Dizemos que ρ é uma representação do grupo G, e a $dimV$ é chamada grau da representação ρ. Observe que sendo $|G| = m$, então $\rho_s^m = \rho_{s^m} = \rho_1 = I$.

Seja V um espaço vetorial sobre o corpo dos complexos e considere $dimV = n$. Conforme visto na seção 1.2, fixada uma base de V podemos definir um isomorfismo

$$\begin{array}{rcl} \phi : GL(V) & \longrightarrow & GL_n(\mathbb{C}) \\ T & \longmapsto & [T]_\beta \ . \end{array}$$

Sendo assim, uma representação de G é o mesmo que um homomorfismo $\rho : G \longrightarrow GL_n(\mathbb{C})$ onde, para cada $s \in G$.

$$\rho_{\mathbf{s}} = \begin{pmatrix} a_{11}(s) & a_{12}(s) & \dots & a_{1n}(s) \\ a_{21}(s) & a_{22}(s) & \dots & a_{2n}(s) \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1}(s) & a_{n2}(s) & \dots & a_{nn}(s) \end{pmatrix}$$

$$\text{com, } a_{ij} : \begin{array}{ccc} G & \longrightarrow & \mathbb{C} \\ s & \longmapsto & a_{ij}(s) \end{array} \text{, para } 1 \leq i, j \leq n.$$

Seja β uma base de V e denotemos por $[\rho_s]_\beta$ a matriz de ρ_s na base β. Como a matriz da composta é o produto das matrizes e $\rho_s\rho_t = \rho_{st}$ temos que $[\rho_{st}]_\beta = [\rho_s]_\beta[\rho_t]_\beta$.

Exemplo 5. *Uma representação de grau* 1 *do grupo* G *é um homomorfismo*

$$\rho : \begin{array}{ccc} G & \longrightarrow & \mathbb{C}^* \\ s & \longmapsto & \rho(s) = \rho_s \end{array}.$$

Observe que os elementos ρ_s *são raízes da unidade. Em particular,* $|\rho(s)| = 1$*, para todo* $s \in G$*. Com efeito, tomando* $V = \mathbb{C}$*, temos* $GL(\mathbb{C}) = \mathbb{C}^*$*. Além disso, temos que*

$$(\rho_s)^{|G|} = \rho(s^{|G|}) = \rho(1) = 1.$$

Ou seja, tomando $n = |G|$*, temos* $(\rho_s)^n = 1$*, para todo* $s \in G$*. Assim,* $|\rho_s|^n = |\rho_s^n| = 1$ *e daí* $|\rho_s| = 1$*.*

Considerando $\rho_s = 1$*, para todo* $s \in G$*, essa representação é chamada representação unitária ou trivial de* G*.*

Exemplo 6. *Uma representação de grau* 1 *para o grupo* $\mathbb{Z}_3$ *é*

$$\rho : \begin{array}{ccc} \mathbb{Z}_3 & \longrightarrow & \mathbb{C}^* \\ \overline{k} & \longmapsto & \rho_{\overline{k}} = (e^{\frac{2\pi}{3}i})^k \end{array}$$

De fato, sejam $\overline{k_1}, \overline{k_2} \in \mathbb{Z}_3$*, temos que*

$$\begin{aligned} \rho_{\overline{k_1}}\rho_{\overline{k_2}} &= (e^{\frac{2\pi}{3}i})^{k_1}(e^{\frac{2\pi}{3}i})^{k_2} \\ &= (e^{\frac{2\pi}{3}i})^{k_1+k_2} \\ &= \rho_{\overline{k_1+k_2}} \end{aligned}$$

Exemplo 7. *Uma representação de grau 2 para S_3. Seja $S_3 = \{e, (23), (13), (12), (123), (132)\}$ e note que $S_3 =< \alpha, \beta >$, onde $\alpha = (123)$ e $\beta = (12)$. Ademais,*

$$(I) \begin{cases} \alpha^3 = e = \beta^2 \\ \beta\alpha = \alpha^2\beta \end{cases}$$

Sendo assim, para definirmos uma representação, basta definirmos a imagem dos geradores α e β e verificarmos que as relações (I) são preservadas para essas imagens (veja [3], página 165). Considere as matrizes $A, B \in GL_2(\mathbb{C})$, onde

$$A = \begin{pmatrix} \frac{-1}{2} + \frac{\sqrt{3}}{2}i & 0 \\ 0 & \frac{-1}{2} - \frac{\sqrt{3}}{2}i \end{pmatrix} \quad e \quad B = \begin{pmatrix} 0 & \frac{-1}{2} + \frac{\sqrt{3}}{2}i \\ \frac{-1}{2} + \frac{\sqrt{3}}{2}i & 0 \end{pmatrix}.$$

Claramente, $[A]^3 = I_2 = [B]^2$ e

$$AB = \begin{pmatrix} 0 & 1 \\ \frac{-1}{2} + \frac{\sqrt{3}}{2}i & 0 \end{pmatrix} = A^2B.$$

Assim existe de fato um homomorfismo $U : S_3 \longrightarrow GL_2(\mathbb{C})$ tal que $U(\alpha) = A$ e $U(\beta) = B$.

Exemplo 8. *Representação de grau 6 para S_3. Procedendo de maneira análoga, considere as matrizes $A, B \in GL_6(\mathbb{C})$, onde*

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

Observe que $[A]^3 = I_6 = [B]^2$ e $BA = A^2B$. Assim, existe de fato um homomorfismo $\rho : S_3 \longrightarrow GL_6(\mathbb{C})$ tal que $U(\alpha) = A$ e $U(\beta) = B$.

Exemplo 9. *Sejam $|G| = n$ e V um espaço vetorial com $dimV = n$ e com uma base $(e_t)_{t\in G}$. Para cada $s \in G$, tomando*

$$\begin{array}{rccc} \rho_s & : V & \longrightarrow & V \\ & e_t & \longmapsto & \rho_s(e_t) = e_{st} \end{array},$$

*definimos uma representação linear que é chamada **representação regular do grupo** G. Note que as imagens de $(e_{st})_{t\in G}$ é uma base para V, para todo $s \in G$.*

Definição 33. Sejam $\tau : G \longrightarrow GL(V)$ e $\tau' : G \longrightarrow GL(W)$ duas representações de G. Um isomorfismo de representações é um isomorfismo linear $\psi : V \longrightarrow W$ tal que $\psi \circ \tau_s = \tau'_s \circ \psi$, para todo $s \in G$. Equivalentemente, $\tau'_s = \psi \circ \tau_s \circ \psi^{-1}$. Neste caso, dizemos que τ e τ' são representações isomorfas. Quando τ_s e τ'_s são dadas na forma de matriz por R_s e R'_s, respectivamente, dizemos que R e R' são equivalentes se existe uma matriz inversível T tal que $TR = R'T$, para todo $s \in G$.

Definição 34. Sejam $\rho : G \longrightarrow GL(V)$ uma representação de G e W um subspaço qualquer de V. Dizemos que W é estável por ρ se $\rho_s(W) \subseteq W$, para todo $s \in G$.

Observe que, como $\rho_s(W) \subseteq W$ para todo $s \in G$, então $\rho_{s^{-1}}(W) \subseteq W$, o que implica que $\rho_s^{-1}(W) \subseteq W$, e daí $W \subseteq \rho_s(W)$, donde segue $\rho_s(W) = W$, para todo $s \in G$.

Exemplo 10. *Sejam $\rho : G \longrightarrow GL(V)$ uma representação de G, W um subespaço vetorial de V e $\rho_s : W \longrightarrow W$ definida por $\rho_s(x) = \alpha_x I$. Temos que $\rho_s(W) \subseteq W$, isto é, W é estável por ρ.*

Definição 35. Sejam $\rho : G \longrightarrow GL(V)$ uma representação de G e W um subspaço vetorial de V estável por ρ. Então a restrição de ρ_s a W, $\rho_s|_W : W \longrightarrow W$, é um isomorfismo e podemos definir a representação:

$$\begin{array}{rcl} \rho|_W : G & \longrightarrow & GL(W) \\ s & \longmapsto & \rho_s|_W \end{array}$$

Dessa forma, $\rho|_W$ é chamada uma subrepresentação de V.

Exemplo 11. *Tome agora $dimV = |G|$ e a representação regular de G*

$$\begin{array}{rcl} \rho_s : V & \longrightarrow & V \\ e_t & \longmapsto & \rho_s(e_t) = e_{st} \end{array},$$

onde $(e_t)_{t \in G}$ é uma base para V. Seja W o subespaço de V, com $dimW = 1$, gerado pelo elemento $x = \sum_{s \in G} e_s$. Temos que $\rho_s(x) = x$, para todo $s \in G$, pois

$$\begin{array}{rcl} \rho_s(x) & = & \rho_s(e_{g_1} + ... + e_{g_n}) \\ & = & \rho_s(e_{g_1}) + ... + \rho_s(e_{g_n}) \\ & = & e_{sg_1} + ... + e_{sg_n} \\ & = & x \end{array}$$

Logo, $\rho_s(W) = W$.

Teorema 5 (Teorema de Maschke)**.** *Seja $\rho : G \longrightarrow GL(V)$ uma representação linear de G em V e seja W um subspaço de V estável por ρ. Então existe um complemento W^0 de W em V que é estável por ρ.*

Demonstração. Sejam W' um complemento de W em V, isto é, $V = W \oplus W'$ e p a projeção correspondente de V sobre W com núcleo $W^{'}$, isto é:

$$\begin{array}{rcl} p : V & \longrightarrow & V \\ x & \longmapsto & w \end{array}$$

onde $x = w + w'$, com $w \in W$ e $w' \in W^{'}$. Sejam $p^{\circ} : V \longrightarrow V$ definida por

$$p^{\circ} = \frac{1}{|G|} \sum_{t \in G} \rho_t \circ p \circ \rho_t^{-1} \quad .$$

e $W^{\circ} = kerp^{\circ}$. Como a imagem de p está contida em W e ρ_t preserva W, vemos que a imagem de p° está contida em W. Observe que $\rho_t^{-1}(x) \in W$ para todo $x \in W$, pois W é estável por ρ, então $p(\rho_t^{-1}(x)) = \rho_t^{-1}(x)$, o que implica que $\rho_t(p(\rho_t^{-1}(x))) = \rho_t(\rho_t^{-1}(x)) = x$, para todo $x \in W$. Portanto

$$p^{\circ}(x) = \frac{1}{|G|} \sum_{t \in G} x = x$$

para todo $x \in W$.

Vejamos que $V = W \oplus W^{\circ}$. De fato, tomando $w \in W \cap W^{\circ}$, temos que $w = p^{\circ}(w) = 0_V$. Além disso, para todo $v \in V$, temos $v = (v - p^{\circ}(v)) + p^{\circ}(v) \in W^{\circ} + W$, pois $p^{\circ}(v - p^{\circ}(v)) = p^{\circ}(v) - p^{\circ}(p^{\circ}(v)) = p^{\circ}(v) - p^{\circ}(v) = 0_V$.

Observe agora que $\rho_s \circ p^{\circ} = p^{\circ} \circ \rho_s$, para todo $s \in G$. De fato,

$$\begin{array}{rcl} \rho_s \circ p^{\circ} \circ \rho_s^{-1} & = & \rho_s \circ \left(\dfrac{1}{|G|} \displaystyle\sum_{t \in G} \rho_t \circ p \circ \rho_t^{-1} \right) \circ \rho_s^{-1} \\ & = & \dfrac{1}{|G|} \displaystyle\sum_{t \in G} \rho_s \circ \rho_t \circ p \circ \rho_t^{-1} \circ \rho_s^{-1} \\ & = & \dfrac{1}{|G|} \displaystyle\sum_{t \in G} \rho_{st} \circ p \circ \rho_{st}^{-1} \\ & = & p^{\circ}. \end{array}$$

Donde, para todo $x \in W^{\circ}$, temos

$$p^{\circ}(\rho_s(x)) = \rho_s(p^{\circ}(x)) = \rho_s(0) = 0_V.$$

Logo, $\rho_s(x) \in W^{\circ}$, para todo $x \in W^{\circ}$, e portanto, W° é estável por ρ. $\square$

Sejam $\rho : G \longrightarrow GL(V)$ uma representação de G e W um subespaço de V estável por ρ. Pelo Teorema 5 (Teorema de Maschke) vimos que existe W^1 complemento de W em V que é estável por ρ. Consideremos as subrepresentações $\rho|_W = \tau : G \longrightarrow GL(W)$ e $\rho|_{W^1} = \phi : G \longrightarrow GL(W^1)$. Diante disso, dizemos que ρ é a soma direta das subrepresentações τ e ϕ, e escrevemos

$$\begin{array}{rcl} \rho = \tau \oplus \phi : G & \longrightarrow & GL(W \oplus W^1) \\ s & \longmapsto & \tau_s \oplus \phi_s \end{array}$$

onde

$$\begin{array}{rcl} \tau_s \oplus \phi_s : W \oplus W^1 & \longrightarrow & W \oplus W^1 \\ w_1 + w_2 & \longmapsto & \tau_s(w_1) + \phi_s(w_2) \end{array}$$

Claramente a aplicação está bem definida, pois dado $v \in V$, temos que $v = w_1 + w_2$, com $w_1 \in W$ e $w_2 \in W^1$. Além disso,

$$\begin{array}{rcl} \rho_s(v) & = & \rho_s(w_1 + w_2) \\ & = & \rho_s(w_1) + \rho_s(w_2) \\ & = & \tau_s(w_1) + \phi_s(w_2) \\ & = & (\tau_s \oplus \phi_s)(v) \end{array}$$

Se τ_s e ϕ_s são dadas na forma matricial por R_s e R'_s, respectivamente, então $(\tau \oplus \phi)_s$ é dada na forma matricial (em relação a uma base adequada) por

$$\begin{pmatrix} R_s & 0 \\ 0 & R'_s \end{pmatrix}$$

Para um número finito de subrepresentações $\rho_1 : G \longrightarrow GL(W_1)$, ..., $\rho_n : G \longrightarrow GL(W_n)$ de ρ, tais que $W_1, \ldots, W_n$ são subspaços de V estáveis por ρ com $V = W_1 \oplus \ldots \oplus W_n$, dizemos que ρ é a soma direta das representações $\rho_1, \ldots, \rho_n$ e escrevemos

$$\begin{array}{rcl} \rho = \rho_1 \oplus \ldots \oplus \rho_n : G & \longrightarrow & GL(W_1 \oplus \ldots \oplus W_n) \\ s & \longmapsto & \rho_1(s) \oplus \ldots \oplus \rho_n(s). \end{array}$$

E na forma matricial se $\rho_1, \cdots, \rho_n$ são representados por $R_s^1, \cdots, R_s^n$, respectivamente, temos que a soma direta é dada por uma matriz diagonal em blocos.

2.2 Representações Irredutíveis

Definição 36. Seja $\rho : G \longrightarrow GL(V)$ uma representação linear de G (com $V \neq \{0\}$). Dizemos que ρ é uma representação irredutível ou simples se nenhum subespaço vetorial de V é estável por ρ, exceto, é claro, $\{0\}$ e V.

Pelo Teorema de Maschke, essa condição é equivalente a dizer que ρ não é soma direta de duas representações (exceto para a decomposição trivial $V = 0 \oplus V$).

Exemplo 12. *Uma representação de grau 1 é evidentemente irredutível, pois se $dimV = 1$, então $\{0\}$ e V são os únicos subespaços de V.*

Teorema 6. *Dados um subespaço vetorial V, com $dimV \neq 0$ e uma representação $\rho : G \longrightarrow GL(V)$, temos que existem $W_1, \ldots, W_n$ subespaços de V estáveis por ρ tais $V = W_1 \oplus \ldots \oplus W_n$ e as subrepresentações $\rho|_{W_i} : G \longrightarrow GL(W_i)$ são irredutíveis, para todo $i = 1, \ldots, n$.*

Demonstração. Faremos indução na dimensão de V. Se $dimV = 1$, então ρ é irredutível. Agora se $dimV > 1$ temos dois casos:

i) $\rho : G \longrightarrow GL(V)$ é irredutível, e neste caso nada há para mostrar;

ii) $\rho : G \longrightarrow GL(V)$ não é irredutível;

Suponha por hipótese de indução que o resultado vale para representações com grau menor do que o grau de ρ. Como ρ não é irredutível, existe W_1 subespaço de V, intermediário, que é estável por ρ. Pelo Teorema de Maschke, existe W_2 subespaço de V também estável por ρ tal que $V = W_1 \oplus W_2$. Basta considerar as subrepresentações $\rho|_{W_i}$, com $i = 1, 2$, e como os graus dessas subrepresentações são menores do que o grau de ρ, segue da hipótese de indução que o resultado para $\rho|_{W_i}$, $i = 1, 2$. Juntando as decomposições de W_1 e W_2 como somas direta de subspaços invariantes, cujas subrepresentações associadas são irredutíveis, temos o resultado. □

2.3 Representações Unitárias

Definição 37. Seja $\rho : G \longrightarrow GL(V)$ uma representação de G. Dizemos que ρ é unitária e relação a um produto interno $\langle \cdot, \cdot \rangle$ em V se

$$\langle \rho_s(u), \rho_s(v) \rangle = \langle u, v \rangle$$

para todo $s \in G$ e $u, v \in V$

Vamos agora ver que através desse conceito, podemos dar uma nova demonstração do Teorema de Maschke.

Proposição 4. *Seja V um espaço vetorial munido de um produto interno $\langle \cdot, \cdot \rangle$ e $\rho : G \longrightarrow GL(V)$ uma representação de G. Então podemos obter um produto interno $\langle \cdot, \cdot \rangle_\rho$ em relação ao qual ρ é unitária.*

Demonstração. Definamos a seguinte aplicação:

$$\begin{aligned} \langle \cdot, \cdot \rangle_\rho : V \times V &\longrightarrow \mathbb{C} \\ (u, v) &\longmapsto \langle u, v \rangle_\rho = \sum_{s \in G} \langle \rho_s(u), \rho_s(v) \rangle \ . \end{aligned}$$

Temos que essa aplicação é um produto interno. De fato,

i)

$$\begin{aligned} \overline{\langle v, u \rangle_\rho} &= \overline{\sum_{s \in G} \langle \rho_s(v), \rho_s(u) \rangle} \\ &= \sum_{s \in G} \overline{\langle \rho_s(v), \rho_s(u) \rangle} \\ &= \sum_{s \in G} \langle \rho_s(u), \rho_s(v) \rangle \\ &= \langle u, v \rangle_\rho \end{aligned}$$

ii)

$$\begin{aligned} \langle u + v, w \rangle_\rho &= \sum_{s \in G} \langle \rho_s(u + v), \rho_s(w) \rangle \\ &= \sum_{s \in G} \langle \rho_s(u) + \rho_s(v), \rho_s(w) \rangle \\ &= \sum_{s \in G} \langle \rho_s(u), \rho_s(w) \rangle + \langle \rho_s(v), \rho_s(w) \rangle \\ &= \sum_{s \in G} \langle \rho_s(u), \rho_s(w) \rangle + \sum_{s \in G} \langle \rho_s(v), \rho_s(w) \rangle \\ &= \langle u, w \rangle_\rho + \langle v, w \rangle_\rho \end{aligned}$$

iii)

$$\begin{aligned} \langle \lambda u, v \rangle_\rho &= \sum_{s \in G} \langle \rho_s(\lambda u), \rho_s(v) \rangle \\ &= \lambda \sum_{s \in G} \langle \rho_s(u), \rho_s(v) \rangle \\ &= \lambda \langle u, v \rangle_\rho \end{aligned}$$

iv) Como $\langle \rho_s(u), \rho_s(u) \rangle > 0$, para todo $u \neq 0$, temos que

$$\langle u, u \rangle_\rho = \sum_{s \in G} \langle \rho_s(u), \rho_s(v) \rangle > 0 \ .$$

Ademais, para todo $t \in G$,

$$\begin{aligned} \langle \rho_t(u), \rho_t(v) \rangle_\rho &= \sum_{s \in G} \langle \rho_{st}(u), \rho_{st}(v) \rangle \\ &= \sum_{s \in G} \langle \rho_{st}(u), \rho_{st}(v) \rangle \\ &= \sum_{r \in G} \langle \rho_r(u), \rho_r(v) \rangle \\ &= \langle u, v \rangle_\rho \ . \end{aligned}$$

Concluindo o resultado. □

Considere $\rho : G \longrightarrow GL(V)$ e o produto interno $\langle \ , \ \rangle_\rho$ como na proposição acima. Sejam W um subespaço de V estável por ρ e $W^\perp$ o complemento ortogonal de W em relação a esse produto interno. Mostremos que $W^\perp$ é estável por ρ. De fato, como $\rho_s(W) = W$, temos que dado $w \in W$, existe $w' \in W$ tal que $\rho_s(w') = w$. Assim, dado $w_1 \in W^\perp$ temos:

$$\begin{aligned} \langle \rho_s(w_1), w \rangle_\rho &= \langle \rho_s(w_1), \rho_s(w') \rangle_\rho \\ &= \langle w_1, w' \rangle_\rho \\ &= 0 \end{aligned}$$

Logo, $\rho_s(w_1) \in W^\perp$, para todo $w_1 \in W^\perp$, ou seja, $W^\perp$ é estável por ρ.

Capítulo 3

Teoria dos Caracteres

3.1 O Caracter de uma Representação

Definição 38. Seja $\rho : G \longrightarrow GL(V)$ uma representação linear de um grupo finito G em um espaço vetorial V. Definimos o caracter de uma representação ρ por:

$$\begin{array}{rcl} \chi_\rho : G & \longrightarrow & \mathbb{C} \\ s & \longmapsto & \chi_\rho(s) = Tr(\rho_s) \end{array}$$

Proposição 5. *Se χ é o caracter de uma representação $\rho : G \longrightarrow GL(V)$ de grau n temos:*

1. $\chi(1_G) = n$.
2. $\chi(s^{-1}) = \overline{\chi(s)}$, *para* $s \in G$.
3. $\chi(tst^{-1}) = \chi(s)$, *para* $s, t \in G$.

Demonstração.

1.

$$\begin{array}{rcl} \chi_\rho(1_G) & = & Tr(\rho_{1_G}) \\ & = & Tr(I_n) \\ & = & n \end{array}$$

2. Fixado $s \in G$, arbitrário, considere $\lambda_1, \lambda_2, \cdots, \lambda_n \in \mathbb{C}$ os autovalores

(não necessariamente distintos) de ρ_s. Então

$$\begin{aligned}
\overline{\chi_\rho(s)} &= \overline{Tr(\rho_s)} \\
&= \sum_{i=1}^{n} \bar{\lambda_i} \\
&= \sum_{i=1}^{n} \lambda_i^{-1} \\
&= Tr(\rho_s^{-1}) \\
&= Tr(\rho_{s^{-1}}) \\
&= \chi_\rho(s^{-1})
\end{aligned}$$

3. Sejam $ts = u$ e $v = t^{-1}$, temos:

$$\begin{aligned}
\chi_\rho(tst^{-1}) &= \chi_\rho(uv) \\
&= Tr(\rho_u \rho_v) \\
&= Tr(\rho_v \rho_u) \\
&= \chi_\rho(vu) \\
&= \chi_\rho(s)
\end{aligned}$$

□

Proposição 6. *Sejam $\rho^1 : G \longrightarrow GL(V_1)$ e $\rho^2 : G \longrightarrow GL(V_2)$ duas representações lineares de G, e sejam χ_1 e χ_2 seus caracteres, então o caracter da soma direta $\rho_s^1 \oplus \rho_s^2$ é $\chi = \chi_1 + \chi_2$.*

Demonstração. Considere R_s^1 e R_s^2 as formas matriciais de ρ_s^1 e ρ_s^2, respectivamente. A representação da soma direta em forma de matriz é dada pela matriz quandrada de ordem $n + m$:

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

Daí, $Tr(R_s) = Tr(R_s^1) + Tr(R_s^2)$, o que implica $\chi(s) = \chi_1(s) + \chi_2(s)$. □

Proposição 7 (Lema de Schur)**.** *Seja $\rho : G \longrightarrow GL(V_1)$ e $\varphi : G \longrightarrow GL(V_2)$ duas representações irredutíveis de G e $f : V_1 \longrightarrow V_2$ uma aplicação linear tal que $\varphi_s \circ f = f \circ \rho_s$, para todo $s \in G$. Temos que:*

1. *Se ρ e φ não são isomorfas, então $f \equiv 0$.*
2. *Se $V_1 = V_2$ e $\rho = \varphi$, então f é uma homotetia.*

Demonstração.

1. Suponhamos que $f \neq 0$ e tome $x \in Kerf$, arbitrário. Temos que

$$f(\rho_s(x)) = \varphi_s(f(x)) = \varphi_s(0_{V_2}) = 0_{V_2}$$

e então $\rho_s(x) \in Kerf$, o que implica $Kerf$ estável por ρ. Mas como ρ é irredutível, temos que $Kerf = V_1$ ou $Kerf = \{0_{V_1}\}$. Como estamos supondo $f \neq 0$, segue-se $Kerf = \{0_{V_1}\}$. Analogamente, tomando $y \in Imf$, temos que $\varphi_s(y) = \varphi_s(f(x))$, para algum $x \in V_1$, e daí $\varphi_s(y) = f(\rho_s(x)) \in Imf$, pois $\rho_s(x) \in V_1$. Daí, Imf é estável por φ e, sendo φ irredutível e $f \neq 0$, segue-se que que $Imf = V_2$. Logo, ρ e φ são isomorfas.

2. Seja $\lambda \in \mathbb{C}$ um autovalor de f e vamos trabalhar com a representação irredutível de G, $\rho : G \longrightarrow GL(V)$. Defina $f' = f - \lambda I$. Como λ é autovalor de f, existe $v \neq 0$, tal que $fv = \lambda v$, o que implica $f'(v) = 0$, e daí $Kerf' \neq \{0\}$. Agora observe que

$$(\rho_s \circ f')(v) = (f' \circ \rho_s)(v).$$

Análogo ao que fizemos no ítem 1, obtemos que $\ker f'$ é estável por ρ, implicando $\ker f' = V$. Assim $f'(x) = 0$, para todo $x \in V$, e daí $f(x) = \lambda x$, para todo $x \in V$.

□

Corolário 1. *Sejam $h : V_1 \to V_2$ uma transformação linear e $h^\circ = \frac{1}{|G|} \sum_{t \in G} (\varphi_t)^{-1} h \rho_t$, então:*

1. *Se ρ e φ não são isomorfas, então $h^\circ = 0$.*

2. *Se $V_1 = V_2$ e $\rho = \varphi$, h° é uma homotetia de raio $\frac{1}{n} Tr(h)$, com $n = dimV$.*

Demonstração.

1. Já sabemos que ρ e φ são irredutíveis. Basta verificar que $\varphi_s \circ h^\circ =$

$h^\circ \circ \rho_s$, para todo $s \in G$. De fato,

$$\begin{aligned}(\varphi_s)^{-1} \circ h^\circ \circ \rho_s &= (\varphi_s)^{-1} \frac{1}{|G|} \sum_{t \in G} (\varphi_t)^{-1} h \rho_t \rho_s \\ &= \frac{1}{|G|} \sum_{t \in G} (\varphi_s)^{-1} (\varphi_t)^{-1} h \rho_t \rho_s \\ &= \frac{1}{|G|} \sum_{t \in G} (\varphi_{ts})^{-1} h \rho_{ts} \\ &= h^\circ\end{aligned}$$

Segue da Proposição 7 (Lema de Schur), ítem 1, que $h^\circ = 0$.

2. Pela Proposição h° é uma homotetia e

$$\begin{aligned}Tr(h^\circ) &= Tr\left(\frac{1}{|G|} \sum_{t \in G} (\varphi_t)^{-1} \circ h \circ \rho_t\right) \\ &= \frac{1}{|G|} \sum_{t \in G} Tr((\rho_t)^{-1} \circ h \circ \rho_t) \\ &= \frac{1}{|G|} \sum_{t \in G} Tr(h) \\ &= Tr(h).\end{aligned}$$

Seja λ o raio de h°, ou seja, $h^\circ(x) = \lambda x$, para todo $x \in V_1$. Temos $n\lambda = Tr(\lambda I_n) = Tr(h)$ e assim $\lambda = \frac{1}{n} Tr(h)$.

□

Definição 39. Dizemos que uma função $f : G \longrightarrow \mathbb{C}$ é de classe se para todo $s, t \in G$ temos:

$$f(tst^{-1}) = f(s)$$

Como vimos na Proposição 5, um exemplo de uma função de classe é o caracter.

Chamemos de H o conjunto de todas as funções complexas definidas em G. Temos que H, munido da adição e da multiplicação por escalar ponto a ponto, é um espaço vetorial. Considerando agora

$$\mathbb{C}[G] = \{f : G \longrightarrow \mathbb{C}; f \text{ é de classe}\},$$

temos que $\mathbb{C}[G]$ é um subespaço vetorial de H, chamado de espaço das funções de classe.

Definamos a aplicação

$$\begin{aligned} \langle\ ,\ \rangle : \mathbb{C}[G] \times \mathbb{C}[G] &\longrightarrow \mathbb{C} \\ (f,g) &\longmapsto \langle f,g\rangle = \frac{1}{|G|}\sum_{t\in G} f(t)\overline{g(t)}\ . \end{aligned}$$

Temos que $\langle\ ,\ \rangle$ é um produto interno. Com efeito,
i)

$$\begin{aligned} \overline{\langle g,f\rangle} &= \overline{\frac{1}{|G|}\sum_{t\in G} g(t)\overline{f(t)}} \\ &= \frac{1}{|G|}\sum_{t\in G}\overline{g(t)}f(t) \\ &= \langle f,g\rangle \end{aligned}$$

ii)

$$\begin{aligned} \langle f+g,h\rangle &= \frac{1}{|G|}\sum_{t\in G}(f+g)(t)\overline{h(t)} \\ &= \frac{1}{|G|}\sum_{t\in G} f(t)\overline{h(t)} + g(t)\overline{h(t)} \\ &= \frac{1}{|G|}\left(\sum_{t\in G} f(t)\overline{h(t)} + \sum_{t\in G} g(t)\overline{h(t)}\right) \\ &= \langle f,h\rangle + \langle g,h\rangle \end{aligned}$$

iii)

$$\begin{aligned} \langle \lambda f,g\rangle &= \frac{1}{|G|}\sum_{t\in G}\lambda f(t)\overline{g(t)} \\ &= \lambda\frac{1}{|G|}\sum_{t\in G} f(t)\overline{g(t)} \\ &= \lambda\langle f,g\rangle \end{aligned}$$

iv) Como para todo $w\in\mathbb{C}^*$, $w\overline{w} = |w|^2 > 0$ temos

$$\langle f,f\rangle = \frac{1}{|G|}\sum_{s\in G} f(t)\overline{f(t)} > 0\ .$$

para $f \in \mathbb{C}[G]$ não nula.
Segue o resultado.

Em particular, o caracter é uma função de classe e $\chi(s^{-1}) = \overline{\chi(s)}$, e assim, para qualquer $f \in \mathbb{C}[G]$, temos:

$$\begin{aligned} \langle f, \chi \rangle &= \frac{1}{|G|} \sum_{t \in G} f(t)\overline{\chi(t)} \\ &= \frac{1}{|G|} \sum_{t \in G} f(t)\chi(t^{-1}) \ . \end{aligned}$$

Observação 10. *Definimos a matriz unitária $E_{kl} \in M_{m\times n}(\mathbb{C})$ como sendo a matriz cuja entrada na linha k conluna l é igual a 1, e as demais são 0. Assim, se $A = (a_{ij}) \in M_m(\mathbb{C})$ e $B = (b_{ij}) \in M_n(\mathbb{C})$, então*

$$AE_{kl}B = \begin{pmatrix} a_{1k}b_{l1} & a_{1k}b_{l2} & \cdots & a_{1k}b_{ln} \\ a_{2k}b_{l1} & a_{2k}b_{l2} & \cdots & a_{2k}b_{ln} \\ \vdots & \vdots & \ddots & \vdots \\ a_{mk}b_{l1} & a_{mk}b_{l2} & \cdots & a_{mk}b_{ln} \end{pmatrix} \ ,$$

ou seja, $AE_{kl}B = (a_{ik}b_{lj})_{m\times n}$, com $k \in \{1, \ldots, m\}$ e $l \in \{1, \ldots, n\}$ fixos.

Teorema 7 (Relações de Ortogonalidade)**.**

1. *Se χ_1 e χ_2 são os caracteres de duas representações irredutíveis não isomorfas, então $\langle \chi_1, \chi_2 \rangle = 0$.*

2. *Se χ é o caracter de uma representação irredutível, então $\langle \chi, \chi \rangle = 1$.*

Demonstração.

1. Seja $\rho : G \longrightarrow GL(V_1)$ e $\varphi : G \longrightarrow GL(V_2)$ duas representações irredutíveis não isomorfas de G e χ_1, χ_2 seus caracteres, respectivamente.

   Fixadas bases β de V_1 e γ de V_2, tomemos $[\rho_t]_\beta = (r_{ij}(t))_{n\times n}$ e $[\varphi_t]_\gamma = (s_{ij}(t))_{m\times m}$, onde $n = dim V_1$ e $m = dim V_2$. Pelo Corolário 1, temos $0_{m\times n} = [h^\circ]_\gamma^\beta = \frac{1}{|G|} \sum\limits_{t\in G} [\varphi_{t^{-1}}]_\gamma [h]_\gamma^\beta [\rho_t]_\beta$. Como essa relação vale para qualquer transformação linear de V_1 em V_2, em particular, vale para uma h tal que $[h]_\gamma^\beta = E_{kl} \in M_{m\times n}(\mathbb{C})$ (com k e l fixos, arbitrários), temos

   $$\begin{aligned} 0_{m\times n} &= \frac{1}{|G|} \sum_{t\in G} [\varphi_{t^{-1}}]_\gamma E_{ij} [\rho_t]_\beta \\ &= \left(\frac{1}{|G|} \sum_{t\in G} s_{ik}(t^{-1}) r_{lj}(t) \right)_{m\times n} \ . \end{aligned}$$

Isto implica que $\sum_{t\in G} s_{ik}(t^{-1})r_{lj}(t) = 0$, para quaisquer $k, i = 1, \ldots, m$ e $l, j = 1, \ldots, n$. Assim, no caso em que $k = i$ e $l = j$, temos $\sum_{t\in G} s_{ii}(t^{-1})r_{jj}(t) = 0$.
Por outro lado,

$$\begin{aligned}\langle \chi_1, \chi_2 \rangle &= \frac{1}{|G|}\sum_{t\in G}\chi_2(t^{-1})\chi_1(t) = \frac{1}{|G|}\sum_{t\in G}\left(\sum_{i=1}^{m} s_{ii}(t^{-1})\sum_{j=1}^{n} r_{jj}(t)\right) \\ &= \sum_{i=1}^{m}\sum_{j=1}^{n}\left(\frac{1}{|G|}\sum_{t\in G} s_{ii}(t^{-1})r_{jj}(t)\right) = 0\end{aligned}$$

2. Consideremos a representação irredutível $\rho : G \longrightarrow GL(V)$ de grau n, caracter χ, e dada na forma matricial por $[\rho_t]_\beta = (r_{ij}(t))_{n\times n}$. Análogo ao que fizemos no ítem 1, consideramos uma transformação $h : V \longrightarrow V$ tal que $[h]_\beta = E_{kl}$, com $k, l \in \{1, \ldots, n\}$ fixos e arbitrários. Pelo Corolário 1

$$\lambda_h I_n = \frac{1}{|G|}\sum_{t\in G}[\rho_{t^{-1}}]_\beta E_{kl}[\rho_t]_\beta$$

e

$$\lambda_h = \frac{Tr(h)}{n} = \frac{\delta_{kl}}{n}.$$

Por outro lado,

$$\left(\frac{1}{|G|}\sum_{t\in G} r_{ik}(t^{-1})r_{lj}(t)\right)_{n\times n} = \frac{\delta_{kl}}{n}I.$$

Daí, quando $k = i = j = l$

$$\frac{1}{|G|}\sum_{t\in G} r_{ii}(t^{-1})r_{ii}(t) = \frac{1}{n}\ ,$$

e, quando $k = i \neq j = l$

$$\frac{1}{|G|}\sum_{t\in G} r_{ii}(t^{-1})r_{jj}(t) = 0.$$

Portanto,

$$\begin{aligned}\langle\chi,\chi\rangle &= \frac{1}{|G|}\sum_{t\in G}\left(\sum_{i=1}^{n} r_{ii}(t^{-1})\sum_{j=1}^{n} r_{jj}(t)\right) = \frac{1}{|G|}\sum_{t\in G}\left(\sum_{i=1}^{n}\sum_{j=1}^{n} r_{ii}(t^{-1})r_{jj}(t)\right)\\ &= \sum_{i=1}^{n}\sum_{j=1}^{n}\left(\frac{1}{|G|}\sum_{t\in G} r_{ii}(t^{-1})r_{jj}(t)\right) = \sum_{i=1}^{n}\left(\frac{1}{|G|}\sum_{t\in G} r_{ii}(t^{-1})r_{ii}(t)\right)\\ &= \sum_{i=1}^{n}\frac{1}{n} = 1.\end{aligned}$$

□

Para concluir esse capítulo, vamos definir a **multiplicidade** de um caracter irrdutível na composição de um caracter.

Seja $\rho : G \longrightarrow GL(V)$ uma representação do grupo G com caracter ϕ. Vimos que existem $W_1, \ldots, W_n$ subespaços de V estáveis por ρ tais que $V = W_1 \oplus \ldots \oplus W_n$, e $\rho_i = \rho|_{W_i}$ é irredutível para cada $i = 1, \ldots, n$. Assim ϕ é a soma dos caracteres das representações ρ_i's, os quais são irredutíveis, e assim concluímos que

$$\phi = m_1\chi_1 + \ldots + m_k\chi_k$$

onde $\chi_1, \ldots, \chi_k$ são caracteres irredutíveis, dois a dois distintos, e cada m_i é um inteiro não negativo. Definimos a *multiplicidade* de χ_i em ϕ como sendo o inteiro m_i. Observe que, para cada $i = 1, \ldots, k$,

$$\langle\phi,\chi_i\rangle = m_1\langle\chi_1,\chi_i\rangle + \ldots + m_i\langle\chi_i,\chi_i\rangle + \ldots + m_k\langle\chi_k,\chi_i\rangle = m_i$$

pelas relações de ortogonalidade.

3.2 Decomposição da Representação Regular

Considere G um grupo e denote os seus caracteres irredutíveis por $\chi_1, \ldots, \chi_h$ e seus graus por $n_1, \ldots, n_h$. Temos $n_i = \chi_i(1)$ (Proposição 5).

Relembre que, dado um grupo G, com $|G| = n$ e V um espaço vetorial de dimensão n com base $\beta = \{e_s\}_{s \in G}$ (indexada pelos elementos de G), a representação regular de G é definida por

$$\begin{array}{rccc} \rho_s & : G & \longrightarrow & GL(V) \\ & t & \longmapsto & \rho_t \end{array} ,$$

onde $\rho_t : V \longrightarrow V$ é o operador linear definido por $\rho_t(e_s) = e_{ts}$.

Proposição 8. *O caracter $r_G(t)$ da representação regular é dado por:*

$$r_G(t) = \begin{cases} n, & se \quad t = e \\ 0, & se \quad t \neq e. \end{cases}$$

Demonstração.

i) O caso em que $t = e$ temos

$$r_G(t) = r_G(e) = Tr(Id_V) = n \ .$$

ii) No caso em que $t \neq e$, temos que $ts \neq s$, para todo $s \in G$. Logo, a matriz de ρ_t na base β terá todos os elementos da diagonal principal nulos. Então, $r_G(t) = Tr(\rho_t) = 0$. □

Corolário 2. *Todo caracter irredutível de G aparece na expressão do caracter da representação regular, com multiplicidade igual ao seu grau.*

Demonstração. De fato, sendo χ um caracter irredutível de G essa multiplicidade é dada por

$$\begin{aligned} \langle r_G, \chi \rangle &= \frac{1}{|G|} \sum_{s \in G} r_G(s^{-1}) \chi(s) \\ &= \frac{1}{|G|} r_G(e) \chi(e) \ , \text{ pois } r_G(s) = 0 \text{ se } s \neq e \\ &= \frac{1}{|G|} \cdot |G| \cdot \chi(e) \\ &= \chi(e) \end{aligned}$$

□

Corolário 3. *Os graus $n_i's$ satisfazem as relações $\sum_{i=1}^{k} n_i^2 = n$ e $\sum_{i=1}^{k} n_i\chi_i(s) = 0$, para todo $s \in G - \{e\}$.*

Demonstração. Vimos do Corolário 2 que a multiplicidade com que χ_i aparece na expressão do caracter r_G da representação regular é n_i, e então $r_G(s) = \sum_{i=1}^{k} n_i\chi_i(s)$. Logo,

i) Se $s = e$, temos:

$$n = r_G(e) = \sum_{i=1}^{k} n_i\chi_i(e) = \sum_{i=1}^{k} n_i n_i = \sum_{i=1}^{k} n_i^2$$

ii) Se $s \neq e$, temos

$$0 = r_G(s) = \sum_{i=1}^{k} n_i\chi_i(s)$$

□

3.3 Número de Representações Irredutíveis

Proposição 9. *Sejam $f : G \longrightarrow \mathbb{C}$ uma função de classe e $\rho : G \longrightarrow GL(V)$ uma representação linear de G. Seja a transformação linear $\rho_f : V \longrightarrow V$ definida por $\rho_f = \sum_{t\in G} f(t)\rho_t$. Se ρ é irredutível de grau n e caracter χ, então ρ_f é uma homotetia de raio λ, com $\lambda = \frac{|G|}{n}\langle f, \overline{\chi}\rangle$.*

Demonstração. Observe que ρ_f é um isomorfismo de representações. De fato,

$$\begin{aligned}
\rho_s^{-1}\rho_f\rho_s &= \rho_s^{-1}\sum_{t\in G} f(t)\rho_t\rho_s \\
&= \sum_{t\in G} f(t)\rho_s^{-1}\rho_t\rho_s \\
&= \sum_{t\in G} f(t)\rho_{s^{-1}ts} \\
&= \sum_{u\in G} f(sus^{-1})\rho_u, \text{ fazendo } u = s^{-1}ts \\
&= \sum_{u\in G} f(u)\rho_u \\
&= \rho_f
\end{aligned}$$

o que impica $\rho_f \rho_s = \rho_s \rho_f$, e pelo Lema de Schur temos que ρ_f é uma homotetia de raio λ, ou seja, $\rho_f = \lambda Id_V$. Daí, $Tr(\rho_f) = Tr(\lambda Id_V) = n\lambda$, onde $n = dim V$ (I). Por outro lado, $\rho_f = \sum_{t \in G} f(t)\rho_t$. Daí,

$$\begin{aligned} Tr(\rho_f) &= Tr\left(\sum_{t \in G} f(t)\rho_t\right) \\ &= \sum_{t \in G} f(t) Tr(\rho_t) \\ &= \sum_{t \in G} f(t)\chi(t) \qquad \text{(II)}. \end{aligned}$$

De (I) e (II) temos $\lambda = \frac{1}{n}\sum_{t \in G} f(t)\chi(t)$. E, como $\langle f, \overline{\chi}\rangle = \frac{1}{|G|}\sum_{t \in G} f(t)\chi(t)$, segue-se que $\lambda = \frac{|G|}{n}\langle f, \overline{\chi}\rangle$. □

Teorema 8. *Os caracteres $\chi_1, \chi_2, ..., \chi_h$ formam uma base ortogonal de $\mathbb{C}[G]$.*

Demonstração. Pelo Teorema 7, vimos que se χ é o caracter de uma representação irredutível $\langle \chi, \chi\rangle = 1$, e se χ e χ' são caracteres irredutíveis de representações não isomorfas, então $\langle \chi, \chi'\rangle = 0$. Isso mostra que os $\chi_i^{'}s$ formam um conjunto ortogonal, e portanto linearmente independente, em $\mathbb{C}[G]$.

Resta mostrar que os ${\chi_i}'s$ geram $\mathbb{C}[G]$. Para isto é suficiente mostrar que cada elemento de $\mathbb{C}[G]$ ortogonal a todos os ${\chi_i}'s$ é nulo. De fato, tome $f \in \mathbb{C}[G]$ um elemento ortogonal a todos os caracteres irredutíveis. Daí, f deve ser ortogonal a todos os caracteres de G.

Considere agora a função $\bar{f} : G \longrightarrow \mathbb{C}$, definida por $\bar{f}(t) = \overline{f(t)}$. Temos que $\bar{f} \in \mathbb{C}[G]$. Para cada representação ρ de G, façamos $\rho_{\bar{f}} = \sum_{t \in G} \overline{f(t)}\rho_t$. Sendo χ o caracter de ρ, temos $\langle f, \chi\rangle = 0$ e daí $\langle \bar{f}, \bar{\chi}\rangle = 0$. Pela proposição anterior, temos que $\rho_{\bar{f}} = 0$.

Aplicando isso à representação regular ρ e calculando a imagem do vetor e_1 sob ρ_f, temos

$$\rho_{\bar{f}}(e_1) = \sum_{t \in G} \overline{f(t)}\rho_t(e_1) = \sum_{t \in G} \overline{f(t)}e_t \ .$$

Como $\rho_{\bar{f}}$ é nula, temos $\rho_{\bar{f}}(e_1) = 0$, e da igualdade acima segue-se que $\overline{f(t)} = 0$, para todo $t \in G$, uma vez que o conjunto $\{e_t; t \in G\}$ é linearmente independente. Logo, $\bar{f}$ é nula e portanto f é nula. □

Teorema 9. *O número de representações irredutíveis de G é igual ao número de classes de conjugação de G.*

Demonstração. Sejam $C_1, C_2, ..., C_k$ as distintas classes de conjugação de G. Dizer que a função f em G é uma função de classe é equivalente a dizer que f é constante em cada um dos $C_1, ..., C_k$. Consequentemente, a dimensão do espaço $\mathbb{C}[G]$ das funções de classe é igual a k. Por outro lado, a dimensão é, pelo Teorema 8, igual ao número de representações irredutíveis de G, donde segue o resultado. □

Proposição 10. *Seja $s \in G$ e seja c_s o número de elementos na classe de conjugação de s.*

1. *Temos* $\sum_{i=1}^{h} \overline{\chi_i(s)}\chi_i(s) = \frac{|G|}{c_s}$.

2. *Para $t \in G$ não conjugado de s, temos* $\sum_{i=1}^{h} \overline{\chi_i(s)}\chi_i(t) = 0$.

Demonstração. Seja $f_s : G \longrightarrow \mathbb{C}$ igual a 1 na classe de conjugação s e igual a 0 nos demais elementos de G. Uma vez que, f_s é uma função de classe, ou seja, $f_s \in \mathbb{C}[G]$, pelo Teorema 8 podemos escrever $f_s = \sum_{i=1}^{h} \lambda_i \chi_i$, com $\lambda_i = \langle f_s, \chi_i \rangle = \frac{c_s}{|G|}\overline{\chi_i(s)}$, ou seja,

$$\begin{aligned} f_s(t) &= \sum_{i=1}^{h} \frac{c_s}{|G|}\overline{\chi_i(s)}\chi_i(t) \\ &= \frac{c_s}{|G|}\sum_{i=1}^{h} \overline{\chi_i(s)}\chi_i(t) \end{aligned}$$

Temos dois casos:

1. Caso em que $s = t$: $1 = f_s(s) = \frac{c_s}{|G|}\sum_{i=1}^{h} \overline{\chi_i(s)}\chi_i(s)$ e daí $\sum_{i=1}^{h} \overline{\chi_i(s)}\chi_i(s) = \frac{|G|}{c_s}$.

2. Caso em que t não é conjugado de s: $0 = f_s(t) = \frac{c_s}{|G|}\sum_{i=1}^{h} \overline{\chi_i(s)}\chi_i(t)$ e daí $\sum_{i=1}^{h} \overline{\chi_i(s)}\chi_i(t) = 0$.

□

Capítulo 4

Teorema $p^a q^b$ de Burnside

Lema 3. *Se χ é o caracter de uma representação de G ,então $\chi(g)$ é um inteiro algébrico para todo $g \in G$.*

Demonstração. Seja

$$\begin{array}{rccc} \varphi & : G & \longrightarrow & GL_n(\mathbb{C}) \\ & g & \longmapsto & \varphi(g) = \varphi_g \end{array} \quad \text{uma representação de } G.$$

Fixado $g \in G$, considere a matriz φ_g. Como $\mathbb{C}$ é algebricamenete fechado, toda matriz quadrada com entradas complexas é triangulável sobre $\mathbb{C}$, ou seja, existe $X \in GL_n(\mathbb{C})$ tal que $X^{-1}\varphi_g X$ é triangular. Daí,

$$\mathbf{X^{-1}\varphi_g X} = \begin{pmatrix} a_{11} & * & * & * \\ 0 & a_{22} & \dots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & a_{nn} \end{pmatrix}$$

e portanto

$$(\mathbf{X^{-1}\varphi_g X})^{\mathbf{m}} = \begin{pmatrix} (a_{11})^m & * & * & * \\ 0 & (a_{22})^m & \dots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & (a_{nn})^m \end{pmatrix} \text{, para } m \in \mathbb{N}.$$

Por outro lado, se $m = |G|$,

$$\begin{aligned} (X^{-1}\varphi_g X)^m &= X^{-1}(\varphi_g)^m X \\ &= X^{-1}\varphi_{g^m} X \\ &= X^{-1}\varphi_e X \\ &= X^{-1} I_m X \\ &= I_m \end{aligned}$$

Daí, $a_{11}^m = a_{22}^m = \ldots = a_{nn}^m = 1$, implicando que cada a_{ii}, com $i = 1, \ldots, n$ é raiz do polinômio mônico $p(x) = x^m - 1$, ou seja, cada a_{ii} é um inteiro algébrico. E como

$$\begin{aligned} \chi(g) &= Tr(\varphi_g) \\ &= Tr(X^{-1}\varphi_g X) \\ &= \sum_{i=1}^{h} a_{ii} \end{aligned}$$

e soma de inteiros algébricos é inteiro algébrico, segue-se que $\chi(g)$ é um inteiro algébrico. □

Observação 11. *Sejam $\lambda_1, \ldots, \lambda_n \in \mathbb{C}$, todos com mesmo módulo, tais que $|\lambda_1 + \ldots + \lambda_n| = |\lambda_1| + \ldots + |\lambda_n|$. Então $\lambda_1 = \ldots = \lambda_n$. De fato, afirmamos que $|\lambda_i + \lambda_j| = |\lambda_i| + |\lambda_j|$ para quaisquer $i, j \in \{1, \ldots, n\}$. Suponhamos por absurdo que $|\lambda_1 + \lambda_2| < |\lambda_1| + |\lambda_2|$, então*

$$|\lambda_1 + \lambda_2 + \ldots + \lambda_n| \leq |\lambda_1 + \lambda_2| + |\lambda_3 + \ldots + \lambda_n| < |\lambda_1| + |\lambda_2| + \cdots + |\lambda_n|.$$

Absurdo. Logo, existe $\alpha \geq 0$ tal que $\lambda_i = \alpha\lambda_j$, o que implica que $|\lambda_i| = |\alpha||\lambda_j|$, ou seja, $\alpha = 1$, donde segue que $\lambda_i = \lambda_j$.

Lema 4. *Seja ρ uma representação de um grupo G com caracter χ, e seja $N = \{x \in G; |\chi(x)| = \chi(1)\}$, então*

1. *$N = \{x \in G; \rho(x) = \alpha I,\ \alpha \in \mathbb{C}\}$.*
2. *N é um subgrupo normal de G.*

Demonstração.

1. Tome $x \in N$ e considere $\lambda_1, \lambda_2, \ldots, \lambda_n$ os autovalores de $\rho(x)$. Observe que,
$$n = |\chi(x)| = |\lambda_1 + \ldots + \lambda_n| \leq |\lambda_1| + \ldots + |\lambda_n| = n$$
o que implica $|\lambda_1 + \ldots + \lambda_n| = |\lambda_1| + \ldots + |\lambda_n|$. Assim, da observação feita anteriormente, temos que os autovalores são todos iguais, digamos α.

   Considere β uma base de V tal que

$$[\rho(\mathbf{x})]_\beta = \begin{pmatrix} \alpha & * & * & * \\ 0 & \alpha & \ldots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & \alpha \end{pmatrix} = \quad \alpha I + A$$

onde A é nilpotente, pois é uma matriz triangular superior com diagonal igual a 0. Assim, existe $k \in \mathbb{N}$ tal que $([T]_\beta - \alpha I)^k = 0$, onde $T = \rho(x)$.

Observe que o polinômio $g(x) = (x-\alpha)^k$ anula T e consequentemente é divisível pelo minimal de T, o que implica que $m_T(x) = (x-\alpha)^l$, com $l \leq k$.

Sendo $|G| = m$, observe que $T^m = I$ e então o polinômio $f(x) = x^m - 1$ anula T e assim também é divisível pelo minimal de T. Mas como as raízes de $f(x)$ são todas distintas $m_T(x)$ não terá raízes múltiplas, donde $m_T(x) = x - \alpha$. Portanto, $T - \alpha I = 0$, o que implica $T = \alpha I$.

2. De fato, dados g_1, $g_2 \in N$ temos que

$$\begin{aligned} \rho(g_1^{-1}) &= \rho(g_1)^{-1} \\ &= (\lambda_{g_1} I)^{-1} \\ &= \lambda_{g_1}^{-1} I \end{aligned}$$

e

$$\begin{aligned} \rho(g_1 g_2) &= \rho(g_1)\rho(g_2) \\ &= (\lambda_{g_1} I)(\lambda_{g_2} I) \\ &= (\lambda_{g_1}\lambda_{g_2}) I^2 \\ &= (\lambda_{g_1}\lambda_{g_2}) I \end{aligned}$$

implicando g_1^{-1}, $g_1 g_2 \in N$, ou seja, $N \leqslant G$. Ademais, dados $g \in G$, e $n \in N$ temos

$$\rho(gng^{-1}) = \rho(g)\rho(n)\rho(g^{-1}) = \rho(g)(\lambda_n I)\rho(g)^{-1} = \lambda_n(\rho(g)\rho(g)^{-1}) = \lambda_n I$$

implicando $gng^{-1} \in N$, isto é, $N \trianglelefteq G$.

□

Seja $\rho_i : G \longrightarrow GL_{n_i}(\mathbb{C})$ uma representação irredutível do grupo G. Fixado $g \in G$, arbitrário, defina

$$C_g = \sum_{y \in C_G(g)} \rho_i(y) \ .$$

Para cada $a \in G$ temos que $\rho_i(a)^{-1} C_g \rho_i(a) = \sum_{y \in G_g(a)} \rho_i(a^{-1}ya) = C_g$. Logo, $C_g\rho_i(a) = \rho_i(a)C_g$. Pelo Lema de Schur, segue-se que $C_g = w(g)I$, onde $w(g) \in \mathbb{C}$.

Ademais, $Tr(C_g) = n_i w(g)$, e também

$$Tr(C_g) = \sum_{y \in C_G(g)} Tr(\rho_i(y)) = \sum_{y \in C_G(g)} \chi_i(y) = c_g \chi_i(g).$$

Logo, $w(g) = \dfrac{c_g \chi_i(g)}{n_i}$.

Lema 5. *Sendo G um grupo, temos que para cada $g \in G$, $w(g) = \dfrac{c_g \chi_i(g)}{n_i}$ é um inteiro algébrico.*

Demonstração. Veja [4], página 133. □

Lema 6. *Se ρ_i é uma representação irredutível de G de grau n_i, caracter χ_i, e se $g \in G$ é tal que $mdc(c_g, n_i) = 1$, então $\chi_i(g) = 0$ ou $\rho_i(g)$ é uma matriz escalar.*

Demonstração. Sabendo que $\dfrac{c_g \chi_i(g)}{n_i}$ é um inteiro algébrico. Como $mdc(c_g, n_i) = 1$, existem $k_1, k_2 \in \mathbb{Z}$ tais que $c_g k_1 + n_i k_2 = 1$, o que implica que $\dfrac{c_g \chi_i(g)}{n_i} k_1 + \chi_i(g) k_2 = \dfrac{\chi_i(g)}{n_i}$. Donde segue-se que $\dfrac{\chi_i(g)}{n_i}$ é um inteiro algébrico.

Como $\chi_i(g)$ é a soma de n_i raízes da unidade, digamos, $\chi_i(g) = w_1 + w_2 + \ldots + w_{n_i}$, temos

$$\left| \frac{\chi_i(g)}{n_i} \right| = \left| \frac{w_1 + w_2 + \ldots + w_{n_i}}{n_i} \right| \leq \frac{|w_1| + \ldots + |w_{n_i}|}{n_i} \leq 1 \ .$$

No caso em que $\left| \dfrac{\chi_i(g)}{n_i} \right| = 1$, segue do Lema 4 que $\rho_i(g)$ é um múltiplo escalar da identidade.

No caso em que $\left| \dfrac{\chi_i(g)}{n_i} \right| < 1$, temos $|w_1 + \ldots + w_{n_i}| < n_i$ e então $w_1, \ldots, w_{n_i}$ não são todas iguais. Segue do Lema 2 que $\dfrac{\chi_i(g)}{n_i} = 0$, assim $\chi_i(g) = 0$.

□

Teorema 10. *Se num grupo G o número de conjugados de algum elemento $g \neq 1$ é potência de um primo, então G não pode ser simples.*

Demonstração. Seja $g \neq 1$ e suponha $c_g = p^\alpha$, com p primo e $\alpha \in \mathbb{N}$. Como o caracter r_G da representação regular é dado por $r_G = \sum_{i=1}^{k} n_i \chi_i$, onde $\chi_1, \ldots, \chi_h$

são os caracteres irredutíveis e $n_1, \ldots, n_h$ os seus graus.

$$\begin{aligned} r_G(g) &= \sum_{i=1}^{h} n_i\chi_i(g) \\ &= n_1\chi_1(g) + \sum_{i=2}^{h} n_i\chi_i(g) \\ &= 1 + \sum_{i=2}^{h} n_i\chi_i(g) \end{aligned}$$

Como $r_G(g) = 0$, para $g \neq 1$, temos $1 + \sum_{i=2}^{h} n_i\chi_i(g) = 0$.

Suponha, por absurdo, que G é simples. Do Lema 4, vimos que $N = \{x \in G; \rho(x) = \alpha_x I\}$ é normal em G, então $N = \{e\}$ ou $N = G$. Se $N = G$, então pelo Exemplo 10, qualquer subespaço vetorial W de V é estável por ρ, absurdo, pois ρ é irredutível. Logo $N = \{e\}$, e então para todo $i = 1, 2, \ldots, h$, $\rho_i(g)$ não pode ser uma matriz escalar. Assim, analisemos os casos.

Se $p \nmid n_i$, como p é primo, $mdc(p, n_i) = 1$, o que implica que $mdc(p^\alpha, n_i) = 1$, e do Lema 6 segue-se que $\chi_i(g) = 0$. Neste caso, para cada $i = 1, 2, \ldots, h$ temos $n_i\chi_i(g) = 0$.

Se $p \mid n_i$, para cada $i = 1, 2, \ldots, h$, temos $n_i\chi_i(g) = pq_i\chi_i(g)$, com $q_i \in \mathbb{Z}$. Logo, $\sum_{i=2}^{h} n_i\chi_i(g) = p\gamma$, onde γ é um inteiro algébrico, pois como $q_i \in \mathbb{Z}$, q_i é um inteiro algébrico, além disso $\chi_i(g)$ também é.

Daí, $1 + p\gamma = 0$, o que implica $\gamma = \frac{-1}{p}$. Absurdo, pois $\mathbb{Q} \cap I_{\mathbb{C}}(\mathbb{Z}) = \mathbb{Z}$. □

Teorema 11 (Teorema p^aq^b de Burnside)**.** *Se $|G| = p^aq^b$, com p e q primos, então G é solúvel.*

Demonstração. Sabemos que se $N \trianglelefteq G$, com N e $\frac{G}{N}$ solúveis em G, então G é solúvel. Em vista disso, basta mostrarmos que G não é simples e depois usarmos indução em $|G|$. Como q divide $|G|$, pelo Primeiro Teorema de Sylow temos que G possui algum S_q - subgrupo, a saber, H, ou seja, $|H| = q^b$, pois q^b é maior potência de q que divide $|G|$.

Tome $g \in H - \{1\}$, com $g \in Z(H)$. Isso ocorre se, e somente se $H \subseteq C_G(g)$. Sendo c_g o número de conjugados de g, temos que

$$c_g = |G : C_G(g)| = \frac{|G|}{|C_G(g)|} = \frac{p^aq^b}{p^kq^b} = p^{a-k}$$

com $0 \leq k \leq a$, pois $|H|$ divide $|C_G(g)|$ e $|C_G(g)|$ divide $|G| = p^a q^b$. Daí, pelo Teorema 10, existe $N \trianglelefteq G$ tal que $\{e\} \neq N \trianglelefteq G$.

Suponhamos agora por indução que o resultado vale para todo grupo de ordem menor que $|G|$ e divisível por, no máximo, dois primos.

Observe que $1 < |N| < |G|$, já que $N \trianglelefteq G$ não trivial e é próprio. Pelo teorema de Lagrange $|N|$ e $\frac{|G|}{|N|}$ dividem $|G|$ e são ambos menores que $|G|$. Logo, por hipótese de indução, N e $\frac{G}{N}$ são solúveis e assim G é solúvel. $\square$

Referências Bibliográficas

[1] COELHO, F. H., LOURENÇO, M. L. *Um Curso de Álgebra Linear*. São Paulo, Brasil: Editora da Universidade de São Paulo, 2001.

[2] ENDLER, O. *Teoria dos Números Algébricos*. Projeto Euclides. Rio de Janeiro, Brasil: Associação Instituto de Matemática Pura e Aplicada, CNPq, 2003.

[3] GARCIA, A. *Elementos de Álgebra*. Projeto Euclides. Rio de Janeiro, Brasil: Associação Instituto de Matemática Pura e Aplicada, 2003.

[4] HERSTEIN, I. N. *Noncommutative rings*. The carus mathematical monographs. 3ª edição. The mathematical associaton of America, 1973.

[5] HOFFMAN, K. M., KUNZE, R. *Álgebra Linear*. 2ª edição. Livros técnicos e científicos, 1979.

[6] LIMA, E. L. *Álgebra Linear*. Coleção Matemática Universitária. 6ª edição. Rio de Janeiro, Brasil: Associação Instituto de Matemática Pura e Aplicada, 2003.

[7] SERRE, J. P. *Linear Representations of Finite Group*. 2ª edição. Springer-Verlag, 1977.