

O Teorema de Burnside

Guilherme da Costa Cruz

Instituto de Matemática e Estatística - USP

2 de Abril de 2021

Teorema (Burnside, 1904)

Todo grupo de ordem $p^a q^b$, onde p e q são primos e $a, b \in \mathbb{N}$, é solúvel.

Teorema (Burnside, 1904)

Todo grupo de ordem $p^a q^b$, onde p e q são primos e $a, b \in \mathbb{N}$, é solúvel.

- ▶ Por exemplo, o menor grupo não-solúvel é A_5 , que tem ordem $60 = 2^2 \cdot 3 \cdot 5$.

Proposição

Dado um grupo G , são equivalentes:

1. A série de grupos derivados

$$G = G^{(0)} \triangleright G^{(1)} \triangleright G^{(2)} \triangleright \dots$$

chega no grupo trivial $\{1\}$, onde $G^{(j)} = [G^{(j-1)}, G^{(j-1)}]$.

2. Existe uma série

$$G = G_0 \triangleright G_1 \triangleright G_2 \triangleright \dots \triangleright G_n = \{1\}$$

tal que os fatores G_{j-1}/G_j são abelianos.

Quando esses itens são satisfeitos, dizemos que G é solúvel.

Proposição

Dado um grupo G , são equivalentes:

1. A série de grupos derivados

$$G = G^{(0)} \triangleright G^{(1)} \triangleright G^{(2)} \triangleright \dots$$

chega no grupo trivial $\{1\}$, onde $G^{(j)} = [G^{(j-1)}, G^{(j-1)}]$.

2. Existe uma série

$$G = G_0 \triangleright G_1 \triangleright G_2 \triangleright \dots \triangleright G_n = \{1\}$$

tal que os fatores G_{j-1}/G_j são abelianos.

Quando esses itens são satisfeitos, dizemos que G é solúvel.

- ▶ Usando (1): se G é simples e não-abeliano, então G não é solúvel.
- ▶ Usando (2): se $H \triangleleft G$ é solúvel e G/H é solúvel, então G é solúvel.

Reformulando o Teorema

Suponha que exista algum grupo G não-solúvel de ordem $p^a q^b$.
Tomando-o com a menor ordem possível, afirmo que G é simples e não-abeliano: se G possuir um subgrupo H normal, próprio e não-trivial, então G/H e H são grupos de ordem $p^c q^d < |G|$; pela minimalidade da ordem de G , teríamos que G/H e H são solúveis e, portanto, G seria solúvel (absurdo!).

Reformulando o Teorema

Suponha que exista algum grupo G não-solúvel de ordem $p^a q^b$. Tomando-o com a menor ordem possível, afirmo que G é simples e não-abeliano: se G possuir um subgrupo H normal, próprio e não-trivial, então G/H e H são grupos de ordem $p^c q^d < |G|$; pela minimalidade da ordem de G , teríamos que G/H e H são solúveis e, portanto, G seria solúvel (absurdo!).

Teorema (Burnside)

Não existem grupos simples não-abelianos de ordem $p^a q^b$, onde p e q são primos e $a, b \in \mathbb{N}$.

O Burnside



Figura 1: [1, p.89]

- ▶ William Burnside (1852-1927) foi um dos pioneiros no estudo de representações.



Figura 1: [1, p.89]

- ▶ William Burnside (1852-1927) foi um dos pioneiros no estudo de representações.
- ▶ 1890-1900: estudou grupos simples e suas ordens.



Figura 1: [1, p.89]

- ▶ William Burnside (1852-1927) foi um dos pioneiros no estudo de representações.
- ▶ 1890-1900: estudou grupos simples e suas ordens.
- ▶ Em 1897, publicou o primeiro tratado em língua inglesa de teoria de grupos finitos.



Figura 1: [1, p.89]

- ▶ William Burnside (1852-1927) foi um dos pioneiros no estudo de representações.
- ▶ 1890-1900: estudou grupos simples e suas ordens.
- ▶ Em 1897, publicou o primeiro tratado em língua inglesa de teoria de grupos finitos.
- ▶ 1900-1905: resultados em representações de grupos.



Figura 1: [1, p.89]

- ▶ William Burnside (1852-1927) foi um dos pioneiros no estudo de representações.
- ▶ 1890-1900: estudou grupos simples e suas ordens.
- ▶ Em 1897, publicou o primeiro tratado em língua inglesa de teoria de grupos finitos.
- ▶ 1900-1905: resultados em representações de grupos.
- ▶ Demonstrou o teorema em 1904, utilizando conceitos de representações e teoria algébrica dos números.

► Faleceu em 1927:

"Rowing men will regret to hear of the death of W. Burnside, one of the best known Cambridge athletes of his day. He missed his Blue but captained the Pembroke boat."

- ▶ Faleceu em 1927:

"Rowing men will regret to hear of the death of W. Burnside, one of the best known Cambridge athletes of his day. He missed his Blue but captained the Pembroke boat."

- ▶ Antes de sua morte, escreveu uma carta contendo problemas relevantes a Philip Hall (1904-1982), que se tornou seu sucessor.

- ▶ Faleceu em 1927:

"Rowing men will regret to hear of the death of W. Burnside, one of the best known Cambridge athletes of his day. He missed his Blue but captained the Pembroke boat."

- ▶ Antes de sua morte, escreveu uma carta contendo problemas relevantes a Philip Hall (1904-1982), que se tornou seu sucessor.
- ▶ O resultado de que todo grupo de ordem ímpar é solúvel foi provado em 1963 por Feit e Thompson.

Representações de Grupos

Representações de Grupos: Definições [2]

Definição

Dado um grupo G , uma **representação (linear) de G** é um espaço vetorial V , sobre um corpo \mathbb{K} , munido de um homomorfismo de grupos $\rho : G \rightarrow GL(V)$, isto é:

$$\forall g, h \in G \quad \rho(gh) = \rho(g)\rho(h), \quad \rho(1) = Id, \quad \rho(g^{-1}) = \rho(g)^{-1}.$$

Representações de Grupos: Definições [2]

Definição

Dado um grupo G , uma **representação (linear) de G** é um espaço vetorial V , sobre um corpo \mathbb{K} , munido de um homomorfismo de grupos $\rho : G \rightarrow GL(V)$, isto é:

$$\forall g, h \in G \quad \rho(gh) = \rho(g)\rho(h), \quad \rho(1) = Id, \quad \rho(g^{-1}) = \rho(g)^{-1}.$$

Exemplo:

O grupo diedral $D_n = \{a^i b^j \mid a^n = 1, b^2 = 1, bab = a^{-1}\}$ é o grupo das simetrias de um n -ágono.

Representações de Grupos: Definições [2]

Definição

Dado um grupo G , uma **representação (linear) de G** é um espaço vetorial V , sobre um corpo \mathbb{K} , munido de um homomorfismo de grupos $\rho : G \rightarrow GL(V)$, isto é:

$$\forall g, h \in G \quad \rho(gh) = \rho(g)\rho(h), \quad \rho(1) = Id, \quad \rho(g^{-1}) = \rho(g)^{-1}.$$

Exemplo:

O grupo diedral $D_n = \{a^i b^j \mid a^n = 1, b^2 = 1, bab = a^{-1}\}$ é o grupo das simetrias de um n -ângono. Tome $V = \mathbb{R}^2$ e $\rho : D_n \rightarrow GL(V)$ para ser o homomorfismo que satisfaz

$$\rho(a) = \begin{bmatrix} \cos \frac{2\pi}{n} & -\sin \frac{2\pi}{n} \\ \sin \frac{2\pi}{n} & \cos \frac{2\pi}{n} \end{bmatrix} \quad \rho(b) = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Convenção: a é a rotação no sentido anti-horário e b é a reflexão em relação ao eixo y .

Representações de Grupos: Definições

Representação Regular:

Sendo G um grupo e k um corpo, construa o espaço vetorial, denotado por $k[G]$, que tenha como base o próprio grupo G :

$$k[G] = \left\{ \sum_{g \in G} c_g g : c_g \in k, g \in G \right\}.$$

Representações de Grupos: Definições

Representação Regular:

Seja G um grupo e k um corpo, construa o espaço vetorial, denotado por $k[G]$, que tenha como base o próprio grupo G :

$$k[G] = \left\{ \sum_{g \in G} c_g g : c_g \in k, g \in G \right\}.$$

- ▶ Se $|G| = n$, então $\dim(k[G]) = n$.
- ▶ A operação de G define um produto nos elementos da base e , estendendo bilinearmente essa operação para todo o espaço, temos que $k[G]$ é vista como uma álgebra (a álgebra do grupo G).

Representações de Grupos: Definições

Representação Regular:

Sendo G um grupo e k um corpo, construa o espaço vetorial, denotado por $k[G]$, que tenha como base o próprio grupo G :

$$k[G] = \left\{ \sum_{g \in G} c_g g : c_g \in k, g \in G \right\}.$$

- ▶ Se $|G| = n$, então $\dim(k[G]) = n$.
- ▶ A operação de G define um produto nos elementos da base e, estendendo bilinearmente essa operação para todo o espaço, temos que $k[G]$ é vista como uma álgebra (a álgebra do grupo G).

A representação regular é a função $\rho : G \rightarrow \text{GL}(k[G])$ de multiplicação à esquerda:

$$\rho(h) \left(\sum_{g \in G} c_g g \right) = \sum_{g \in G} c_g (hg).$$

Definição

Dizemos que V é **irredutível** se V não possui uma subrepresentação própria não nula, ou seja, se suas únicas subrepresentações são as triviais, V e $\{0\}$.

Teorema (Maschke, 1899)

Se G é um grupo finito e k é um corpo tal que $\text{char}(k) \nmid |G|$. Então, toda representação de G (de dimensão finita) pode ser decomposta como uma soma direta de representações irredutíveis.

- ▶ Ou seja, a álgebra $k[G]$ é semissimples (nas hipóteses do teorema).

Teorema (Lema de Schur)

Seja $\rho: G \rightarrow \text{GL}(V)$ uma representação de dimensão finita irredutível sobre um corpo algebricamente fechado. Se $g \in G$ é um elemento central, então $\rho(g) = \lambda Id$, para algum $\lambda \in k$.

Teorema (Lema de Schur)

Seja $\rho: G \rightarrow \text{GL}(V)$ uma representação de dimensão finita irredutível sobre um corpo algebricamente fechado. Se $g \in G$ é um elemento central, então $\rho(g) = \lambda \text{Id}$, para algum $\lambda \in k$.

Corolário

Suponha que $|G| < \infty$ e que k é um corpo algebricamente fechado tal que $\text{char}(k) \nmid |G|$. Se $\rho: G \rightarrow \text{GL}(V)$ é uma representação de dimensão finita sobre k , então, dado $g \in G$, $\rho(g)$ é diagonalizável.

Representações de Grupos Finitos: Caracteres

Definição

Seja $\rho: G \rightarrow GL(V)$ uma representação do grupo G (sobre \mathbb{C}), onde V tem dimensão finita. Chamamos a função seguinte de *caracter da representação V* :

$$\begin{aligned}\chi_V: G &\rightarrow \mathbb{C} \\ g &\mapsto \text{Tr}(\rho(g))\end{aligned}$$

Representações de Grupos Finitos: Caracteres

Definição

Seja $\rho: G \rightarrow GL(V)$ uma representação do grupo G (sobre \mathbb{C}), onde V tem dimensão finita. Chamamos a função seguinte de *caracter da representação V* :

$$\begin{aligned}\chi_V: G &\rightarrow \mathbb{C} \\ g &\mapsto \text{Tr}(\rho(g))\end{aligned}$$

Teorema

Duas representações de um grupo finito são isomorfas se, e somente se, seus caracteres são iguais.

Representações de Grupos Finitos: Caracteres

Teorema

Os caracteres irredutíveis de um grupo finito G formam um conjunto ortonormal.

Ou seja, se U e V representações irredutíveis de G , então

$$(\chi_U, \chi_V) = \frac{1}{|G|} \sum_{g \in G} \chi_U(g) \overline{\chi_V(g)} = \begin{cases} 1, & \text{se } U \cong V \\ 0, & \text{se } U \not\cong V \end{cases}.$$

Representações de Grupos Finitos: Caracteres

Teorema

Os caracteres irredutíveis de um grupo finito G formam um conjunto ortonormal.

Ou seja, se U e V representações irredutíveis de G , então

$$(\chi_U, \chi_V) = \frac{1}{|G|} \sum_{g \in G} \chi_U(g) \overline{\chi_V(g)} = \begin{cases} 1, & \text{se } U \cong V \\ 0, & \text{se } U \not\cong V \end{cases}.$$

Proposição (Ortogonalidade das Colunas)

Sejam χ_1, \dots, χ_r os caracteres irredutíveis de um grupo G , então:

$$\sum_{i=1}^r \chi_i(g) \overline{\chi_i(h)} = \begin{cases} |C_G(g)|, & \text{se } h \text{ e } g \text{ são conjugados} \\ 0, & \text{c.c.} \end{cases},$$

onde $C_G(g)$ é o centralizador de $g \in G$.

Os Inteiros Algébricos

Os Inteiros Algébricos

Definição

Um *inteiro algébrico* é um número (complexo) que é raiz de um polinômio mônico com coeficientes em \mathbb{Z} .

Definição

Um *inteiro algébrico* é um número (complexo) que é raiz de um polinômio mônico com coeficientes em \mathbb{Z} .

Proposição

Denote por \mathbb{A} o conjunto dos inteiros algébricos:

1. $\mathbb{A} \cap \mathbb{Q} = \mathbb{Z}$.
2. \mathbb{A} é um anel.

Definição

Um *inteiro algébrico* é um número (complexo) que é raiz de um polinômio mônico com coeficientes em \mathbb{Z} .

Proposição

Denote por \mathbb{A} o conjunto dos inteiros algébricos:

1. $\mathbb{A} \cap \mathbb{Q} = \mathbb{Z}$.
2. \mathbb{A} é um anel.

Exemplos no nosso caso:

Os valores $\chi(g)$ de todo caracter são inteiros algébricos: como $\rho(g)$ é diagonalizável e $\rho(g)^{|G|} = 1$, então $\chi(g)$ é uma soma de raízes $|G|$ -ésimas da unidade.

Nossos inteiros algébricos

Lema (22.8 em [3])

Se $r = \sum_{g \in G} a_g g \in \mathbb{C}[G]$ satisfaz que $a_g \in \mathbb{Z} \forall g \in G$ e existem $0 \neq v \in V$, $\lambda \in \mathbb{C}$ tais que $r \cdot v = \lambda v$, então λ é um inteiro algébrico.

Nossos inteiros algébricos

Lema (22.8 em [3])

Se $r = \sum_{g \in G} a_g g \in \mathbb{C}[G]$ satisfaz que $a_g \in \mathbb{Z} \forall g \in G$ e existem $0 \neq v \in V$, $\lambda \in \mathbb{C}$ tais que $r \cdot v = \lambda v$, então λ é um inteiro algébrico.

Teorema (Frobenius, 1896)

Se χ é o caracter de uma representação irredutível V e $g \in G$, então $\frac{|O_g| \cdot \chi(g)}{\dim(V)}$ é um inteiro algébrico.

Nossos inteiros algébricos

Lema (22.8 em [3])

Se $r = \sum_{g \in G} a_g g \in \mathbb{C}[G]$ satisfaz que $a_g \in \mathbb{Z} \forall g \in G$ e existem $0 \neq v \in V$, $\lambda \in \mathbb{C}$ tais que $r \cdot v = \lambda v$, então λ é um inteiro algébrico.

Teorema (Frobenius, 1896)

Se χ é o caracter de uma representação irredutível V e $g \in G$, então $\frac{|O_g| \cdot \chi(g)}{\dim(V)}$ é um inteiro algébrico.

Demonstração:

Sendo O_g a classe de conjugação de $g \in G$, tomando a soma dos elementos de O_g

$$\bar{C} = \sum_{h \in O_g} h \in \mathbb{C}[G],$$

temos que \bar{C} é um elemento central de $\mathbb{C}[G]$.

Nossos inteiros algébricos

Pensando na representação irredutível $\rho: G \rightarrow GL(V)$ estendida para $\rho: \mathbb{C}[G] \rightarrow GL(V)$, temos que $\rho(\bar{C}) = \lambda \text{Id}_V$.

Pelo lema, temos que λ é um inteiro algébrico e o seguinte nos diz que λ é exatamente o número do enunciado:

$$|O_g| \chi(g) = \sum_{h \in O_g} \chi(h) = \chi(\bar{C}) = \lambda \dim(V) \Rightarrow \lambda = \frac{|O_g| \chi(g)}{\dim(V)}.$$

Nossos inteiros algébricos

Pensando na representação irredutível $\rho: G \rightarrow GL(V)$ estendida para $\rho: \mathbb{C}[G] \rightarrow GL(V)$, temos que $\rho(\bar{C}) = \lambda \text{Id}_V$.

Pelo lema, temos que λ é um inteiro algébrico e o seguinte nos diz que λ é exatamente o número do enunciado:

$$|O_g| \chi(g) = \sum_{h \in O_g} \chi(h) = \chi(\bar{C}) = \lambda \dim(V) \Rightarrow \lambda = \frac{|O_g| \chi(g)}{\dim(V)}.$$

Corolário (Divisibilidade de Frobenius, 1896)

Se V é uma representação irredutível de G , então $\dim(V)$ divide $|G|$.

Ideia:

Basta provar que $\frac{|G|}{\dim(V)}$ é um inteiro algébrico.

Teorema (Burnside, 1904)

Se G é um grupo (finito) com uma classe de conjugação de ordem p^r , onde p é primo e $r \geq 1$, então G não é simples.

Teorema (Burnside, 1904)

Se G é um grupo (finito) com uma classe de conjugação de ordem p^r , onde p é primo e $r \geq 1$, então G não é simples.

Demonstração:

Seja $g \in G$ o elemento tal que $|O_g| = p^r > 1$ e denote por χ_0, \dots, χ_k os caracteres irredutíveis de G , onde χ_0 é o caracter trivial. Pela ortogonalidade das colunas e por $g \neq 1$, temos que

$$1 + \sum_{i=1}^k \chi_i(g) \overline{\chi_i(1)} = 0 \Rightarrow \sum_{i=1}^k \chi_i(g) \frac{\chi_i(1)}{p} = -\frac{1}{p}.$$

Teorema (Burnside, 1904)

Se G é um grupo (finito) com uma classe de conjugação de ordem p^r , onde p é primo e $r \geq 1$, então G não é simples.

Demonstração:

Seja $g \in G$ o elemento tal que $|O_g| = p^r > 1$ e denote por χ_0, \dots, χ_k os caracteres irredutíveis de G , onde χ_0 é o caracter trivial. Pela ortogonalidade das colunas e por $g \neq 1$, temos que

$$1 + \sum_{i=1}^k \chi_i(g) \overline{\chi_i(1)} = 0 \Rightarrow \sum_{i=1}^k \chi_i(g) \frac{\chi_i(1)}{p} = -\frac{1}{p}.$$

Como $-1/p$ é um racional não-inteiro, temos que a soma da esquerda não é um inteiro algébrico e, já que $\chi_i(g)$ é um inteiro algébrico para todo i , segue que existe $j \geq 1$ tal que $\chi_j(1)/p$ não é um inteiro algébrico e $\chi_j(g) \neq 0$.

A ponte

Em outras palavras: $\chi_j(1)$ não é divisível por p . Como $|O_g| = p^r$, isso quer dizer que $\chi_j(1)$ e $|O_g|$ são primos entre si e, portanto, existem inteiros a e b tais que

$$a|O_g| + b\chi_j(1) = 1 \Rightarrow a \frac{|O_g| \cdot \chi_j(g)}{\chi_j(1)} + b\chi_j(g) = \frac{\chi_j(g)}{\chi_j(1)}.$$

A ponte

Em outras palavras: $\chi_j(1)$ não é divisível por p . Como $|O_g| = p^r$, isso quer dizer que $\chi_j(1)$ e $|O_g|$ são primos entre si e, portanto, existem inteiros a e b tais que

$$a|O_g| + b\chi_j(1) = 1 \Rightarrow a \frac{|O_g| \cdot \chi_j(g)}{\chi_j(1)} + b\chi_j(g) = \frac{\chi_j(g)}{\chi_j(1)}.$$

Do teorema anterior, temos que o lado esquerdo (e, portanto, o lado direito) é um inteiro algébrico. Agora, lembre que $n = \chi_j(1)$ é a dimensão da j -ésima representação ρ_j e que $\chi_j(g)$ é uma soma de n raízes da unidade.

A ponte

Em outras palavras: $\chi_j(1)$ não é divisível por p . Como $|O_g| = p^r$, isso quer dizer que $\chi_j(1)$ e $|O_g|$ são primos entre si e, portanto, existem inteiros a e b tais que

$$a|O_g| + b\chi_j(1) = 1 \Rightarrow a \frac{|O_g| \cdot \chi_j(g)}{\chi_j(1)} + b\chi_j(g) = \frac{\chi_j(g)}{\chi_j(1)}.$$

Do teorema anterior, temos que o lado esquerdo (e, portanto, o lado direito) é um inteiro algébrico. Agora, lembre que $n = \chi_j(1)$ é a dimensão da j -ésima representação ρ_j e que $\chi_j(g)$ é uma soma de n raízes da unidade. Pelo lema abaixo, segue que todas essas raízes da unidade são iguais.

Lema (5.4.5 em [4])

Se $\epsilon_1, \dots, \epsilon_n$ são raízes da unidade tais que $a = \frac{1}{n}(\epsilon_1 + \dots + \epsilon_n)$ é um inteiro algébrico, então $a = \epsilon_1 = \dots = \epsilon_n$ ou $a = 0$.

Com isso, as entradas da diagonal de $[\rho_j]$ são todas iguais:

$$\rho_j(g) = \lambda \text{Id}.$$

Para concluirmos que G não é simples: tome $K = \ker(\rho_j)$, que é um subgrupo normal de G . Como ρ_j não é a representação trivial, vale que $K \neq G$.

Com isso, as entradas da diagonal de $[\rho_j]$ são todas iguais:

$$\rho_j(g) = \lambda \text{Id}.$$

Para concluirmos que G não é simples: tome $K = \ker(\rho_j)$, que é um subgrupo normal de G . Como ρ_j não é a representação trivial, vale que $K \neq G$.

- ▶ Se $K \neq \{1\}$, então G não é simples.
- ▶ Se $K = \{1\}$, então $\rho_j: G \rightarrow GL(V)$ é injetora. Como $\rho_j(g)$ é elemento central de $GL(V)$, segue que g é elemento central de G , ou seja, $1 \neq g \in Z(G)$. Assim, dado que $Z(G)$ é subgrupo normal de G e $Z(G) \neq G$ (pois $|O_g| > 1$), concluímos novamente que G não é simples.

Teorema (Burnside)

Não existem grupos simples não-abelianos de ordem $p^a q^b$, onde p e q são primos e $a, b \in \mathbb{N}$.

Teorema (Burnside)

Não existem grupos simples não-abelianos de ordem $p^a q^b$, onde p e q são primos e $a, b \in \mathbb{N}$.

Demonstração.

Suponha que exista tal grupo G . Como G não é abeliano, temos que $Z(G) \neq G$, então, por G ser simples, segue que $Z(G) = \{1\}$. Além disso, as ordens das classes de conjugação de G não podem ser potências de primo, então, com exceção da classe $\{1\}$, pq deve dividir a ordem de cada uma das classes de conjugação. Com isso, sendo $k + 1$ o número de classes de conjugação de G , existem $m_i > 0$ tal que

$$p^a q^b = |G| = 1 + \sum_{i=1}^k (pq)^{m_i} \Rightarrow pq \cdot R - p^a q^b = 1, \text{ onde } R \in \mathbb{N}.$$

Os casos em que $a = 0$ ou $b = 0$ implicam que $p^a q^b = 1$ e, para $a, b > 0$, segue que $pq \mid 1$, isto é, $p = q = 1$ (absurdos!). \square

- [1] C. W. Curtis, *Pioneers of representation theory: Frobenius, Burnside, Schur and Brauer*. American Mathematical Society, 1999.
- [2] J.-P. Serre, *Linear Representations of Finite Groups*, first. New York: Springer-Verlag, 1977.
- [3] J. Gordon e M. Liebeck, *Representations and Characters of Groups*, first. Cambridge University Press, 1993.
- [4] P. Etingof, [al.] e S. Gerovitch, *Introduction to Representation Theory*. AMS, 2011.

Obrigado!
e
Feliz Páscoa!