Groups and Representation

Wesley Quaresma Cota

Universidade Federal de Minas Gerais, Belo Horizonte.

1 Introdução

O Teorema de Burnside, nos diz que se ϕ é uma representação irredutível de grau n sobre um corpo algebricamente fechado, então o conjunto $\{g\phi \mid g \in G\}$ gera $End_F(M)$ onde M é o $FG-$módulo associado e portanto contém n^2 elementos linearmente independentes. Neste trabalho iremos apresentar algumas aplicações interessantes desse teorema.

Se G é um subgrupo de $GL(n, F)$, então a inclusão de $G \hookrightarrow GL(n, F)$ é uma representação de G sobre F. Neste caso, se a representação é irreduvível, então diremos que G é *irredutível*, caso contrário, dizemos que G é *redutível*. Além disso, definimos o expoente de um grupo G como o menor inteiro m tal que $x^m = 1 \, \forall x \in G$.

2 Aplicações

Theorem 1. *Seja G um subgrupo irredutível de $GL(n, F)$ onde F é um corpo algebricamente fechado. Suponha que o conjunto $\{tr(g) \mid g \in G\}$ possui um número finito de elementos, digamos m. Então G é finito e $|G| \leq m^{n^2}$*

Proof. Seja ρ a inclusão $G \hookrightarrow GL(n, F)$; então pelo Teorema de Burnside $\{g\rho \mid g \in G\}$ tem no máximo n^2 elementos linearmente independentes, digamos $\{g_1, ..., g_{n^2}\}$. Tome $g \in G$, denotamos por $g_{i,j}$ a entrada (i, j) da matriz $n \times n$ de g e por $t_i = Tr(g_i g)$. Logo:

$$t_i = \sum_{j,k=1}^{n} g_{i_{j,k}} g_{k,j}\,, \quad i = 1,\, 2,\, \ldots\,,\, n^2.$$

Note que o sistema consiste de n^2 variáveis $g_{k,j}$. Como $g_i' s$ são linearmente independentes, o sistema possui única solução, o que determina g completamente. Desde que t_1, ..., t_{n^2} pode ser escolhido de m^{n^2} formas, segue que $| G | \leq m^{n^2}$

$\square$

Theorem 2 (Burnside)**.** *Seja F um corpo de característica 0. Então todo subgrupo de $GL(n,F)$ de expoente finito é finito. De fato, se G tem expoente m, então contém no máximo m^{n^3} elementos.*

Proof. Como $GL(n,F) \leq GL(n,\overline{F})$, onde $\overline{F}$ é o corpo algebricamente fechado de F, podemos supor, sem perda de generalidade que F é algebricamente fechado. Provaremos o resultado por indução em n.

Se $n = 1$, então $G \leq F^*$ de expoente m. Desde que o número de soluções da equação $x^m = 1$ em F é no máximo m, a ordem de um subgrupo de F^* de expoente m é no máximo $m = m^{1^3}$.

Assuma que o resultado é verdadeiro para subgrupos de $GL(r,F)$ onde $r < n$. Então, provaremos para os subgrupos de $GL(n,F)$. Seja G um subgrupo de $GL(n,F)$ de expoente m, onde F é algebricamente fechado. Se G é irredutível, desde que $g^m = 1$, $\forall g \in G$, todo autovalor de g são raízes $m-$ésimas da unidade. Como o traço da matriz é a soma dos seus autovalores, então há m^n possíveis valores para os traços dos elementos de G. Segue do teorema anterior que G tem ordem finita e $| G | \leq (m^n)^{n^2} = m^{n^3}$.

Se G é redutível, existe um G-submódulo próprio não trivial W de V. Logo $dim\, W = s < n$ e $dim\, V/W = t < n$. Portanto, podemos considerar o homomorfirmo $\rho : G \to GL(W)$ dado pela restrição de V ao subespaço W. Desse modo, $(G)\rho$ é um subgrupo de $GL(W)$ de expoente no máximo m. O que, pela hipótese de indução, $(G)\rho$ é finito e de ordem até m^{s^3}. Seja $H_1 = Ker\, \rho = \{A \in G \mid A \cdot w = w\}$, então $H_1 \triangleleft G$ tal que, pelo Teorema do Isomorfismo, $| G : H_1 | \leq m^{s^3}$.

Desde que W é invariante pela ação de G, temos também um homorfismo $\psi : G \to GL(V/W)$ definido por $\psi(A)(v + W) = A.v + W$. Pela hipótese de indução, $(G)\psi$ tem expoente no máximo m, logo é finito de ordem no máximo m^{t^3}. Definindo $H_2 = Ker\, \psi = \{A \in G \mid A \cdot (v + W) = v + W\}$, temos que, $H_2 \triangleleft G$ e $| G : H_2 | \leq m^{t^3}$.

Tome $H = H_1 \cap H_2$; como

$$[G : H_1 \cap H_2] \leq [G : H_1]\,[G : H_2] = m^{s^3+t^3} \leq m^{(s+t)^3} = m^{n^3}.$$

Segue que G/H tem ordem no máximo m^{n^3}.

Note que H age trivialmente em W e em V/W. Então podemos considerar uma base $\{w_1, ..., w_s\}$ de W e completá-la a uma base $\{v_1, ..., v_t, w_1, ..., w_s\}$

de V. Tomando $h \in H$ temos que $(v_i + W)h = v_ih + W = v_i + W$ então $v_ih - v_i \in W$, logo $v_ih = v_i + \alpha_1 w_1 + ... + \alpha_s w_s$. Logo a matriz h nessa base é dada pela representação na seguinte forma:

$$\begin{pmatrix} 1 & 0 & \dots & 0 & \alpha_{1,t+1} & \dots & \alpha_{1,t+s} \\ 0 & 1 & \dots & 0 & \alpha_{2,t+1} & \dots & \alpha_{2,t+s} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 & \alpha_{t,t_1} & \dots & \alpha_{t,t+s} \\ 0 & 0 & \dots & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & 0 & \dots & 1 \end{pmatrix}$$

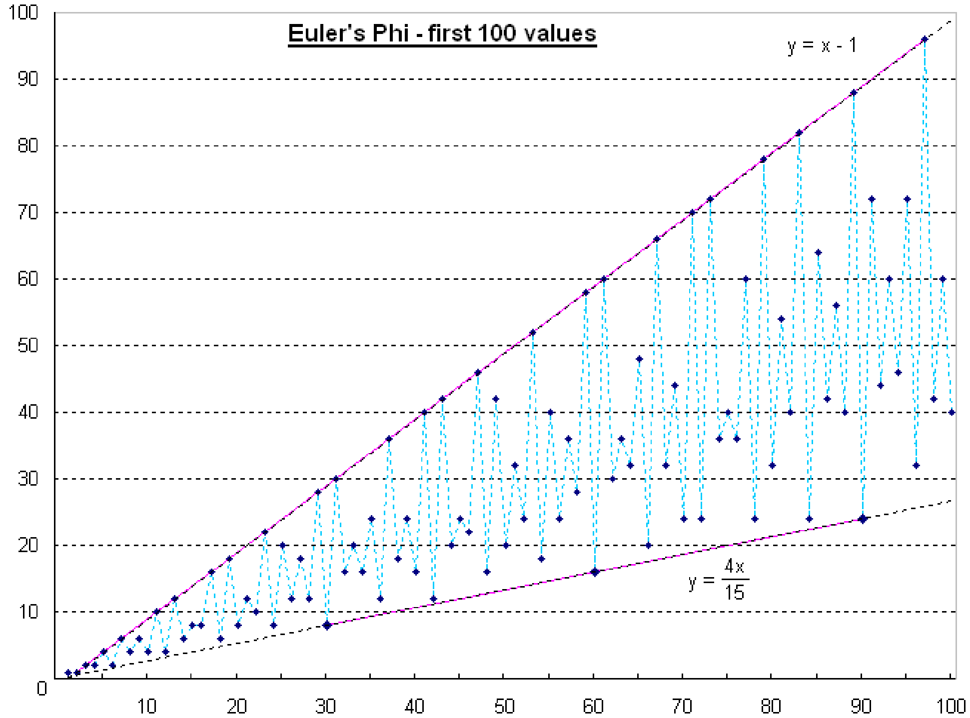
Portanto, podemos encontrar uma base de V com respeito a representação cujos elementos são unitriangulares, isto é, são matrizes triangulares superiores cujas entradas das diagonais são 1. Desde que F tem característica 0, toda matriz unitriangular diferente da identidade tem ordem infinita, o que contradiz o fato de G ter expoente finito, então H é trivial e $G/H = G$ tem ordem no máximo m^{n^3}.

□

Theorem 3 (Schur)**.** *Todo subgrupo de torção de $GL(n, \mathbb{Q})$ é finito. De fato, existe uma função $f : \mathbb{N} \to \mathbb{N}$ tal que a ordem de todo subgrupo de torção de $GL(n, \mathbb{Q})$ é menor ou igual a $f(n)$.*

Proof. É suficiente mostrar que existe uma função $\tau : \mathbb{N} \to \mathbb{N}$ que limita a ordem dos elementos (de ordem finita) de $GL(n, \mathbb{Q})$. Então, pelo Teorema de Burnside, a ordem de cada subgrupo de torção de $GL(n, \mathbb{Q})$ é no máximo $f(n)$ onde $f(n) = (\tau(n))^{n^3}$.

Vamos mostrar que se m é a ordem de um elemento de $GL(n, \mathbb{Q})$, então $\Phi(m) \leq n$ onde Φ é a função de Euler. De fato, como o conjunto $\{m \in \mathbb{N} \mid \Phi(m) \leq k\}$ é finito, isto implica que existe uma função tal que m é limitada por $\tau(n)$. O gráfico abaixo nos mostra a relação dos valores da função de Euler para os 100 primeiros números.



Usando indução em n, temos que para $n = 1$, $GL(1, \mathbb{Q}) = \mathbb{Q}^*$. Como os únicos elementos de ordem finita de $\mathbb{Q}^*$ são $\{1, -1\}$ e $\Phi(1) = \Phi(2) = 1$, o resultado segue.

Assuma que o resultado é verdadeiro para todo $GL(r, \mathbb{Q})$ com $r < n$. Considere o subgrupo $G =< x >$ de $GL(n, \mathbb{Q})$ onde x é um elemento de ordem m. Pela hipótese de indução, podemos supor que G é irredutível,caso contrário podemos considerar a ação de G num $G-$ submódulo próprio não trivial de dimensão menor que n e então G seria finito. Como G é irredutível, $\mathbb{Q}^n$ é um $\mathbb{Q}G-$módulo simples. Então $End_{\mathbb{Q}G}(\mathbb{Q}^n) = D$ é uma anel de divisão sobre $\mathbb{Q}$ e seu centro $Z(D)$ é um corpo que contém $\mathbb{Q}$ e x. De fato, se $\phi \in D$ e $v \in \mathbb{Q}^n$, então $(vx)\phi = v\phi x$.

Desde que x tem ordem m, x é raiz de um polinômio ciclotômico, portanto irredutível, $\Psi_m(t)$ de grau $\Phi(m)$ sobre $\mathbb{Q}$. Então, existe $v \in \mathbb{Q}^n$, $v \neq 0$ tal que $\{v, xv, x^2v, ..., x^{\Phi(m)-1}v\}$ são linearmente independentes, caso contrário x seria raiz de um polinômio de grau menor que $\Phi(m)$. Isto significa que $\Phi(m) \leq n$, o que conclui a prova do teorema. $\square$

3 Referências

References

[1] D. J. S. Robinson.A Course in the Theory of Groups. 1996.

[2] Lal, Ramji. Algebra 2 - Linear Algebra, Galois Theory, Representation theory, Group extensions and Schur Multiplier.