

DUAS APLICAÇÕES DA TOPOLOGIA À ÁLGEBRA LINEAR

José Carlos Santos

Departamento de Matemática

Faculdade de Ciências da Universidade do Porto

e-mail: jcsantos@fc.up.pt

Resumo: Este artigo contém duas aplicações simples (mas não imediatas) da Topologia elementar à Álgebra Linear. Estão relacionadas com a seguinte questão: quando é que duas matrizes são semelhantes?

Abstract This article presents two simple (although not straightforward) applications of elementary Topology to Linear Algebra. They are related to the following question: when are two matrices similar?

palavras-chave: Álgebra Linear; Topologia; matrizes semelhantes

keywords: Linear Algebra; Topology; similar matrices

1 Quando são duas matrizes semelhantes?

Sejam $n \in \mathbb{N} \setminus \{1\}$, \mathbb{k} um corpo e $M_n(\mathbb{k})$ o espaço vectorial formado pelas matrizes quadradas com n linhas e n colunas com entradas em \mathbb{k} . Considerem-se duas matrizes $M, N \in M_n(\mathbb{k})$ e suponha-se que se quer saber se são ou não semelhantes, ou seja, que se quer saber se existe ou não alguma matriz invertível $A \in M_n(\mathbb{k})$ tal que

$$M = A^{-1}.N.A.$$

Naturalmente, para resolver o problema basta encontrar as formas normais de Jordan de M e de N e compará-las. No entanto, isto pode ser difícil, visto que envolve a resolução de uma equação polinomial de grau n . Em contrapartida, se os determinantes ou os traços de M e de N forem diferentes, então M e N não são semelhantes. Por outras palavras, se $(M, N) \in M_n(\mathbb{k}) \times M_n(\mathbb{k})$ for um par ordenado de matrizes semelhantes, então é um zero das funções polinomiais

$$\begin{array}{ccc} M_n(\mathbb{k}) \times M_n(\mathbb{k}) & \longrightarrow & \mathbb{k} \\ (A, B) & \mapsto & \det(A) - \det(B) \end{array}$$

e

$$\begin{array}{ccc} M_n(\mathbb{k}) \times M_n(\mathbb{k}) & \longrightarrow & \mathbb{k} \\ (A, B) & \mapsto & \operatorname{tr}(A) - \operatorname{tr}(B). \end{array}$$

Poder-se-ia pensar que talvez haja um conjunto \mathcal{P} de funções polinomiais de $M_n(\mathbb{k}) \times M_n(\mathbb{k})$ em \mathbb{k} tal que (M, N) é um par de matrizes semelhantes se e só se $P(M, N) = 0$ para cada $P \in \mathcal{P}$. De facto, se \mathbb{k} for um corpo infinito, então, como veremos, não existe nenhum conjunto nessas condições. Será também explicado como obter todos os polinómios que, tal como o traço ou o determinante, tomam os mesmos valores em quaisquer duas matrizes semelhantes.

Teorema 1.1 *Seja \mathbb{k} um corpo. São então condições equivalentes:*

1. O corpo \mathbb{k} é finito.
2. Existe um conjunto \mathcal{P} de funções polinomiais de $M_n(\mathbb{k}) \times M_n(\mathbb{k})$ em \mathbb{k} tal que, para cada par de matrizes $M, N \in M_n(\mathbb{k})$, M e N são semelhantes se e só se

$$(\forall P \in \mathcal{P}) : P(M, N) = 0.$$

O facto de a primeira condição do enunciado implicar a segunda é bastante fácil de demonstrar. Isto vai ser feito somente no caso em que $n = 2$, mas o caso geral é análogo. Dado um par de matrizes $(M, N) = \left(\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}, \begin{pmatrix} a_5 & a_6 \\ a_7 & a_8 \end{pmatrix} \right)$ de $M_2(\mathbb{k}) \times M_2(\mathbb{k})$ e dado $i \in \{1, 2, \dots, 8\}$, considere-se a função polinomial

$$P_{(M,N),i} : \begin{array}{ccc} M_2(\mathbb{k}) \times M_2(\mathbb{k}) & \longrightarrow & \mathbb{k} \\ \left(\begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix}, \begin{pmatrix} x_5 & x_6 \\ x_7 & x_8 \end{pmatrix} \right) & \longmapsto & x_i - a_i. \end{array}$$

Então $\{(M, N)\}$ é o conjunto dos zeros comuns a todas as funções do tipo $P_{(M,N),i}$. Caso \mathbb{k} seja finito, então o conjunto S dos pares de matrizes semelhantes de $M_2(\mathbb{k}) \times M_2(\mathbb{k})$ também é finito. Se se definir \mathcal{P} como sendo o conjunto das funções polinomiais de $M_2(\mathbb{k}) \times M_2(\mathbb{k})$ em \mathbb{k} que se podem exprimir como um produto da forma

$$\prod_{(M,N) \in S} P_{(M,N),i(M,N)},$$

onde i é alguma função de S em $\{1, 2, \dots, 8\}$, então $(M, N) \in S$ se e só se $P(M, N) = 0$, para cada $P \in \mathcal{P}$.

É óbvio que a demonstração anterior não usou o facto de se estar a trabalhar com matrizes semelhantes. De facto, a demonstração não dependeu sequer de se estar a trabalhar com matrizes, pois o argumento empregue permite provar que, para *qualquer* parte finita F de \mathbb{k}^m ($m \in \mathbb{N}$) e para *qualquer* corpo \mathbb{k} (finito ou não), existe algum conjunto \mathcal{P} de funções polinomiais de \mathbb{k}^m em \mathbb{k} tal que $(x_1, \dots, x_m) \in F$ se e só se (x_1, \dots, x_m) for um zero de cada elemento de \mathcal{P} .

2 Primeira aplicação

2.1 A topologia de Zariski

A demonstração de que a segunda condição do enunciado do teorema 1.1 implica a primeira irá empregar Topologia, o que poderá parecer estranho, visto que se está aqui a lidar com corpos infinitos arbitrários e não apenas com o corpo dos números complexos ou com um subcorpo deste. A topologia que vai ser usada é a *topologia de Zariski* [9, §3], que pode ser definida em \mathbb{k}^m ($m \in \mathbb{N}$) do seguinte modo: uma parte S de \mathbb{k}^m é *fechada* se e só se existir algum conjunto Z de funções polinomiais de \mathbb{k}^m em \mathbb{k} tal que

$$S = \{(x_1, \dots, x_n) \in \mathbb{k}^n \mid (\forall P \in Z) : P(x_1, \dots, x_n) = 0\}.$$

Posto de outro modo, S é o conjunto dos zeros comuns a todos os elementos de Z .

Considere-se, por exemplo, a superfície S da esfera unitária de \mathbb{R}^3 e o seu «equador» E . Ambos os conjuntos são fechados relativamente à topologia de Zariski pois, se se definir $P_1(x, y, z) = x^2 + y^2 + z^2 - 1$ e $P_2(x, y, z) = z$, então S é o conjunto dos zeros de todos os elementos de $\{P_1\}$ e E é o conjunto dos zeros de todos os elementos de $\{P_1, P_2\}$.

Vai-se considerar em $M_n(\mathbb{k}) \times M_n(\mathbb{k})$ (que pode ser encarado como \mathbb{k}^{2n^2}) a topologia de Zariski, bem como em \mathbb{k} . Repare-se que, relativamente a esta topologia, os fechados de \mathbb{k} são os conjuntos de zeros comuns a conjuntos de funções polinomiais de \mathbb{k} em \mathbb{k} , que são precisamente as partes finitas de \mathbb{k} , juntamente com o próprio \mathbb{k} . Quando $m > 1$ e \mathbb{k} for infinito então, tal como nos exemplos vistos acima, há outros fechados de \mathbb{k}^m além das partes finitas de \mathbb{k}^m e do próprio \mathbb{k}^m embora, como já foi provado, seja verdade que qualquer parte finita de \mathbb{k}^m seja o conjunto dos zeros comuns a um conjunto de polinómios e, portanto, seja um fechado de \mathbb{k}^m .

Quando \mathbb{k} for um subcorpo de \mathbb{C} , a demonstração continuará a ser válida se se considerar a topologia usual em $M_n(\mathbb{k}) \times M_n(\mathbb{k})$ e em \mathbb{k} . De facto, quaisquer topologias definidas em $M_n(\mathbb{k}) \times M_n(\mathbb{k})$ e em \mathbb{k} para as quais

- qualquer função polinomial de $M_n(\mathbb{k}) \times M_n(\mathbb{k})$ em \mathbb{k} seja contínua;
- o conjunto dos não-zeros de qualquer função polinomial for denso (caso \mathbb{k} seja infinito);
- $\mathbb{k} \setminus \{0\}$ seja denso em \mathbb{k} (novamente, caso \mathbb{k} seja infinito)

será apropriada para qualquer demonstração deste artigo.

2.2 Fim da demonstração do teorema 1.1

A fim de demonstrar que a segunda condição do teorema 1.1 implica a primeira, basta ver que se \mathbb{k} for um corpo infinito e se existisse um conjunto \mathcal{P} nas condições descritas no enunciado, então o conjunto

$$\mathcal{S} = \bigcap_{P \in \mathcal{P}} P^{-1}(\{0\}),$$

onde $P^{-1}(\{0\})$ é a imagem recíproca de $\{0\}$ por P , seria fechado. Posto de outro modo, o conjunto dos pares (M, N) de matrizes semelhantes seria um fechado de $M_n(\mathbb{k}) \times M_n(\mathbb{k})$. No entanto, isto é impossível, mesmo para $n = 2$. Para se ver porquê, considere-se o conjunto

$$\mathcal{T} = \left\{ \left(\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right) \mid t \in \mathbb{k} \setminus \{0\} \right\}.$$

Então $\mathcal{T} \subset \mathcal{S}$; por outras palavras, qualquer elemento de \mathcal{T} é um par de matrizes semelhantes. Mas \mathcal{T} não é fechado; de facto, a sua aderência contém o par ordenado $(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix})$. Isto é óbvio quando \mathbb{k} é um subcorpo de \mathbb{C} e a topologia é a usual e, no caso da topologia de Zariski é uma consequência de, para cada função polinomial P de $M_n(\mathbb{k}) \times M_n(\mathbb{k})$ em \mathbb{k} tal que cada elemento de \mathcal{T} é um zero de P , cada $t \in \mathbb{k} \setminus \{0\}$ ser um zero da função polinomial

$$\begin{array}{ccc} \mathbb{k} & \longrightarrow & \mathbb{k} \\ t & \mapsto & P \left(\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right). \end{array} \quad (1)$$

Mas, visto que \mathbb{k} é um corpo infinito e que qualquer função polinomial de uma variável tem somente um número finito de zeros (a menos que seja a função nula), 0 é necessariamente um zero da função (1). Logo, o conjunto \mathcal{S} teria que conter o par ordenado $(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix})$, o que não é possível, visto que as matrizes que formam o par não são semelhantes. Um argumento análogo permite demonstrar o teorema 1.1 para cada $n > 1$.

Antes de se prosseguir, vejamos que uma demonstração mais topológica do facto de que, relativamente à topologia de Zariski, o par ordenado $(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix})$ adere a \mathcal{T} pode ser obtida pelo seguinte processo: a função

$$\begin{array}{ccc} \psi: \mathbb{k} & \longrightarrow & \left\{ \left(\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right) \mid t \in \mathbb{k} \right\} \\ t & \mapsto & \left(\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right) \end{array}$$

é um homeomorfismo e $\mathcal{T} = \psi(\mathbb{k} \setminus \{0\})$. Visto que 0 adere a $\mathbb{k} \setminus \{0\}$ em \mathbb{k} (pois $\mathbb{k} \setminus \{0\}$ é uma parte infinita de \mathbb{k}), o par ordenado $((\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}), (\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}))$ adere necessariamente a \mathcal{T} .

Corolário 2.1 *Se \mathbb{k} for um corpo infinito e se $n > 1$, então não há nenhum conjunto \mathcal{P} de funções polinomiais de $M_n(\mathbb{k})$ em \mathbb{k} tais que, para quaisquer duas matrizes $M, N \in M_n(\mathbb{k})$, as seguintes condições sejam equivalentes:*

1. as matrizes M e N são semelhantes;
2. $(\forall P \in \mathcal{P}) : P(M) = P(N)$.

De facto, se um tal conjunto \mathcal{P} existisse, então seja \mathcal{P}' o conjunto das funções polinomiais de $M_n(\mathbb{k}) \times M_n(\mathbb{k})$ em \mathbb{k} da forma

$$(M, N) \mapsto P(M) - P(N) \quad (P \in \mathcal{P}).$$

É então claro que, para quaisquer duas matrizes $M, N \in M_n(\mathbb{k})$, as condições

1. M e N são semelhantes;
2. $(\forall P \in \mathcal{P}') : P(M, N) = 0$

seriam equivalentes, o que contraria o teorema 1.1.

3 Segunda aplicação

3.1 Polinómios invariantes

Haverá outras funções polinomiais $P: M_n(\mathbb{k}) \rightarrow \mathbb{k}$, além do traço e do determinante, tais que $P(M) = P(N)$ sempre que $M, N \in M_n(\mathbb{k})$ são matrizes semelhantes? Tais polinómios vão ser designados por «polinómios invariantes» e o conjunto de todos esses polinómios vai ser representado por $\mathcal{I}(M_n(\mathbb{k}))$. Obviamente, é possível construir novos polinómios invariantes a partir do traço e do determinante (tal como $\det^3 - 3 \det \times \text{tr} + 5$, por exemplo) mas, como veremos, quando $n > 2$ há outros polinómios invariantes além daqueles que podem ser obtidos por este processo.

Convém observar que $\mathcal{I}(M_n(\mathbb{k}))$ é uma *álgebra*, ou seja, que se $P_1, P_2 \in \mathcal{I}(M_n(\mathbb{k}))$ e se $\lambda \in \mathbb{k}$, então $P_1 + P_2$, $P_1 \times P_2$ e λP_1 pertencem todos a $\mathcal{I}(M_n(\mathbb{k}))$. Em geral, quando se tem uma álgebra \mathcal{F} de funções de um conjunto X em \mathbb{k} , há duas propriedades que uma parte finita $S = \{a_1, \dots, a_n\}$ de \mathcal{F} pode ter ou não:

- o conjunto S pode gerar a álgebra \mathcal{A} , ou seja, \mathcal{A} pode ser a única subálgebra de \mathcal{A} que contém S ;
- o conjunto S pode ser *algebricamente independente*, ou seja, é possível que a única função polinomial $p: \mathcal{A}^n \rightarrow \mathcal{A}$ tal que $p(a_1, \dots, a_n) = 0$ seja a função nula.

Considerem-se os polinômios P_1, P_2, \dots, P_n de $\mathcal{P}(M_n(\mathbb{k}))$ tais que, para cada $M \in M_n(\mathbb{k})$,

$$\det(M - x\text{Id}) = (-1)^n x^n + (-1)^{n-1} P_1(M) x^{n-1} + \dots + P_n(M).$$

Obviamente, $P_n = \det$ and $P_1 = \text{tr}$. Observe-se que $\det(M - x\text{Id})$ é o *polinômio característico* de M .

Teorema 3.1 *Se \mathbb{k} for um corpo infinito, então os polinômios P_1, \dots, P_n são algebricamente independentes e geram $\mathcal{I}(M_n(\mathbb{k}))$.*

Por exemplo, se $n = 3$, então

$$P_1 \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} = a_{11}a_{22} + a_{11}a_{33} + a_{22}a_{33} - a_{12}a_{21} - a_{13}a_{31} - a_{23}a_{32}.$$

Visto que o traço, o determinante e P_1 são algebricamente independentes, isto prova que P_1 é um polinômio invariante que não pode ser obtido a partir do traço e do determinante.

Seja $D_n(\mathbb{k}) \subset M_n(\mathbb{k})$ o conjunto das matrizes diagonais e seja $\mathcal{I}(D_n(\mathbb{k}))$ o conjunto das funções polinomiais $P: D_n(\mathbb{k}) \rightarrow \mathbb{k}$ tais que, para qualquer permutação σ do conjunto $\{1, 2, \dots, n\}$ e quaisquer $a_1, a_2, \dots, a_n \in \mathbb{k}$

$$P \begin{pmatrix} a_1 & 0 & \dots & 0 \\ 0 & a_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & a_n \end{pmatrix} = P \begin{pmatrix} a_{\sigma(1)} & 0 & \dots & 0 \\ 0 & a_{\sigma(2)} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & a_{\sigma(n)} \end{pmatrix}. \quad (2)$$

A demonstração do teorema 3.1 terá por base o

Teorema 3.2 *Seja \mathbb{k} um corpo infinito. Se $P \in \mathcal{I}(M_n(\mathbb{k}))$, então a restrição de P a $D_n(\mathbb{k})$ pertence a $\mathcal{I}(D_n(\mathbb{k}))$. Além disso, a função restrição*

$$\begin{array}{ccc} r: & \mathcal{I}(M_n(\mathbb{k})) & \longrightarrow & \mathcal{I}(D_n(\mathbb{k})) \\ & P & \longmapsto & P|_{D_n(\mathbb{k})} \end{array}$$

é um isomorfismo de álgebras.

Observe-se que o espaço vectorial $D_n(\mathbb{k})$ é naturalmente isomorfo a \mathbb{k}^n e que, portanto, a álgebra $\mathcal{I}(D_n(\mathbb{k}))$ é naturalmente isomorfa à álgebra dos polinómios simétricos em n variáveis. Se p_1, p_2, \dots, p_n forem os polinómios simétricos elementares, com

$$\begin{aligned} p_1(x_1, \dots, x_n) &= \sum x_i \\ p_2(x_1, \dots, x_n) &= \sum_{i < j} x_i x_j \\ &\dots \\ p_n(x_1, \dots, x_n) &= x_1 \cdots x_n, \end{aligned}$$

então p_1, p_2, \dots, p_n são algebricamente independentes e geram $\mathcal{I}(D_n(\mathbb{k}))$ (veja-se [5, §4.1.2], [6, §2.13] ou [7, §IV.6]). É claro que se $i \in \{1, 2, \dots, n\}$, então $P_i|_{D_n(\mathbb{k})} = p_i$ e, portanto o teorema 3.1 resulta do teorema 3.2.

Antes de se demonstrar o teorema 3.2, vejamos uma ligação importante entre o polinómio característico de uma matriz M e os polinómios simétricos elementares. Se \mathbb{k} for algebricamente fechado, então a matriz M é semelhante a uma matriz triangular superior ([3, §9.8] ou [6, §3.10])

$$N = \begin{pmatrix} \lambda_1 & a_{12} & a_{13} & \cdots & a_{1n} \\ 0 & \lambda_2 & a_{23} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & & \cdots \\ 0 & 0 & 0 & \cdots & \lambda_n \end{pmatrix},$$

onde os λ_i 's são os valores próprios de M . Mas então o polinómio característico de M é igual ao polinómio característico de N , ou seja, é igual a

$$\begin{aligned} (-1)^n x^n + (-1)^{n-1} p_1(\lambda_1, \dots, \lambda_n) x^{n-1} + (-1)^{n-2} p_2(\lambda_1, \dots, \lambda_n) + \\ + \cdots + p_n(\lambda_1, \dots, \lambda_n). \end{aligned}$$

Para demonstrar o teorema 3.2, iremos começar por demonstrar que, se $P \in \mathcal{I}(M_n(\mathbb{k}))$, então $P|_{D_n(\mathbb{k})} \in \mathcal{I}(D_n(\mathbb{k}))$. Se σ for uma permutação de $\{1, 2, \dots, n\}$ e se $a_1, \dots, a_n \in \mathbb{k}$, considere-se a matriz $A \in M_n(\mathbb{k})$ tal que, se e_1, \dots, e_n for a base canónica de \mathbb{k}^n , então $A \cdot e_i = e_{\sigma(i)}$, para cada $i \in \{1, \dots, n\}$. É então claro que

$$A^{-1} \cdot \begin{pmatrix} a_1 & 0 & \cdots & 0 \\ 0 & a_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a_n \end{pmatrix} \cdot A = \begin{pmatrix} a_{\sigma(1)} & 0 & \cdots & 0 \\ 0 & a_{\sigma(2)} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a_{\sigma(n)} \end{pmatrix}$$

e, portanto, que se tem (2).

A sobrejetividade de r resulta imediatamente do facto de os polinómios simétricos elementares, que estão na imagem de r , gerarem $\mathcal{I}(D_n(\mathbb{k}))$.

Finalmente, para se demonstrar que r é injectiva, toma-se $P \in \mathcal{I}(M_n(\mathbb{k}))$ tal que $r(P) \equiv 0$. Então $P(M) = 0$ para qualquer matriz diagonalizável M . Caso o corpo \mathbb{k} seja algebricamente fechado, então $P \equiv 0$, visto que o conjunto das matrizes diagonalizáveis é denso em $M_n(\mathbb{k})$ relativamente à topologia de Zariski, como será visto mais à frente. Se \mathbb{k} não for algebricamente fechado, seja $\bar{\mathbb{k}}$ a sua aderência algébrica (ou, mais geralmente, algum corpo algebricamente fechado que contenha \mathbb{k}). Seja $GL_n(\bar{\mathbb{k}})$ o conjunto das matrizes invertíveis de $M_n(\bar{\mathbb{k}})$. A função P pode ser prolongada a uma e uma só função polinomial de $M_n(\bar{\mathbb{k}})$ em $\bar{\mathbb{k}}$; com efeito, se P se definir por

$$P \begin{pmatrix} x_{11} & x_{12} & \cdots & x_{1n} \\ x_{21} & x_{22} & \cdots & x_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ x_{n1} & x_{n2} & \cdots & x_{nn} \end{pmatrix} = \sum_{1 \leq i, j \leq n} a_{ij} x_{ij},$$

então exactamente a mesma expressão pode ser usada para definir uma função polinomial (qua será também representada por P) de $M_n(\bar{\mathbb{k}})$ em $\bar{\mathbb{k}}$. Caso $M \in M_n(\mathbb{k})$, então a função

$$R_M : GL_n(\bar{\mathbb{k}}) \longrightarrow \bar{\mathbb{k}} \\ A \longmapsto P(A^{-1} \cdot M \cdot A) - P(M)$$

é uma função racional. Se, por exemplo, $n = 2$ e $M = \begin{pmatrix} x & y \\ z & t \end{pmatrix}$, tem-se

$$R_M \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = P \left(\frac{1}{\alpha\delta - \beta\gamma} \begin{pmatrix} \delta & -\beta \\ -\gamma & \alpha \end{pmatrix} \begin{pmatrix} x & y \\ z & t \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \right) - P \begin{pmatrix} x & y \\ z & t \end{pmatrix}.$$

Esta função pode ser escrita como o quociente de duas funções polinomialis $P^*, P^{**} \in \mathcal{P}(M_n(\bar{\mathbb{k}}))$ e $R_M|_{GL_n(\mathbb{k})} \equiv 0$, o que equivale a afirmar que $P^*|_{GL_n(\mathbb{k})} \equiv 0$. Logo, $P^*|_{M_n(\mathbb{k})} \equiv 0$, pois, uma vez que \mathbb{k} é infinito e que $GL_n(\mathbb{k})$ é o conjunto dos não-zeros do determinante, $GL_n(\mathbb{k})$ é denso em $M_n(\mathbb{k})$. Mas, como P^* é um polinómio com coeficientes em \mathbb{k} , decorre daqui que $P^* \equiv 0$, e isto quer dizer que

$$(\forall A \in GL_n(\bar{\mathbb{k}})) : P(A^{-1} \cdot M \cdot A) = P(M). \quad (3)$$

Por outro lado, $P|_{D_n(\mathbb{k})} \equiv 0$ e, portanto, $P|_{D_n(\bar{\mathbb{k}})} \equiv 0$, novamente por P ser um polinómio com coeficientes em \mathbb{k} . Como já foi visto, resulta daqui, de (3) e de $\bar{\mathbb{k}}$ ser algebricamente fechado que $P \equiv 0$.

A fim de completar a demonstração do teorema 3.2, tudo o que resta então fazer é provar que o conjunto das matrizes diagonalizáveis é denso em $M_n(\mathbb{k})$ quando \mathbb{k} for algebricamente fechado.

Suponha-se que \mathbb{k} é algebricamente fechado e seja D o conjunto das matrizes de $M_n(\mathbb{k})$ cujo polinómio característico tem n raízes distintas. É claro que cada matriz de D é diagonalizável, pelo que, se se provar que D é denso em $M_n(\mathbb{k})$, ficará provado que o conjunto das matrizes diagonalizáveis é denso em $M_n(\mathbb{k})$. Se $M \in M_n(\mathbb{k})$ e se $P_M(x)$ for o seu polinómio característico, como se está a supor que \mathbb{k} é algebricamente fechado, $P_M(x)$ pode-se exprimir como um produto $\prod_{1 \leq i \leq n} (x - \lambda_i)$. Então $M \in D$ se e só se $i \neq j \implies \lambda_i \neq \lambda_j$. Considere-se o *discriminante* de P_M , o qual é, por definição, o número $\prod_{i < j} (\lambda_i - \lambda_j)^2$. Este número é diferente de 0 se e só se $M \in D$. Sabe-se [6, §4.8] que o discriminante de um polinómio mónico P pode ser escrito como um polinómio nos coeficientes de P . Por exemplo, o discriminante de um polinómio mónico de segundo grau $x^2 + ax + b$ é $a^2 - 4b$. Como, por outro lado, os coeficientes de P_M são polinómios nas entradas de M , existe uma função polinomial $\mathcal{D}: M_n(\mathbb{k}) \rightarrow \mathbb{k}$ tal que $M \in D$ se e só se $\mathcal{D}(M) \neq 0$. Logo, os elementos de D são os não-zeros de uma função polinomial de $M_n(\mathbb{k})$ em \mathbb{k} e, portanto, formam uma parte densa de $M_n(\mathbb{k})$.

3.2 Polinómio característico e polinómios invariantes

É consequência da definição dos polinómios P_i e do facto de estes gerarem $\mathcal{I}(M_n(\mathbb{k}))$ que se tem o

Corolário 3.1 *Se duas matrizes $M, N \in M_n(\mathbb{k})$ tiverem os mesmos polinómios característicos, então, para cada $P \in \mathcal{I}(M_n(\mathbb{k}))$, $P(M) = P(N)$.*

Logo, se duas matrizes M e N tiverem os mesmos polinómios característicos, não existe nenhum polinómio invariante P tal que $P(M) \neq P(N)$.

Por outro lado, o corolário 2.1 também é um corolário do teorema 3.1. Com efeito, se existisse um conjunto \mathcal{P} com as propriedades do enunciado desse corolário, então seria um subconjunto de $\mathcal{I}(M_n(\mathbb{k}))$ porque, por hipótese, a primeira condição implica a segunda. Mas se M for uma matriz triangular estritamente superior (ou seja, se for uma matriz triangular superior tal que todas as entradas da diagonal principal sejam nulas) que não seja a matriz nula 0, então o polinómio característico de M é igual a $(-1)^n x^n$, isto é, é igual ao polinómio característico da matriz nula. Resulta do corolário 3.1 que $P(M) = P(0)$, para cada polinómio invariante P e, portanto, que $P(M) = P(0)$ para cada $P \in \mathcal{P}$.

4 Outras abordagens e generalizações

Alguns leitores deste artigo poderão conjecturar que o facto de $\mathcal{I}(M_n(\mathbb{k}))$ ser gerado pelos polinómios $(P_i)_{i \in \{1, \dots, n\}}$ pode ser provado usando Teoria dos Invariantes. De facto, assim é; veja-se [5, ch. 4], por exemplo. No entanto, a demonstração do teorema 3.1 vista acima é muito mais curta do que a demonstração que se obteria pelos métodos genéricos da Teoria dos Invariantes.

Finalmente, convém saber que o teorema 3.2 é um caso particular de um resultado clássico de Teoria das Representações, nomeadamente o teorema da restrição de Chevalley (veja-se [1, §VIII.8.3] para o enunciado e para a demonstração usual quando \mathbb{k} é um corpo de característica 0). Os métodos acima empregues para demonstrar que r é injectiva e que $r(\mathcal{I}(M_n(\mathbb{k}))) \subset \mathcal{I}(D_n(\mathbb{k}))$ são essencialmente os mesmos que são usados na demonstração do teorema. No entanto, no caso geral é muito mais difícil provar que $r(\mathcal{I}(M_n(\mathbb{k}))) = \mathcal{I}(D_n(\mathbb{k}))$. A demonstração usual recorre à classificação de Cartan-Weyl das representações de dimensão finita das álgebras de Lie reductivas. Uma demonstração mais recente e muito mais curta, quando $\mathbb{k} = \mathbb{R}$, usa integração em grupos compactos (veja-se [2, p. 42]). Uma demonstração do teorema 3.2 no caso em que $\mathbb{k} = \mathbb{C}$ pode ser vista em [8, appendix B]; é essencialmente a mesma que foi vista acima no caso dos corpos algebricamente fechados.

5 Existe *algum* algoritmo?

Este artigo só elimina a possibilidade de existir *um* tipo concreto de algoritmo para determinar se duas matrizes são ou não semelhantes, mas não se deve pensar que um tal algoritmo não existe *de todo*. De facto, um tal algoritmo é descrito em [3, ch. 9] e, provavelmente, remonta ao século XIX [4].

Referências

- [1] N. Bourbaki, *Groupes et algèbres de Lie, Chapitres 7–8*, Masson, Paris, 1990.
- [2] M. Duflo e M. Vergne, Orbies codjointes et cohomologie équivariante, in *The orbit method in representation theory*, Birkhäuser, Boston, MA, 1990, 11–60.

-
- [3] H. M. Edwards, *Linear Algebra*, Birkhäuser, Boston, MA, 1995.
 - [4] H. M. Edwards, Comunicação pessoal do autor.
 - [5] R. Goodman and N. R. Wallach, *Representations and invariants of the classical groups*, Cambridge University Press, Cambridge, 1998.
 - [6] N. Jacobson, *Basic Algebra I*, W. H. Freeman and Co., New York, 1985.
 - [7] S. Lang, *Algebra*, Addison-Wesley, Reading, MA, 1993.
 - [8] Ib Madsen and J. Tornehave, *From Calculus to cohomology*, Cambridge University Press, Cambridge, 1997.
 - [9] Miles Reid, *Undergraduate Algebraic Geometry*, Cambridge University Press, Cambridge, 1988.