Universidade de Aveiro Departamento de Matemática
2005

Simão Pedro Silva Santos

Comutadores de matrizes


Universidade de Aveiro Departamento de Matemática
2005

Simão Pedro Silva Santos

Comutadores de matrizes

dissertação apresentada à Universidade de Aveiro para cumprimento dos requisitos necessários à obtenção do grau de Mestre em Matemática, realizada sob a orientação científica da Prof.ª Dr.ª Enide Cascais Silva Andrade Martins, Professora Auxiliar do Departamento de Matemática da Universidade de Aveiro

o júri

presidente

Doutor Vasile Staicu
Professor Catedrático da Universidade de Aveiro

vogais

Doutora Susana Margarida de Sousa Borges Furtado
Professora Auxiliar da Faculdade de Economia da Universidade do Porto

Doutora Enide Cascais Silva Andrade Martins
Professora Auxiliar da Universidade de Aveiro (Orientadora)

agradecimentos

À professora Enide, pela sua orientação e pela sua dedicação.

À minha família, pelo seu carinho.

À Ana, pela sua força e pelo seu amor.

Ao meu Deus.

palavras-chave Matriz, traço, determinante, comutadores aditivos, comutadores multiplicativos.

resumo

O estudo de comutadores aditivos de matrizes ao longo da década de 50 e de comutadores multiplicativos de matrizes ao longo da década de 60 estão na base deste trabalho, que pretende apresentar os resultados mais abrangentes sobre os dois tipos de comutadores.

São caracterizados os comutadores aditivos de matrizes em corpos quaisquer e apresentadas algumas propriedades particulares válidas em corpos algebricamente fechados.

São apresentadas condições para que uma matriz com entradas em GF(2), GF(3) e num corpo distinto dos anteriores, seja um comutador multiplicativo de matrizes.

Finalmente, apresentam-se condições para que uma matriz seja um comutador multiplicativo de matrizes com determinantes quaisquer prescritos.

keywords Matrix, trace, determinant, aditive commutators, multiplicative commutators

abstract The study of additive matrix commutators along the decade of 50 and multiplicative matrix commutators along the decade of 60 are the basis of this work, which intends to present the most including results on the two types of commutators.
We characterize additive matrix commutators over a general field and present some particular properties valid in algebraically closed fields.
We present conditions so that a matrix with elements in GF(2), GF(3) and in a field different from the previous is a multiplicative matrix commutator.
Finally, we present conditions so that a matrix is a multiplicative matrix commutator with any prescribed determinants.

Conteúdo

Este capítulo será utilizado para a introdução de algumas notações e alguns resultados da Teoria de Matrizes, já demonstrados e sobejamente conhecidos, que serão utilizados no desenvolvimento deste trabalho. Todos os resultados poderão ser encontrados na maioria dos livros sobre Teoria de Matrizes indicados na bibliografia, em particular em [1, 3, 5].

Seja F um corpo arbitrário. Sendo p, n inteiros positivos, se p é primo, $GF(p^n)$ denota o corpo finito com p^n elementos. Em [7, pág. 436] poderá ser encontrado o resultado que refere que tal corpo existe sempre.

Define-se *característica do corpo* F como o menor inteiro positivo n tal que $nx = 0$ para todo o $x \in F$. Se não existir n nas condições anteriores, diz-se que F possui característica zero. A característica de um corpo F será denotada por $\text{car}(F)$.

Um elemento $b \in F$ é uma *$n-$ésima raiz da identidade* se $b^n = 1$; se além disso $b^i \neq 1$, para $i \in \{1, 2, \ldots, n-1\}$, diz-se que b é uma *$n-$ésima raiz primitiva da identidade.*

Se n e m forem inteiros positivos, $F^{n\times m}$ denota o conjunto das matrizes de dimensões $n \times m$ com coeficientes em F. Matrizes linha ou coluna serão denotadas através do alfabeto latino minúsculo, sendo o alfabeto latino maiúsculo utilizado para denotar matrizes de outras quaisquer dimensões.

Se n e m forem inteiros positivos, $0_{n,m}, 0_n$ e 0 denotam, respectivamente, a matriz nula de dimensões $n \times m$, a matriz nula de dimensões $n \times n$, e a matriz nula de dimensões não especificadas, mas adequadas ao problema em questão. Denota-se por I_n a matriz identidade de dimensões $n \times n$. Representa-se por $f_i^{(n)}$ a $i-$ésima coluna da matriz I_n.

Um elemento não especificado de uma matriz será denotado por $*$.

Sendo $A \in F^{n\times m}$, a *característica* de A é denotada por $\text{car}(A)$ e a *transposta* de A é denotada por A^T.

Sendo $A \in F^{n\times n}$, o seu *determinante* é denotado por $|A|$. Se $|A| \neq 0$, a matriz A é *invertível* (ou *não singular*) e a sua matriz inversa é denotada por A^{-1}. O *traço* de A é denotado por $\text{tr}(A)$ e o seu *espectro*, conjunto dos seus *valores próprios*, será denotado por $\sigma(A)$.

Por $GL(n, F)$ entenda-se o *grupo multiplicativo das matrizes não singulares* de $F^{n\times n}$. Por $SL(n, F)$ entenda-se o *grupo multiplicativo das matrizes com determinante unitário* em $F^{n\times n}$.

Se $A \in F^{n\times m}$ e $B \in F^{p\times q}$, denota-se a *soma directa* das matrizes A e B por

$$A \oplus B = \left[\begin{array}{c|c} A & 0_{n,q} \\ \hline 0_{p,m} & B \end{array}\right] \in F^{(n+p)\times(m+q)}.$$

Denota-se por $\mathrm{diag}(a_1, a_2, \ldots, a_n)$ a *matriz diagonal* de dimensões $n \times n$ cuja entrada (i, i) é a_i.

Uma matriz $A \in F^{n\times n}$ diz-se *escalar* se e só se $A = \alpha I_n$, com $\alpha \in F$.

Uma matriz $V \in F^{n\times n}$ tal que

$$V = \begin{bmatrix} 1 & a_1 & a_1^2 & a_1^3 & \cdots & a_1^{n-1} \\ 1 & a_2 & a_2^2 & a_2^3 & \cdots & a_2^{n-1} \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ 1 & a_n & a_n^2 & a_n^3 & \cdots & a_n^{n-1} \end{bmatrix}, \quad a_1, a_2, \ldots, a_n \in F$$

chama-se *matriz de Vandermonde*. É um facto que

$$|V| = \prod_{\substack{i,\,j\,=\,1 \\ i\,>\,j}}^{n} (a_i - a_j),$$

e, portanto, V é não singular se e só se $a_1, a_2, \ldots, a_n$ forem distintos.

O determinante de uma matriz em que qualquer linha é obtida da linha anterior colocando o seu último elemento na primeira posição e deslocando os elementos seguintes para a direita é chamado *circulante*; ou seja, um circulante é

$$C = \begin{vmatrix} a_1 & a_2 & \cdots & a_n \\ a_n & a_1 & \cdots & a_{n-1} \\ \vdots & & & \vdots \\ a_2 & a_3 & \cdots & a_1 \end{vmatrix}$$

e será denotado por $C(a_1, a_2, \ldots, a_n)$.

Por vezes, e por uma questão de conveniência, define-se *circulante* como o determinante de uma matriz em que qualquer linha é obtida da anterior colocando o seu primeiro elemento na última posição e deslocando os elementos anteriores para a esquerda; neste caso, um circulante

será

$$C' = \begin{vmatrix} a_1 & a_2 & \cdots & a_n \\ a_2 & a_3 & \cdots & a_1 \\ \vdots & & & \vdots \\ a_n & a_1 & \cdots & a_{n-1} \end{vmatrix}$$

e será denotado por $C'(a_1, a_2, \ldots, a_n)$.

Observe-se que a escolha de uma das definições em detrimento da outra não é um problema adicional, uma vez que, trocando apenas linhas, obtém-se

$$C'(a_1, a_2, \ldots, a_n) = (-1)^{\frac{(n-1)(n-2)}{2}} C(a_1, a_2, \ldots, a_n).$$

O determinante que se obtém alterando o sinal das entradas de um dos lados da diagonal principal de um circulante C é chamado *circulante assimétrico* e denota-se por SC. Se se multiplicar um circulante $C'(a_1, a_2, \ldots, a_n)$ por um *alternante* Δ, que se define da seguinte forma

$$\Delta = \begin{vmatrix} 1 & 1 & \cdots & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \cdots & \cdots & \alpha_n^2 \\ \vdots & \vdots & & & \vdots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \cdots & \cdots & \alpha_n^{n-1} \end{vmatrix},$$

onde $\alpha_1, \alpha_2 \ldots, \alpha_n$ são raízes primitivas da identidade numa extensão algebricamente fechada de F, obtém-se, usando θ_r para representar

$$\theta_r = a_1 + a_2\alpha_r + a_3\alpha_r^2 + \cdots + a_n\alpha_r^{n-1}, \quad r \in \{1, 2, \ldots, n\},$$

que

$$C'(a_1, a_2, \ldots, a_n)\Delta = \Delta',$$

onde

$$\Delta' = \begin{vmatrix} \theta_1 & \theta_2 & \cdots & \theta_n \\ \alpha_1^{n-1}\theta_1 & \alpha_2^{n-1}\theta_2 & \cdots & \alpha_n^{n-1}\theta_n \\ \vdots & & & \vdots \\ \alpha_1\theta_1 & \alpha_2\theta_2 & \cdots & \alpha_n\theta_n \end{vmatrix} = \theta_1\theta_2\cdots\theta_n(-1)^{\frac{(n-1)(n-2)}{2}}\Delta.$$

Tem-se, então, que

$$C'(a_1, a_2, \ldots, a_n) = \theta_1\theta_2\cdots\theta_n(-1)^{\frac{(n-1)(n-2)}{2}}.$$

Da mesma forma, um circulante assimétrico de ordem n pode ser expresso como produto de n factores $\theta_r = a_1 + a_2\alpha_r + a_3\alpha_r^2 + \cdots + a_n\alpha_r^{n-1}$, onde, neste caso, α_r denota uma $2n-$ésima raiz da identidade.

Pode ser encontrada informação adicional sobre determinantes e circulantes em [13].

Sendo $A \in F^{n\times m}$, e $i_1, \ldots, i_p \in \{1, \ldots, n\}$ e $j_1, \ldots, j_q \in \{1, \ldots, m\}$ inteiros positivos, $A(i_1, \ldots, i_p; j_1, \ldots, j_q)$ denota a submatriz que se obtém de A retirando a A as linhas $i_1, \ldots, i_p$ e as colunas $j_1, \ldots, j_q$.

Sendo $1 \leq k \leq n$, define-se *menor de ordem* k de A como o determinante de

$$A(i_1, i_2, \ldots, i_{n-k}; j_1, j_2, \ldots, j_{n-k}) \in F^{k\times k},$$

para $i_1, \ldots, i_p \in \{1, \ldots, n\}$ e $j_1, \ldots, j_q \in \{1, \ldots, n\}$. Um *menor* será *principal* se for o determinante de uma submatriz de A do tipo $A(i_1, i_2, \ldots, i_{n-k}; i_1, i_2, \ldots, i_{n-k}) \in F^{k\times k}$.

Sejam $A, B \in F^{n\times m}$. Diz-se que A e B são *equivalentes (à esquerda)* se existir $U \in F^{n\times n}$, invertível tal que $A = UB$. Diz-se que A e B são *equivalentes (à direita)* se existir $V \in F^{m\times m}$, invertível tal que $A = BV$.

Seguem-se as definições de três *matrizes elementares*:

- $S_{i,j}$, com $i \neq j$, denota a matriz que se obtém de I_n trocando a linha i com a linha j.
- $S_{i,j}(\alpha)$, com $i \neq j$ e $\alpha \in F$, denota a matriz que se obtém de I_n substituindo a entrada (i, j) por α.
- $S_i(\alpha)$, com $\alpha \in F\backslash\{0\}$, denota a matriz que se obtém de I_n substituindo a entrada (i, i) por α.

Dada $A \in F^{n\times m}$, multiplicar A à esquerda por uma das três matrizes anteriores resulta numa matriz equivalente (à esquerda) a A e consiste, respectivamente, em realizar as seguintes operações:

- Trocar as linhas i e j de A.
- Somar à $i-$ésima linha da matriz A a $j-$ésima linha multiplicada por α.
- Multiplicar a $i-$ésima linha da matriz A por α.

Note-se que as matrizes elementares são invertíveis e as suas inversas são:

- $S_{i,j}^{-1} = S_{i,j}$
- $S_{i,j}(\alpha)^{-1} = S_{i,j}(-\alpha)$
- $S_i(\alpha)^{-1} = S_i(\alpha^{-1})$, $\alpha \in F\backslash\{0\}$.

Dada $A \in F^{n\times m}$, multiplicar A à direita por uma das três matrizes elementares anteriores em $F^{m\times m}$ resulta numa matriz equivalente (à direita) a A e consiste, respectivamente, em

- Trocar as colunas i e j de A.
- Somar à $j-$ésima coluna da matriz A a $i-$ésima coluna multiplicada por $-\alpha$.
- Multiplicar a $i-$ésima coluna da matriz A por α^{-1}.

Sejam $A, B \in F^{n\times n}$. Diz-se que A e B são *semelhantes* se existir $U \in F^{n\times n}$, não singular tal que $A = UBU^{-1}$.

A garantia que uma matriz A é semelhante a uma outra matriz B, traduz imensa informação sobre as duas matrizes. De facto, matrizes semelhantes possuem o mesmo determinante, os mesmos valores próprios, o mesmo polinómio característico, entre outras características comuns a definir posteriormente.

Observe-se que, tendo em conta que duas matrizes $A, B \in F^{n\times n}$ *comutam* se e só se $AB = BA$, tem-se que os valores próprios de AB e BA coincidem. Fazendo alguns, poucos, cálculos, tem-se as seguintes igualdades:

$$\underbrace{\left[\begin{array}{c|c} AB & 0_n \\ \hline B & 0_n \end{array}\right]}_{M_1} \underbrace{\left[\begin{array}{c|c} I_n & A \\ \hline 0_n & I_n \end{array}\right]}_{U} = \left[\begin{array}{c|c} AB & ABA \\ \hline B & BA \end{array}\right],$$

$$\left[\begin{array}{c|c} I_n & A \\ \hline 0_n & I_n \end{array}\right] \underbrace{\left[\begin{array}{c|c} 0_n & 0_n \\ \hline B & BA \end{array}\right]}_{M_2} = \left[\begin{array}{c|c} AB & ABA \\ \hline B & BA \end{array}\right].$$

Desta forma, $M_1 = UM_2U^{-1}$ e são, portanto semelhantes. Sendo semelhantes, M_1 e M_2 possuem os mesmos valores próprios e tendo em conta este facto, conclui-se que os valores próprios de AB coincidem com os de BA.

Seja $A \in F^{n\times n}$. Seguem-se três definições de *transformações de semelhança* que serão frequentemente referenciadas:

- A transformação T_i^j com $i \neq j$, aplicada a uma matriz A consiste em multiplicar A à esquerda e à direita, respectivamente, por $S_{i,j}$ e $S_{i,j}^{-1}$.
- A transformação $T_i^j(\alpha)$, com $i \neq j$, $\alpha \in F$ aplicada a uma matriz A consiste em multiplicar A à esquerda e à direita, respectivamente, por $S_{i,j}(\alpha)$ e $S_{i,j}(\alpha)^{-1}$.
- A transformação $T_i(\alpha)$, com $\alpha \in F\backslash\{0\}$, aplicada a uma matriz A consiste em multiplicar A à esquerda e à direita, respectivamente, por $S_i(\alpha)$ e $S_i(\alpha)^{-1}$.

Seja $\mathcal{D}$ um domínio de factorização única e seja $\mathcal{P}$ um conjunto completo de elementos não associados.

Sejam $A \in \mathcal{D}^{n\times m}$ e $r = \text{car}(A)$. O máximo divisor comum mónico dos determinantes das submatrizes de A de dimensões $k \times k$, com $k \in \{1, \ldots, r\}$ é chamado $k-$*ésimo divisor determinantal* e denota-se por $d_k(A)$ ou d_k quando não houver risco de confusão com outros elementos. Convenciona-se que $d_0 = 0$ e demonstra-se que $d_1|d_2|\cdots|d_r$.

Para $k \in \{1, \ldots, r\}$ sejam

$$f_k = \frac{d_k}{d_{k-1}}.$$

$f_1, f_2, \ldots, f_r$ são chamados *factores invariantes* da matriz A e demonstra-se, também, que $f_1|f_2|\cdots|f_r$.

Sejam $A \in \mathcal{D}^{n\times m}$ e $f_1, \ldots, f_r$ os factores invariantes de A. Suponha-se que, para $k \in \{1, \ldots, r\}$, se tem

$$f_k = u_k p_1^{e_{k,1}} p_2^{e_{k,2}} \cdots p_t^{e_{k,t}},$$

onde os elementos p_j são irredutíveis, distintos dois a dois e pertencem a um conjunto de elementos não associados, os elementos u_k são unidades e os elementos $e_{k,j}$ são inteiros.

Os elementos $p_j^{e_{k,j}}$ para os quais $e_{k,j} \geq 0$ designam-se *divisores elementares* de A. A um divisor elementar $p_i^{e_{k,i}}$ tal que $e_{k,i} = 1$, chama-se *divisor elementar linear*.

Demonstra-se que duas matrizes $A, B \in \mathcal{D}^{n\times m}$ são equivalentes se e só se possuem os mesmos divisores determinantais. Como consequências deste resultado, tem-se que duas matrizes

$A, B \in \mathcal{D}^{n\times m}$ são equivalentes se e só se possuem os mesmos factores invariantes e duas matrizes $A, B \in \mathcal{D}^{n\times m}$ são equivalentes se e só se possuem os mesmos divisores elementares.

Sendo $A \in \mathcal{D}^{n\times m}$, então A é equivalente a uma única matriz do tipo

$$F_S(A) = \text{diag}(f_1, f_2, \ldots, f_r) \oplus 0_{(n-r)\times(m-r)},$$

onde $r = \text{car}(A)$ e $f_1|f_2|\cdots|f_r$.

Da mesma forma, se A é equivalente a uma matriz com a forma anterior, onde $f_1|f_2|\cdots|f_r \in \mathcal{P}\backslash\{0\}$, então $r = \text{car}(A)$ e $f_1, f_2, \ldots, f_r$ são dos factores invariantes de A.

À matriz $F_S(A)$ chama-se *forma normal de Smith* de A.

Se λ for uma indeterminada, denota-se por $F[\lambda]$ o anel dos polinómios em λ com coeficientes em F. Se $p(\lambda) \in F[\lambda]$, $\text{gr}(p(\lambda))$ denota o grau de $p(\lambda)$.

Seja $A \in F^{n\times n}$. Diz-se que $f(\lambda) \in F[\lambda]$ é um *polinómio anulador* de A se $f(A) = 0$. Ao único gerador mónico de $I = \{f(\lambda) \in F[\lambda] : \quad f(A) = 0\}$ chama-se *polinómio mínimo* de A. Chama-se *polinómio característico* de A a $|\lambda I_n - A|$.

Um resultado útil para este trabalho e presente em [3] é que,

$$|\lambda I_n - A| = \lambda^n - E_1(A)\lambda^{n-1} + E_2(A)\lambda^{n-2} - \cdots \pm E_{n-1}(A)\lambda \mp E_n(A),$$

onde $E_k(A)$ representa a soma dos menores principais de ordem k de A.

Uma matriz $A \in F^{n\times n}$ diz-se *não derrogatória* se o seu polinómio mínimo coincide com o seu polinómio característico.

Sendo $A \in F^{n\times n}$, chama-se *polinómios invariantes* de A aos factores invariantes de $\lambda I_n - A \in F[\lambda]^{n\times n}$.

A matriz $\lambda I_n - A$ tem característica n e, assim, todos os polinómios invariantes de A são não nulos. Denota-se por $i(A)$ o número de polinómios invariantes de A diferentes de 1.

Demonstra-se que duas matrizes $A, B \in F^{n\times n}$ são semelhantes se e só se $\lambda I_n - A$ e $\lambda I_n - B$ são equivalentes. Assim, duas matrizes $A, B \in F^{n\times n}$ sao semelhantes se e só se tiverem os mesmos polinómios invariantes.

Tem-se, também, que o produto dos polinómios invariantes de uma matriz $A \in F^{n\times n}$ é o seu polinómio característico e demonstra-se que, se $f_1|f_2|\cdots|f_r$ são os polinómios invariantes

não constantes de A, então f_r é o seu polinómio mínimo. Conclui-se, assim, que $A \in F^{n\times n}$ é não derrogatória se e só se $i(A) = 1$.

Chama-se *divisores determinantais* de $A \in F^{n\times n}$ aos divisores determinantais de $\lambda I_n - A$. Semelhantemente, chama-se *divisores elementares* de $A \in F^{n\times n}$ aos divisores elementares de $\lambda I_n - A$. Observe-se que os divisores elementares de uma matriz A são obtidos por decomposição do seu polinómio característico em potências de polinómios não constantes, irredutíveis e primos entre si.

Observe-se, ainda, que se os valores próprios de uma matriz $A \in F^{n\times n}$ são distintos, então A é não derrogatória. De facto, se se suposer que A não é não derrogatória, então existem pelo menos dois polinómios invariantes não constantes tais que $f_i | f_j$, $i \neq j$ e $i \in \{1, 2, \ldots, i(A)\}$. Seja $\alpha \in F$ uma raiz de f_i. Então α também é raiz de f_j. Mas $|\lambda I_n - A| = f_1(\lambda) f_2(\lambda) \cdots f_r(\lambda) = (\lambda - \alpha)^2 h(\lambda)$, com $h \in F[\lambda]$. Assim, α seria um valor próprio de multiplicidade 2, o que contraria o facto de os valores próprios de A serem todos distintos.

Seguem-se alguns conceitos e resultados vulgarmente utilizados em Teoria de Matrizes e denominados por **Formas Normais para a Semelhança**.

Chama-se bloco de Jordan de dimensões $k \times k$ associado a $a \in F$ à matriz

$$J_k(a) = \begin{bmatrix} a & 1 & 0 & \cdots & 0 \\ 0 & a & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ \vdots & & \ddots & \ddots & 1 \\ 0 & \cdots & \cdots & 0 & a \end{bmatrix}.$$

Se $a = 1$, $J_k(1)$ será representado unicamente por J_k.

Observe-se que $J_k(a)$ é uma matriz não derrogatória e possui um único divisor elementar não constante: $(\lambda - a)^k$.

Sendo F um corpo algebricamente fechado e $A \in F^{n\times n}$, considere-se os divisores elementares não constantes de A

$$p_i = (\lambda - a_i)^{e_i}, \quad i \in \{1, 2, \ldots, k\},$$

com $a_1, a_2, \ldots, a_k \in F$, elementos não necessariamente distintos e $e_1, e_2, \ldots, e_k$ inteiros positivos.

Para cada $i \in \{1, 2, \ldots, k\}$, seja $J_{e_i}(a_i) \in F^{e_i \times e_i}$ o bloco de Jordan associado a a_i e correspondente a p_i.

Então, A é semelhante a

$$F_J(A) = J_{e_1}(a_1) \oplus J_{e_2}(a_2) \oplus \cdots \oplus J_{e_k}(a_k).$$

A matriz $F_J(A)$ é denominada *forma normal de Jordan* de A.

Observe-se que, se todos os divisores elementares de uma matriz A são lineares, então $F_J(A)$ é uma matriz diagonal.

Seja $f(\lambda) = \lambda^k - a_{k-1}\lambda^{k-1} - \cdots - a_0 \in F[\lambda]$, com $k \geq 1$. Chama-se *matriz companheira* de $f(\lambda)$ à matriz

$$C(f) = \begin{bmatrix} f_2^{(k)} & f_3^{(k)} & \cdots & f_k^{(k)} & a \end{bmatrix}^T \in F^{k \times k},$$

onde $a = [a_0 \ a_1 \ \cdots \ a_{k-1}]^T$.

Considere-se a matriz $\lambda I_k - C(f) \in F^{k \times k}$ e observe-se que as suas submatrizes de dimensões $j \times j$, que se obtêm escolhendo as linhas e colunas $1, 2, \ldots, j$, com $j \in \{1, 2, \ldots, k-1\}$ são do tipo

$$\begin{bmatrix} -1 & 0 & 0 & \cdots & 0 \\ \lambda & -1 & 0 & & 0 \\ 0 & \lambda & -1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & \lambda & -1 \end{bmatrix}$$

e possuem determinante ± 1. Mas, então, $i(C(f)) = 1$ e desta forma, $C(f)$ é não derrogatória.

Além disso, demonstra-se que o polinómio característico de $C(f)$ é $f(\lambda)$.

Um resultado importante, envolvendo matrizes companheiras é o seguinte: se $p(\lambda), q(\lambda) \in F[\lambda]$ são primos entre si, então $C(p) \oplus C(q))$ e $C(pq)$ são semelhantes. De facto, observe-se que

$$F_S(C(p)) = \text{diag}(1, \ldots, 1, p(\lambda)), \quad F_S(C(q)) = \text{diag}(1, \ldots, 1, q(\lambda)).$$

Desta forma, $\lambda I - (C(p) \oplus C(q))$ é equivalente a $\text{diag}(1, \ldots, 1, p(\lambda), q(\lambda))$. Mas a forma normal de Smith da submatriz $\text{diag}(p(\lambda), q(\lambda))$ é $\text{diag}(1, p(\lambda)q(\lambda))$ e, portanto, $\lambda I - (C(p) \oplus C(q))$ é equivalente a $\text{diag}(1, \ldots, 1, p(\lambda)q(\lambda))$ que é a sua forma normal de Smith.

Mas então, $C(p) \oplus C(q)$ e $C(pq)$ possuem os mesmos polinómios invariantes e são, por isso, semelhantes.

Sejam F um corpo, $A \in F^{n\times n}$ e $f_1|f_2|\cdots|f_r$ os polinómios invariantes não constantes de A. Então A é semelhante a

$$F_C(A) = C(f_1) \oplus C(f_2) \oplus \cdots \oplus C(f_r)$$

A matriz $F_C(A)$ é denominada *forma normal companheira* de A.

Observe-se, ainda, que se uma matriz A é não derrogatória, então possui um único divisor elementar não constante e, portanto, é semelhante à matriz companheira do seu polinómio característico.

Sejam, ainda, $A \in F^{n\times n}$ e $f_1, f_2, \ldots, f_n$ os seus polinómios invariantes. Sejam, ainda, $p_1, p_2, \ldots, p_s$ os factores primos mónicos e distintos que intervêm na decomposição dos polinómios invariantes. Tem-se que, para $i \in \{1, 2, \ldots, n\}$,

$$f_i(\lambda) = p_1^{e_{i,1}} p_2^{e_{i,2}} \cdots p_t^{e_{i,t}}$$

onde cada expoente é um inteiro não negativo.

Para todos os pares (i, k), $i \in \{1, 2, \ldots, n\}$, $k \in \{1, 2, \ldots, t\}$ para os quais $e_{i,k}$ é positivo, defina-se $F_I(A)$ como a soma directa das matrizes companheiras dos polinómios $p_k(\lambda)^{e_{i,k}}$:

$$F_I(A) = \bigoplus_{\substack{1 \le i \le n \\ 1 \le k \le t}} C(p_k^{e_{i,k}}).$$

É imediato que $F_S(\lambda I_n - F_I(A)) = F_S(\lambda I_n - A)$ e, sendo equivalentes, tem-se que A e $F_I(A)$ são semelhantes. $F_I(A)$ é denominada *forma normal invariante*.

Capítulo 1

Comutadores Aditivos de Matrizes

Com este capítulo pretende apresentar-se conceitos e argumentos envolvendo comutadores aditivos de matrizes e informações que permitam caracterizá-los em corpos arbitrários e em corpos algebricamente fechados.

A menos que se especifique o contrário, F representa um corpo arbitrário.

1.1 Caracterização de Comutadores Aditivos

Definição 1.1. *Sejam $A, B \in F^{n\times n}$. Chama-se comutador aditivo de matrizes à matriz $[A, B] = AB - BA$.*

Observe-se que duas matrizes $A, B \in F^{n\times n}$ comutam se e só se o seu comutador aditivo é a matriz nula.

Observe-se, ainda, que a propriedade ser um comutador aditivo de matrizes é invariante por semelhança. De facto, se $U \in F^{n\times n}$ é uma matriz não singular tal que

$$A = U^{-1}BU,$$

e, se $A = [X, Y]$ para algumas matrizes $X, Y \in F^{n\times n}$, então,

$$B = UAU^{-1} = [UXU^{-1}, UYU^{-1}].$$

Ver-se-á de seguida que tipos de matrizes podem ser escritas como comutadores aditivos.

Em 1936, K. Shoda em [15] demonstrou que se $A \in F^{n\times n}$ onde F é um corpo de característica zero, e $\mathrm{tr}(A) = 0$, então existem $X, Y \in F^{n\times n}$ tais que $A = XY - YX$. No entanto, o resultado anterior não era válido num corpo de característica p, para $p > 0$.

Em 1956, A. A. Albert e B. Muckenhoupt em [2] demonstraram um resultado mais geral do que o resultado inicialmente estabelecido, que caracteriza as matrizes que podem ser escritas como um comutador aditivo. De facto, estes autores demonstraram que se F é um corpo arbitrário e $A \in F^{n\times n}$, então $A = [X, Y]$, para algumas matrizes $X, Y \in F^{n\times n}$ se e só se $\mathrm{tr}(A) = 0$.

Pelo seu interesse, será apresentado esse resultado, não sem antes a apresentação e demonstração de um lema auxiliar.

Lema 1.1. *Seja $A = [a_{i,j}] \in F^{n\times n}$ tal que $\mathrm{tr}(A) = 0$, e $\sum_{i=1}^{n-1} a_{i,i+1} = 0, a_{i,j} = 0$ para $j \geq i+2$. Então $A = XY - YX$, onde $X, Y \in F^{n\times n}$ e X é não singular.*

Demonstração

A matriz $A \in F^{n\times n}$ possui a forma

$$\begin{bmatrix} a_{11} & a_{12} & 0 & \cdots & \cdots & 0 \\ * & a_{22} & a_{23} & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & \ddots & 0 \\ \vdots & & & \ddots & \ddots & a_{n-1,n} \\ * & \cdots & \cdots & \cdots & * & a_{nn} \end{bmatrix}.$$

Seja $K = [k_{i,j}] \in F^{n\times n}$ tal que $k_{j+1,j} = 1$ para $j \in \{1, \cdots, n-1\}$ e as restantes entradas de K são nulas, ou seja, K possui a forma,

$$K = \begin{bmatrix} 0 & \cdots & \cdots & \cdots & 0 \\ 1 & 0 & & & \vdots \\ 0 & 1 & 0 & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & 1 & 0 \end{bmatrix}.$$

Seja $Y = [y_{i,j}] \in F^{n\times n}$ tal que $y_{i,1} = 0$ para $i \in \{1, \cdots, n\}$ e $y_{i,i+3} = 0$ para $i \in \{1, \cdots, n-3\}$, ou seja, Y possui a forma

$$Y = \begin{bmatrix} 0 & y_{1,2} & y_{1,3} & 0 & y_{1,5} & \cdots & \cdots & y_{1,n} \\ 0 & y_{2,2} & y_{2,3} & y_{2,4} & 0 & y_{2,6} & \cdots & y_{2,n} \\ \vdots & & \ddots & \ddots & & \ddots & \ddots & \vdots \\ \vdots & & & & & & 0 & y_{n-4,n} \\ \vdots & & & & & \ddots & & 0 \\ \vdots & & & & & & \ddots & y_{n-2,n} \\ 0 & y_{n-1,2} & & & & & \ddots & y_{n-1,n} \\ 0 & y_{n,2} & \cdots & \cdots & \cdots & \cdots & \cdots & y_{n,n} \end{bmatrix}.$$

Desta forma, a primeira linha de KY é nula e a $i-$ésima linha de KY, $i \in \{2, \cdots, n\}$, é a $(i-1)-$ésima linha de Y, ou seja,

$$KY = \begin{bmatrix} 0 & 0 & 0 & 0 & \cdots & \cdots & \cdots & 0 \\ 0 & y_{1,2} & y_{1,3} & 0 & y_{1,5} & \cdots & \cdots & y_{1,n} \\ \vdots & y_{2,2} & y_{2,3} & y_{2,4} & \ddots & y_{2,6} & \cdots & y_{2,n} \\ \vdots & & & & & \ddots & \ddots & \vdots \\ \vdots & & & & & & \ddots & y_{n-4,n} \\ \vdots & & & & & & & 0 \\ \vdots & & & & & & & y_{n-2,n} \\ 0 & y_{n-1,2} & y_{n-1,3} & y_{n-1,4} & \cdots & \cdots & \cdots & y_{n-1,n} \end{bmatrix}.$$

Além disso, a $n-$ésima coluna de YK é nula e, para $j \in \{1, 2, \ldots, n-1\}$, a $j-$ésima coluna de YK é a $(j+1)-$ésima coluna de Y, ou seja, YK possui a forma

$$YK = \begin{bmatrix} y_{1,2} & y_{1,3} & 0 & y_{1,5} & \cdots & \cdots & y_{1,n} & 0 \\ y_{2,2} & y_{2,3} & y_{2,4} & \ddots & y_{2,6} & \cdots & y_{2,n} & 0 \\ \vdots & & & & \ddots & \ddots & \vdots & \vdots \\ \vdots & & & & & \ddots & y_{n-4,n} & 0 \\ \vdots & & & & & & 0 & 0 \\ \vdots & & & & & & y_{n-2,n} & 0 \\ \vdots & & & & & & y_{n-1,n} & 0 \\ y_{n,2} & y_{n,3} & y_{n,4} & \cdots & \cdots & \cdots & y_{n,n} & 0 \end{bmatrix}.$$

Seja $H = KY - YK = [h_{i,j}] \in F^{n\times n}$. Tem-se que

- $h_{i,1} = -y_{i,2}, \quad i \in \{1, \ldots, n\}$;
- $h_{1,2} = -y_{1,3}$;
- $h_{1,j} = -y_{1,j+1}, \quad j \in \{4, \ldots, n-1\}$;
- $h_{1,n} = 0$;
- $h_{n,n} = y_{n-1,n}$;
- $h_{i+1,n} = y_{i,n}, \quad i \in \{1, \ldots, n-4\}$;
- $h_{n-1,n} = y_{n-2,n}$;
- $h_{i,j} = y_{i-1,j} - y_{i,j+1}, \quad i \in \{2, \ldots, n\},\ j \in \{2, \ldots, \min(n-1, i+1)\}$.

Observe-se que, calculando $KY - YK$ têm-se, ainda, que $h_{i,i+2} = 0$ para $i \in \{1, \ldots, n-2\}$.

Tome-se $y_{i,j} = 0$ para $j > i+2$ e $i \in \{1, 2, \ldots, n-2\}$. Pode constatar-se, facilmente, que com esta escolha se tem $0 = h_{i,j} = a_{i,j}$ para $j \geq i+2$ e $i \in \{1, 2, \ldots, n-2\}$.

Observe-se, também, que as restantes entradas em cada coluna de H, excepto a última, contêm um termo $y_{i,j}$ que não aparece nas colunas anteriores, nem dentro da mesma coluna e cujo coeficiente é 1 ou -1.

Tome-se $y_{i,2} = -a_{i,1}$ para $i \in \{1, \ldots, n\}$ e $y_{1,3} = -a_{1,2}$. Os restantes elementos $y_{i,j}$ podem ser seleccionados por forma a que H coincida com A.

Observe-se, ainda, que depois dos elementos anteriores serem seleccionados sucessivamente, as entradas $h_{n,n}$ e $h_{n-1,n}$ possuem a forma

$$h_{n,n} = -(a_{1,1} + a_{2,2} + \cdots + a_{n-1,n-1})$$

$$h_{n-1,n} = -(a_{1,2} + a_{2,3} + \cdots + a_{n-2,n-1}).$$

Mas da condição de o traço ser nulo tem-se que

$$h_{n,n} = a_{n,n} = -(a_{1,1} + a_{2,2} + \cdots + a_{n-1,n-1})$$

e, uma vez que se pretende que

$$\sum_{i=1}^{n-1} h_{i,i+1} = \sum_{i=1}^{n} a_{i,i+1} = 0,$$

obtém-se, ainda que $h_{n-1,n} = a_{n-1,n}$. Desta forma $KY - YK = H = A$.

Uma vez que a matriz K é singular, o comutador $[K, Y]$ ainda não é o comutador pretendido.

Seja $X = K + I_n \in F^{n\times n}$. Tem-se que $A = (K + I_n)Y - Y(K + I_n) = XY - YX$ e X é uma matriz não singular. Fica assim concluída a demonstração do lema.

■

Apresenta-se de seguida o teorema devido a A. A. Albert e B. Muckenhoupt que caracteriza os comutadores aditivos de matrizes.

Teorema 1.1. *Seja $A \in F^{n\times n}$. Existem $X, Y \in F^{n\times n}$ tais que $A = XY - YX$ se e só se* $\mathrm{tr}(A) = 0$.

Demonstração

É imediato que, se $A = XY - YX$ então $\mathrm{tr}(A) = 0$.

Para iniciar a demonstração da implicação contrária, tome-se em atenção o facto, já demonstrado no início do capítulo, que uma matriz $A \in F^{n\times n}$ é um comutador aditivo de matrizes se e só se qualquer matriz semelhante a A é um comutador de matrizes.

Pode então supor-se que a matriz A coincide com uma qualquer forma normal para a semelhança. Sem perda de generalidade, suponha-se que A coincide com a sua forma normal companheira: $F_C(A) = C(f_1) \oplus C(f_2) \oplus \cdots \oplus C(f_r)$, onde $f_1|f_2|\cdots|f_r$ são os polinómios invariantes não constantes de A.

Considere-se, então, $C(f_i)$, a matriz definida na introdução. Sendo A soma directa de matrizes do tipo anterior, tem-se que A possui as entradas acima da diagonal principal iguais a 1 ou iguais a 0 e é possível, através de uma transformação de semelhança, substituir os elementos iguais a 1 pela sequência $1, -1, 1, -1, \ldots$. De facto, para alterar o sinal de um qualquer elemento $a_{i,i+1}$ não nulo, com $i \in \{1, 2, \ldots, n-1\}$, multiplique-se a $(i+1)-$ésima linha por -1 e de seguida a $(i+1)-$ésima coluna por -1. As operações anteriores correspondem a aplicar a A a transformação de semelhança $T_{i+1}(-1)$.

Através deste argumento é possível, se necessário e através de transformações de semelhança, supor que a matriz $A = [a_{i,j}]$ é tal que $a_{i,j} = 0$ para $j \geq i + 2$, $\mathrm{tr}(A) = 0$, $a_{i,i+1} \in \{-1, 0, 1\}$ e os elementos $a_{i,i+1}$ não nulos , para $i \in \{1, 2, \ldots, n-1\}$, alternam de sinal.

Se houver um número par de elementos $a_{i,i+1}$ não nulos, então $\sum_{i=1}^{n-1} a_{i,i+1} = 0$ e é válido o lema 1.1. Assim, existem matrizes $X, Y \in F^{n\times n}$ com X não singular tais que $A = XY - YX$.

Se o número de elementos $a_{i,i+1}$ não nulos for ímpar, particione-se a matriz A da forma:

$$A = \left[\begin{array}{c|c} 0 & u \\ \hline v^T & A_1 \end{array}\right], \quad u, v \in F^{1\times(n-1)},\ A_1 \in F^{(n-1)\times(n-1)}.$$

Note-se que A_1 possui todas as propriedades do lema 1.1 e, portanto, existem matrizes $X_1, Y_1 \in F^{(n-1)\times(n-1)}$ com X_1 não singular tais que $A_1 = X_1Y_1 - Y_1X_1$.

Tome-se

$$X = \left[\begin{array}{c|c} 0 & 0 \\ \hline 0 & X_1 \end{array}\right] \text{ e } Y = \left[\begin{array}{c|c} 0 & -uX_1^{-1} \\ \hline X_1^{-1}v^T & Y_1 \end{array}\right]$$

e observe-se que $XY - YX = A$. Fica, assim, concluída a prova do teorema.

■

Com o teorema anterior ficam caracterizados os comutadores aditivos de matrizes com entradas num corpo arbitrário: os comutadores aditivos de matrizes possuem traço nulo e qualquer matriz com traço nulo é um comutador aditivo de matrizes.

1.2 Comutadores Aditivos com Entradas num Corpo Algebricamente Fechado

Sejam F um corpo algebricamente fechado, $A \in F^{n\times n}$ tal que $\mathrm{tr}(A) = 0$ e suponha-se que a característica do corpo F não divide n. Nesta secção será demonstrado que é possível escrever a matriz A como um comutador aditivo de matrizes $A = XY - YX$, onde os valores próprios de X e Y são arbitrariamente prescritos sob a condição adicional de os valores próprios de X serem distintos dois a dois.

É conhecido um resultado mais antigo: C. R. Johnson em [10] demonstrou que uma matriz $A \in \mathbb{C}^{n\times n}$ com $\mathrm{tr}(A) = 0$ pode ser escrita como um comutador aditivo de matrizes $[X, Y]$ onde a lista de valores próprios de Y pode ser tomada arbitrariamente e a lista dos valores próprios de X pode, também, ser tomada arbitrariamente desde que os seus valores próprios sejam distintos dois a dois.

Definição 1.2. *Sejam $c_1, \ldots, c_n, b_1, \ldots, b_n \in F$, onde $c_i \neq c_j$, para todo $i \neq j$ e $A \in F^{n\times n}$.*

Diz-se que A goza da propriedade K se e só se

$$A = [X, Y],$$

com $X, Y \in F^{n\times n}$ tais que os valores próprios de X são $c_1, \ldots, c_n$ e, os valores próprios de Y são $b_1, \ldots, b_n$.

O lema seguinte é naturalmente verdadeiro e resulta das propriedades do traço de uma matriz.

Lema 1.2. *Seja $A \in F^{n\times n}$. Se A goza da propriedade K então* $\mathrm{tr}(A) = 0$.

Observe-se que C. R. Johnson em [10] demonstrou o recíproco do lema anterior para $F = \mathbb{C}$.

Apresenta-se, de seguida, um lema que servirá de base a alguns resultados posteriores.

Lema 1.3. *Sejam $A \in F^{n\times n}$ uma matriz não escalar e $\alpha \in F$. Então existe uma matriz $B = [b_{i,j}]$, semelhante a A, e tal que $b_{1,1} = \alpha$ e $b_{2,1} \neq 0$.*

Demonstração

Primeiramente será demonstrado que a matriz A é semelhante a uma matriz $A^{(1)}$ com pelo menos um elemento não nulo fora da diagonal principal. Se A já possui essa propriedade, tome-se $A = A^{(1)}$. Caso contrário, seja $A = \mathrm{diag}(a_{1,1}, a_{2,2}, \ldots, a_{n,n})$, com $a_{1,1}, a_{2,2}, \ldots, a_{n,n} \in F$.

Como A é não escalar, existem pelo menos dois elementos distintos na sua diagonal principal. Suponha-se que são $a_{i,i}$ e $a_{j,j}$. Aplique-se à matriz A a transformação linear $T_j^i(1)$. Obtém-se, assim, uma matriz $A^{(1)} = [a_{i,j}^{(1)}]$, semelhante a A, e cuja entrada (j, i) é $a_{i,i} - a_{j,j} \neq 0$.

Em qualquer dos casos, é possível encontrar uma matriz $A^{(1)} = [a_{i,j}^{(1)}]$ semelhante a A com uma entrada não nula, fora da diagonal principal. Suponha-se que é a entrada $a_{j,i}^{(1)}$.

De seguida, faça-se uma permutação nas linhas da matriz $A^{(1)}$ e a mesma permutação nas suas colunas (para que a transformação seja de semelhança) por forma a trazer o elemento da entrada (j, i) à posição $(2, 1)$. Obtém-se, assim, uma matriz $A^{(2)} = [a_{i,j}^{(2)}]$ semelhante a A e tal que a entrada $(2, 1)$ é não nula.

Para finalizar a demonstração é necessário que a matriz possua a entrada na posição $(1,1)$ igual a α. Dependendo da matriz $A^{(2)}$ haverá dois processos diferentes:

Se $a_{1,1}^{(2)} = 0$, faça-se a transformação $T_1^2((a_{2,1}^{(2)})^{-1}\alpha)$ em $A^{(2)}$.

Se $a_{1,1}^{(2)} \neq 0$, faça-se a transformação $T_1^2((a_{2,1}^{(2)})^{-1}(\alpha - a_{1,1}^{(1)}))$ em $A^{(2)}$.

Em qualquer dos casos, como a relação de semelhança é transitiva, após as transformações de semelhança, obtém-se uma matriz $B = [b_{i,j}]$, semelhante a A, e tal que $b_{1,1} = \alpha$ e $b_{2,1} \neq 0$.

Conclui-se, assim, a demonstração do lema.

■

Serão de seguida apresentados um teorema e um lema que serão utilizados para a demonstração do teorema que estenderá o resultado de C. R. Johnson a qualquer corpo algebricamente fechado.

O seguinte teorema, devido a P. M. Gibson, é válido num corpo algebricamente fechado e foi publicado em [9].

Teorema 1.2. *Seja $A \in F^{n\times n}$ uma matriz não escalar. Então existe uma matriz $B = [b_{i,j}] \in F^{n\times n}$ semelhante a A tal que $b_{i,i} = 0$, para $i \in \{1,\ldots,n-1\}$.*

Demonstração

Note-se que, se a matriz A é semelhante à matriz companheira do seu polinómio característico, então o resultado verifica-se imediatamente.

Suponha-se que $n = 2$. Como A é não escalar, então A é não derrogatória. Assim, A é semelhante à matriz companheira do seu polinómio característico e o resultado é claramente verdadeiro.

Suponha-se que $n = 3$ e que A é não escalar e não é semelhante à matriz companheira do seu polinómio característico. Então, A é semelhante à soma directa de uma matriz não derrogatória e uma outra matriz de dimensões 1×1. Sejam $f_1(\lambda) = 1,\ f_2(\lambda) = \lambda - c,\ f_3(\lambda) = \lambda^2 - b\lambda - a$ os polinómios invariantes de A, onde o polinómio $\lambda - c$ divide o polinómio $\lambda^2 - b\lambda - a$. Assim, A é semelhante à sua forma normal companheira:

$$F_C(A) = \begin{bmatrix} c & 0 & 0 \\ 0 & 0 & 1 \\ 0 & a & b \end{bmatrix},$$

que, quando se lhe aplicam as transformações de semelhança T_1^2 e T_2^3, é semelhante a

$$C_1 = \begin{bmatrix} 0 & 1 & 0 \\ a & b & 0 \\ 0 & 0 & c \end{bmatrix}.$$

Se $b = c = 0$ então o resultado é imediatamente verificado.

Se $b = c \neq 0$ então, atendendo à divisibilidade dos polinómios invariantes, ter-se-á $a = 0$ e poderá verificar-se que aplicando sucessivamente a C_1 as transformações de semelhança $T_1(-b), T_3^1(1)$ e $T_2^3(1)$, C_1 é semelhante a

$$C_2 = \begin{bmatrix} 0 & -b & b \\ -b & 0 & b \\ -b & -b & 2b \end{bmatrix},$$

e o resultado verifica-se novamente.

Se $b \neq c$, considere-se a matriz C_1, semelhante a A, e tome-se a submatriz de C_1,

$$D = \begin{bmatrix} b & 0 \\ 0 & c \end{bmatrix}.$$

Note-se que $D \in F^{2\times 2}$ é não escalar e, portanto, é não derrogatória. Assim, existe $P \in GL(2, F)$ tal que

$$PDP^{-1} = \begin{bmatrix} 0 & 1 \\ w & z \end{bmatrix}, \quad w, z \in F.$$

Escolhendo

$$X = \left[\begin{array}{c|c} 1 & 0 \\ \hline 0 & P \end{array}\right] \in GL(3, F), \quad \text{tem-se que} \quad XC_1X^{-1} = \left[\begin{array}{c|cc} 0 & 1 & 0 \\ \hline * & 0 & 1 \\ * & w & z \end{array}\right].$$

Assim, o teorema verifica-se para $n = 3$.

Para $n > 3$ a prova será feita por indução. Suponha-se que o teorema é válido para matrizes em $F^{(n-1)\times(n-1)}$.

Seja $A \in F^{n\times n}$ uma matriz não escalar. Como A é não escalar, pelo lema 1.3, A é semelhante a uma matriz com um elemento não nulo na posição $(1, 2)$. Suponha-se, então, que a matriz $A(n|n)$ é não escalar.

Pela hipótese de indução existe uma matriz não singular $P \in F^{(n-1)\times(n-1)}$ tal que

$$(P \oplus [1])A(P \oplus [1])^{-1} = C = [c_{i,j}] \in F^{n\times n},$$

onde $c_{i,i} = 0$, para $i \in \{1, 2, \ldots, n-2\}$.

Se $c_{n-1,n-1} = 0$, então o resultado está provado.

Se $c_{n-1,n-1} \neq 0$, então a matriz $C(1|1) \in F^{(n-1)\times(n-1)}$ é não escalar e aplicando a hipótese de indução a $C(1|1)$, existe uma matriz não singular $Q \in F^{(n-1)\times(n-1)}$ tal que $QC(1|1)Q^{-1} = [d_{i,j}]$ e $d_{i,i} = 0$, para $i \in \{1, 2, \ldots, n-2\}$.

Assim,

$$([1] \oplus Q)C([1] \oplus Q)^{-1} = B = [b_{i,j}] \in F^{n\times n},$$

onde $b_{i,i} = 0$, para todo $i \in \{1, \ldots, n-1\}$.

Como A é semelhante a C, fica assim, concluída a demonstração do teorema.

■

O seguinte resultado é devido a S. Friedland em [8] e a demonstração, pela sua complexidade e porque se encontra à margem do âmbito deste trabalho, não será incluída. O resultado será utilizado na demonstração do próximo teorema.

Lema 1.4. *Seja. $A = [a_{i,j}] \in F^{n\times n}$, onde F é um corpo algebricamente fechado. Sejam, ainda, $\alpha_1, \ldots, \alpha_n$ elementos prescritos. Então os elementos $a_{i,i}, i \in \{1, \ldots, n\}$ podem ser escolhidos de tal forma que $\sigma(A) = \{\alpha_1, \ldots, \alpha_n\}$.*

Segue-se, então, a extensão a um qualquer corpo algebricamente fechado do resultado de C. R. Johnson em [10].

Teorema 1.3. *Seja F um corpo algebricamente fechado e suponha-se que a característica de F não divide n. Sejam $A \in F^{n\times n}$ tal que $\mathrm{tr}(A) = 0$ e $b_1, b_2, \ldots, b_n, c_1, c_2, \ldots, c_n \in F$, onde $c_i \neq c_j$ para todo o $i \neq j$. Sob estas condições. A goza da propriedade K.*

Demonstração

Se $A = 0$, o resultado é trivial. De facto, escolha-se $Y = \text{diag}(b_1, \ldots, b_n)$ e $X = \text{diag}(c_1, \ldots, c_n)$ e ter-se-é o resultado pretendido.

Suponha-se que $A \neq 0$ e seja $p = \text{car}(F)$. Como $\text{tr}(A) = 0$ e p não divide n tem-se que A é não escalar. De facto, se A fosse escalar, $A = \alpha I_n$ com $\alpha \neq 0$ e $\text{tr}(A) = n\alpha = 0$, então, porque $p \nmid n$, $n = xp + r$ com $r \in \{1, \ldots, p-1\}$ e $x \in F$. Mas, $xp = 0$ porque $p = \text{car}(F)$ e, portanto, $n = r$ e $r\alpha = 0$, que contraria a hipótese de $p = \text{car}(F)$. Tem-se, então, que A é não escalar.

Pelo teorema 1.2 e uma vez que $\text{tr}(A) = 0$, existe uma matriz não singular $P \in F^{n\times n}$ tal que

$$PAP^{-1} = B = [b_{i,j}] \in F^{n\times n},$$

onde $b_{i,i} = 0$, para $i \in \{1, \ldots, n-1\}$. Observe-se que, como $\text{tr}(A) = 0$, então $b_{n,n} = 0$.

Sejam $b_1, \ldots, b_n, c_1, \ldots, c_n \in F$ tais que $c_i \neq c_j$, $i \neq j$, $i, j \in \{1, \ldots, n\}$. Definam-se

$$U = \text{diag}(c_1, \ldots, c_n) \in F^{n\times n}$$

e $V = [v_{i,j}] \in F^{n\times n}$ tal que

$$v_{i,j} = \frac{b_{i,j}}{(c_i - c_j)}, i \neq j, i, j \in \{1, \ldots, n\}.$$

As entradas $v_{1,1}, v_{2,2}, \ldots, v_{n,n}$ são escolhidos por forma a que V tenha valores próprios $b_1, \ldots, b_n$. Observe-se que essa escolha é possível pelo lema 1.4.

Sejam $X = P^{-1}UP$, $Y = P^{-1}VP$.

Tem-se, então, que

$$A = XY - YX,$$

onde os valores próprios de X e Y são $c_1, \ldots, c_n$ e $b_1, \ldots, b_n$, respectivamente.

Assim, A tem a propriedade K e fica concluída a demonstração do teorema.

■

Vale a pena referir que a condição de os valores próprios de X serem distintos dois a dois não pode ser, em geral, dispensada.

De facto, suponha-se que $n = 2$ e $A = \begin{bmatrix} 0 & \beta \\ 0 & 0 \end{bmatrix}$ com $\beta \neq 0$. Então, $\text{tr}(A) = 0$, mas não existem matrizes $X, Y \in \mathbb{C}^{2\times 2}$ tais que $\sigma(X) = \{\alpha, \alpha\}$, $\sigma(Y) = \{\beta, \beta\}$ e $A = XY - YX$.

Note-se que se existirem matrizes

$$X = \begin{bmatrix} \alpha & x_1 \\ 0 & \alpha \end{bmatrix}, \quad Y = \begin{bmatrix} \beta & y_1 \\ 0 & \beta \end{bmatrix} \quad \text{com} \quad x_1, y_1 \in \mathbb{C}$$

e tais que $A = XY - YX$, então $\beta = 0$, o que é absurdo.

A condição de o corpo F ser algebricamente fechado também não pode ser removida do teorema anterior: suponha-se que $A \in F^{2\times 2}$ e que A não possui valores próprios em F. Seja $Y \in F^{2\times 2}$ tal que Y tem os dois valores próprios iguais a $a \in F$. Existem duas possibilidades: ou Y é uma matriz escalar ou então Y é não derrogatória. Em qualquer dos casos, Y é semelhante a Y', onde

$$Y' = \begin{bmatrix} a & b \\ 0 & a \end{bmatrix} \quad a, b \in F.$$

Sem perda de generalidade suponha-se que $Y' = Y$.

Seja $X = \begin{bmatrix} x_1 & x_2 \\ x_3 & x_4 \end{bmatrix} \in F^{2\times 2}$. Tem-se que

$$XY - YX = \begin{bmatrix} -x_3 b & x_1 b - b x_4 \\ 0 & x_3 b \end{bmatrix}$$

e, portanto, $XY - YX$ possui os dois valores próprios em F. Assim A não goza da propriedade K.

Conclui-se, então, que a condição de o corpo F ser algebricamente fechado não pode ser removida do teorema anterior.

Apresenta-se de seguida o teorema que caracteriza as matrizes com a propriedade K em corpos algebricamente fechados.

Teorema 1.4. *Seja F um corpo algebricamente fechado e $A \in F^{n\times n}$ tal que* $\mathrm{tr}(A) = 0$. *Então A goza da propriedade K se e só se $A \neq \alpha I_n$ com $\alpha \in F\backslash\{0\}$.*

Demonstração

Suponha-se que $\mathrm{tr}(A) = 0$ e que $A \neq \alpha I_n$ com $\alpha \in F\backslash\{0\}$. Nestas circunstâncias, basta seguir a demonstração do teorema 1.3 e alcança-se o resultado pretendido.

Suponha-se, agora, que $\mathrm{tr}(A) = 0$, que A possui a propriedade K e que $A = \alpha I_n$ com $\alpha \in F\backslash\{0\}$. Ver-se-á de seguida que esta situação resulta num absurdo.

Se A possui a propriedade K então $A = XY - YX$ com $X, Y \in F^{n\times n}$ e X possui n valores próprios distintos.

Como os valores próprios de X são distintos dois a dois, a sua forma normal de Jordan é uma matriz diagonal $F_J(X)$. Assim, existe $P \in F^{n\times n}$ não singular tal que $PXP^{-1} = F_J(X)$. Tem-se, então, que A é semelhante a $PAP^{-1} = [PXP^{-1}, PYP^{-1}] = [F_J(X), Y']$ com $Y' = PYP^{-1}$.

Calculando $F_J(X)Y' - Y'F_J(X)$, observa-se que $F_J(X)Y' - Y'F_J(X) = A$ possui todas as suas entradas da diagonal principal iguais a zero. Esta situação contraria o facto de A ser matriz escalar não nula. Portanto, se $\mathrm{tr}(A) = 0$ e A possui a propriedade K, então $A \neq \alpha I_n$ com $\alpha \in F\backslash\{0\}$.

Conclui-se, assim, a demonstração do teorema.

■

Finaliza-se desta forma, o estudo de comutadores aditivos de matrizes com entradas num corpo algebricamente fechado.

Capítulo 2

Comutadores Multiplicativos de Matrizes

Seja G um grupo. Um elemento da forma

$$aba^{-1}b^{-1}, \quad \text{para alguns} \quad a, b \in G$$

é chamado *comutador multiplicativo* em G.

De acordo com [7], existe um subgrupo de G, C, formado por todos os comutadores multiplicativos em G.

Demonstra-se que para o grupo $SL(n, F)$, C coincide com $SL(n, F)$ excepto para os casos em que $n = 2$ e, ou $F = GF(2)$, ou $F = GF(3)$. Para o grupo $GL(2, GF(3))$, demonstra-se que $SL(2, GF(3))$ é o subgrupo de $GL(2, GF(3))$ que contém todos o comutadores multiplicativos deste grupo.

O seguinte problema foi colocado por diversos autores e será uma das bases deste capítulo.

Se $x \in C$, onde C é o subgrupo formado por comutadores em G, quantos comutadores são necessários para escrever x como um produto de comutadores em G.

O objectivo deste capítulo é resolver este problema para os grupos $SL(n, F)$ e $GL(n, F)$.

Demonstrar-se-á que se $A \in SL(n, F)$ e o corpo F possui pelo menos 4 elementos, então A é um comutador multiplicativo em $SL(n, F)$. No entanto, os argumentos utilizados para a demonstração do resultado anterior não são válidos quando o número de elementos de F é 2 ou 3.

Para esse casos particulares, será demonstrado que se $n > 2$ e $A \in SL(n, GF(2))$ então, A é um comutador multiplicativo em $SL(n, GF(2))$. Da mesma forma, será demonstrado que se $n > 2$ e $A \in SL(n, GF(3))$, então A é um comutador multiplicativo em $SL(n, GF(3))$.

Todo este capítulo tem por base o trabalho desenvolvido por R. C. Thompson.

Definição 2.1. *Sejam $X, Y \in GL(n, F)$. Chama-se comutador multiplicativo de matrizes à matriz $XYX^{-1}Y^{-1}$ e denota-se por (X, Y).*

Observe-se que, tal como para os comutadores aditivos de matrizes, a propriedade ser um comutador multiplicativo de matrizes é invariante por semelhança. De facto, se $A = (X, Y)$ para algumas matrizes não singulares $X, Y \in F^{n\times n}$ e, se $U \in F^{n\times n}$ é uma matriz não singular tal que

$$A = U^{-1}BU,$$

então,

$$B = UAU^{-1} = (UXU^{-1}, UYU^{-1}).$$

Observe-se, ainda, que, se $X, Y \in F^{n\times n}$ forem não singulares, então X e Y comutam se e só se o seu comutador multiplicativo é a matriz identidade.

2.1 Comutadores Multiplicativos com Entradas em $F \neq GF(2), GF(3)$

Nesta secção apresentam-se resultados que revelam sob que condições uma matriz $A \in SL(n, F)$ pode ser escrita como um comutador $XYX^{-1}Y^{-1}$ de matrizes em $SL(n, F)$ ou $GL(n, F)$, quando $F \neq GF(2)$ e $F \neq GF(3)$.

Seguem-se alguns lemas que serão posteriormente utilizados nas demonstrações dos teoremas 2.1 e 2.2, resultados principais desta secção. Se nada se disser em contrário, F é um corpo arbitrário.

A seguinte matriz D será tão frequentemente utilizada que terá uma nomenclatura particular. Será chamada *matriz standard*.

Sejam, então, $d_1, d_2, \ldots, d_n, c_1, c_2, \ldots, c_r \in F$ e $r, s(1), s(2), \ldots, s(r)$ inteiros positivos que satisfazem $s(1) + s(2) + \cdots + s(r) = n - 1$.

Quando $n \geq 2$,

$$D = \begin{bmatrix} d_1 & d_2 & d_3 & \cdots & \cdots & d_n \\ & J_{s(1)}(c_1) & & & & \\ & & J_{s(2)}(c_2) & & & 0 \\ & & & \ddots & & \\ & & & & \ddots & \\ & 0 & & & & J_{s(r)}(c_r) \end{bmatrix} \in F^{n\times n}. \tag{2.1}$$

Quando $n = 1$, $D = [d_1]$.

As matrizes standard serão sempre descritas em função dos elementos anteriores.

Lema 2.1. *Seja D a matriz standard definida em (2.1). Se $n \geq 2$, e se $d_1 \neq c_i$ para $i \in \{1, 2, \ldots, r\}$ então os divisores elementares de D são*

$$\lambda - d_1, (\lambda - c_1)^{s(1)}, (\lambda - c_2)^{s(2)}, \ldots, (\lambda - c_r)^{s(r)}.$$

Se $n = 1$, o único divisor elementar de D é $\lambda - d_1$.

Demonstração

O resultado é óbvio quando $n = 1$.

Seja, agora, $n \geq 2$. Com o objectivo de transformar D numa matriz semelhante em que as entradas $(1, 2), \ldots, (1, n)$ são nulas, note-se que, para $j \in \{2, \ldots, n\}$, a aplicação da transformação de semelhança $T_1^j(u_j)$ a D corresponde a

$$S_{1,j}(u_j) D S_{1,j}(u_j)^{-1}, \quad S_{1,j}(u_j) \in SL(n, F)$$

onde cada u_j pode ser escolhido em F de forma conveniente para que a matriz resultante da transformação de semelhança possua a entrada $(1, j)$ nula.

Assim, obtém-se uma matriz semelhante a D e que coincide com D excepto na entrada d_j que é substituída por zero e na entrada d_{j+1} que é alterada, quando $j < n$.

O importante a reter é que, uma vez que $d_1 \neq c_i$ para $i \in \{1, 2, \ldots, r\}$, então o elemento $u_j \in F$, para $j \in \{1, 2, \ldots, n\}$ pode sempre ser escolhido por forma a que a entrada $(1, j)$ da matriz resultante e semelhante a D seja nula.

Seja $S = S_{1,2}(u_2) S_{1,3}(u_3) \cdots S_{1,n}(u_n) \in SL(n, F)$, onde $u_2, u_3, \ldots, u_n$ são elementos de F escolhidos convenientemente por forma a anular as entradas $(1, 2), (1, 3), \ldots, (1, n)$.

Note-se que

$$SDS^{-1} = [d_1] \oplus J_{s(1)}(c_1) \oplus \cdots \oplus J_{s(r)}(c_r).$$

Considerando a matriz $\lambda I_n - SDS^{-1}$, os divisores elementares de SDS^{-1} ficam explícitos e são de facto

$$\lambda - d_1, (\lambda - c_1)^{s(1)}, (\lambda - c_2)^{s(2)}, \ldots, (\lambda - c_r)^{s(r)}.$$

Mas, como D e SDS^{-1} são semelhantes, obtém-se que os divisores elementares de D coincidem com os de SDS^{-1}.

Conclui-se assim a demonstração do lema.

■

Lema 2.2. *Sejam $n \geq 2$ e $p(\lambda) = \lambda^n - w_n\lambda^{n-1} - \cdots - w_2\lambda - w_1 \in F[\lambda]$. Seja $L \in F^{n\times n}$ a matriz seguinte*

$$L = \begin{bmatrix} 0 & l_{1,2} & l_{1,3} & \cdots & l_{1,n} \\ \vdots & 0 & l_{2,3} & & l_{2,n} \\ \vdots & & \ddots & \ddots & \vdots \\ 0 & \cdots & \cdots & 0 & l_{n-1,n} \\ x_1 & x_2 & \cdots & x_{n-1} & x_n \end{bmatrix}$$

com $l_{i,i+1} \neq 0$ para $i \in \{1, 2, \ldots, n-1\}$.

Então existe $S \in GL(n, F)$ tal que $SLS^{-1} = C(p(\lambda))$, onde

$$\begin{aligned} &w_n = x_n; \\ &w_i = l_{i,i+1}l_{i+1,i+2}\cdots l_{n-1,n}(x_i - \textstyle\sum_{k=1}^{i-1} u_{k,i}x_k),\ u_{k,i} \in F,\ i \in \{2, 3, \cdots n-1\}; \\ &w_1 = l_{1,2}l_{2,3}\cdots l_{n-1,n}x_1. \end{aligned} \tag{2.2}$$

Demonstração

Sejam $u_{i,n-1} = -l_{n-1,n}^{-1}l_{i,n}$.

A matriz $L^{(1)} = S_{1,n-1}(u_{1,n-1})LS_{1,n-1}(u_{1,n-1})^{-1}$ é a matriz que se obtém de L adicionando à primeira linha a $(n-1)-$ésima linha multiplicada por $u_{1,n-1}$ e, de seguida, adicionando à $(n-1)-$ésima coluna a primeira coluna multiplicada por $-u_{1,n-1}$. A matriz $L^{(1)}$ que se obtém de L aplicando a transformação de semelhança $T_1^{n-1}(u_{1,n-1})$, coincide com L à excepção das entradas $(1, n)$ e $(n, n-1)$ que são, respectivamente, 0 e $x_{n-1} - u_{1,n-1}x_1$.

Aplicando sucessivamente as transformações de semelhança $T_2^{n-1}(u_{2,n-1}), \ldots, T_{n-2}^{n-1}(u_{n-2,n-1})$ a $L^{(1)}$, obtém-se uma matriz

$$L^{(n)} = S_{n-2,n-1}(u_{n-2,n-1}) \cdots \underbrace{S_{1,n-1}(u_{1,n-1}) L S_{1,n-1}(u_{1,n-1})^{-1}}_{L^{(1)}} \cdots S_{n-2,n-1}(u_{n-2,n-1})^{-1},$$

semelhante a L, que possui a mesma estrutura de L, excepto nas entradas que estão acima de $l_{n-1,n}$ que são nulas e a $(n-1)-$ésima coluna de $L^{(n)}$ é, agora, a $(n-1)-$ésima coluna de L adicionada com combinações lineares das colunas $n-2, n-1, \ldots, 1$ de L :

$$L^{(n)} = \begin{bmatrix} 0 & l_{1,2} & l_{1,3} & \cdots & \cdots & l'_{1,n-1} & 0 \\ \vdots & 0 & l_{2,3} & & & l'_{2,n-1} & 0 \\ \vdots & & \ddots & \ddots & & \vdots & \vdots \\ \vdots & & & \ddots & \ddots & l'_{n-3,n-1} & \vdots \\ \vdots & & & & \ddots & l_{n-2,n-1} & 0 \\ 0 & 0 & 0 & \cdots & \cdots & 0 & l_{n-1,n} \\ x_1 & x_2 & x_3 & \cdots & \cdots & x'_{n-1} & x_n \end{bmatrix},$$

onde

$$l'_{i,n-1} = l_{i,n-1} - u_{i+1,n-1} l_{i,i+1} - \cdots - u_{n-2,n-1} l_{i,n-2}, \quad i \in \{1, \ldots, n-3\}$$

e

$$x'_{n-1} = x_{n-1} - u_{1,n-1} x_1 - \cdots - u_{n-2,n-1} x_{n-2}.$$

Seja $S_n = S_{n-2,n-1}(u_{n-2,n-1}) \cdots S_{1,n-1}(u_{1,n-1})$.

Repetindo este processo, e aplicando as transformações de semelhança sucessivamente, é possível, para cada coluna j, com $j \in \{3, \ldots, n-1\}$, escolher elementos adequados $u_{i,j} \in F$, com $i \in \{1, \ldots, j-1\}$, tais que as entradas da matriz resultante que se encontram acima dos elementos $l_{t,t+1}$, $t \in \{2, \ldots, n-2\}$ são nulas.

Assim, existe uma matriz

$$S_3 = [S_{1,2}(u_{1,2})][S_{2,3}(u_{2,3}) S_{1,3}(u_{1,3})] \cdots \underbrace{[S_{n-4,n-3}(u_{n-4,n-3}) \cdots S_{1,n-3}(u_{1,n-3})]}_{\text{anula os elementos acima da entrada } (n-3,n-2)} \times$$

$$\times [S_{n-3,n-2}(u_{n-3,n-2}) \cdots S_{1,n-2}(u_{1,n-2})] \in SL(n, F),$$

tal que $S_3 L^{(n)} S_3^{-1} = L^{(3)}$, com

$$L^{(3)} = \begin{bmatrix} 0 & l_{1,2} & 0 & \cdots & \cdots & 0 \\ \vdots & 0 & l_{2,3} & 0 & & 0 \\ \vdots & & \ddots & \ddots & \ddots & \vdots \\ \vdots & & & \ddots & \ddots & 0 \\ 0 & 0 & 0 & \cdots & 0 & l_{n-1,n} \\ x_1 & x'_2 & x'_3 & \cdots & x'_{n-1} & x_n \end{bmatrix},$$

onde $x'_i = x_i - \sum_{k=1}^{i-1} u_{k,i} x_k$ para $i \in \{2, \ldots, n-1\}$.

Seja agora $S_1 = [s_{i,j}] \in GL(n, F)$ uma matriz diagonal tal que $s_{n,n} = 1$ e $s_{i,i} = (l_{i,i+1} \cdots l_{n-1,n})^{-1}$ para $i \in \{1, 2, \ldots, n-1\}$. Então $S_1 L^{(3)} S_1^{-1}$ é a matriz companheira referida no enunciado do lema.

Fazendo $S = S_1 S_3 S_n \in GL(n, F)$, tem-se que $SLS^{-1} = C(p(\lambda))$ com, $p(\lambda) = \lambda^n - w_n \lambda^{n-1} - \cdots - w_2 \lambda - w_1$ satisfazendo (2.2).

Fica, assim, concluída a demonstração do lema.

■

Lema 2.3. *Sejam $A = C(\lambda^n - a_n \lambda^{n-1} - \cdots - a_2 \lambda - (-1)^{n-1}|A|) \in GL(n, F)$ e $D \in GL(n, F)$ a matriz standard definida anteriormente.*

Se $n \geq 2$, seja $q(\lambda) = \lambda^n + q_n \lambda^{n-1} + \cdots + q_2 \lambda + (-1)^n |A| d_1 (c_1)^{s(1)} \cdots (c_r)^{s(r)} \in F[\lambda]$. Então, para inteiros fixos $r, s(1), \ldots, s(r)$ e elementos fixos do corpo $d_1, c_1, \ldots, c_r$ é possível escolher elementos $d_2, d_3, \ldots, d_n \in F$ por forma a que $q(\lambda)$ seja o polinómio característico e mínimo de AD (ou seja, AD é não derrogatória).

Quando $n = 1$, seja $q(\lambda) = \lambda - |A| d_1$. Então, o polinómio característico e mínimo de AD é, também, $q(\lambda)$.

Demonstração

Se $n = 1$ não existem elementos d_i a determinar pois $D = [d_1]$ com d_1 definido pelo polinómio $q(\lambda)$. Assim, o resultado é óbvio.

Se $n \geq 2$, calculando o produto AD é possível ver que AD é uma matriz com a estrutura da matriz L do lema 2.2 e tal que os elementos que estão acima da diagonal principal são $c_1, \ldots, c_1, c_2, \ldots, c_2, \ldots, c_r, \ldots, c_r$, onde cada elemento c_i aparece $s(i)$ vezes, para

$i \in \{1, 2, \ldots, r\}$, e onde

$$\begin{aligned} &x_1 = (-1)^{n-1}|A|d_1; \\ &x_i = (-1)^{n-1}|A|d_i + \text{termos independentes de } d_2, \ldots, d_n, \quad i \in \{2, \ldots, n\}. \end{aligned} \tag{2.3}$$

Através do cálculo de AD é imediato que os termos independentes de $d_2, \ldots, d_n$ são combinações lineares de $a_2, \ldots, a_n$.

Mas, pelo lema 2.2, existe uma matriz $S \in GL(n, F)$ tal que $S(AD)S^{-1} = C(p(\lambda))$ onde os coeficientes de $p(\lambda)$ são dados por (2.2). Como o polinómio característico de uma matriz companheira coincide com o seu polinómio mínimo, o lema ficará demonstrado se for possível escolher $d_2, \ldots, d_n \in F$ tais que $p(\lambda) = q(\lambda)$.

Note-se que $p(\lambda)$ e $q(\lambda)$ possuem o mesmo termo independente:

$$(-1)^n|A|d_1(c_1)^{s(1)} \cdots (c_r)^{s(r)}.$$

Tendo em conta que AD possui a mesma estrutura da matriz L, denotem-se os elementos de AD por $l_{i,j}$, $i \in \{1, 2, \ldots, n-1\}$, $j \in \{1, 2, \ldots, n\}$ e por $x_1, x_2, \ldots, x_n$ os elementos da $n-$ésima linha.

Fazendo $w_i = -q_i$ para $i \in \{2, \ldots, n\}$, obtém-se o sistema triangular seguinte

$$\begin{cases} (i = n-1) & -q_{n-1} = l_{n-1,n}(x_{n-1} - u_{1,n-1}x_1 - u_{2,n-1}x_2 \cdots - u_{n-2,n-1}x_{n-2}) \\ (i = n-2) & -q_{n-2} = l_{n-2,n}l_{n-1,n}(x_{n-2} - u_{1,n-2}x_1 - u_{2,n-2}x_2 \cdots - u_{n-3,n-2}x_{n-3}) \\ \cdots & \cdots \\ (i = 3) & -q_3 = l_{3,4}l_{4,5} \cdots l_{n-1,n}(x_3 - u_{1,3}x_1 - u_{2,3}x_2) \\ (i = 2) & -q_2 = l_{2,3}l_{3,4} \cdots l_{n-1,n}(x_2 - u_{1,2}x_1) \end{cases}$$

Note-se que, como nenhum dos factores $l_{i,i+1}$ se anula pois $|D| \neq 0$, é possível obter

$$x_2 = (l_{2,3}l_{3,4} \cdots l_{n-1,n})^{-1}(-q_2 + u_{1,2}x_1)$$

e a partir de $x_1 = (-1)^n|A|d_1(c_1)^{s(1)} \cdots (c_r)^{s(r)}$ e x_2 obter x_3 e, recursivamente, resolver o sistema em ordem a $x_2, x_3, \ldots, x_n$.

Mas então, a partir de (2.3) e uma vez que $|A| \neq 0$ pois $A \in GL(n, F)$, é possível obter $d_2, \ldots, d_n$ a partir de $x_2, \ldots, x_n$.

Com $d_2, \ldots, d_n$ determinados desta forma, tem-se que $p(\lambda) = q(\lambda)$ e o lema fica demonstrado.

■

Nas considerações que se seguem os divisores elementares de uma matriz são considerados não constantes.

O seguinte resultado é a principal base da demonstração do teorema 2.2.

Lema 2.4. *Suponha-se que $A \in GL(n, F)$ é a matriz companheira de um polinómio. Suponha-se, ainda, que $d_1 \in F$ e que são dados polinómios*

$$(\lambda - \gamma_1)^{v(1)}, (\lambda - \gamma_2)^{v(2)}, \ldots, (\lambda - \gamma_t)^{v(t)}$$

onde $v(1), v(2), \ldots, v(t)$ são inteiros não negativos tais que $v(1) + v(2) + \cdots + v(t) = n - 1$, e $|A|d_1, \gamma_1, \ldots, \gamma_t \in F\backslash\{0\}$ são distintos dois a dois e $d_1 \neq \gamma_i$ para $i \in \{1, 2, \ldots, t\}$.

Então, existe uma matriz standard $D \in GL(n, F)$ tal que

Os divisores elementares de D são

$$\lambda - d_1, (\lambda - \gamma_1)^{v(1)}, \ldots, (\lambda - \gamma_t)^{v(t)} \quad e \tag{2.4}$$

os divisores elementares de AD são

$$\lambda - |A|d_1, (\lambda - \gamma_1)^{v(1)}, \ldots, (\lambda - \gamma_t)^{v(t)}. \tag{2.5}$$

Demonstração

Quando $n = 1$, tome-se $D = [d_1]$ e note-se que $A = [|A|]$. Assim, o divisor elementar de D é $\lambda - d_1$ e o divisor elementar de $AD = [|A|d_1]$ é $\lambda - |A|d_1$. Verifica-se, assim, o resultado quando $n = 1$.

Suponha-se que $n \geq 2$. De entre a lista $v(1), \ldots, v(t)$, escolha-se $v(i_1), \ldots, v(i_r) > 0$.

Seja $D \in GL(n, F)$ uma matriz standard cujos parâmetros são o inteiro r, juntamente com os inteiros $s(1) = v(i_1), \ldots, s(r) = v(i_r)$, os elementos $d_1, c_1 = \gamma_{i_1}, \ldots, c_r = \gamma_{i_r} \in F$ e os elementos ainda indeterminados $d_2, \ldots, d_n \in F$.

Pelo lema 2.1, para qualquer escolha de elementos $d_2, \ldots, d_n$, os divisores elementares de D são dados por (2.4). Mas, pelo lema 2.3, pode escolher-se $d_2, \ldots, d_n$ tais que os polinómios característico e mínimo de AD seja

$$q(\lambda) = (\lambda - |A|d_1)(\lambda - \gamma_1)^{v(1)} \cdots (\lambda - \gamma_t)^{v(t)}.$$

Note-se que os polinómios $\lambda - |A|d_1,\ (\lambda-\gamma_1)^{v(1)}, \cdots, (\lambda-\gamma_t)^{v(t)}$ são irredutíveis sobre F e primos entre si.

Assim, analisando $q(\lambda)$, é claro que os divisores elementares de AD são

$$\lambda - |A|d_1, (\lambda-\gamma_1)^{v(1)}, \ldots, (\lambda-\gamma_t)^{v(t)}.$$

Fica, assim, demonstrado o lema.

■

O seguinte resultado está demonstrado num corpo em geral, no entanto, é particularmente útil para o estudo dos casos em que $F = GF(5)$ ou $F = GF(4)$.

Lema 2.5. *Sejam $A \in GL(n,F)$ a matriz companheira de um polinómio e $n \geq 2$.*

Sejam $d_1 \in F$ e $\lambda-\gamma_1, (\lambda-\gamma_2)^{v(2)}, \ldots, (\lambda-\gamma_t)^{v(t)}$ polinómios dados onde $v(2), \ldots, v(t)$ são inteiros não negativos tais que $v(2)+\cdots+v(t) = n-2$, e $d_1, |A|\gamma_1, \ldots, \gamma_t \in F\backslash\{0\}$ são distintos dois a dois e onde $d_1 \neq \gamma_1$.

Então, existe uma matriz standard $D \in GL(n,F)$ tal que

Os divisores elementares de D são

$$\lambda - d_1, \lambda-\gamma_1, (\lambda-\gamma_2)^{v(2)}, \ldots, (\lambda-\gamma_t)^{v(t)} \quad e \tag{2.6}$$

os divisores elementares de AD são

$$\lambda - d_1, \lambda - |A|\gamma_1, (\lambda-\gamma_2)^{v(2)}, \ldots, (\lambda-\gamma_t)^{v(t)}. \tag{2.7}$$

Demonstração

De entre a lista $v(2), \ldots, v(t)$ escolham-se os inteiros não nulos $v(i_2), \ldots, v(i_r)$. Convenciona-se que, se os elementos $v(i)$, $i \in \{2, \ldots, t\}$ são todos nulos, então $r = 1$.

Seja $D \in GL(n,F)$ uma matriz standard cujos parâmetros são os inteiros $r, s(1) = 1, s(2) = v(i_2) \ldots, s(r) = v(i_r)$ e os elementos $d_1, c_1 = \gamma_1, c_2 = \gamma_{i_2}, \ldots, c(r) = \gamma_{i_r} \in F$, juntamente com os elementos ainda indeterminados $d_2, \ldots, d_n \in F$.

Pelo lema 2.1, os divisores elementares de D são dados por (2.6). Mas, pelo lema 2.3, pode escolher-se $d_2, \ldots, d_n$ tais que o polinómio característico e mínimo de AD seja

$$q(\lambda) = (\lambda-d_1)(\lambda-|A|\gamma_1)(\lambda-\gamma_2)^{v(2)} \cdots (\lambda-\gamma_t)^{v(t)}.$$

Por análise do polinómio anterior, é claro que os divisores elementares de AD são

$$\lambda - d_1, \lambda - |A|\gamma_1, (\lambda - \gamma_2)^{v(2)}, \ldots, (\lambda - \gamma_t)^{v(t)}.$$

O lema fica, então, demonstrado.

■

Lema 2.6. *Sejam $A, B \in GL(n, F)$ tais que B é semelhante a A.*

Se A possui um divisor elementar linear, $\lambda - \alpha$, com $\alpha \in F$, então existe uma matriz $S \in GL(n, F)$ tal que $B = SAS^{-1}$ e se $s \in F\backslash\{0\}$, então $|S| = s$.

Demonstração

Suponha-se que A possui um divisor elementar do tipo $\lambda - \alpha$, $\alpha \in F$. Seja $T \in GL(n, F)$ tal que $B = TAT^{-1}$.

Tendo em conta a forma normal de Jordan de A, existe $W_1 \in GL(n, F)$ tais que

$$W_1 A W_1^{-1} = F_J(A) = \left[\begin{array}{c|c} \alpha & 0 \\ \hline 0 & A_1 \end{array}\right], \quad \text{com } A_1 \in GL(n-1, F).$$

Da igualdade $B = TAT^{-1}$ tem-se que

$$B = (TW_1^{-1})(W_1 A W_1^{-1})(W_1 T^{-1}) = Z^{-1} \left[\begin{array}{c|c} \alpha & 0 \\ \hline 0 & A_1 \end{array}\right] Z, \quad Z = W_1 T^{-1} \in GL(n, F).$$

Assim, existe $Z \in GL(n, F)$ tal que

$$ZBZ^{-1} = \left[\begin{array}{c|c} \alpha & 0 \\ \hline 0 & A_1 \end{array}\right], \quad A_1 \in GL(n-1, F).$$

Seja $s_1 = s|ZW_1^{-1}|$ e seja $S_1 = \left[\begin{array}{c|c} s_1 & 0 \\ \hline 0 & I_{n-1} \end{array}\right]$.

Então $S_1 W_1 A W_1^{-1} S_1^{-1} =$

$$\left[\begin{array}{c|c} s_1 & 0 \\ \hline 0 & I_{n-1} \end{array}\right] \left[\begin{array}{c|c} \alpha & 0 \\ \hline 0 & A_1 \end{array}\right] \left[\begin{array}{c|c} s_1^{-1} & 0 \\ \hline 0 & I_{n-1} \end{array}\right] = \left[\begin{array}{c|c} \alpha & 0 \\ \hline 0 & A_1 \end{array}\right] = ZBZ^{-1}.$$

Desta forma, $B = (Z^{-1} S_1 W_1) A (W_1^{-1} S_1^{-1} Z)$.

Considere-se S definida como $Z^{-1}S_1W_1$. O seu determinante $|Z^{-1}S_1W_1| = |Z^{-1}||S_1||W_1| = s$ e portanto, S é a matriz pretendida.

Conclui-se, assim, a demonstração do lema.

■

Seja, agora, $b \in F$ uma $n-$ésima raiz primitiva da identidade.

Tendo em conta os lemas atrás estabelecidos, será demonstrado um dos resultados mais importantes desta secção:

Teorema 2.1. *Seja $bI_n \in SL(n, F)$. Então existem matrizes $X, Y \in GL(n, F)$ tais que $bI_n = (X, Y)$.*

Além disso, existem matrizes $X, Y \in SL(n, F)$ tais que $bI_n = (X, Y)$, a menos que b seja uma $n-$ésima raiz primitiva da identidade em F e $n \equiv 2(\text{mod } 4)$.

Se b é uma $n-$ésima raiz primitiva da identidade em F e $n \equiv 2(\text{mod } 4)$, existem matrizes $X, Y \in SL(n, F)$ tais que $bI_n = (X, Y)$ se e só se a equação $w^2 + w'^2 = -1$ possui uma solução $w, w' \in F$. No caso de tal não acontecer, bI_n poderá ser escrita como produto de dois comutadores multiplicativos em $SL(n, F)$. (A condição $w^2 + w'^2 = -1$ é satisfeita sempre que F possui característica diferente de zero.)

Demonstração

A demonstração será feita em 5 passos:

Passo 1 Começar-se-á por demonstrar que bI_{mn} é um comutador em $GL(mn, F)$ para qualquer inteiro $m \geq 1$;

Passo 2 Depois, demonstrar-se-á que, quando n é ímpar, bI_{mn} é um comutador em $SL(mn, F)$ para qualquer inteiro $m \geq 1$;

Passo 3 De seguida, demonstrar-se-á que se n é par, bI_{mn} é um comutador em $SL(mn, F)$ para qualquer inteiro $m > 1$;

Passo 4 De seguida, revelar-se-á em que condições bI_n, com n par, é um comutador em $SL(n, F)$;

Passo 5 Finalmente, demonstrar-se-á que bI_n é um produto de dois comutadores em $SL(n,F)$ quando $n \equiv 2(\text{mod } 4)$ e F possui característica zero.

Passo 1: Sejam $D = \text{diag}(1, b, b^2, \ldots, b^{n-1})$ e m um inteiro positivo.

Observe-se que D e $bI_nD = bD$ possuem os mesmos divisores elementares e, portanto, são semelhantes. Em particular, $\lambda - 1$ é um divisor elementar comum a D e bD. É, assim, válido o lema 2.6 e, então, existe $S \in SL(n,F)$, com $|S| = 1$, tal que $bD = SDS^{-1}$. Assim, $bI_n = SDS^{-1}D^{-1}$. Note-se que, sendo $b \neq 0$, a matriz D é invertível.

Sejam $W = S \oplus S \oplus \cdots \oplus S, Z = D \oplus D \oplus \cdots \oplus D \in GL(mn,F)$. Tem-se que $bI_{mn} = WZW^{-1}Z^{-1}$ e é, portanto, um comutador multiplicativo de matrizes em $GL(mn,F)$, para $m \geq 1$. Conclui-se, assim, o **Passo 1**.

Note-se que, quando n é ímpar, $|D| = (b^n)^{\frac{n-1}{2}} = 1$ e, portanto, bI_{mn} é um comutador em $SL(mn,F)$, para $m \geq 1$. Conclui-se, assim, o **Passo 2**.

Observe-se que, assim como é possível $S \in SL(n,F)$ tal que $|S| = 1$, pelo mesmo lema 2.6 é possível encontrar $T \in GL(n,F)$ tal que $|T| = -1$ e $bI_n = TDT^{-1}D^{-1}$.

Passo 3: Usando as matrizes S, D, T definidas atrás e considerando $m = 2$, tem-se que

$$bI_{2n} = \left[\begin{array}{c|c} S & 0 \\ \hline 0 & S \end{array}\right] \left[\begin{array}{c|c} D & 0 \\ \hline 0 & D \end{array}\right] \left[\begin{array}{c|c} S & 0 \\ \hline 0 & S \end{array}\right]^{-1} \left[\begin{array}{c|c} D & 0 \\ \hline 0 & D \end{array}\right]^{-1} =$$

$$= \left[\begin{array}{c|c} SDS^{-1}D^{-1} & 0 \\ \hline 0 & SDS^{-1}D^{-1} \end{array}\right] = (X_2, Y_2)$$

onde $S \oplus S = X_2, D \oplus D = Y_2 \in SL(2n,F)$.

Tendo em conta que D^{-1} e $b^{-1}D^{-1}$ são semelhantes e possuem um divisor elementar linear, é também, válido o lema 2.6 e, assim, existe $V \in SL(n,F)$ tal que $b^{-1}D^{-1} = VD^{-1}V^{-1}$. Mas, então $bI_n = D^{-1}VDV^{-1}$ e, portanto, existem $U = D^{-1} \in GL(n,F)$ tal que $|U| = -1$ e $V \in SL(n,F)$ tais que $bI_n = UVU^{-1}V^{-1}$.

Desta forma,

$$bI_{3n} = \left[\begin{array}{c|c|c} S & 0 & 0 \\ \hline 0 & U & 0 \\ \hline 0 & 0 & T \end{array}\right]\left[\begin{array}{c|c|c} D & 0 & 0 \\ \hline 0 & V & 0 \\ \hline 0 & 0 & D \end{array}\right]\left[\begin{array}{c|c|c} S & 0 & 0 \\ \hline 0 & U & 0 \\ \hline 0 & 0 & T \end{array}\right]^{-1}\left[\begin{array}{c|c|c} D & 0 & 0 \\ \hline 0 & V & 0 \\ \hline 0 & 0 & D \end{array}\right]^{-1} =$$

$$\left[\begin{array}{c|c|c} SDS^{-1}D^{-1} & 0 & 0 \\ \hline 0 & UVU^{-1}V^{-1} & 0 \\ \hline 0 & 0 & TDT^{-1}D^{-1} \end{array}\right] = (X_3, Y_3)$$

onde $S \oplus U \oplus T = X_3, D \oplus V \oplus D = Y_3 \in SL(3n, F)$.

Assim, bI_{2n} e bI_{3n} são comutadores multiplicativos de matrizes em $SL(2n, F)$ e $SL(3n, F)$, respectivamente.

Observe-se que se $m > 1$, então, ou o inteiro m é par, ou o inteiro $m-3$ é par. Demonstra-se, agora, o caso mais geral, recorrendo aos dois casos particulares anteriores.

Se m é par então $m = 2k$ para algum k inteiro positivo. Assim, bI_{mn} pode ser decomposta como

$$bI_{mn} = \underbrace{bI_{2n} \oplus bI_{2n} \oplus \cdots \oplus bI_{2n}}_{k \text{ blocos}}.$$

Mas, como foi dito anteriormente, existem matrizes $X_2, Y_2 \in SL(2n, F)$ tais que $bI_{2,n} = X_2 Y_2 X_2^{-1} Y_2^{-1}$.

Sejam $W = X_2 \oplus \cdots \oplus X_2, Z = Y_2 \oplus \cdots \oplus Y_2 \in SL(mn, F)$. Então $bI_{mn} = WZW^{-1}Z^{-1}$ e é, portanto, um comutador multiplicativo de matrizes em $SL(mn, F)$, $m > 1$.

Se m é ímpar, pode decompor-se m como $m = 3 + (m-3)$. Assim,

$$bI_{mn} = bI_{3n} \oplus bI_{(m-3)n}.$$

Já foi demonstrado que bI_{3n} é um comutador multiplicativo de matrizes em $SL(3n, F)$ e, portanto, existem matrizes $X_3, Y_3 \in SL(3n, F)$ tais que $bI_{3n} = X_3 Y_3 X_3^{-1} Y_3^{-1}$. Como $m-3$ é par, tem-se que

$$bI_{(m-3)n} = \underbrace{bI_{2n} \oplus bI_{2n} \oplus \cdots \oplus bI_{2n}}_{\frac{(m-3)}{2} \text{ blocos}}.$$

À semelhança do caso em que m é par, $bI_{(m-3)n} = W_1 Z_1 W_1^{-1} Z_1^{-1}$, onde

$$W_1 = X_2 \oplus \cdots \oplus X_2, \ Z_1 = Y_2 \oplus \cdots \oplus Y_2 \in SL((m-3)n, F).$$

Sejam $W = X_3 \oplus W_1, Z = Y_3 \oplus Z_1 \in SL(mn, F)$. Então $bI_{mn} = WZW^{-1}Z^{-1}$ e é, portanto, um comutador multiplicativo de matrizes em $SL(mn, F)$, $m > 1$.

Conclui-se, assim, o **Passo 3**.

Note-se que neste passo não está contemplado o caso em que $m = 1$. Assim, de seguida, será determinado em que condições bI_n com n par é um comutador multiplicativo de matrizes em $SL(n, F)$.

Passo 4:

Suponha-se que $bI_n = BCB^{-1}C^{-1}$ onde n é par e $B, C \in SL(n, F)$ e note-se que BC e CB possuem os mesmos valores próprios.

Seja $\beta \in \widetilde{F}$ um valor próprio de BC, onde $\widetilde{F}$ é uma extensão algebricamente fechada de F. Então, β é também um valor próprio de CB e $b\beta$ é um valor próprio de $bCB = BC$. Analogamente, $b\beta$ é um valor próprio de BC e, portanto, $b^2\beta$ é um valor próprio de $bCB = BC$ e assim sucessivamente.

Tem-se, então, que $\beta, b\beta, \ldots, b^{n-1}\beta$ são valores próprios de BC. De facto, uma vez que b é uma $n-$ésima raiz primitiva da identidade, a lista anterior constitui a lista dos valores próprios de BC na sua totalidade. Observe-se, ainda, que, pelo mesmo motivo, os valores próprios são distintos dois a dois.

Como $|BC| = |B||C| = 1$, tem-se que

$$|BC| = \beta\ b\beta \cdots b^{n-1}\beta = b^{\frac{n(n-1)}{2}}\ \beta^n = 1$$

Observe-se que $b^n = 1 \Leftrightarrow (b^{\frac{n}{2}})^2 = 1 \Leftrightarrow b^{\frac{n}{2}} = 1 \vee b^{\frac{n}{2}} = -1$. Mas $b^{\frac{n}{2}} = 1$ é uma impossibilidade, pois b é uma $n-$ésima raiz primitiva da identidade. Tem-se, então, que $b^{\frac{n}{2}} = -1$.

Mas como

$$b^{\frac{n(n-1)}{2}} = (b^{\frac{n}{2}})^{n-1} = (-1)^{n-1} = -1,$$

obtém-se que $\beta^n = -1$ e, portanto, $\beta^n + 1 = 0$.

Assim, se β é valor próprio de BC, então $p(\beta) = 0$ onde $p(\lambda) = \lambda^n - \beta^n$ é o único polinómio mónico de grau n que possui os valores próprios de BC como raízes. $p(\lambda) = \lambda^n + 1$ é, assim, o polinómio característico de BC.

Mas, como BC possui n valores próprios distintos dois a dois, é não derrogatória e, portanto, o seu polinómio mínimo coincide com o seu polinómio característico, $p(\lambda) = \lambda^n + 1$.

Além disso, como BC é não derrogatória, é semelhante à matriz companheira do seu polinómio característico.

Assim, existe $S \in GL(n, F)$ tal que $S(BC)S^{-1} = C(p(\lambda))$. Defina-se $Z = C(p(\lambda))$.

Então,

$$bI_n = S(bI_n)S^{-1} = S(BCB^{-1}C^{-1})S^{-1} = ZYZ^{-1}Y^{-1} \quad \text{onde} \quad Y = SCS^{-1}.$$

Note-se que $|Z| = 1$ e, portanto, $Z \in SL(n, F)$.

Serão apresentadas de seguida condições para que Y seja uma matriz de $SL(n, F)$. Seja $Y = [y_{i,j}] \in F^{n \times n}$. Da igualdade $bI_n = ZYZ^{-1}Y^{-1}$ vem que $bYZ = ZY$. Observe-se que, atendendo à forma de $Z = C(p(\lambda))$, e efectuando os cálculos de bYZ e ZY pode obter-se uma relação de recorrência nas entradas da matriz Y. Tendo em atenção que todas as entradas de Y são determinadas pelas entradas da sua primeira coluna, fixem-se esses elementos $y_{i,1} = y_i$ para $i \in \{1, 2, \ldots, n\}$.

Tem-se, assim que

$$Y = \begin{bmatrix} y_1 & -by_n & -b^2y_{n-1} & \cdots & -b^{n-1}y_2 \\ y_2 & by_1 & -b^2y_n & \cdots & -b^{n-1}y_3 \\ y_3 & by_2 & b^2y_1 & \cdots & -b^{n-1}y_4 \\ \vdots & \vdots & \vdots & & \vdots \\ y_n & by_{n-1} & b^2y_{n-2} & \cdots & b^{n-1}y_1 \end{bmatrix}.$$

Tendo em conta as entradas de Y e o facto de $bYZ = ZY$, considere-se

$$Y_1 = \begin{bmatrix} y_1 & -y_n & -y_{n-1} & \cdots & -y_2 \\ y_2 & y_1 & -y_n & \cdots & -y_3 \\ y_3 & y_2 & y_1 & \cdots & -y_4 \\ \vdots & \vdots & \vdots & & \vdots \\ y_n & y_{n-1} & y_{n-2} & \cdots & y_1 \end{bmatrix}$$

e note-se que

$$Y = Y_1 \text{diag}(1, b, b^2, \ldots, b^{n-1}).$$

Tem-se, então, que $|Y| = b^{\frac{n(n-1)}{2}}|Y_1| = (b^{\frac{n}{2}})^{n-1}|Y_1| = (-1)^{n-1}|Y_1| = -|Y_1|$.

Desta forma, demonstra-se que uma condição necessária e suficiente para que bI_n seja um comutador multiplicativo de matrizes em $SL(n,F)$ é que existam $y_1, y_2, \ldots, y_n \in F$ tais que $|Y_1| = -1$.

Seja, agora, w uma $2n-$ésima raiz primitiva da identidade numa extensão algebricamente fechada do corpo F. Então, $w^{2n} = (w^2)^n = 1$ e w^2 é raiz do polinómio $\lambda^n - b^n$ e, consequentemente, raiz do polinómio $\lambda^n - 1$.

Assim, $w^2 \in \{1, b, \ldots, b^{n-1}\}$ e é, portanto uma $n-$ésima raiz da identidade. Assim, $w^2 = b^t$ para algum $t \in \{1, 2, \ldots, n-1\}$. Escolha-se w tal que $w^2 = b$.

Seja $w_i = b^i w$ para $i \in \{1, 2, \ldots, n\}$. Note-se que $|Y_1|$ é um circulante assimétrico e, de acordo com o que foi referido na introdução e com [13], tem-se que

$$|Y_1| = \prod_{i=1}^{n} \left(\sum_{j=1}^{n} w_i^{j-1} y_j \right) =$$

$$= \prod_{i=1}^{n} \left(w_i^0 y_1 + w_i y_2 + w_i^2 y_3 + \cdots + w_i^{n-1} y_n \right).$$

Note-se que $w_i^2 = (b^i w)^2 = b^{2i} w^2$ e $w_i^3 = (b^i w)^3 = b^{3i} w^2 w = b^{3i} w^3$ e, portanto, separando os termos y_i de índices par e ímpar, tem-se que

$$|Y_1| = \prod_{i=1}^{n} \left[(w_i^0 y_1 + w_i^2 y_3 + \cdots + w_i^{n-2} y_{n-1}) + (w_i y_2 + w_i^3 y_4 + \cdots + w_i^{n-1} y_n) \right]$$

$$= \prod_{i=1}^{n} \left[\left(y_1 + b^{2i} w^2 y_3 + \cdots b^{(n-2)i} w^{n-2} y_{n-1} \right) + \left(b^i w^i y_2 + b^{3i} w^3 y_4 + \cdots + b^{(n-1)i} w^{n-1} y_n \right) \right]$$

$$= \prod_{i=1}^{n} \left[\left(\sum_{j=1}^{n/2} b^{i(2j-2)} w^{2j-2} y_{2j-1} \right) + \left(\sum_{j=1}^{n/2} b^{i(2j-1)} w^{2j-1} y_{2j} \right) \right].$$

Como $w^{2j-2} = (w^2)^j (w^2)^{-1} = b^j b^{-1}$ e $w^{2j} = b^j$, a expressão acima é igual a

$$\prod_{i=1}^{n} \left[\left(\sum_{j=1}^{n/2} b^{2ij-2i} b^j b^{-1} y_{2j-1} \right) + \left(w^{-1} \sum_{j=1}^{n/2} b^{2ij-i} b^j y_{2j} \right) \right]$$

$$= \prod_{i=1}^{n} \left[\left(\sum_{j=1}^{n/2} b^{(j-1)(2i+1)} y_{2j-1} \right) + \left(w^{-1} \sum_{j=1}^{n/2} b^{j(2i+1)-i} y_{2j} \right) \right].$$

Observe-se que, para $p \in \{1, 2, \ldots, \frac{n}{2}\}$, $b^{k(2(\frac{n}{2}+p)+1)} = b^{k(2p+1)}$, se k é um inteiro positivo. Da mesma forma, tem-se que $b^{-(\frac{n}{2}+p)} = -b^{-p}$.

Assim, rearranjando os produtos anteriores é possível juntar as somas correspondentes a $i = 1$ com $i = \frac{n}{2} + 1$, $i = 2$ com $i = \frac{n}{2} + 2$ e assim sucessivamente, podendo escrever que

$$
\begin{aligned}
|Y_1| &= \prod_{i=1}^{n/2} \left(\sum_{j=1}^{n/2} b^{(j-1)(2i+1)} y_{2j-1} + w^{-1} \sum_{j=1}^{n/2} b^{j(2i+1)-i} y_{2j} \right) \times \\
&\quad \times \left(\sum_{j=1}^{n/2} b^{(j-1)(2i+1)} y_{2j-1} - w^{-1} \sum_{j=1}^{n/2} b^{j(2i+1)-i} y_{2j} \right) \\
&= \prod_{i=1}^{n/2} \left[\left(\sum_{j=1}^{n/2} b^{(j-1)(2i+1)} y_{2j-1} \right)^2 - \underbrace{(w^{-1})^2}_{b^{-1}} \left(\sum_{j=1}^{n/2} b^{j(2i+1)-i} y_{2j} \right)^2 \right] \\
&= \prod_{i=1}^{n/2} \left[\left(\sum_{j=1}^{n/2} b^{(j-1)(2i+1)} y_{2j-1} \right)^2 - b^{-1} \left((b^{-i}) \sum_{j=1}^{n/2} b^{j(2i+1)} y_{2j} \right)^2 \right].
\end{aligned}
$$

Considere-se, agora, o sistema de $\frac{n}{2}$ equações em $\frac{n}{2}$ incógnitas:

$$
\sum_{j=1}^{n/2} b^{(j-1)(2i+1)} y_{2j-1} = w_{2i-1} \quad i \in \{1, 2, \ldots, \frac{n}{2}\}. \tag{2.8}
$$

$$
\begin{cases}
b^0 y_1 + b^3 y_3 + b^6 y_5 + b^9 y_7 + \cdots + b^{(\frac{n}{2}-1)3} y_{n-1} = w_1 \\
b^0 y_1 + b^5 y_3 + b^{10} y_5 + b^{15} y_7 + \cdots + b^{(\frac{n}{2}-1)5} y_{n-1} = w_3 \\
b^0 y_1 + b^7 y_3 + b^{14} y_5 + b^{21} y_7 + \cdots + b^{(\frac{n}{2}-1)7} y_{n-1} = w_5 \\
\vdots \\
b^0 y_1 + b^{n+1} y_3 + b^{2(n+1)} y_5 + b^{3(n+1)} y_7 + \cdots + b^{(\frac{n}{2}-1)(n+1)} y_{n-1} = w_{n-1}
\end{cases}
$$

A matriz dos coeficientes é:

$$
\begin{bmatrix}
b^0 & b^3 & b^6 & b^9 & \cdots & b^{(\frac{n}{2}-1)3} \\
b^0 & b^5 & b^{10} & b^{15} & \cdots & b^{(\frac{n}{2}-1)5} \\
b^0 & b^7 & b^{14} & b^{21} & \cdots & b^{(\frac{n}{2}-1)7} \\
\vdots & \vdots & \vdots & \vdots & & \vdots \\
\vdots & \vdots & \vdots & \vdots & & \vdots \\
b^0 & b^{2n+1} & b^{(2n+1)2} & b^{(2n+1)3} & \cdots & b^{(2n+1)(\frac{n}{2}-1)}
\end{bmatrix}
$$

que é uma matriz de Vandermonde e é não singular porque, sendo b uma $n-$ésima raiz primitiva da identidade, os elementos da segunda coluna são sempre distintos dois a dois.

De facto, se houver algum k inteiro tal que $b^k = b^{k+2}$, então $b^2 = 1$, que no caso de n ser maior que 2, contraria o facto de b ser uma $n-$ésima raiz primitiva da identidade.

No caso em que $n = 2$, tem-se que o sistema (2.8) se resume a $y_1 = w_1$ e é sempre possível determinar y_1 para qualquer escolha de w_1.

Assim, a matriz anterior é invertível e, tendo em atenção a Teoria sobre Sistemas Lineares, para qualquer escolha de $w_1, w_3, \ldots, w_{n-1} \in F$ é possível encontrar $y_1, y_3, \ldots, y_{n-1} \in F$ que satisfaçam (2.8)

De forma semelhante, o conjunto de $\frac{n}{2}$ equações em $\frac{n}{2}$ incógnitas

$$(b^{-i}) \sum_{j=1}^{n/2} b^{j(2i+1)} y_{2j} = w_{2i} \quad i \in \{1, 2, \ldots, \frac{n}{2}\},$$

que é equivalente a

$$\sum_{j=1}^{n/2} b^{j(2i+1)} y_{2j} = b^i w_{2i} \quad i \in \{1, 2, \ldots, \frac{n}{2}\},$$

possui um conjunto de soluções $y_2, y_4, \ldots, y_n \in F$, para qualquer escolha de elementos em F, $w_2, w_4, \ldots, w_n$.

Então, para que $|Y_1| = -1$, é necessário e suficiente que existam $w_1, w_2, \ldots, w_n \in F$ tais que

$$-1 = \prod_{i=1}^{n/2} \left((w_{2i-1})^2 - b^{-1}(w_{2i})^2 \right). \tag{2.9}$$

Se $n = 4m$, para m inteiro positivo, tome-se

$w_1 = b^m$;

$w_{2i-1} = 1 \quad i \in \{2, 3, \ldots, \frac{n}{2}\}$;

$w_{2i} = 0 \quad i \in \{1, 2, \ldots, \frac{n}{2}\}$.

Com esta escolha, a expressão (2.9) assume a forma

$$-1 = (w_1^2 - b^{-1}0)(1 - b^{-1}0)(1 - b^{-1}0) \cdots (1 - b^{-1}0)$$

e que se resume a $w_1^2 = -1$, que equivale a $b^{2m} = -1$, e que é uma afirmação verdadeira pois $n = 4m$, e b é uma $n-$ésima raiz primitiva da unidade.

Assim, quando $n = 4m$, para algum inteiro positivo m, existem $w_1, w_2, \ldots, w_n \in F$ que verificam (2.9) e então existem matrizes $Z, Y \in SL(n, F)$ tais que $bI_n = ZYZ^{-1}Y^{-1}$.

Tem-se, então que, quando $n = 4m$, para m inteiro positivo, bI_n é um comutador multiplicativo de matrizes em $SL(n, F)$.

Se $n = 4m + 2$ para algum inteiro não negativo, ou seja, $n \equiv 2(\text{mod } 4)$, note-se que $b^{2m+1} = b^{\frac{n}{2}} = -1$ e, portanto, $-b^{-1} = b^{2m}$.

Considere-se, agora, $w'_{2i} = b^m w_{2i}$. Então, (2.9) toma a forma

$$-1 = \prod_{i=1}^{n/2} \left((w_{2i-1})^2 + (w'_{2i})^2\right). \tag{2.10}$$

Observe-se que, de acordo com [12], o conjunto formado por somas de quadrados é fechado para a adição e multiplicação. De facto, no que diz respeito à multiplicação, para $x_1, x_2, y_1, y_2 \in F$, tem-se que

$$(x_1^2 + y_1^2)(x_2^2 + y_2^2) = (x_1x_2 + y_1y_2)^2 + (x_1y_2 - x_2y_1)^2.$$

Assim, tem-se que (2.10) equivale a (2.11):

$$-1 = W^2 + (W')^2, \quad \text{para alguns} \quad W, W' \in F. \tag{2.11}$$

Reciprocamente, se (2.11) possui solução em F e se em (2.10) se fizer

$w_1 = W$; $w'_2 = W'$;

$w_{2i-1} = 1 \quad i \in \{2, 3, \ldots, \frac{n}{2}\}$;

$w'_{2i} = 0 \quad i \in \{2, 3, \ldots, \frac{n}{2}\}$.

obtém-se que

$$|Y_1| = \prod_{i=1}^{n/2} \left(w_{2i-1}^2 + (w'_{2i})^2\right) = (W^2 + (W')^2) \underbrace{(1+0)\cdots(1+0)}_{\frac{n}{2}-1 \text{ factores}} = -1.$$

Demonstrou-se, então, que, se $n = 4m + 2$ para algum m inteiro não negativo, então uma condição necessária e suficiente para que

$$bI_n = ZYZ^{-1}Y^{-1}, \quad Z, Y \in SL(n, F)$$

é que (2.11) possua solução $W, W' \in F$.

É conhecido de [12] que existem inteiros x, y tais que

$$x^2 + y^2 + 1 \equiv 0 (\text{mod } p), \quad \text{onde } p \text{ é primo.} \tag{2.12}$$

De facto, se $p = 2$, basta escolher x, y com paridades diferentes.

Se $p > 2$, sejam $x, y \in \{0, 1, 2, \ldots, \frac{p-1}{2}\}$ e observe-se que todos os elementos x^2 são distintos (mod p). Se houvesse $x_i, x_j \in \{0, 1, 2, \ldots, \frac{p-1}{2}\}$ distintos e tais que $x_i^2 \equiv x_j^2 (\text{mod } p)$, então ter-se-ia que $p|(x_i - x_j)(x_i + x_j)$ e como $0 < x_i + x_j < p$, a menos que $x_i = x_j = 0$, o que não acontece, então $p|(x_i - x_j)$, o que significa que $x_i \equiv x_j (\text{mod } p)$. Mas isso só é possível se $x_i = x_j$, o que é absurdo.

O mesmo argumento é utilizado para concluir que os elementos $-(1+y^2)$ são todos distintos (mod p) quando $y \in \{0, 1, 2, \ldots, \frac{p-1}{2}\}$.

Observe-se, agora, que os conjuntos $K_1 = \{x^2 : \quad x \in \{0, 1, \ldots, \frac{p-1}{2}\}\}$ e $K_2 = \{-(1 + y^2) : y \in \{0, 1, \ldots, \frac{p-1}{2}\}\}$ possuem $\frac{p+1}{2}$ elementos cada e, portanto, entre os dois conjuntos, contam-se $p + 1$ elementos distintos.

Assim, como em $\mathbb{Z}_p$ só existem p elementos distintos, tem-se que existem, $x^2 \in K_1$ e $-(1 + y^2) \in K_2$ tais que $x^2 \equiv -(1 + y^2) (\text{mod } p)$ e portanto em $\mathbb{Z}_p$, (2.12) possui solução.

Tendo em conta o isomorfismo existente entre $\mathbb{Z}_p$ e $GF(p)$, conclui-se que existem elementos $x, y \in GF(p)$ tais que $x^2 + y^2 = -1$.

Note-se ainda que, se F possui característica p, então F é isomorfo a $\mathbb{Z}_p$ e, portanto, em qualquer corpo de característica p tem-se, também, que existem $x, y \in F$ tais que $x^2 + y^2 = -1$.

Desta forma, conclui-se que, quando $n = 4m + 2$, para algum inteiro não negativo m, e se F é um corpo de característica p, com p um número primo, existem matrizes $Z, Y \in SL(n, F)$ tais que $bI_n = ZYZ^{-1}Y^{-1}$.

Fica assim concluído o **Passo 4**. No entanto, antes da passagem ao passo seguinte, serão apresentados alguns exemplos ilustrativos das conclusões retiradas neste Passo.

É um resultado conhecido que, um corpo ou possui característica p com p primo, ou possui característica zero.

Observe-se que, se F possui característica zero, então a equação $-1 = w^2 + (w')^2$ é, por vezes, impossível.

Tome-se o exemplo em que $n = 2$, $b = -1$ é a $2-$ésima raiz primitiva da identidade e $F = \mathbb{R}$. Uma vez que $b^2 = 1$, a equação $x^2 + y^2 = -1$ é impossível em $\mathbb{R}$.

Da mesma forma a expressão (2.10) assume a forma

$$-1 = |Y_1| = \prod_{i=1}^{2/2} \left(w_{2i-1}^2 + (w'_{2i})^2\right) = w_1^2 + (w'_2)^2$$

que é, também, impossível em $\mathbb{R}$.

Em muitos outros casos (2.11) possui solução. São de seguida apresentados dois desses casos:

1. Se F possui a $2n-$ésima raiz primitiva da identidade, w, então os elementos $W = w^{n/2}$ e $W' = 0$ são as soluções de (2.11).

   De facto, como w é $2n-$ésima raiz primitiva da identidade, tem-se que $w^{2n} = 1$. Assim,

   $$W^2 + (W')^2 = (w^{\frac{n}{2}})^2 + 0^2 = w^n = -1$$

   e, sob as condições do exemplo, bI_n é um comutador multiplicativo de matrizes em $SL(n, F)$.

2. Sejam F um corpo com uma $n-$ésima raiz primitiva da identidade e $n = 2(2m+1)$, com m inteiro não negativo. Se para algum divisor $r > 1$ de $2m+1$ existirem inteiros s, h tais que

   $$r(h+1) = 2^s + 1,$$

   então é possível encontrar uma solução de (2.11).

   De facto, usando uma técnica devida a Landau [11] e usando a seguinte identidade polinomial

   $$\begin{aligned}(1 + \lambda + \lambda^2 + \cdots + \lambda^{r-1})(1 + \lambda^r + \lambda^{2r} + \cdots + \lambda^{hr}) \\ = 1 + \lambda + \lambda^2 + \cdots + \lambda^{rh+r-1} \\ = (1+\lambda)(1+\lambda^2)(1+\lambda^4)\cdots(1+\lambda^{2^{s-1}}) + \lambda^{2^s},\end{aligned} \tag{2.13}$$

   note-se que, como $r > 1$ é divisor de um número ímpar, tem-se que $n > 2$. Além disso, F contém a $n-$ésima raiz primitiva da identidade, b, e como qualquer outra raiz da identidade é uma potência de b, essa raiz está também em F.

Seja $\rho = b^{\frac{n}{2r}}$. Então $\rho^2 \neq 1$ pois $\rho^2 = b^{\frac{n}{r}}$ e $\frac{n}{r} < n$. Mais, ρ satisfaz

$$\frac{\rho^{2r}-1}{\rho^2-1} = \rho^{2r-2} + \rho^{2r-4} + \cdots + \rho^2 + 1 = 0$$

Note-se, de seguida que na expressão (2.13), substituindo λ por ρ^2, tem-se

$$(1+\rho^2)(1+\rho^4)(1+\rho^8)\cdots(1+(\rho^2)^{2^{s-1}}) + (\rho^2)^{2^s}$$

$$= (1+\rho^2)(1+\rho^4)(1+\rho^8)\cdots(1+\rho^{2^s}) + (\rho^2)^{2^s}$$

$$= 1 + \rho^2 + \rho^4 + \rho^8 + \cdots + (\rho^2)^{r(h+1)-1}$$

$$= 1 + \rho^2 + \rho^4 + \rho^8 + \cdots + \rho^{2^{s+1}}$$

$$= \underbrace{(1+\rho^2+\rho^4+\cdots+\rho^{2(r-1)})}_{=0}(1+(\rho^2)^r+(\rho^2)^{2r}+\cdots+(\rho^2)^{hr})$$

Assim,

$$(1+\rho^2)(1+\rho^4)(1+\rho^8)\cdots(1+\rho^{2^s}) + (\rho^2)^{2^s} = 0$$

e, portanto,

$$-(\rho^2)^{2^s} = (1+\rho^2)(1+\rho^4)(1+\rho^8)\cdots(1+\rho^{2^s}). \tag{2.14}$$

Mas, sendo o conjunto das somas de quadrados fechado para a multiplicação, tem-se que o segundo membro de (2.14) é igual a $1+a^2$, para algum $a \in F$. Além disso, $(\rho^2)^{2^s} = (\rho^{2^s})^2$.

Tem-se, assim, que (2.14) é equivalente a

$$-(\rho^{2^s})^2 = 1 + a^2, \quad \text{que equivale ainda a} \quad -1 = \left(\frac{1}{\rho^{2^s}}\right)^2 + \left(\frac{a}{\rho^{2^s}}\right)^2$$

de onde se deduz que -1 é soma de dois quadrados e, sob as condições do exemplo, tem-se que bI_n é um comutador multiplicativo de matrizes em $SL(n,F)$.

Completa-se, de seguida, a demonstração do teorema 2.1 executando o **Passo 5**.

Como anteriormente foi demonstrado que existem sempre matrizes $X, Y \in SL(n,F)$ tais que $bI_n = (X,Y)$, excepto no caso em que $n \equiv 2(\text{mod } 4)$ e F possui característica zero.

Demonstra-se de seguida que, quando $n \equiv 2(\text{mod } 4)$ e F é um corpo de característica zero, bI_n é um produto de dois comutadores de $SL(n,F)$.

Para $n = 2$, tome-se

$$P = \begin{bmatrix} 5 & 14 \\ -4 & -11 \end{bmatrix} \quad Q = \begin{bmatrix} 2 & 4 \\ 0 & 2^{-1} \end{bmatrix}.$$

Note-se que b é uma $2-$ésima raiz primitiva da identidade e, portanto, $b = -1$. Desta forma,

$$bI_2 = -I_2 = (PQP^{-1}Q^{-1})^2.$$

Tendo em conta que $|P| = |Q| = 1$, fica completa a demonstração para $n = 2$.

Suponha-se, agora, que $n = 4m + 2 > 2$, $m \geq 1$. Como b é uma $n-$ésima raiz primitiva da identidade, no grupo cíclico $< b >$, qualquer elemento da forma b^s, para s inteiro, gera um subgrupo que contém $\frac{n}{\text{mdc}(n,s)}$ elementos.

Pela observação anterior, b^{2m} é uma raiz primitiva da identidade de ordem $\frac{n}{\text{mdc}(n,2m)}$. Mas,

$$\frac{n}{\text{mdc}(n, 2m)} = \frac{4m+2}{\text{mdc}(4m+2, 2m)} = \frac{2m+1}{\text{mdc}(2m+1, m)} = 2m + 1.$$

Assim, b^{2m} é uma raiz primitiva da identidade de ordem ímpar e, tendo em conta o passo 2, $b^{2m}I_n$ é um comutador multiplicativo de matrizes em $SL(n, F)$, ou seja, $b^{2m}I_n = XYX^{-1}Y^{-1}$, para $X, Y \in SL(n, F)$.

Mas, $-I_n = b^{2m+1}I_{2(2m+1)}$ e, pelo passo 3, é também um comutador multiplicativo de matrizes em $SL(n, F)$, ou seja $-I_n = ZWZ^{-1}W^{-1}$, para $Z, W \in SL(n, F)$.

Tem-se então que $(b^{2m}I_n)(bI_n) = b^{\frac{n}{2}}I_n = -I_n$ ou seja,

$$(XYX^{-1}Y^{-1})(bI_n) = ZWZ^{-1}W^{-1}$$

o que equivale a

$$bI_n = (ZWZ^{-1}W^{-1})(YXY^{-1}X^{-1}).$$

Desta forma, bI_n é produto de dois comutadores multiplicativos de matrizes em $SL(n, F)$. Conclui-se, assim, o **Caso 5** e demonstração do teorema 2.1.

■

Apresenta-se de seguida o resultado mais significativo desta secção.

Teorema 2.2. *Seja $A \in SL(n,F)$. Se A não é escalar e F possui pelo menos 4 elementos, então existem matrizes $X, Y \in SL(n,F)$ tais que $A = (X,Y)$.*

A demonstração do teorema 2.2 apresentada de seguida para corpos em geral, depende do número de elementos de F e não é válida quando F possui 5 ou menos elementos. No entanto, utilizando alguns argumentos da demonstração seguinte e propriedades específicas de $GF(4)$ e $GF(5)$, serão apresentadas posteriormente demonstrações particulares para cada um destes casos.

Os métodos aplicados nesta secção falham completamente quando $F = GF(2)$ e $F = GF(3)$ e, portanto, esses casos serão alvo de estudos particulares e independentes que constituem as secções 2.2 e 2.3.

Demonstração

Sejam F um corpo com, pelo menos, 6 elementos e $A \in SL(n,F)$. Tal como referido no início do capítulo a propriedade ser um comutador multiplicativo de matrizes é invariante para a semelhança. Assim, a demonstração que uma matriz $A \in SL(n,F)$ é um comutador multiplicativo de matrizes em $SL(n,F)$, pode ser reduzida a demonstrar que uma qualquer matriz semelhante a A é um comutador multiplicativo de matrizes em $SL(n,F)$.

Suponha-se, então, sem perda de generalidade, que A coincide com a sua forma normal invariante:

$$A = A_1 \oplus A_2 \oplus \cdots \oplus A_r,$$

onde $A_i \in F^{j(i)\times j(i)}$ é a matriz companheira de um polinómio com coeficientes em F e $i \in \{1,2,\ldots,r\}$.

Rearranjando as matrizes A_i, $i \in \{1,2,\ldots,r\}$, utilizando, se necessário, transformações de semelhança, suponha-se que

$$j(1) \leq j(2) \leq \cdots \leq j(r).$$

A demonstração será dividida em vários casos dependendo dos valores atribuídos a n, r e $j(1), j(2), \ldots, j(r)$.

Caso 1: $n = 2$.

Como A é uma matriz não escalar de dimensões 2×2, tem-se que A é não derrogatória e, portanto, é semelhante à matriz companheira do seu polinómio característico. Sem perda de generalidade, pelas observações feitas atrás, pode supor-se que

$$A = F_C(A) = \begin{bmatrix} 0 & 1 \\ a & b \end{bmatrix}, \quad a, b \in F.$$

Escolha-se $\rho \in F$ tal que $\rho^2 \neq 1$ e $\rho^2 \neq 0$. Tal é possível pois $F \neq GF(2)$ e $F \neq GF(3)$.

Pelo lema 2.4, é possível encontrar uma matriz standard $D \in SL(2, F)$ com $d_1 = \rho$, com divisores elementares

$$\lambda - \rho, \ \lambda - \rho^{-1}$$

e tal que os divisores de AD são também $\lambda - \rho, \ \lambda - \rho^{-1}$.

Mas, pelo lema 2.6, e porque A e AD tendo o mesmos divisores elementares, são semelhantes, é possível encontrar $S \in SL(2, F)$ tal que

$$A = SDS^{-1}D^{-1}, \quad S, D \in SL(2, F).$$

A matriz A é, desta forma, um comutador multiplicativo de matrizes em $SL(n, F)$ e conclui-se, assim, o estudo do **Caso 1**.

Caso 2: $j(r) \geq 3$.

Seja $\delta_1 \in F \backslash \{0\}$ e defina-se

$$\delta_{i+1} = |A_i|\delta_i, \quad i \in \{1, 2, \ldots, r\}.$$

Então,

$$\delta_2 = |A_1|\delta_1;$$

$$\delta_3 = |A_2|\delta_2 = |A_2||A_1|\delta_1;$$

$$\vdots$$

$$\delta_{r+1} = |A_r|\delta_r = |A_r||A_{r-1}| \cdots |A_1|\delta_1.$$

Como $A \in SL(n,F)$, tem-se que$|A| = |A_1 A_2 \cdots A_r| = 1$ e, portanto, $\delta_{r+1} = \delta_1$.

Para $i \in \{1,2,\ldots,r\}$, seja $\gamma_i \in F\backslash\{\delta_i, \delta_{i+1}, 0\}$. Note-se que tal é possível uma vez que F possui pelo menos 6 elementos.

Defina-se γ''' como a solução de

$$\left(\prod_{i=1}^{r} \delta_i\right)\left(\prod_{i=1}^{r-1} (\gamma_i)^{j(i)-1}\right)(\gamma_r)^{j(r)-2}\gamma''' = 1 \tag{2.15}$$

e escolha-se $x \in F\backslash\{0\}$ tal que

$$\gamma_r x \neq \delta_r \text{ ou } \gamma_r x \neq \delta_1, \quad \gamma''' x^{-1} \neq \delta_r \text{ ou } \gamma''' x^{-1} \neq \delta_1. \tag{2.16}$$

As condições (2.16) exigem a existência de, pelo menos, 4 elementos não nulos: δ_1, γ_r, x e $\gamma_r x$. Como F possui pelo menos 6 elementos, é sempre possível satisfazer tais condições.

Sejam $\gamma' = \gamma_r x$ e $\gamma'' = \gamma''' x^{-1}$ e note-se que $\gamma_r \gamma''' = \gamma'\gamma''$. Então (2.15) é equivalente a

$$\left(\prod_{i=1}^{r} \delta_i\right)\left(\prod_{i=1}^{r-1} (\gamma_i)^{j(i)-1}\right)(\gamma_r)^{j(r)-3}\gamma'\gamma'' = 1. \tag{2.17}$$

Pretende-se que a expressão (2.17) seja o determinante de uma matriz standard a determinar posteriormente.

Para cada $i \in \{1,2,\ldots,r-1\}$ tem-se que A_i é a matriz companheira de um polinómio e $\delta_{i+1} = |A_i|\delta_i$. Defina-se então para cada i, utilizando o lema 2.4, uma matriz standard $D_i \in GL(j(i),F)$ com $d_1 = \delta_i$, divisores elementares

$$\lambda - \delta_i,\ (\lambda - \gamma_i)^{j(i)-1}$$

e tal que os divisores elementares de $A_i D_i$ são

$$\lambda - \delta_{i+1},\ (\lambda - \gamma_i)^{j(i)-1}.$$

Uma vez mais utilizando o lema 2.4 construa-se uma matriz standard $D_r \in GL(j(r),F)$ em que $d_1 = \delta_r$ e que verifique uma das seguintes cinco condições:

1. Se $\gamma_r, \gamma', \gamma''$ são elementos de F distintos dois a dois, escolha-se D_r de forma a que os divisores elementares de D_r sejam

$$\lambda - \delta_r,\ (\lambda - \gamma_r)^{j(r)-3},\ \lambda - \gamma',\ \lambda - \gamma''$$

e os divisores elementares de $A_r D_r$ sejam

$$\lambda - \delta_1,\ (\lambda - \gamma_r)^{j(r)-3},\ \lambda - \gamma',\ \lambda - \gamma''.$$

Recorde-se que $\delta_1 = |A_r|\delta_r$.

2. Se $\gamma_r = \gamma' \neq \gamma''$, escolha-se D_r de forma a que os divisores elementares de D_r sejam

$$\lambda - \delta_r,\ (\lambda - \gamma_r)^{j(r)-2},\ \lambda - \gamma''$$

e os divisores elementares de $A_r D_r$ sejam

$$\lambda - \delta_1,\ (\lambda - \gamma_r)^{j(r)-2},\ \lambda - \gamma''.$$

3. Se $\gamma_r = \gamma'' \neq \gamma'$, escolha-se D_r de forma a que os divisores elementares de D_r sejam

$$\lambda - \delta_r,\ (\lambda - \gamma_r)^{j(r)-2},\ \lambda - \gamma'$$

e os divisores elementares de $A_r D_r$ sejam

$$\lambda - \delta_1,\ (\lambda - \gamma_r)^{j(r)-2},\ \lambda - \gamma'.$$

4. Se $\gamma_r \neq \gamma'' = \gamma'$, escolha-se D_r de forma a que os divisores elementares de D_r sejam

$$\lambda - \delta_r,\ (\lambda - \gamma')^2,\ (\lambda - \gamma_r)^{j(r)-3}$$

e os divisores elementares de $A_r D_r$ sejam

$$\lambda - \delta_1,\ (\lambda - \gamma')^2,\ (\lambda - \gamma_r)^{j(r)-3}.$$

5. Se $\gamma_r = \gamma'' = \gamma'$, escolha-se D_r de forma a que os divisores elementares de D_r sejam

$$\lambda - \delta_r,\ (\lambda - \gamma_r)^{j(r)-1}$$

e os divisores elementares de $A_r D_r$ sejam

$$\lambda - \delta_1,\ (\lambda - \gamma_r)^{j(r)-1}.$$

Seja, agora, $D = D_1 \oplus D_2 \oplus \cdots \oplus D_r$. Mas, para $i \in \{1, 2, \ldots, r-1\}$, $|D_i| = \delta_i \gamma_i^{j(i)-1}$ e $|D_r| = \delta_r \gamma_r^{j(r)-3} \gamma' \gamma''$, em qualquer dos cinco casos anteriores.

Assim, pela igualdade (2.17), tem-se $|D| = |D_1||D_2| \cdots |D_r| = 1$ e, portanto, $D \in SL(n, F)$.

Observe-se ainda que D e AD possuem os mesmos divisores elementares, particularmente um divisor elementar linear. Assim, pelo lema 2.6 existe $S \in SL(n, F)$ tal que $AD = SDS^{-1}$. Desta forma,

$$A = SDS^{-1}D^{-1} \quad S, D \in SL(n, F)$$

e é, portanto, um comutador multiplicativo de matrizes. Conclui-se assim, o estudo do **Caso 2**.

Caso 3: $r \geq 2;\ j(r) = j(r-1) = 2$

Para $i \in \{1, 2, \ldots, r\}$ definam-se δ_i, γ_i tal como no Caso 2. Defina-se, ainda, γ''' como solução de (2.15) e seja $x \in F \backslash \{0\}$ tal que

$$\gamma' = \gamma_{r-1} x, \quad \gamma'' = \gamma''' x^{-1}$$

e

$$\gamma' \neq \delta_{r-1} \quad \text{ou} \quad \gamma' \neq \delta_r$$

e

$$\gamma'' \neq \delta_r \quad \text{ou} \quad \gamma' \neq \delta_1.$$

Para $i \in \{1, 2, \ldots, r-2\}$ construa-se, utilizando o lema 2.4 uma matriz standard $D_i \in GL(j(i), F)$ com $d_1 = \delta_i$, com divisores elementares

$$\lambda - \delta_i,\ (\lambda - \gamma_i)^{j(i)-1}$$

e tal que os divisores elementares de $A_i D_i$ sejam

$$\lambda - \delta_{i+1},\ (\lambda - \gamma_i)^{j(i)-1}.$$

Construa-se, de seguida uma matriz standard $D_{r-1} \in GL(2, F)$ com $d_1 = \delta_{r-1}$, com divisores elementares

$$\lambda - \delta_{r-1},\ \lambda - \gamma'$$

e tal que os divisores elementares de $A_{r-1}D_{r-1}$ sejam

$$\lambda - \delta_r,\ \lambda - \gamma'.$$

Construa-se, ainda, uma matriz standard $D_r \in GL(2, F)$ com $d_1 = \delta_r$, com divisores elementares

$$\lambda - \delta_r,\ \lambda - \gamma''$$

e tal que os divisores elementares de $A_r D_r$ sejam

$$\lambda - \delta_1,\ \lambda - \gamma''.$$

Seja $D = D_1 \oplus D_2 \oplus \cdots \oplus D_r$. Com D definida desta forma, tem-se que $|D| = |D_1||D_2| \cdots |D_r|$ e, uma vez mais, por (2.15) tem-se que $|D| = 1$ e, portanto, $D \in SL(n, F)$.

Uma vez que A e AD possuem os mesmos divisores elementares, em particular um divisor elementar linear, é possível aplicar o lema 2.6 e encontrar $S \in SL(n, F)$ tal que $AD = SDS^{-1}$.

Desta forma,

$$A = SDS^{-1}D^{-1} \quad S, D \in SL(n, F)$$

e é, portanto, um comutador multiplicativo de matrizes em $SL(n, F)$.

Conclui-se assim, o estudo do **Caso 3**.

A matriz D utilizada atrás é uma matriz diagonal por blocos. O argumento da demonstração nos dois casos anteriores teve por base a manipulação de dois blocos em posições extremas da matriz D com o objectivo de controlar o valor do seu determinante.

Se $n = 2$, ou se $j(i) = 1$ para $i \in \{1, 2, \ldots, r-1\}$ e $j(r) = 1$ ou $j(r) = 2$, os elementos nessas duas posições não existem. Como o caso em que $n = 2$ já foi abordado, pode passar-se a estudar o caso $n > 2$ e $j(i) = 1$ para $i \in \{1, 2, \ldots, r-1\}$ e $j(r) = 1$ ou $j(r) = 2$.

Se $n > 2$, note-se, inicialmente, que, se os polinómios $p(\lambda)$ e $q(\lambda)$ forem primos entre si, então, $C(p(\lambda)) \oplus C(q(\lambda))$ é semelhante a $C(p(\lambda)q(\lambda))$. Este resultado será utilizado sempre que possível.

Note-se ainda que, se $j(i) = 1$ para $i \in \{1, 2, \ldots, r\}$, a matriz A é semelhante a uma matriz $A' = A_1 \oplus A_2 \oplus \cdots \oplus A_r$, onde cada matriz $A_i = C(f_i)$, e $f_i = \lambda - d_i$, $d_i \in F$, para $i \in \{1, 2, \ldots, r\}$. Sem perda de generalidade, suponha-se que $A = A'$.

Suponha-se que o número de divisores elementares distintos da matriz A é maior ou igual a 3. Pela observação anterior, e a menos de transformações de semelhança, pode dizer-se que A' é semelhante a

$$B = B_1 \oplus B_2 \oplus \cdots \oplus B_{r-1} \oplus B_r,$$

onde $B_i = C(g_i) \in F^{j(i)\times j(i)}$, $g_i \in F[\lambda]$, $i \in \{1, 2, \ldots, r\}$ e uma das situações seguintes ocorre:

- $j(r-1) = j(r) = 2$;
- $j(r) = 3$.

Observe-se que tais situações foram já abordadas nos casos 2 e 3.

Se o número de divisores elementares não constantes distintos da matriz A for 2, nomeadamente $\lambda - f$ e $\lambda - g$, com $f, g \in F$, então A é semelhante a

$$A' = A_1 \oplus \cdots \oplus A_i \oplus \cdots A_j \oplus \cdots \oplus A_r,$$

onde $A_i = C(\lambda - f)$, $A_j = C(\lambda - g)$ e $A_k = C(\lambda - f)$ para $k \neq j$.

Mas, usando novamente transformações de semelhança, pode dizer-se que A' é semelhante a

$$B' = A_1 \oplus \cdots \oplus A_{i-1} \oplus A_{i+1} \oplus \cdots \oplus A_{j-1} \oplus A_{j+1} \oplus \cdots \oplus A_r \oplus C((\lambda - f)(\lambda - g)),$$

onde $A_1 = \cdots A_r = C(\lambda - f)$.

Assim, resta apenas, considerar o Caso 4:

Caso 4: $A = fI_{n-2} \oplus A_r$, com $A_r = C((\lambda - f)(\lambda - g))$; $f, g \in F$;

Note-se que $|A| = f^{n-2}fg$ e, como $A \in SL(n, F)$, tem-se que $f^{n-1}g = 1$.

Seja $\delta \in F\backslash\{0\}$. Defina-se $c(\delta)$ como uma função de δ por

$$f^{(n-1)(n-2)/2}\delta^{n-1}c(\delta) = 1, \tag{2.18}$$

ou seja, se $f^{(n-1)(n-2)/2} = a \in F$, então, $c(\delta) = \delta^{1-n}a^{-1}$.

À semelhança das demonstrações já efectuadas, escolha-se $\delta \in F\backslash\{0\}$ tal que

$$c(\delta) \neq \delta \tag{2.19}$$

$$c(\delta) \neq f^{n-2}\delta. \tag{2.20}$$

Se existir tal δ defina-se

$$D = [\delta] \oplus [f\delta] \oplus [f^2\delta] \oplus \cdots \oplus [f^{n-3}\delta] \oplus \underbrace{\begin{bmatrix} f^{n-2}\delta & d_2 \\ 0 & c(\delta) \end{bmatrix}}_{D_1}.$$

Atendendo à estrutura de D, observe-se que $|D| = f^{(n-1)(n-2)/2}\delta^{n-1}c(\delta) = 1$ e, se $c(\delta) \neq f^{n-2}\delta$, os seus divisores elementares são

$$\lambda - \delta,\ \lambda - f\delta,\ \lambda - f^2\delta,\ \ldots, \lambda - f^{n-2}\delta,\ \lambda - c(\delta).$$

Note-se que os divisores elementares de AD são

$$\lambda - f\delta,\ \lambda - f^2\delta,\ \ldots, \lambda - f^{n-2}\delta,$$

juntamente com os divisores elementares associados a $C((\lambda - f)(\lambda - g))D_1 = A_rD_1$.

Mas pelo lema 2.4, aplicado a A_r, é possível escolher $d_2 \in F$ tal que os divisores elementares de AD sejam

$$\lambda - \delta,\ \lambda - f\delta,\ \lambda - f^2\delta,\ \ldots, \lambda - f^{n-2}\delta,\ \lambda - c(\delta).$$

De facto, A_r é uma matriz companheira e escolhendo $d_1 = f^{n-2}\delta,\ \gamma_1 = c(\delta)$, tem-se que existe uma matriz standard D_1 (na qual só falta determinar d_2) tal que o divisores de D_1 são

$$\lambda - f^{n-2}\delta,\ \lambda - c(\delta)$$

e os divisores elementares de A_rD_1 são

$$\lambda - f^{n-2}\delta|A_r|,\ \lambda - c(\delta).$$

Mas, como $|A_r| = fg$, tem-se que $\lambda - f^{n-2}\delta|A_r| = \lambda - \delta$, pois $f^{n-1}g = 1$, e, de facto, é possível determinar d_2 de forma a que os divisores elementares de AD sejam os referidos acima.

Desta forma, D e AD possuem os mesmos divisores elementares e são, portanto, semelhantes. Como, além disso, possuem um divisor elementar linear, pelo lema 2.6, existe $S \in SL(n,F)$ tal que $AD = SDS^{-1}$.

Desta forma

$$A = SDS^{-1}D^{-1}, \quad S, D \in SL(n,F),$$

sendo, portanto, um comutador multiplicativo de matrizes em $SL(n,F)$.

É necessário, no entanto, fazer ainda diversas considerações sobre a existência de tal elemento δ.

Um elemento δ nas condições desejadas existirá sempre que F possua um número infinito de elementos.

Observe-se que como $c(\delta) = \delta^{1-n}a^{-1}$, com $a = f^{\frac{(n-1)(n-2)}{2}} \in F$, a equação $c(\delta) = \delta$ é uma equação polinomial que possui um número finito de soluções. Seja $C^{(1)}$ esse conjunto de soluções. Analogamente, $c(\delta) = f^{n-2}\delta$ é, também, uma equação polinomial que possui um número finito de soluções. Seja $C^{(2)}$ esse conjunto de soluções. Assim, se F possui um número infinito de elementos, é sempre possível escolher δ que não pertence a $C^{(1)} \cup C^{(2)}$.

Portanto, se F possui um número infinito de elementos, A será sempre um comutador multiplicativo de matrizes em $SL(n,F)$.

Para completar a demonstração, suponha-se que F possui característica $p \neq 0$ e considerem-se os casos particulares seguintes:

Caso 4.1.: $f = g$.

Suponha-se, inicialmente que $f^2 \neq 1$ e tome-se $\delta = 1$. Considere-se os seguintes conjuntos:

$$C^{(1)} = \{a \in F\backslash\{0\} : \quad c(a) = a\},$$

$$C^{(2)} = \left\{a \in F\backslash\{0\} : \quad c(a) = f^{n-2}a\right\}.$$

Ver-se-á, de seguida, que $1 \notin C^{(1)} \cup C^{(2)}$. Se $c(1) = 1$ ou se $c(1) = f^{n-2}$ obtém-se que $f^2 = 1$, o que é absurdo.

De facto, se $c(1) = 1$, então

$$f^{\frac{(n-1)(n-2)}{2}} = 1.$$

Mas a igualdade anterior é equivalente a

$$f^{\frac{n(n-3)}{2}} f = 1$$

e, uma vez que, $f^{n-1}g = 1$, e se $f = g$, vem que $f^n = 1$ e, então

$$\left((f^n)^{n-3}\right)^{1/2} f = 1^{1/2} f = 1.$$

Da igualdade anterior vem que $f = \pm 1$ e, portanto, $f^2 = 1$, o que contradiz a hipótese de $f^2 \neq 1$. Note-se que $1^{1/2}$ tem o significado de $2-$ésima raiz da identidade de 1, que em qualquer corpo é 1 ou -1.

Semelhantemente, se $c(1) = f^{n-2}$, então

$$f^{\frac{(n-1)(n-2)}{2}} f^{n-2} = 1.$$

Mas igualdade equivale a

$$f^{\frac{(n-1)n}{2}} f^{-1} = \left((f^n)^{n-1}\right)^{1/2} f^{-1} = 1$$

e tendo em conta que $f^n = 1$, tem-se que $f^{-1} = \pm 1$, de onde se retira que $f^2 = 1$. Uma vez mais, a suposição que $c(1) = f^{n-2}$, contradiz a hipótese de $f^2 \neq 1$.

Assim, se $f^2 \neq 1$, existe $\delta = 1$ tal que $\delta(1) \neq 1$ e $\delta(1) \neq f^{n-2}\delta$. Verificam-se, assim, (2.18), (2.19) e (2.20) e, portanto, A é um comutador multiplicativo de matrizes em $SL(n, F)$.

Se $f^2 = 1$, então $A_r = C(\lambda^2 - 2f\lambda + f^2) \in SL(2, F)$ e, pelo Caso 1, é um comutador multiplicativo de matrizes em $SL(2, F)$, digamos (W, Z).

Note-se que, se $f^2 = 1$, então $f = 1$ ou $f = -1$.

Se $f = 1$, então $A = I_{n-2} \oplus A_r$. Definindo $X = I_{n-2} \oplus W,\ Y = I_{n-2} \oplus Z \in SL(n, F)$, tem-se que $A = XYX^{-1}Y^{-1}$ e é, portanto, um comutador multiplicativo de matrizes em $SL(n, F)$.

Se $f = -1$, observe-se que -1 é uma $2-$ésima raiz primitiva da identidade. Além disso, por hipótese, o corpo F possui característica p, com p primo e, portanto a equação $x^2 + y^2 = -1$ possui sempre solução $x, y \in F$. Verificam-se, assim, as condições do teorema 2.1 e então $-I_2$ é um comutador multiplicativo de matrizes em $SL(2, F)$, digamos (P, Q).

Desta forma, $A = -I_{n-2} \oplus A_r = (-I_2) \oplus \cdots \oplus (-I_2) \oplus A_r$ e, definindo,

$$X = \underbrace{P \oplus P \oplus \cdots \oplus P}_{\frac{n-2}{2} \text{ factores}} \oplus W, \quad Y = \underbrace{Q \oplus Q \oplus \cdots \oplus Q}_{\frac{n-2}{2} \text{ factores}} \oplus Z, \in SL(n, F),$$

tem-se que $A = XYX^{-1}Y^{-1}$, sendo, portanto, um comutador multiplicativo de matrizes em $SL(n, F)$.

É importante fazer a observação que, como $f = -1$ e $f^n = 1$, obtém-se que n é par e o factor $\frac{n-2}{2}$ está bem definido.

Fica, assim, terminada a demonstração do Caso 4.1.

Caso 4.2.: $f \neq g$ e n par.

Será demonstrado que existe $\delta \in \{1, f, f^2\}$ nas condições desejadas.

Com objectivo de tornar a notação mais ligeira dir-se-á que um elemento não nulo $\delta \in F$ é *admissível* se verificar (2.19), isto é, δ é *admissível* se $c(\delta) \neq \delta$.

Se $1, f$ são ambos não admissíveis, então $c(1) = 1$ e $c(f) = f$. Mas então,

$$f^{\frac{(n-1)(n-2)}{2}} = f^{\frac{(n-1)(n-2)}{2}} f^{n-1} f = 1$$

de onde se conclui que $f^n = 1$. Isso contradiz o facto de $f^{n-1}g = 1$ e $f \neq g$. Conclui-se então que 1 e f não podem ser ambos não admissíveis e, portanto, F possui elementos admissíveis.

Suponha-se que δ' é um elemento admissível. Então, uma das seguintes possibilidades verifica-se:

(i) $c(\delta') \neq f^{n-2}\delta'$;

(ii) $c(\delta') = f^{n-2}\delta'$, $f\delta'$ é admissível e $c(f\delta') \neq f^{n-2}(f\delta')$;

(iii) $c(\delta') = f^{n-2}\delta'$, $f\delta'$ é admissível e $c(f\delta') = f^{n-2}(f\delta')$;

(iv) $c(\delta') = f^{n-2}\delta'$, $f\delta'$ é não admissível.

Se (iii) se verificar, tem-se que

$$c(\delta') = f^{n-2}\delta', \ c(f\delta') \neq f\delta', \ c(f\delta') = f^{n-2}f\delta'.$$

Como $f\delta' \neq 0$, tem-se que

$$f^{\frac{(n-1)(n-2)}{2}} (f\delta')^{n-1} c(f\delta') = 1. \tag{2.21}$$

Por outro lado, tem-se que $c(\delta') = f^{n-2}\delta'$ e, para $\delta' \neq 0$,

$$f^{\frac{(n-1)(n-2)}{2}}(\delta')^{n-1}c(\delta') = 1$$

o que equivale a

$$f^{\frac{(n-1)(n-2)}{2}}f^{n-2}(\delta')^{n} = 1. \tag{2.22}$$

Mas de (2.21) vem que

$$f^{\frac{(n-1)(n-2)}{2}}f^{n-1}(\delta')^{n-1}f^{n-2}(f\delta') = 1$$

e, portanto,

$$\underbrace{f^{\frac{(n-1)(n-2)}{2}}f^{n-2}(\delta')^{n}}_{=1, \text{ por (2.22)}}f^{n-1}(\delta')^{-1}(f\delta') = 1,$$

de onde se obtém que $f^n = 1$, o que, uma vez mais contraria a hipótese de $f^{n-1}g = 1$ e $f \neq g$. Assim, (iii) não se verifica.

Se (iv) se verificar, então para $\delta' \neq 0$, tem-se que

$$f^{\frac{(n-1)(n-2)}{2}}(\delta')^{n-1}c(\delta') = 1,$$

mas como $c(\delta') = f^{n-2}\delta'$, obtém-se que

$$f^{\frac{(n-1)(n-2)}{2}}(\delta')^{n}f^{n-2} = 1. \tag{2.23}$$

Por outro lado, para $f\delta' \neq 0$, tem-se

$$f^{\frac{(n-1)(n-2)}{2}}(f\delta')^{n-1}c(f\delta') = 1. \tag{2.24}$$

Mas, então, a igualdade (2.24) equivale a

$$f^{\frac{(n-1)(n-2)}{2}}(f\delta')^{n-1}f\delta' = 1$$

ou seja,

$$\underbrace{f^{\frac{(n-1)(n-2)}{2}}f^{n-2}(\delta')^{n}}_{=1, \text{ por (2.23)}}f^{2} = 1$$

de onde se deduz que $f^2 = 1$.

Como n é par, $n = 2k$ para algum k inteiro positivo e como $f^{n-1}g = 1$ tem-se que $(f^2)^k f^{-1} g = 1$, de onde se conclui que $f = g$. Tal situação contraria a hipótese e, portanto, (iv) também não se verifica.

Assim, ou se verifica (i) ou (ii) o que, em qualquer das situações, garante a existência de uma solução de (2.19) e (2.20).

Tendo a garantia da existência de solução para as equações anteriores, conclui-se que, quando $f \neq g$ e n par, A é um comutador multiplicativo de matrizes em $SL(n, F)$.

Caso 4.3.: $f \neq g$; n ímpar.

Neste caso não será demonstrada a existência de um elemento δ conveniente.

Sob estas condições, A é semelhante em $GL(n, F)$ a uma matriz

$$A_1 = fI_{n-2} \oplus \begin{bmatrix} f & 1 \\ 0 & g \end{bmatrix}.$$

Assim, existe $U \in SL(n, F)$ tal que $A = UA_1U^{-1}$.

Seja

$$D = [u] \oplus [fu] \oplus [f^2u] \oplus \cdots \oplus [f^{n-1}u]$$

onde $u = f^{-(n-1)/2}$, e note-se que $|D| = u^n f^{\frac{n(n-1)}{2}} = f^{-\frac{n(n-1)}{2}} f^{\frac{n(n-1)}{2}} = 1$ e, portanto, $D \in SL(n, F)$.

Note-se que

$$A_1D = [fu] \oplus [f^2u] \oplus \cdots \oplus \begin{bmatrix} f^{n-1}u & * \\ 0 & \underbrace{f^{n-1}ug}_{=u} \end{bmatrix}$$

e que os divisores elementares de D e A_1D coincidem e são

$$\lambda - u,\ \lambda - fu,\ \ldots, \lambda - f^{n-1}u.$$

Desta forma, D e A_1D são semelhantes e possuem um divisor elementar linear comum. Então, pelo lema 2.6, existe uma matriz $S \in SL(n, F)$ tal que $A_1D = SDS^{-1}$.

Conclui-se assim que $A_1 = SDS^{-1}D^{-1}$ e, portanto, é um comutador multiplicativo de matrizes em $SL(n, F)$.

Da mesma forma, como $A = UA_1U^{-1}$, vem que

$$A = U(SDS^{-1}D^{-1})U^{-1} = (USU^{-1})(UDU^{-1})(US^{-1}U^{-1})(UD^{-1}U^{-1})$$

e é, também um comutador multiplicativo de matrizes em $SL(n, F)$.

Fica, assim, concluída a demonstração do teorema 2.2 quando F não é $GF(4)$ ou $GF(5)$.

■

Apresenta-se de seguida, a demonstração do **teorema 2.2** para o caso específico $F = GF(5)$.

Demonstração

Note-se, inicialmente, que o corpo $GF(5)$ pode ser entendido como formado pelos elementos $0, 1, 2, 3, 4$.

À semelhança do que foi feito atrás, o objectivo desta secção é demonstrar que, se $A \in SL(n, GF(5))$, então A é um comutador multiplicativo de matrizes em $SL(n, GF(5))$.

Suponha-se, sem perda de generalidade, porque a propriedade ser um comutador multiplicativo de matrizes é invariante por semelhança, que A coincide com a sua forma normal invariante:

$$A = F_I(A) = A_1 \oplus \cdots \oplus A_m,$$

onde cada $A_i \in GL(j(i), GF(4))$ é a matriz companheira de um polinómio com coeficientes em $GF(5)$.

Observe-se que, usando transformações de semelhança, é possível rearranjar os blocos da matriz A de forma a que $|A_{i_1} \cdots A_{i_k}| \neq 1$ sempre que $\{i_1, \ldots, i_k\} \neq \phi$ é subconjunto próprio de $\{1, 2, \ldots, m\}$.

Com esta suposição adicional e para que $|A| = 1$, existem apenas quatro possibilidades para a estrutura de A :

$m = 1, \quad |A_1| = 1;$

$m = 2, \quad |A_1| = 2, = |A_2| = 3$ ou $|A_1| = |A_2| = 4;$

$m = 3, \quad |A_1| = |A_2| = 2, |A_3| = 4$ ou $|A_1| = |A_2| = 3, |A_3| = 4;$

$m = 4, \quad |A_1| = |A_2| = |A_3| = |A_4| = 2$ ou $|A_1| = |A_2| = |A_3| = |A_4| = 3.$

A demonstração será divida em diversos casos, dependendo do valor de m.

Se $m = 1$, escolha-se $\rho \in GF(5)$ tal que $\rho^2 \neq 1$ e $\rho^2 \neq 0$. Pelo lema 2.4, existe uma matriz standard $D \in SL(n, GF(5))$ com $d_1 = \rho$ e tal que os divisores elementares de D e de AD são

$$\lambda - \rho,\ \lambda - \rho^{-1},\ (\lambda - 1)^{n-2}.$$

Desta forma, AD e D são semelhantes e possuem um divisor elementar (linear) comum. Então, pelo lema 2.6, existe $S \in SL(n, GF(5))$ tal que $AD = SDS^{-1}$. Mas então, $A = SDS^{-1}D^{-1}$ e é, assim, um comutador multiplicativo de matrizes em $SL(n, GF(5))$.

No argumento anterior supõe-se, obviamente que $n \geq 2$. O caso em que $n = 1$ é trivial: $A = [1] = (I_1, I_1)$.

Note-se, ainda, que esta parte da demonstração é, também, válida quando a matriz A possui entradas em $GF(4)$.

Se $m \geq 2$, tome-se um elemento não nulo $\delta_1 \in GF(5)$ e, para $i \in \{1, 2, \ldots, m\}$, defina-se $\delta_{i+1} = |A_i|\delta_i$. Tome-se, ainda, $\gamma_{i,1}$ e $\gamma_{i,2}$ tais que $\delta_i, \delta_{i+1}, \gamma_{i,1}$ e $\gamma_{i,2}$ sejam quatro elementos não nulos e distintos de $GF(5)$. Seja, ainda, $e(i)$ um inteiro tal que $0 \leq e(i) \leq j(i) - 1$.

Pelo lema 2.4 existem matrizes standard $D_i \in GL(j(i), GF(5))$, $i \in \{1, 2, \ldots, m\}$, com $d_1 = \delta_i$, com divisores elementares

$$\lambda - \delta_i,\ (\lambda - \gamma_{i,1})^{e(i)},\ (\lambda - \gamma_{i,2})^{j(i)-1-e(i)}$$

e tal que os divisores elementares de A_iD_i são

$$\lambda - \delta_{i+1},\ (\lambda - \gamma_{i,1})^{e(i)},\ (\lambda - \gamma_{i,2})^{j(i)-1-e(i)}.$$

Fazendo $D = D_1 \oplus \cdots \oplus D_m$, tem-se que D e AD são semelhantes uma vez que possuem os mesmos divisores elementares, em particular, um divisor linear. Mas então, pelo lema 2.6, tem-se que existe $S \in SL(n, GF(5))$ tal que $A = SDS^{-1}D^{-1}$. Desta forma, A é um comutador multiplicativo de matrizes .

Para que A seja um comutador multiplicativo de matrizes em $SL(n, GF(5))$ é necessário que $|D| = 1$.

Para tal, é necessário escolher $\delta_1, \gamma_{i,1}, \gamma_{i,2} \in GF(5)$ e inteiros $e(i)$, $i \in \{1, 2, \ldots, m\}$, de forma a que

$$|D| = \prod_{i=1}^{m} \left(\delta_i (\gamma_{i,1})^{e(i)} (\gamma_{i,2})^{j(i)-1-e(i)}\right) = 1. \tag{2.25}$$

Em qualquer um dos três casos restantes, o objectivo é determinar $\delta_1, \gamma_{i,1}, \gamma_{i,2} \in GF(5)$ e inteiros $e(i)$, $i \in \{1, 2, \ldots, m\}$, de forma a que satisfaçam (2.25) ou reduzir o caso a um outro já abordado.

Se $m = 2$ e $|A_1| = |A_2| = 4$, tome-se $\gamma_{1,1} = \gamma_{2,1} = 2\delta_1$ e $\gamma_{1,2} = \gamma_{2,2} = 3\delta_1$.

Então, se $e = e(1) + e(2)$,

$$|D| = \delta_1^n 3^{n+2e},$$

onde $0 \leq e \leq n-2$.

Escolhendo $\delta_1 = 3$ e $e \in \{0, 1\}$ por forma a que $2n + 2e \equiv 0 (\text{mod } 4)$, tem-se que

$$|D| = 3^{2n+2e} = 3^{4k} = 81^k = 1, \quad (k \text{ inteiro positivo}).$$

Observe-se que $81 \equiv 1 (\text{mod } 5)$.

Tem-se, então que, se $m = 2$ e $|A_1| = |A_2| = 4$, a equação (2.25) é possível e, portanto, A é um comutador multiplicativo de matrizes em $SL(n, GF(5))$.

Se $m = 2$ e $|A_1| = 2, |A_2| = 3$ tome-se $\gamma_{1,1} = \gamma_{2,1} = 3\delta_1$ e $\gamma_{1,2} = \gamma_{2,2} = 4\delta_1$.

Então, se $e = e(1) + e(2)$,

$$|D| = \delta_1^n 2^{1+2n+e}.$$

Se $n \geq 5$ ou se $n = 3$, tome-se $\delta_1 = 1$ e $e \in \{1, 3\}$ por forma a que $1 + 2n + e \equiv 0 (\text{mod } 4)$.

Desta forma,

$$|D| = 1^n 2^{1+2n+e} = 2^{4k} = 16^k = 1, \quad (k \text{ inteiro positivo}).$$

Tem-se, assim que, se $m = 2$ e $|A_1| = 2, |A_2| = 3$, a equação (2.25) é satisfeita e, portanto, A é um comutador multiplicativo de matrizes em $SL(n, GF(5))$.

Se $n = 2$, então $A = [2] \oplus [3] = C(\lambda - 2) \oplus C(\lambda - 3)$ e, porque $\lambda - 2$ e $\lambda - 3$ são primos entre si, A é semelhante em $SL(2, GF(5))$ a $C((\lambda - 2)(\lambda - 3))$.

Mas, pelo caso já abordado em que $m = 1$, tem-se que $C((\lambda - 2)(\lambda - 3))$ é um comutador multiplicativo de matrizes em $SL(n, GF(5))$ e, sendo A semelhante à matriz anterior, é também um comutador multiplicativo de matrizes em $SL(n, GF(5))$.

O caso em que $n = 4$ requer mais algumas considerações.

Se $n = 4$ e $j(1) = 1,\ j(2) = 3$ então $A = [2] \oplus A_2$ onde $A_2 \in GL(3, GF(5))$ é a matriz companheira de um polinómio de grau 3 e $|A_2| = 3$.

Pelo lema 2.5 é possível encontrar uma matriz standard $D_2 \in SL(3, GF(5))$ com $d_1 = 4$, com divisores elementares

$$\lambda - 4,\ \lambda - 2,\ \lambda - 2$$

tal que os divisores elementares de $A_2 D_2$ são

$$\lambda - 4,\ \lambda - 1,\ \lambda - 2.$$

Fazendo $D = [1] \oplus D_2$ tem-se que $D \in SL(4, GF(5))$ e D e AD possuem os mesmos divisores elementares, em particular, um divisor linear. A conclusão da demonstração neste caso é idêntica às conclusões efectuadas atrás: pelo lema 2.6, existe $S \in SL(4, GF(4))$ tal que $AD = SDS^{-1}$ e, desta forma, A é um comutador multiplicativo de matrizes em $SL(4, GF(4))$.

Se $n = 4$ e $j(1) = 3,\ j(2) = 1$ seja $D_1 \in SL(3, GF(5))$ uma matriz standard, uma vez mais determinada usando o lema 2.5, com $d_1 = 4$, com divisores elementares

$$\lambda - 4,\ \lambda - 3,\ \lambda - 3$$

e tal que os divisores elementares de $A_1 D_1$ são

$$\lambda - 4,\ \lambda - 1,\ \lambda - 3.$$

Seja $D = D_1 \oplus [1] \in SL(4, GF(5))$.

Tem-se que D e AD possuem os mesmos divisores elementares (em particular um divisor linear) e, pelo lema 2.6, existe $S \in SL(4, GF(4))$ tal que $AD = SDS^{-1}$. Assim, $A = SDS^{-1}D^{-1}$ é um comutador multiplicativo de matrizes em $SL(4, GF(4))$.

Para finalizar o estudo do caso em que $n = 4$ e $|A_1| = 2, |A_2| = 3$, resta considerar o caso em que $j(1) = j(2) = 2$.

Se os polinómios característicos de A_1 e A_2 são primos entre si então A é semelhante em $GL(4, GF(5))$ à matriz companheira do polinómio produto dos polinómios característicos de A_1 e A_2. Este caso foi já abordado quando $m = 1$ e, dele, conclui-se que, sob esta condição, A é um comutador multiplicativo de matrizes em $SL(4, GF(4))$.

Suponha-se, agora, que os polinómios característicos de A_1 e A_2 não são primos entre si.

Tendo em conta que $|A_1| = 2, |A_2| = 3$, os valores próprios de A_1 são $r, 2r^{-1}$ e os valores próprios de A_2 são $r, 3r^{-1}$ com $r \in GF(5)$. Assim, A é semelhante a

$$\left[\begin{array}{c|c} C((\lambda - r)(\lambda - 2r^{-1})) & 0 \\ \hline 0 & C((\lambda - r)(\lambda - 3r^{-1})) \end{array}\right]$$

e tendo em conta que as igualdades $r = 2r^{-1}$ e $r = 3r^{-1}$ são impossíveis em $GF(5)$, a matriz A possui divisores elementares lineares e é semelhante em $GL(4, GF(5))$ a:

$$\left[\begin{array}{cccc} C(\lambda - r) & 0 & 0 & 0 \\ 0 & C(\lambda - 2r^{-1}) & 0 & 0 \\ 0 & 0 & C(\lambda - r) & 0 \\ 0 & 0 & 0 & C(\lambda - 3r^{-1}) \end{array}\right]. \tag{2.26}$$

Observe-se, ainda, que para $r = 1, 2, 3, 4$ os polinómios $\lambda - 2r^{-1},\ \lambda - r,\ \lambda - 3r^{-1}$ são primos entre si e portanto, a matriz (2.26) e A são semelhantes a

$$C(\lambda - r) \oplus C((\lambda - 2r^{-1})(\lambda - r)(\lambda - 3r^{-1})).$$

Tem-se então, que a matriz (2.26) e, consequentemente, A é semelhante a

$[1] \oplus C((\lambda - 2)(\lambda - 1)(\lambda - 3))$ se $r = 1$;

$[2] \oplus C((\lambda - 1)(\lambda - 2)(\lambda - 4))$ se $r = 2$;

$[3] \oplus C((\lambda - 1)(\lambda - 3)(\lambda - 4))$ se $r = 3$;

$[4] \oplus C((\lambda - 4)(\lambda - 2)(\lambda - 3))$ se $r = 4$.

Mas, o género das quatro matrizes anteriores foi já abordado no parágrafo em que $j(1) = 1, j(2) = 3$ e, por isso, são comutadores multiplicativos de matrizes em $SL(4, GF(4))$.

Como a matriz A é semelhante a um comutador multiplicativo de matrizes em $SL(4, GF(4))$, tem-se que, pela observação feita no início do capítulo, A é, também, um comutador multiplicativo de matrizes em $SL(4, GF(4))$

Finaliza-se, assim, o caso $m = 2$.

Quando $m = 3$, suponha-se que $A = A_1 \oplus A_2 \oplus A_3$ onde $|A_1| = |A_2| = 2, |A_3| = 4$. Tome-se $\gamma_{1,2}, \gamma_{2,1}, \gamma_{3,2} = 3\delta_1,\ \gamma_{1,1} = 4\delta_1,\ \gamma_{2,2} = \delta_1,\ \gamma_{3,1} = 2\delta_1$. Assim,

$$|D| = \prod_{i=1}^{m} \left(\delta_i(\gamma_{i,1})^{e(i)}(\gamma_{i,2})^{j(i)-1-e(i)}\right)$$

$$= \left(\delta_1\gamma_{1,1}^{e(1)}\gamma_{1,2}^{j(1)-1-e(1)}\right)\left(\delta_2\gamma_{2,1}^{e(2)}\gamma_{2,2}^{j(2)-1-e(2)}\right)\left(\delta_3\gamma_{3,1}^{e(3)}\gamma_{3,2}^{j(3)-1-e(3)}\right)$$

$$= \left(\delta_1(4\delta_1)^{e(1)}(3\delta_1)^{j(1)-1-e(1)}\right)\left(2\delta_1(3\delta_1)^{e(2)}(\delta_1)^{j(2)-1-e(2)}\right)\left(4\delta_1(2\delta_1)^{e(3)}(3\delta_1)^{j(3)-1-e(3)}\right)$$

$$= \delta_1^n 3^{j(1)-1-e(1)+e(2)+j(3)-1-e(3)} 4^{e(1)} 2^{e(3)} 8$$

$$= \delta_1^n 3^{j(1)-2+e(2)+j(3)} 4^{e(1)} 3^{-e(1)} 2^{e(3)} 3^{-e(3)} 3$$

$$= \delta_1^n 3^{j(1)-2+e(2)+j(3)} 3^{e(1)} 4^{e(3)} 3$$

$$= \delta_1^n 3^{j(1)-2+e(2)+j(3)} 3^{e(1)} 3^{2e(3)} 3$$

$$= \delta_1^n 3^{j(1)-2+e(2)+j(3)+e(1)+2e(3)+1}$$

$$= \delta_1^n 3^{j(1)-1+e(2)+j(3)+e(1)+2e(3)}.$$

Finalmente, multiplicando a expressão anterior por $81 = 3^4$ (corresponde à identidade em $GF(5)$) vem que a expressão (2.25) toma a forma

$$|D| = \delta_1^n 3^{3+j(1)+j(3)+e(1)+e(2)+2e(3)}. \tag{2.27}$$

Sem perda de generalidade, suponha-se que $j(1) \geq j(2)$. Na seguinte tabela indicam-se os valores de $\delta_1, e(1), e(2), e(3)$ como funções de $j(1), j(2), j(3)$ e que satisfazem (2.27). Os elementos $j(i)$ que não estão completamente determinados podem assumir valores arbitrários desde que não entrem em conflito com outras indicações. Os elementos $e(i)$ que não estão totalmente determinados podem ser escolhidos de forma a que

$$3 + j(1) + j(3) + e(1) + e(2) + 2e(3) \equiv 0 (\text{mod } 4).$$

Dessa forma,

$$|D| = \delta_1^n 3^{4k} = \delta_1^n 81^k = \delta_1^n, \quad (k \text{ inteiro}).$$

Caso	$j(1)+j(2)$	$j(1)$	$j(2)$	$j(3)$	δ_1	$e(1)$	$e(2)$	$e(3)$
i	≥ 5				1	$< j(1)$	$< j(2)$	0
ii	4	3 ou 2	1 ou 2	≥ 2	1	$< j(1)$	$< j(2)$	$< j(3)$
iii	4	3 ou 2	1 ou 2	1	1	$< j(1)$	$< j(2)$	0
iv	3	2	1	≥ 2	1	$0, 1$	$0, 1$	$0, 1$
v	3	2	1	1				
vi	2	1	1	par	1	0	0	$j(3)/2$
vii	2	1	1	ímpar	3	0	0	0

Note-se que no caso (i) da tabela, uma vez que $e(1) + e(2)$ pode ser qualquer inteiro de entre $0, 1, \ldots, j(1) + j(2) - 2$ e, como $j(1) + j(2) \geq 5$, pode encontrar-se $e(1)$ e $e(2)$ tais que $e(1) + e(2) \equiv 0, 1, 2, 3 (\text{mod } 4)$. Observe-se que, neste caso, $j(1) + j(2) - 2 \geq 3$.

No caso (v), a matriz A é semelhante em $GL(n, GF(5))$ a alguma matriz $C(\lambda^2 + u\lambda + 2) \oplus C((\lambda - 2)(\lambda - 4))$. Este caso foi já abordado atrás quando $m = 2$.

No caso (vi), note-se que

$$2e(3) + 3 + j(1) + j(3) = 4 + 4(j(3)/2) \equiv 0 (\text{mod } 4).$$

No caso (vii), note-se que

$$n + 3 + j(1) + j(3) = 8 + 4((j(3) - 1)/2) \equiv 0 (\text{mod } 4).$$

Tem-se assim, que é sempre possível escolher $\delta_1, e(1), e(2), e(3)$ tais que $|D| = 1$. Desta forma, quando $m = 3$ e $|A_1| = |A_2| = 2, |A_3| = 4$, A é um comutador multiplicativo de matrizes em $SL(n, GF(4))$.

Observe-se que, se $A = A_1 \oplus A_2 \oplus A_3$ onde $|A_1| = |A_2| = 3, |A_3| = 4$, então A^{-1} é uma matriz do tipo $A^{-1} = A_1^{-1} \oplus A_2^{-1} \oplus A_3^{-1}$ onde $|A_1^{-1}| = |A_2^{-1}| = 2, |A_3^{-1}| = 4$ e, pelo que foi escrito anteriormente, A^{-1} é um comutador multiplicativo de matrizes em $SL(n, GF(4))$, por exemplo, $A^{-1} = (X, Y)$. Mas, então, $A = (Y, X)$ e é, portanto, um comutador multiplicativo de matrizes em $SL(n, GF(4))$.

Finaliza-se, assim, o estudo do caso $m = 3$.

Será, finalmente, abordado o caso em que $m = 4$.

Suponha-se, inicialmente, que $A = A_1 \oplus A_2 \oplus A_3 \oplus A_4$ onde $|A_1| = |A_2| = |A_3| = |A_4| = 2$. Tome-se $\gamma_{1,1} = \gamma_{2,1} = 3\delta_1,\ \gamma_{1,2} = \gamma_{4,2} = 4\delta_1,\ \gamma_{2,2} = \gamma_{3,2} = \delta_1,\ \gamma_{3,1} = \gamma_{4,1} = 2\delta_1$ e, utilizando o mesmo raciocínio do caso em que $m = 3$, tem-se que (2.25) toma a forma:

$$|D| = \delta_1^n 3^{2(1+j(1)+j(4))-e(1)+e(2)+3e(3)+e(4)}.$$

Se dois dos elementos $j(i)$ são maiores do que 1, sem perda de generalidade suponha-se que são $j(2), j(4)$, tome-se $\delta_1 = 1,\ e(1) = e(3) = 0$ e $e(2), e(3)$ de entre $\{0, 1\}$ por forma a que

$$e(2) + e(4) + 2(1 + j(1) + j(4)) \equiv 0(\text{mod } 4).$$

Sob essas condições, $|D| = 1$ e, portanto, A é um comutador multiplicativo de matrizes em $SL(n, GF(4))$.

Se apenas um dos elementos $j(i)$ é diferente de 1, sem perda de generalidade suponha-se que $j(1) = j(2) = j(4) = 1$ e $j(3) > 1$, tome-se $\delta_1 = 3^k$ com $k \in \{0, 1, 2, 3\}$ e $e(3)$ tal que $0 \leq e(3) \leq j(3) - 1$ por forma a que

$$k(3 + j(3)) + 3e(3) + 6 \equiv 0(\text{mod } 4).$$

Desta forma, com $e(1) = e(2) = e(4) = 0$,

$$|D| = 3^{kn} 3^{2(1+1+1)+3e(3)} = 3^{k(3+j(3))+3e(3)+6} \equiv 1(\text{mod } 5).$$

As escolhas adequadas para k e $e(3)$ são:

$k = 2$ e $e(3) = 0$ quando $j(3) \equiv 0, 2(\text{mod } 4)$;

$k = 1$ e $e(3) = 0$ quando $j(3) \equiv 3(\text{mod } 4)$;

$k = 0$ e $e(3) = 2$ quando $j(3) \equiv 1(\text{mod } 4)$ mas $j(3) \neq 1$;

Com tal escolha, tem-se que $|D| = 1$ e, assim, A é um comutador multiplicativo de matrizes em $SL(n, GF(4))$.

Se todos os elementos $j(i)$ são iguais a 1, então A é escalar e o teorema 2.1 permite concluir que A é um comutador multiplicativo de matrizes em $SL(n, GF(4))$.

No início do estudo do caso em que $m = 4$ fez-se a suposição que $A = A_1 \oplus A_2 \oplus A_3 \oplus A_4$ onde $|A_1| = |A_2| = |A_3| = |A_4| = 2$. No entanto, se $A = A_1 \oplus A_2 \oplus A_3 \oplus A_4$ onde $|A_1| = |A_2| = |A_3| = |A_4| = 3$, tem-se que $A^{-1} = A_1^{-1} \oplus A_2^{-1} \oplus A_3^{-1} \oplus A_4^{-1}$ onde $|A_1^{-1}| = |A_2^{-1}| = |A_3^{-1}| = |A_4^{-1}| = 2$ e, pelo que foi escrito anteriormente, A^{-1} é um comutador multiplicativo de matrizes em $SL(n, GF(4))$, por exemplo (X, Y). Mas então, $A = (Y, X)$ é uma comutador multiplicativo de matrizes em $SL(n, GF(4))$.

Fica assim concluída a prova do teorema 2.2 quando $F = GF(5)$.

■

Para finalizar esta secção, apresenta-se a demonstração do teorema 2.2 para o caso particular $F = GF(4)$.

Demonstração

O corpo $GF(4)$ é constituído pelos elementos $0, 1, \theta, \theta + 1$, distintos, onde $\theta^2 = \theta + 1$. De facto, $\theta^2 \neq \theta$, caso contrário $\theta = 1$. Mas, como também se tem $\theta^2 \neq 0$ e $\theta^2 \neq 1$, tem-se que $\theta^2 = \theta + 1$.

À semelhança da demonstração anterior, suponha-se, sem perda de generalidade, porque a propriedade ser um comutador multiplicativo de matrizes é invariante por semelhança, que A coincide com a sua forma normal invariante:

$$A = F_I(A) = A_1 \oplus \cdots \oplus A_m,$$

onde cada $A_i \in GL(j(i), GF(4))$ é a matriz companheira de um polinómio com coeficientes em $GF(4)$.

Observe-se, uma vez mais, que, usando transformações de semelhança, é possível rearranjar os blocos da matriz A de forma a que $|A_{i_1} \cdots A_{i_k}| \neq 1$ sempre que $\{i_1, \ldots, i_k\} \neq \phi$ é subconjunto próprio de $\{1, 2, \ldots, m\}$.

Com esta suposição adicional e tendo em conta que $|A| = 1$, obtém-se apenas três possibilidades para a estrutura de A :

$m = 1, \quad |A_1| = 1;$

$m = 2, \quad |A_1| = \theta, \ |A_2| = \theta + 1;$

$m = 3, \quad |A_1| = |A_2| = |A_3| = \theta$ ou $|A_1| = |A_2| = |A_3| = \theta + 1.$

Se $m = 1$, a demonstração feita para $GF(5)$ é válida também para $GF(4)$ e conclui-se que $A = A_1$ é um comutador multiplicativo de matrizes em $SL(n, GF(4))$.

Se $m = 2$ e $|A_1| = \theta$ e $|A_2| = \theta + 1$, pelo lema 2.4, existe uma matriz standard $D_1 \in GL(j(1), GF(4))$ com $d_1 = \theta$, com divisores elementares

$$\lambda - \theta,\ (\lambda - 1)^{j(1)-1}$$

e tal que os divisores elementares de $A_1 D_1$ são

$$\lambda - \theta^2,\ (\lambda - 1)^{j(1)-1}.$$

Pelo mesmo lema, existe uma outra matriz standard $D_2 \in GL(j(2), GF(4))$ com $d_1 = \theta^2$, com divisores elementares

$$\lambda - \theta^2,\ (\lambda - 1)^{j(2)-1}$$

e tal que os divisores elementares de $A_2 D_2$ são

$$\lambda - \underbrace{\theta}_{\theta^2(\theta+1)},\ (\lambda - 1)^{j(2)-1}.$$

Fazendo $D = D_1 \oplus D_2$, tem-se que $D \in SL(n, GF(4))$ e D e AD possuem os mesmos divisores elementares. Mas, então, D e AD são semelhantes e possuem um divisor elementar linear, é válido o lema 2.6 e, portanto, existe uma matriz $S \in SL(n, GF(4))$ tal que $AD = SDS^{-1}$.

Tem-se assim que $A = SDS^{-1}D^{-1}$ e é, desta forma, um comutador multiplicativo de matrizes em $SL(n, GF(4))$.

Se $m = 3$, suponha-se que $|A_1| = |A_2| = |A_3| = \theta$.

Inicialmente estude-se o caso em que os elementos $j(1), j(2), j(3)$ não são distintos (mod 3) entre si. Por exemplo, $j(1) \equiv j(3) (\text{mod } 3)$.

Pelo lema 2.4, existe uma matriz standard $D_1 \in GL(j(1), GF(4))$ com $d_1 = 1$, com divisores elementares

$$\lambda - 1,\ (\lambda - \theta^2)^{j(1)-1}.$$

e tal que os divisores elementares de $A_1 D_1$ são

$$\lambda - \theta,\ (\lambda - \theta^2)^{j(1)-1}.$$

Pelo mesmo lema, existe uma outra matriz standard $D_2 \in GL(j(2), GF(4))$ com $d_1 = \theta$, com divisores elementares

$$\lambda - \theta,\ (\lambda - 1)^{j(2)-1}$$

e tal que os divisores elementares de $A_2 D_2$ são

$$\lambda - \theta^2,\ (\lambda - 1)^{j(2)-1}.$$

Usando o mesmo resultado, existe uma terceira matriz standard $D_3 \in GL(j(3), GF(4))$ com $d_1 = \theta^2$, com divisores elementares

$$\lambda - \theta^2,\ (\lambda - \theta)^{j(3)-1}$$

e tal que os divisores elementares de $A_3 D_3$ são

$$\lambda - 1,\ (\lambda - \theta)^{j(3)-1}.$$

Fazendo $D = D_1 \oplus D_2 \oplus D_3$, tem-se que

$$|D| = (\theta^2)^{j(1)-1}\theta\theta^2\theta^{j(3)-1} = \theta^{2j(1)+j(3)} \equiv \theta^{2j(1)+j(1)+3\alpha} (\text{mod } 3), \quad \alpha \in \mathbb{Z}$$

$$\equiv \theta^3 \equiv 1 (\text{mod } 3)$$

e, portanto, $D \in SL(n, GF(4))$ e D e AD possuem os mesmos divisores elementares.

Desta forma, A e AD são semelhantes e, além disso, possuem um divisor elementar linear. É, então, válido o lema 2.6 e, então, existe uma matriz $S \in SL(n, GF(4))$ tal que $AD = SDS^{-1}$.

Tem-se assim que $A = SDS^{-1}D^{-1}$ e é, desta forma, um comutador multiplicativo de matrizes em $SL(n, GF(4))$.

Suponha-se, agora, que $j(1), j(2), j(3)$ são distintos (mod 3), por exemplo, $j(1) \equiv 2 (\text{mod } 3)$, $j(2) \equiv 0 (\text{mod } 3)$, $j(3) \equiv 1 (\text{mod } 3)$.

Desta forma, $j(1) \geq 2$ e $j(2) \geq 3$.

Pelo lema 2.5, existe uma matriz standard $D_1 \in GL(j(1), GF(4))$ com $d_1 = 1$, com divisores elementares

$$\lambda - 1,\ \lambda - \theta,\ (\lambda - \theta)^{j(1)-2}$$

e tal que os divisores elementares de $A_1 D_1$ são

$$\lambda - 1,\ \lambda - \theta^2,\ (\lambda - \theta)^{j(1)-2}.$$

Ainda pelo lema 2.5, existe uma matriz standard $D_2 \in GL(j(2), GF(4))$ com $d_1 = \theta$, com divisores elementares

$$\lambda - \theta,\ \lambda - \theta^2,\ (\lambda - \theta^2)^{j(2)-2}$$

e tal que os divisores elementares de $A_2 D_2$ são

$$\lambda - \theta,\ \lambda - 1,\ (\lambda - \theta^2)^{j(2)-2}.$$

Mas, pelo lema 2.4, existe uma terceira matriz standard $D_3 \in GL(j(3), GF(4))$ com $d_1 = 1$, com divisores elementares

$$\lambda - 1,\ (\lambda - \theta^2)^{j(3)-1}$$

e tal que os divisores elementares de $A_3 D_3$ são

$$\lambda - \theta,\ (\lambda - \theta^2)^{j(3)-1}.$$

Fazendo $D = D_1 \oplus D_2 \oplus D_3$, tem-se que $D \in SL(n, GF(4))$ e D e AD possuem os mesmos divisores elementares. Completa-se a demonstração da mesma forma: A e AD são semelhantes e, além disso, possuem um divisor elementar linear. Por isso, é válido o lema 2.6 e, então, existe uma matriz $S \in SL(n, GF(4))$ tal que $AD = SDS^{-1}$.

Assim, $A = SDS^{-1}D^{-1}$ é um comutador multiplicativo de matrizes em $SL(n, GF(4))$.

Se $m = 3$ e $A = A_1 \oplus A_2 \oplus A_3$, com $|A_1| = |A_2| = |A_3| = \theta + 1$, então A^{-1} é uma matriz do tipo $A^{-1} = A_1^{-1} \oplus A_2^{-1} \oplus A_3^{-1}$, com $|A_1^{-1}| = |A_2^{-1}| = |A_3^{-1}| = \theta$. Pelo que foi escrito atrás, A^{-1} é um comutador multiplicativo de matrizes em $SL(n, GF(4))$, digamos, $A^{-1} = (X, Y)$. Mas, então, $A = (Y, X)$ e é também um comutador multiplicativo de matrizes em $SL(n, GF(4))$.

Conclui-se, assim, a demonstração do teorema 2.2 quando $F = GF(4)$, concluindo-se também a demonstração geral do mesmo teorema.

■

Com a demonstração do teorema anterior, retira-se a conclusão principal desta secção: se $A \in SL(n, F)$ é não escalar e F possui pelo menos 4 elementos, então A é um comutador multiplicativo de matrizes em $SL(n, F)$.

2.2 Comutadores Multiplicativos com Entradas em $GF(2)$

Nesta secção será determinado em que condições uma matriz $A \in SL(n, GF(2))$ pode ser escrita como um comutador multiplicativo de matrizes

$$(X, Y), \quad \text{onde} \quad X, Y \in SL(n, GF(2)).$$

Observe-se que, como $F = GF(2)$, então $SL(n, GF(2)) = GL(n, GF(2))$. Os dois elementos de $GF(2)$ serão denotados por 0 e 1. O elemento -1, simétrico de 1, será, por vezes, denotado simplesmente por 1.

Será apresentada uma série de lemas que servirá de base à demonstração do resultado principal desta secção, que depende unicamente das dimensões da matriz A: se $n > 2$ e $A \in SL(n, GF(2))$, então A é um comutador multiplicativo de matrizes em $SL(n, GF(2))$.

Lema 2.7. *Para $n \geq 3$, a matriz*

$$M_n = \left[\begin{array}{c|c} J_2 & 0 \\ \hline 0 & J_{n-2} \end{array}\right] \in SL(n, GF(2))$$

é um comutador multiplicativo de matrizes em $SL(n, GF(2))$.

Demonstração

Através de cálculo puro e directo é possível ver que, para $n \in \{3, 4, 5, 6\}$, $M_n = U_n V_n U_n^{-1} V_n^{-1}$, onde

$$U_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}, \qquad V_3 = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix};$$

$$U_4 = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \qquad V_4 = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix};$$

$$U_5 = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}, \qquad V_5 = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix};$$

$$U_6 = \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}, \qquad V_6 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

Para a demonstração do caso em que $n \geq 7$, defina-se, para $k \geq 4$, as seguintes matrizes $R_1(k)$ e $R_2(k)$ de dimensões $k \times k$.

$$R_1(k) = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 1 & 0 & 1 & \cdots & 1 \\ 0 & 0 & 1 & 1 & 1 & \cdots & 1 \\ 0 & 0 & 0 & 1 & 1 & \cdots & 1 \\ 0 & 0 & 0 & 0 & 1 & \cdots & 1 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 0 & 1 \end{bmatrix}, \qquad R_2(k) = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & 1 & 0 & 1 & \cdots & 1 \\ 0 & 0 & 1 & 1 & 1 & \cdots & 1 \\ 0 & 0 & 0 & 1 & 1 & \cdots & 1 \\ 0 & 0 & 0 & 0 & 1 & \cdots & 1 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 0 & 1 \end{bmatrix}.$$

Note-se que os polinómios mínimos de $R_1(k)$ e de $R_2(k)$ coincidem e são $(\lambda - 1)^k$. Ir-se-á verificar que os polinómios mínimo e característico de $R_1(k)$, e consequentemente de $R_2(k)$, coincidem.

Observe-se que o menor de $\lambda I_k - R_2(k)$ que se obtém retirando a primeira coluna e a última linha é um polinómio $p(\lambda)$ para o qual $p(1) = 1$ e, portanto, 1 não é raiz desse polinómio. Observe-se, também, que o menor de $\lambda I_k - R_2(k)$ que se obtém retirando a primeira linha e a primeira coluna é $q(\lambda) = (\lambda - 1)^{k-1}$ e $q(1) = 0$.

Como 1 é raiz de $p(\lambda)$ mas não de $q(\lambda)$, e como em $GF(2)$ só existem dois elementos distintos, tem-se que o máximo divisor comum dos menores de ordem $k - 1$ de $\lambda I_k - R_2(k)$ é 1.

Assim, o último polinómio invariante não constante, que é o polinómio mínimo, é também o polinómio característico: $(\lambda-1)^k$.

O mesmo argumento é válido para $R_1(k)$.

Seja ainda,

$$R_3 = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}.$$

A matriz R_3 é semelhante em $SL(n, GF(2))$ à matriz

$$\begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

que possui como polinómios invariantes $1,\ \lambda-1,\ (\lambda-1)^2$ e, portanto, os divisores de elementares de R_3 são $\lambda-1, (\lambda-1)^2$.

Considere-se, agora, o caso em que $n \geq 8$ e n é par.

Seja $j = \frac{n-2}{2}$ e observe-se que, desta forma, $j \geq 3$ e $n-j \geq 5$.

Defina-se $R_4 = R_3 \oplus I_{j-3} \oplus R_1(n-j)$. Os divisores elementares de R_4 são

$$\lambda-1,\ (\lambda-1)^2, \underbrace{\lambda-1, \ldots, \lambda-1}_{j-3 \text{ factores}},\ (\lambda-1)^{n-j}.$$

Seja, também, $S = [s_{i,t}] \in GF(2)^{n\times n}$ definida da seguinte forma:

$s_{i,i} = 1, \quad i \in \{1, 2, \ldots, j+1, j+3, \ldots, n\}$;

$s_{j+1,j+2} = s_{j+3,j+2} = \cdots = s_{j+2,t} = 1, \quad t \in \{j+3, j+4, \ldots, n\}$;

Todas as restantes entradas de S são nulas.

Assim, de forma a visualizar melhor a matriz S, tem-se que $S = I_j \oplus B$, onde B é a matriz:

$$B = \begin{bmatrix} 1 & 1 & 0 & \cdots & \cdots & 0 \\ 0 & 0 & 1 & 1 & \cdots & 1 \\ \vdots & 1 & 1 & 0 & \cdots & 0 \\ \vdots & & 0 & 1 & \ddots & \vdots \\ \vdots & & & \ddots & \ddots & 0 \\ 0 & \cdots & \cdots & \cdots & 0 & 1 \end{bmatrix}.$$

Observe-se que S pode ser decomposta como um produto de matrizes elementares. De facto,

$$S = S_{j+2,n}(1)S_{j+2,n-1}(1)\cdots S_{j+2,j+4}(1)S_{j+3,j+2}(1)S_{j+2,j+3}S_{j+1,j+2}(1)$$

e, uma vez que $|S| = |B| = 1$, tem-se que $S \in SL(n, GF(2))$. Além disso, após cálculo directo, tem-se que

$$S(M_nR_4) = (J_{j+2} \oplus J_2 \oplus I_{n-j-4})S.$$

Desta forma, $S(M_nR_4)S^{-1} = J_{j+2} \oplus J_2 \oplus I_{n-j-4}$ e, portanto, M_nR_4 e $J_{j+2} \oplus J_2 \oplus I_{n-j-4}$ são semelhantes e possuem os mesmos divisores elementares,

$$(\lambda-1)^{j+2},\ (\lambda-1)^2,\ \underbrace{\lambda-1,\ \ldots,\lambda-1}_{n-j-4 \text{ factores}}.$$

Mas como $j+2 = n-j = \frac{n+2}{2}$, tem-se que M_nR_4 e R_4 possuem os mesmos divisores elementares e, portanto, existe $Q \in SL(n, GF(2))$ tal que $QR_4Q^{-1} = M_nR_4$. Observe-se que as matrizes com entradas em $GF(2)$ invertíveis são aquelas que possuem determinante igual a 1. Assim,

$$M_n = (Q, R_4)$$

é um comutador multiplicativo de matrizes em $SL(n, GF(2))$, quando $n \geq 8$ e n é par.

Considere-se, agora, o último caso em que $n \geq 7$ e n é ímpar.

Sejam $j = (n-1)/2$ e $R_5 = R_3 \oplus I_{j-3} \oplus R_2(n-j)$. Os divisores elementares de R_5 são

$$(\lambda-1)^2,\ \lambda-1,\ \underbrace{\lambda-1,\ldots,\lambda-1}_{j-3 \text{ factores}},\ (\lambda-1)^{n-j}.$$

Defina-se, também, $S_1 = [s_{i,t}] \in GF(2)^{n\times n}$ da seguinte forma:

$s_{i,i} = 1, \quad i \in \{1, 2, \ldots, j+2, j+4, \ldots, n\}$;

$s_{j+4,j+3} = s_{j+3,j+4} = s_{j+1,t} = 1, \quad t \in \{j+2, \ldots, n\}$;

Todas as restantes entradas de S_1 são nulas.

De forma análoga à anterior, tem-se que $S_1 = I_j \oplus B_1$, onde B_1 possui a forma

$$B_1 = \left[\begin{array}{cccc|cccc} 1 & 1 & 1 & 1 & 1 & \cdots & \cdots & 1 \\ 0 & 1 & 0 & 0 & 0 & \cdots & \cdots & 0 \\ 0 & 0 & 0 & 1 & 0 & \ldots & \ldots & 0 \\ 0 & 0 & 1 & 0 & 0 & \ldots & \ldots & 0 \\ \hline 0 & 0 & 0 & 0 & 1 & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & 0 & 1 & \ddots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \ddots & 0 \\ 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 1 \end{array}\right].$$

Observe-se que S_1 é não singular e que, decomposta num produto de matrizes elementares, obtém-se que

$$S_1 = S_{j+1,j+2}(1)S_{j+1,j+3}(1)\cdots S_{j+1,n}(1)S_{j+3,j+4}.$$

Tal como no caso anterior, tem-se que

$$S_1(M_nR_5)S_1^{-1} = J_{j+1} \oplus J_2 \oplus I_{n-j-3}.$$

e então, M_nR_5 e $J_{j+1} \oplus J_2 \oplus I_{n-j-3}$ são semelhantes e, portanto, possuem os mesmos divisores elementares:

$$\underbrace{\lambda - 1, \ldots, \lambda - 1}_{n-j-3 \text{ factotes}},\ (\lambda - 1)^2,\ (\lambda - 1)^{j+1}.$$

Uma vez que $j + 1 = n - j$, R_5 e M_nR_5 possuem os mesmos divisores elementares e são, por isso, semelhantes, existe $P \in SL(n, GF(2))$ tal que $M_nR_5 = PR_5P^{-1}$. Desta forma,

$$M_n = (P, R_5)$$

é um comutador multiplicativo de matrizes em $SL(n, GF(2))$, quando $n \geq 7$ e n é ímpar.

Conclui-se, assim, a demonstração do lema.

■

Lema 2.8. *Considere-se $J_2 \oplus J_2 \oplus J_2$. Então $J_2 \oplus J_2 \oplus J_2 = UVU^{-1}V^{-1}$ onde*

$$U = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \end{bmatrix} \quad V = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

Demonstração

Um cálculo directo demonstra o resultado.

■

Para $n \geq 3$, defina-se a matriz $A_n \in GF(2)^{n \times n}$ por

$$A_n = \begin{bmatrix} 1 & a_2 & a_3 & \cdots & a_{n-1} & a_n \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & 0 & \cdots & 1 & 0 \\ \cdot & \cdot & \cdot & & \cdot & \cdot \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \end{bmatrix}. \tag{2.28}$$

Lema 2.9. *Suponha-se que $n \geq 3$. Se $a_2 + a_n = 1$, então os divisores elementares não constantes de A_n são $(\lambda - 1)^3$, $\lambda - 1$, juntamente com $(\lambda - 1)^2$ repetido $m - 2$ vezes se $n = 2m$ é par ou repetido $m - 1$ vezes se $n = 2m + 1$ é ímpar. (m inteiro positivo)*

Demonstração

Para encontrar os divisores elementares da A_n reduza-se a matriz polinomial $\lambda I_n - A_n$ à sua forma normal de Smith:

$$F_S(A_n) = \text{diag}(f_1, f_2, \ldots, f_n)$$

onde $f_i | f_{i+1}$ para $i \in \{1, 2, \ldots, n-1\}$. Esta redução é feita através de operações de equivalência.

De forma a determinar os divisores elementares da matriz $\lambda I_n - A$, serão, de seguida, dadas transformações elementares a realizar nas linhas e colunas de $\lambda I_n - A$ de modo a escrevê-la na forma pretendida.

Se $n = 2m$ é par, seja $e = 0$. Se $n = 2m + 1$ é ímpar, seja $e = 1$.

Passo 1: Para cada $k \in \{2, 3, \ldots, m + e\}$, multiplique-se à esquerda $\lambda I_n - A_n$ pelas matrizes elementares $S_{k,n+2-k}(\lambda)$ e $S_{1,n+2-k}(a_k)$, por esta ordem, e de seguida à direita pelas suas matrizes inversas. Note-se que em $SL(n, GF(2))$ as matrizes anteriores e as suas inversas coincidem.

Estas operações devem ser entendidas em termos das operações em linhas e colunas definidas no capítulo de introdução.

Após estas transformações, obtém-se uma matriz equivalente a $\lambda I_n - A_n$ em que a entrada $(1, n)$ é $a_2 + a_n = 1$.

Passo 2: Continue-se, transformando a segunda linha da matriz resultante do passo anterior pela multiplicação à esquerda por $S_{2,1}((\lambda - 1)^2)$. Note-se que, em $GF(2)$, $(\lambda - 1)^2 = \lambda^2 - 1 = \lambda + 1$.

Passo 3: De seguida, se n for par e só nesse caso, multiplique-se à esquerda a matriz resultante do passo anterior por $S_{2,m+1}(a_{m+1}(\lambda - 1))$.

Passo 4: Independentemente da paridade de n, multiplique-se à esquerda a matriz resultante do passo anterior por $S_{2,k}(a_{n+2-k} + a_k)$, para cada $k \in \{m + e, m + e - 1, \ldots, 3\}$ e multiplique-se à direita por $S_{n,1}(\lambda - 1)$ e $S_{n,n+2-k}(a_{n+2-k} + a_k)$, respectivamente, para cada $k \in \{3, 4, \ldots, m + e\}$.

Passo 5: Finalmente, e apenas para n par, alterem-se as colunas da matriz anterior multiplicando à direita por $S_{n,m+1}(a_{m+1})$.

Tem-se assim, uma matriz equivalente a $\lambda I_n - A_n$ que em cada linha e em cada coluna possui no máximo um elemento não nulo e pode, portanto, ser transformada, por trocas nas suas linhas e colunas, na sua forma normal de Smith:

$$F_S(A_n) = \mathrm{diag}(\underbrace{1, \ldots, 1}_{n-m-e \text{ factores}}, \lambda - 1, \underbrace{(\lambda - 1)^2, \ldots, (\lambda - 1)^2}_{m-2+e \text{ factores}}, (\lambda - 1)^3)$$

Tendo em conta a forma da matriz diagonal anterior, os seus divisores elementares ficam explícitos.

Conclui-se assim, a demonstração do lema.

■

Apresenta-se de seguida um exemplo para ilustrar o lema anterior, no caso em que $n = 4$. Desta forma, $m = 2$ e $e = 0$.

Considere-se

$$A_4 = \begin{bmatrix} 1 & a_2 & a_3 & a_4 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}.$$

Passo 1: Neste caso, $k = 2$ e fazendo na matriz polinomial

$$\lambda I_4 - A_4 = \begin{bmatrix} \lambda - 1 & -a_2 & -a_3 & -a_4 \\ 0 & \lambda & 0 & -1 \\ 0 & 0 & \lambda - 1 & 0 \\ 0 & -1 & 0 & \lambda \end{bmatrix}$$

transformações nas linhas multiplicando à esquerda por $S_{2,4}(\lambda)$ e de seguida por $S_{1,4}(a_2)$, tem-se que $\lambda I_4 - A_4$ é equivalente, respectivamente, a

$$\begin{bmatrix} \lambda - 1 & -a_2 & -a_3 & -a_4 \\ 0 & 0 & 0 & -1 + \lambda^2 \\ 0 & 0 & \lambda - 1 & 0 \\ 0 & -1 & 0 & \lambda \end{bmatrix} \quad \text{e} \quad \begin{bmatrix} \lambda - 1 & 0 & -a_3 & -a_4 + a_2\lambda \\ 0 & 0 & 0 & (\lambda - 1)^2 \\ 0 & 0 & \lambda - 1 & 0 \\ 0 & -1 & 0 & \lambda \end{bmatrix}.$$

Fazendo, agora, transformações nas colunas multiplicando à direita a matriz resultante por $S_{2,4}(\lambda)$ e $S_{1,4}(a_2)$, tem-se que a matriz anterior é equivalente, respectivamente, a

$$\begin{bmatrix} \lambda - 1 & 0 & -a_3 & -a_4 + a_2\lambda \\ 0 & 0 & 0 & (\lambda - 1)^2 \\ 0 & 0 & \lambda - 1 & 0 \\ 0 & -1 & 0 & 0 \end{bmatrix} \quad \text{e} \quad \begin{bmatrix} \lambda - 1 & 0 & -a_3 & \underbrace{-a_4 - a_2}_{=1} + \underbrace{2a_2\lambda}_{=0} \\ 0 & 0 & 0 & (\lambda - 1)^2 \\ 0 & 0 & \lambda - 1 & 0 \\ 0 & -1 & 0 & 0 \end{bmatrix}.$$

Note-se que a entrada $(1, 4)$ é, de facto, 1.

Continuando para o **Passo 2**, faça-se uma transformação na segunda linha da matriz resultante, multiplicando à esquerda a matriz anterior por $S_{2,1}((\lambda-1)^2)$ e, então, a matriz polinomial anterior será equivalente a

$$\begin{bmatrix} \lambda-1 & 0 & -a_3 & 1 \\ (\lambda-1)^3 & 0 & -a_3(\lambda-1)^2 & 0 \\ 0 & 0 & \lambda-1 & 0 \\ 0 & -1 & 0 & 0 \end{bmatrix}.$$

Porque n é par, execute-se o **Passo 3** e, multiplique-se à esquerda a matriz anterior por $S_{2,3}(a_3(\lambda-1))$, tem-se que a matriz anterior é equivalente a

$$\begin{bmatrix} \lambda-1 & 0 & -a_3 & 1 \\ (\lambda-1)^3 & 0 & 0 & 0 \\ 0 & 0 & \lambda-1 & 0 \\ 0 & -1 & 0 & 0 \end{bmatrix}.$$

No **Passo 4**, k não assume qualquer valor e não há transformações a fazer nas linhas da matriz anterior. Alterem-se as colunas da matriz resultante multiplicando à direita por $S_{4,1}(\lambda-1)$. Tem-se, assim, que a matriz polinomial inicial é equivalente à matriz

$$\begin{bmatrix} 0 & 0 & -a_3 & 1 \\ (\lambda-1)^3 & 0 & 0 & 0 \\ 0 & 0 & \lambda-1 & 0 \\ 0 & -1 & 0 & 0 \end{bmatrix}.$$

Passando ao **Passo 5** e multiplicando à direita a matriz anterior por $S_{4,3}(a_3)$, tem-se uma nova matriz equivalente à anterior:

$$\begin{bmatrix} 0 & 0 & 0 & 1 \\ (\lambda-1)^3 & 0 & 0 & 0 \\ 0 & 0 & \lambda-1 & 0 \\ 0 & -1 & 0 & 0 \end{bmatrix}.$$

Finalmente, trocando apenas linhas e colunas, tem-se que $\lambda I_4 - A_4$ é equivalente à sua forma normal de Smith

$$F_S(A_4) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \lambda-1 & 0 \\ 0 & 0 & 0 & (\lambda-1)^3 \end{bmatrix}.$$

Os polinómios invariantes de A_4 são $1,\ 1,\ \lambda-1,\ (\lambda-1)^2$, os divisores elementares estão explícitos e estão, de facto, de acordo com os dados pelo lema anterior.

Para $n \geq 3$ seja

$$C_n = \begin{bmatrix} 0 & 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ 1 & c_2 & c_3 & \cdots & c_{n-1} & c_n \end{bmatrix}. \tag{2.29}$$

Lema 2.10. *Suponha-se que* $n \geq 3$.

Se $n = 2m$ *é par, se* $c_{2m} = 0,\ c_m = c_{m+1} = 1$ *e se, quando* $m > 2$, *se tem* $c_{m+2+i} + c_{m-1-i} = 0$ *para* $i \in \{0, 1, \ldots, m-3\}$, *então os divisores elementares não constantes de* C_n *são:* $(\lambda-1)^3,\ \lambda-1$ *juntamente com* $(\lambda-1)^2$ *repetido* $m-2$ *vezes.*

Se $n = 2m+1$ *é ímpar, se* $c_{2m+1} = 0,\ c_{m+1} = 1$ *e se, quando* $m > 1$, *se tem* $c_{m+2+i} + c_{m-i} = 0$ *para* $i \in \{0, 1, \ldots, m-2\}$, *então os divisores elementares não constantes de* C_n *são* $(\lambda-1)^3$ *juntamente com* $(\lambda-1)^2$ *repetido* $m-1$ *vezes.*

Demonstração

Tal como no lema 2.9, são utilizadas transformações nas linhas e colunas de $\lambda I_n - C_n$, multiplicando, respectivamente, à esquerda e à direita por matrizes elementares por forma a transformá-la na sua forma normal de Smith, a partir da qual ficam explícitos os factores invariantes e, por conseguinte, os divisores elementares.

Uma vez mais, seja $e = 0$, se n é par, e $e = 1$ se n é ímpar.

Passo 1: Alterem-se as colunas de $\lambda I_n - C_n$ multiplicando à direita por $S_{n+1-k,k}(\lambda)$ para $k \in \{1, 2, \ldots, m\}$ e de seguida, alterem-se as linhas da matriz resultante, multiplicando à esquerda por $S_{n+1-k,k}(\lambda)$ para $k \in \{1, 2, \ldots, m\}$.

Passo 2: Multiplique-se à esquerda a matriz resultante no passo anterior por $S_{n,k}(c_{n+1-k})$ para $k \in \{2, 3, \ldots, m\}$.

Após os passos anteriores, obtém-se uma matriz equivalente a $\lambda I_n - C_n$ em que, quando n é par, a entrada (n, m) é $(\lambda - 1)$, e quando n é ímpar, a entrada $(n, m+1)$ é $c_{m+1} = 1$.

Independentemente da paridade de n, efectue-se o passo seguinte.

Passo 3: Façam-se transformações nas colunas da matriz resultante multiplicando à direita por $S_{m+e,1}((\lambda-1)^{e+1})$ e de seguida por $S_{m+2,k}(c_{n+1-k}(\lambda-1)^e)$, $k \in \{2, 3, \ldots, m-1+e\}$.

Neste ponto, as entradas da última linha da matriz resultante são nulas, exceptuando a entrada $(n, m+e)$.

Passo 4: Façam-se transformações nas linhas da matriz que se obteve no passo anterior multiplicando à esquerda por $S_{m+1,n+1-k}(c_{n+1-k})$ para $k \in \{2, 3, \ldots, m-1+e\}$ e de seguida por $S_{m+1,n}(\lambda - 1)$.

Após os quatro passos anteriores, uma matriz equivalente a $\lambda I_n - C_n$ que em cada linha e em cada coluna possui no máximo um elemento não nulo e pode, portanto, ser transformada, por trocas nas suas linhas e colunas, na sua forma normal de Smith:

$$F_S(C_n) = \text{diag}(\underbrace{1, \ldots, 1}_{m+e \text{ factores}}, (\lambda-1)^{1-e}, \underbrace{(\lambda-1)^2, \ldots, (\lambda-1)^2}_{m-2+e \text{ factores}}, (\lambda-1)^3)$$

Tendo em conta a forma da matriz, os seus divisores elementares ficam explícitos e conclui-se a demonstração do lema. ■

Ilustra-se, de seguida, o lema anterior, utilizando o seguinte exemplo. Considere-se a matriz C_4,

$$C_4 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & c_2 & c_3 & c_4 \end{bmatrix}.$$

Desta forma, $m = 2$ e $e = 0$. Tem-se ainda, que $c_4 = 0$ e $c_2 = c_3 = 1$.

Considere-se a matriz polinomial,

$$\lambda I_4 - C_4 = \begin{bmatrix} \lambda & 0 & 0 & -1 \\ 0 & \lambda & -1 & 0 \\ 0 & -1 & \lambda & 0 \\ -1 & -1 & -1 & \lambda \end{bmatrix}.$$

Passo 1: Neste caso, $k \in \{1, 2\}$ e multiplicando à direita a matriz polinomial por $S_{4,1}(\lambda)$ e por $S_{3,2}(\lambda)$ tem-se que é equivalente, respectivamente, a

$$\begin{bmatrix} 0 & 0 & 0 & -1 \\ 0 & \lambda & -1 & 0 \\ 0 & -1 & \lambda & 0 \\ (\lambda-1)^2 & -1 & -1 & \lambda \end{bmatrix} \quad \text{e} \quad \begin{bmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \\ 0 & (\lambda-1)^2 & \lambda & 0 \\ (\lambda-1)^2 & \lambda-1 & -1 & \lambda \end{bmatrix}.$$

Multiplique-se de seguida a matriz anterior à esquerda por $S_{4,1}(\lambda)$ e $S_{3,2}(\lambda)$, e obtenham-se as matrizes equivalentes a $\lambda I_4 - C_4$

$$\begin{bmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \\ 0 & (\lambda-1)^2 & \lambda & 0 \\ (\lambda-1)^2 & \lambda-1 & -1 & 0 \end{bmatrix} \quad \text{e} \quad \begin{bmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \\ 0 & (\lambda-1)^2 & 0 & 0 \\ (\lambda-1)^2 & \lambda-1 & -1 & 0 \end{bmatrix}.$$

Passo 2: Neste caso, $k = 2$ e multiplicando à esquerda a matriz resultante por $S_{4,2}(c_3)$, onde $c_3 = 1$, obtém-se uma matriz equivalente

$$\begin{bmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \\ 0 & (\lambda-1)^2 & 0 & 0 \\ (\lambda-1)^2 & \lambda-1 & 0 & 0 \end{bmatrix}.$$

Note-se que, de facto, sendo n par, a entrada (n, m), ou seja, $(4, 2)$, é $\lambda - 1$.

Passo 3: Neste caso k não assume qualquer valor. Tome-se a matriz anterior e multiplique-se à direita por $S_{2,1}(\lambda - 1)$. Obtém-se a matriz equivalente

$$\begin{bmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \\ (\lambda-1)^3 & (\lambda-1)^2 & 0 & 0 \\ 0 & \lambda-1 & 0 & 0 \end{bmatrix}.$$

Passo 4: Neste caso $k = 2$. Multiplique-se à esquerda a matriz resultante por $S_{3,4}(\lambda - 1)$. Obtém-se a seguinte matriz, equivalente a $\lambda I_4 - C_4$.

$$\begin{bmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \\ (\lambda-1)^3 & 0 & 0 & 0 \\ 0 & \lambda-1 & 0 & 0 \end{bmatrix}.$$

Fazendo, apenas trocas nas linhas e colunas da matriz anterior obtém-se que $\lambda I_4 - C_4$ é equivalente à sua forma normal de Smith:

$$F_S(C_4) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \lambda-1 & 0 \\ 0 & 0 & 0 & (\lambda-1)^3 \end{bmatrix}.$$

Os divisores elementares estão explícitos e estão, de facto, de acordo com os dados pelo lema anterior.

Sejam $f(\lambda) = \lambda^n + b_2\lambda^{n-1} + \cdots b_n\lambda + 1 \in GF(2)[\lambda]$ e $E_n = C(f)$.

Lema 2.11. *Seja $n \geq 1$ e suponha-se que, quando $n = 2$, $E_2 \neq C(\lambda^2 + 1)$. Então, E_n é um comutador multiplicativo de matrizes em $SL(n, GF(2))$.*

Demonstração

Para $n = 1$ o resultado do lema é óbvio.

Para $n = 2$, note-se que o único polinómio mónico com 1 como termo independente e distinto de $\lambda^2 + 1$ é $\lambda^2 + \lambda + 1$ e que $C(\lambda^2 + \lambda + 1) = J_2 C(\lambda^2 + 1) J_2^{-1} C(\lambda^2 + 1)^{-1}$.

De facto, efectuando cálculos simples, tem-se que

$$\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^{-1} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}^{-1}.$$

Suponha-se, agora, que $n \geq 3$.

Seja A_n a matriz definida em (2.28), onde os elementos a_i serão determinados posteriormente.

$$E_nA_n = \begin{bmatrix} 0 & 1 & 0 & \cdots & \cdots & 0 \\ \vdots & 0 & 1 & 0 & & \vdots \\ \vdots & & \ddots & \ddots & & \vdots \\ \vdots & & & \ddots & \ddots & 0 \\ 0 & \cdots & \cdots & \cdots & 0 & 1 \\ 1 & b_n & \cdots & \cdots & b_3 & b_2 \end{bmatrix} \begin{bmatrix} 1 & a_2 & a_3 & \cdots & a_{n-1} & a_n \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & 0 & \cdots & 1 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \end{bmatrix}$$

$$= \begin{bmatrix} 0 & 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 \\ \cdot & \cdot & \cdot & & \cdot & \cdot \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ 1 & c_2 & c_3 & \cdots & c_{n-1} & c_n \end{bmatrix} = C_n$$

onde $C_n = E_nA_n$ é do tipo de (2.29), com a particularidade de se ter $c_i = a_i + b_i$, para $i \in \{2, 3, \ldots, n\}$.

Os casos $n = 2m$ par e $n = 2m+1$ ímpar, sendo m um inteiro maior que 1, serão abordados separadamente.

Suponha-se que $n = 2m$ é par. Se

$$\begin{cases} a_{2m} + b_{2m} = 0 \\ a_m + b_m = a_{m+1} + b_{m+1} = a_2 + a_{2m} = 1 \end{cases} \tag{2.30}$$

e se, para $m > 2$ se tiver

$$a_{m+2+i} + b_{m+2+i} + a_{m-1-i} + b_{m-1-i} = 0, \quad i \in \{0, 1, \ldots, m-3\}, \tag{2.31}$$

então as condições dos lemas 2.9 e 2.10 são satisfeitas e A_n e C_n possuem os mesmos divisores elementares. Se tal acontecer, existe $Q \in SL(n, GF(2))$ tal que $C_n = QA_nQ^{-1}$ e, portanto $E_n = QA_nQ^{-1}A_n^{-1}$.

É necessário, no entanto, garantir que existem elementos a_i, $i \in \{2, 3, \ldots, n\}$, que verifiquem as condições (2.30) e (2.31).

Se $m > 2$, escolham-se

$a_{2m} = b_{2m}$;

$a_m = 1 + b_m$;

$a_{m+1} = 1 + b_{m+1}$;

$a_2 = 1 + a_{2m}$.

Tal escolha é possível tendo em conta que $2, m, m+1$ e $2m$ são inteiros distintos. Note-se, ainda, que com esta escolha a condição (2.30) verifica-se.

Para $m > 3$, tomem-se $a_3, a_4, \ldots, a_{m-1}$ quaisquer. É agora possível escolher $a_{m+2}, \ldots, a_{2m-1}$ de forma a que as igualdades (2.31) se verifiquem.

Como de facto existem elementos $a_2, \ldots, a_n$ que verificam (2.30) e (2.31) para o caso em que $n = 2m$ com m inteiro positivo maior do que 2, conclui-se que, sob estas condições, E_n é um comutador multiplicativo de matrizes em $SL(n, GF(2))$.

Quando $n = 4$, as equações (2.30) possuem uma solução quando $b_2 + b_4 = 0$. Esta situação é facilmente verificada pois de (2.30) tem-se que

$$\begin{cases} a_4 + b_4 = 0 \\ a_2 + b_2 = a_3 + b_3 = a_2 + a_4 = 1 \end{cases}.$$

Assim, sob a condição $b_2 + b_4 = 0$, E_4 é um comutador multiplicativo de matrizes em $SL(4, GF(2))$.

Os casos para os quais $n = 4$ e $b_2 + b_4 = 1$ não estão contemplados no argumento anterior. Para demonstrar estes casos, realizam-se alguns cálculos directos.

Sejam

$$X_1 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}, \; Y_1 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix} \in SL(4, GF(2))$$

e

$$X_2 = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \end{bmatrix}, \; Y_2 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \end{bmatrix} \in SL(4, GF(2))$$

e note-se que para finalizar o estudo do caso n par, resta considerar o caso em que E_4 é a matriz companheira de um dos polinómios $p(\lambda) = \lambda^4 + b_2\lambda^3 + b_3\lambda^2 + b_4\lambda + 1$ tais que $b_2 + b_4 = 1$; tem-se, então, as seguintes possibilidades:

$$\begin{aligned}
&\text{(i) } p(\lambda) = \lambda^4 + \lambda^3 + 1;\\
&\text{(ii) } p(\lambda) = \lambda^4 + \lambda^3 + \lambda^2 + 1;\\
&\text{(iii) } p(\lambda) = \lambda^4 + \lambda + 1;\\
&\text{(iv) } p(\lambda) = \lambda^4 + \lambda^2 + \lambda + 1.
\end{aligned}$$

Tem-se que

$$C(\lambda^4 + \lambda^3 + 1) = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix} = X_1 Y_1 X_1^{-1} Y_1^{-1}$$

e

$$C(\lambda^4 + \lambda^3 + \lambda^2 + 1) = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix} = X_2 Y_2 X_2^{-1} Y_2^{-1}.$$

Além disso, $C(\lambda^4 + \lambda + 1)$ e $C(\lambda^4 + \lambda^2 + \lambda + 1)$ são, respectivamente, semelhantes em $SL(4, GF(2))$ a $[C(\lambda^4 + \lambda^3 + 1)]^{-1}$ e $[C(\lambda^4 + \lambda^3 + \lambda^2 + 1)]^{-1}$.

De facto, $[C(\lambda^4 + \lambda^3 + 1)]^{-1}$ pode ser obtida de $C(\lambda^4 + \lambda + 1)$ através das transformações de semelhança T_1^4 e T_2^3. As mesmas transformações permitem obter $[C(\lambda^4 + \lambda^3 + \lambda^2 + 1)]^{-1}$ a partir de $C(\lambda^4 + \lambda^2 + \lambda + 1)$.

Observe-se que as inversas de comutadores multiplicativos de matrizes são, ainda, comutadores multiplicativos de matrizes: se $A = XYX^{-1}Y^{-1}$, então $A^{-1} = YXY^{-1}X^{-1}$.

Assim, $C(\lambda^4 + \lambda + 1)$ e $C(\lambda^4 + \lambda^2 + \lambda + 1)$ são semelhantes a comutadores multiplicativos de matrizes em $SL(4, GF(2))$ e, portanto, são também comutadores de matrizes em $SL(4, GF(2))$.

Com a conclusão do estudo do caso $n = 4$ conclui-se, também, que se $n > 2$ é par, então E_n é um comutador multiplicativo de matrizes em $SL(n, GF(2))$.

Suponha-se, agora, que $n = 2m + 1$ é ímpar.

Se

$$\begin{cases} a_{2m+1} + b_{2m+1} = 0 \\ a_{m+1} + b_{m+1} = a_2 + a_{2m+1} = 1 \end{cases} \tag{2.32}$$

e se, para $m > 1$ se tiver

$$a_{m+2+i} + b_{m+2+i} + a_{m-i} + b_{m-i} = 0, \quad i \in \{0, 1, \ldots, m-2\}, \tag{2.33}$$

então as condições dos lemas 2.9 e 2.10 são satisfeitas e conclui-se que A_n e C_n possuem os mesmos divisores elementares. Então, existe $P \in SL(n, GF(2)$ tal que $C_n = PA_nP^{-1}$ e, portanto $E_n = PA_nP^{-1}A_n^{-1}$ é um comutador multiplicativo de matrizes em $SL(n, GF(2))$.

Uma vez mais, ver-se-á que é possível escolher $a_2, \ldots, a_n$ por forma a que as condições anteriores se verifiquem.

Se $m > 1$, os números inteiros $2, m+1, 2m+1$ são distintos e é possível tomar

$a_{2m+1} = b_{2m+1}$;

$a_{m+1} = 1 + b_{m+1}$;

$a_2 = 1 + b_{2m+1}$

e assim, a condição (2.32) verifica-se.

Escolha-se $a_3, \ldots, a_m$ arbitrários (quando $m > 2$) e resolva-se as equações (2.33) em ordem a $a_{m+2}, \ldots, a_{2m}$. Assim, as condições (2.32) e (2.33) verificam-se e E_n é um comutador multiplicativo de matrizes em $SL(n, GF(2))$, quando $n > 3$ é ímpar.

Quando $n = 3$, as equações (2.32) possuem solução se $b_2 + b_3 = 0$. Sob esta condição E_3 é um comutador multiplicativo de matrizes sobre $SL(3, GF(2))$.

Para finalizar a demonstração, note-se que resta considerar o caso em que E_3 é a matriz companheira de um polinómio $p(\lambda) = \lambda^3 + b_2\lambda^2 + b_3\lambda + 1$ em que $b_2 + b_3 = 1$. As possibilidades para $p(\lambda)$ são:

$$\text{(i) } p(\lambda) = \lambda^3 + \lambda + 1;$$
$$\text{(ii) } p(\lambda) = \lambda^3 + \lambda^2 + 1.$$

Considere-se

$$X_3 = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix}, \; Y_3 = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} \in SL(3, GF(2)).$$

Então, $C(\lambda^3+\lambda+1) = X_3Y_3X_3^{-1}Y_3^{-1}$ e é um comutador multiplicativo de matrizes em $SL(3, GF(2))$.

Além disso, $C(\lambda^3+\lambda^2+1)$ é semelhante a $[C(\lambda^3+\lambda+1)]^{-1}$, que sendo um comutador multiplicativo de matrizes em $SL(3, GF(2))$, implica que $C(\lambda^3+\lambda^2+1)$ é, também, um comutador multiplicativo de matrizes em $SL(3, GF(2))$. De facto, $C(\lambda^3+\lambda^2+1)$ obtém-se de $[C(\lambda^3+\lambda+1)]^{-1}$ através da transformação de semelhança T_1^3.

Conclui-se, então que, sempre que n é ímpar, E_n é um comutador multiplicativo de matrizes em $SL(n, GF(2))$.

Fica, assim, completamente demonstrado o lema 2.11. ■

É, agora possível demonstrar o seguinte teorema que revela em que condições uma matriz de $SL(n, GF(2))$ pode ser escrita como um comutador multiplicativo de matrizes em $SL(n, GF(2))$:

Teorema 2.3. *Se $n > 2$ e $A \in SL(n, GF(2))$, então A é um comutador multiplicativo de matrizes em $SL(n, GF(2))$.*

Demonstração

Note-se que, para demonstrar que $A \in SL(n, GF(2))$ é um comutador multiplicativo de matrizes em $SL(n, GF(2))$, pela observação feita no início do capítulo, é suficiente demonstrar que uma matriz semelhante a A é um comutador de matrizes em $SL(n, GF(2))$.

Assim, sem perda de generalidade, é possível supor que a matriz A coincide com a sua forma normal invariante: $F_I(A)$.

Tem-se, então, que A é soma directa de matrizes companheiras de potências de polinómios irredutíveis com coeficientes em $GF(2)$:

$$A = F_I(A) = C(p_1(\lambda)^{e_1}) \oplus \cdots \oplus C(p_r(\lambda)^{e_r}),$$

onde $e_1, \ldots, e_r$ são inteiros não negativos.

Se nenhuma das potências de polinómios, $p_i(\lambda)^{e_i}$, é $(\lambda+1)^2 = \lambda^2+1$, então, pelo lema 2.11, cada matriz $C(p_i(\lambda)^{e_i})$ é um comutador multiplicativo de matrizes em $SL(e_i, GF(2))$, ou seja, existem $X_i, Y_i \in SL(e_i, GF(2))$ tais que $C(p_i(\lambda)^{e_i}) = X_iY_iX_i^{-1}Y_i^{-1}$ para $i \in \{1, 2, \ldots, r\}$.

Sejam $X = X_1 \oplus \cdots \oplus X_r, Y = Y_1 \oplus \cdots \oplus Y_r \in SL(n, GF(2))$. Então $A = XYX^{-1}Y^{-1}$ e é, portanto, um comutador multiplicativo de matrizes em $SL(n, GF(2))$.

Se exactamente s das potências de polinómios, $p_i(\lambda)^{e_i}$, (com $s > 1$) são $(\lambda + 1)^2$, pode supor-se, sem perda de generalidade, que são as primeiras:

$$p_1(\lambda)^{e_1} = p_2(\lambda)^{e_2} = \cdots = p_s(\lambda)^{e_s} = (\lambda + 1)^2 = \lambda^2 + 1.$$

Note-se que J_e é semelhante a $C((\lambda - 1)^e)$.

Se s é par, pelo lema 2.7 (quando $n = 4$), existem matrizes $X_k, Y_k \in SL(4, GF(2))$ tais que

$$C(p_{2k-1}(\lambda)^{e_{2k-1}}) \oplus C(p_{2k}(\lambda)^{e_{2k}}) = X_k Y_k X_k^{-1} Y_k^{-1}, \quad k \in \{1, 2, \ldots, \frac{s}{2}\}.$$

Sejam $X^{(1)} = X_1 \oplus \cdots \oplus X_{\frac{s}{2}}$ e $Y^{(1)} = Y_1 \oplus \cdots \oplus Y_{\frac{s}{2}}$.

Como as restantes matrizes bloco $C(p_{s+1}(\lambda)^{e_{s+1}}), \ldots, C(p_r(\lambda)^{e_r})$ são diferentes de $C((\lambda + 1)^2)$, pelo lema 2.11 são comutadores multiplicativos de matrizes. Assim, existem matrizes $X_t, Y_t \in SL(e_t, GF(2))$ tais que

$$C(p_t(\lambda)^{e_t}) = X_t Y_t X_t^{-1} Y_t^{-1}, \quad t \in \{s + 1, \ldots, r\}.$$

Sejam $X^{(2)} = X_{s+1} \oplus \cdots \oplus X_r$ e $Y^{(2)} = Y_{s+1} \oplus \cdots \oplus Y_r$. Sejam, ainda, $X = X^{(1)} \oplus X^{(2)}, Y = Y^{(1)} \oplus Y^{(2)} \in SL(n, GF(2))$.

Desta forma, $A = XYX^{-1}Y^{-1}$, sendo, portanto, um comutador multiplicativo de matrizes em $SL(n, GF(2))$.

Suponha-se, agora que $s > 1$ é ímpar. Desta forma, $s - 3$ é par e, pelo lema 2.8, existem matrizes $X_1, Y_1 \in SL(6, GF(2))$ tais que

$$C((\lambda + 1)^2) \oplus C((\lambda + 1)^2) \oplus C((\lambda + 1)^2) = X_1 Y_1 X_1^{-1} Y_1^{-1}.$$

Uma vez $s - 3$ é par, pode usar-se o mesmo argumento usado atrás: pelo lema 2.7 existem matrizes $X_k, Y_k \in SL(4, GF(2))$ tais que

$$C(p_{2k}(\lambda)^{e_{2k}}) \oplus C(p_{2k+1}(\lambda)^{e_{2k+1}}) = X_k Y_k X_k^{-1} Y_k^{-1}, \quad k \in \{2, \ldots, \frac{s-1}{2}\}.$$

Sejam $X^{(1)} = X_1 \oplus X_2 \oplus \cdots \oplus X_{\frac{s-1}{2}}$ e $Y^{(1)} = Y_1 \oplus Y_2 \oplus \cdots \oplus Y_{\frac{s-1}{2}}$.

Como os restantes factores $C(p_{s+1}(\lambda)^{e_{s+1}}), \ldots, C(p_r(\lambda)^{e_r})$ são diferentes de $C((\lambda+1)^2)$, pelo lema 2.11 são comutadores multiplicativos de matrizes, ou seja, existem matrizes $X_t, Y_t \in SL(e_t, GF(2))$ tais que

$$C(p_t(\lambda)^{e_t}) = X_t Y_t X_t^{-1} Y_t^{-1}, \quad t \in \{s+1, \ldots, r\}.$$

Sejam $X^{(2)} = X_{s+1} \oplus \cdots \oplus X_r$ e $Y^{(2)} = Y_{s+1} \oplus \cdots \oplus Y_r$. Sejam, ainda, $X = X^{(1)} \oplus X^{(2)}, Y = Y^{(1)} \oplus Y^{(2)} \in SL(n, GF(2))$.

Desta forma, $A = XYX^{-1}Y^{-1}$ e é, uma vez mais, um comutador multiplicativo de matrizes em $SL(n, GF(2))$.

Suponha-se, finalmente, que $s = 1$, ou seja, existe apenas uma potência de um polinómio irredutível da forma $(\lambda+1)^2 = p_1(\lambda)^{e_1}$. Como $n \neq 2$, então $r > 1$.

Se $p_2(\lambda) = \lambda + 1$, então $C(p_1(\lambda)^{e_1}) \oplus C(p_2(\lambda)^{e_2}) = C((\lambda+1)^2) \oplus C((\lambda+1)^{e_2})$ é semelhante a $J_2 \oplus J_{e_2}$ e pelo lema 2.7, e existem matrizes $X_1, Y_1 \in SL(2+e_2, GF(2))$ tais que

$$C(p_1(\lambda)^{e_1}) \oplus C(p_2(\lambda)^{e_2}) = X_1 Y_1 X_1^{-1} Y_1^{-1}.$$

Usando, novamente, o lema 2.11, existem matrizes $X_2, Y_2 \in SL(n - e_2 - 2, GF(2))$ tais que

$$C(p_3(\lambda)^{e_3}) \oplus C(p_4(\lambda)^{e_4}) \oplus \cdots \oplus C(p_r(\lambda)^{e_r}) = X_2 Y_2 X_2^{-1} Y_2^{-1}.$$

Sejam $X = X_1 \oplus X_2, Y = Y_1 \oplus Y_2 \in SL(n, GF(2))$.

Desta forma, $A = XYX^{-1}Y^{-1}$ é um comutador multiplicativo de matrizes em $SL(n, GF(2))$.

Finalmente, se $p_2(\lambda) \neq \lambda+1$, então $p_1(\lambda)$ e $p_2(\lambda)$ são primos entre si e $C(p_1(\lambda)^{e_1}) \oplus C(p_2(\lambda)^{e_2})$ é semelhante a $C(p_1(\lambda)^{e_1} p_2(\lambda)^{e_2})$.

Note-se que, sendo $p_1(\lambda)^{e_1}$ e $p_2(\lambda)^{e_2}$ primos entre si, então $p_1(\lambda)^{e_1} p_2(\lambda)^{e_2}$ não é uma potência de $\lambda + 1$ e, pelo lema 2.11, existem matrizes $X_1, Y_1 \in SL(e_1 + e_2, GF(2))$ tais que

$$C(p_1(\lambda)^{e_1} p_2(\lambda)^{e_2}) = X_1 Y_1 X_1^{-1} Y_1^{-1}.$$

Usando o lema 2.11, existem matrizes $X_2, Y_2 \in SL(n - e_2 - e_1, GF(2))$ tais que

$$C(p_3(\lambda)^{e_3}) \oplus C(p_4(\lambda)^{e_4}) \oplus \cdots \oplus C(p_r(\lambda)^{e_r}) = X_2 Y_2 X_2^{-1} Y_2^{-1}.$$

Sejam $X = X_1 \oplus X_2, Y = Y_1 \oplus X_2 \in SL(n, GF(2))$.

Desta forma, $A = XYX^{-1}Y^{-1}$ e é, portanto, um comutador multiplicativo de matrizes em $SL(n, GF(2))$.

Fica assim concluída a demonstração.

■

Tendo estabelecido este teorema, conclui-se que, se $n > 2$, qualquer elemento de $SL(n, GF(2))$ pode ser escrito como um comutador multiplicativo de matrizes em $SL(n, GF(2))$.

2.3 Comutadores Multiplicativos com Entradas em $GF(3)$

Nesta secção serão apresentados resultados que permitem saber em que condições uma matriz $A \in GF(3)^{n\times n}$ pode ser escrita como um comutador multiplicativo de matrizes com entradas em $GF(3)$.

Note-se inicialmente que $SL(2, GF(3))$ contém propriamente o seu subgrupo C, formado por comutadores multiplicativos de matrizes em $SL(2, GF(3))$,

$$C = \{XYX^{-1}Y^{-1} : \quad X, Y \in SL(2, GF(3))\},$$

uma vez que $C((\lambda \pm 1)^2) \in SL(2, GF(3))$, mas não pode ser escrita como um comutador multiplicativo de matrizes em $SL(2, GF(3))$.

O resultado principal desta secção revela que uma matriz $A \in SL(2, GF(3))$ é um comutador multiplicativo de matrizes em $GL(2, GF(3))$ e que, se $n > 2$ e $A \in SL(n, GF(3))$, então A é um comutador multiplicativo de matrizes em $SL(n, GF(3))$.

Serão, de seguida, demonstrados diversos lemas, alguns válidos em corpos em geral, outros apenas em $GF(3)$, e que servirão de base à prova do teorema principal desta secção.

Considere-se $-1, 0, 1$, os três elementos de $GF(3)$.

Lema 2.12. *Sejam $n \geq 2$ e $L \in F^{n\times n}$ a seguinte matriz:*

$$L = \begin{bmatrix} 0 & 1 & l_{1,3} & \cdots & \cdots & l_{1,n} \\ \vdots & 0 & 1 & l_{2,4} & & \vdots \\ \vdots & & \ddots & \ddots & \ddots & \vdots \\ \vdots & & & \ddots & \ddots & l_{n-2,n} \\ 0 & \cdots & \cdots & \cdots & 0 & 1 \\ x_1 & x_2 & \cdots & \cdots & x_{n-1} & x_n \end{bmatrix}.$$

Existe $S \in SL(n, F)$ tal que

(1) *SLS^{-1} é uma matriz companheira.*

(2) *Se $S = [s_{i,j}]$ então $s_{i,i} = 1$ para $i \in \{1, \ldots, n\}$ e $s_{i,n} = 0$ para $i \in \{1, \ldots, n-1\}$. Além disso, $s_{i,j} = 0$ sempre que $i > j$.*

(3) *As entradas de S não dependem de $x_1, x_2, \ldots, x_n$.*

Demonstração

Se $n = 2$, então L já é uma matriz companheira. É suficiente escolher $S = I_2$.

Se $n \geq 3$, seja L_k a matriz que se obtém de L fazendo $l_{1,j} = l_{2,j} = \cdots = l_{j-2,j} = 0$ para $j \geq k+1$ e $k \in \{3, \ldots, n\}$. Observe-se que L_k é uma matriz que coincide com L, excepto nas entradas das colunas $k+1, \ldots, n$ que estão acima da entrada unitária, que são nulas.

Por exemplo, se $k = 4$, tem-se

$$L_4 = \begin{bmatrix} 0 & 1 & l_{1,3} & l_{1,4} & 0 & \cdots & 0 \\ \vdots & 0 & 1 & l_{2,4} & 0 & \cdots & 0 \\ \vdots & & \ddots & 1 & 0 & & \vdots \\ \vdots & & & \ddots & \ddots & \ddots & \vdots \\ \vdots & & & & \ddots & \ddots & 0 \\ 0 & 0 & 0 & \cdots & \cdots & 0 & 1 \\ x_1 & x_2 & x_3 & \cdots & \cdots & \cdots & x_n \end{bmatrix}.$$

Note-se que $L_n = L$ e que L_2 é uma matriz companheira de um polinómio com coeficientes em F.

Recorde-se as matrizes elementares definidas no capítulo de introdução e defina-se

$$S_k = S_{k-2,k-1}(-l_{k-2,k}) S_{k-3,k-1}(-l_{k-3,k}) \cdots S_{1,k-1}(-l_{1,k}) \in SL(n, F).$$

Desta forma, S_k satisfaz as condições (2) e (3) do lema. Além disso, $S_k L_k S_k^{-1}$ é uma matriz semelhante a L_k e que coincide com a matriz L_k excepto nas entradas da $k-$ésima coluna que estão acima da entrada unitária que são nulas e nas entradas da $(k-1)-$ésima coluna; em particular, a entrada $(n, k-1)$ passa a ser

$$x_{k-1} + l_{1,k} x_1 + l_{2,k} x_2 + \cdots + l_{k-2,k} x_{k-2}.$$

Tem-se, então, que $S_k L_k S_k^{-1}$ é uma matriz semelhante a L_k e do tipo L_{k-1}.

Para cada $k \in \{3, 4, \ldots, n\}$ definam-se matrizes elementares S_k, tal como atrás, e note-se que qualquer uma delas verifica (2) e (3) do lema. Além disso, tem-se que existem matrizes $S_n, \ldots, S_{k+1} \in SL(n, F)$ tais que $S_{k+1} \cdots S_n L S_n^{-1} \cdots S_{k+1}^{-1}$ é uma matriz do tipo L_k.

Defina-se, ainda, $S = S_3 S_4 \cdots S_n \in SL(n, F)$ e note-se que SLS^{-1} é uma matriz semelhante a L, e que coincide com L excepto nas entradas $l_{i,j}$, para $i \in \{1, 2, \ldots, n-2\}$, $j \in \{i+2, i+$

$3, \ldots, n\}$ que são nulas e, se $l_{n,k}$ for a entrada (n,k) de SLS^{-1}, então $l_{n,k} = x_{k-1} + l_{1,k}x_1 + l_{2,k}x_2 + \cdots + l_{k-2,k}x_{k-2}$ para $k \in \{3, \ldots, n-1\}$.

Assim, SLS^{-1} é uma matriz companheira e possui as três características referidas no enunciado do lema. Fica, assim, demonstrado o resultado.

■

Para $n \geq 4$ defina-se a seguinte matriz:

$$\Delta_n(g_1, g_2, g_3, g_4, d) = \begin{bmatrix} g_1 & g_2 & d_3 & d_4 & \cdots & d_n \\ 0 & g_3 & g_4 & 0 & \cdots & 0 \\ \vdots & \ddots & 1 & 1 & \ddots & \vdots \\ \vdots & & \ddots & \ddots & \ddots & 0 \\ \vdots & & & \ddots & \ddots & 1 \\ 0 & \cdots & \cdots & \cdots & 0 & 1 \end{bmatrix} \in F^{n \times n}$$

onde d representa a sequência de elementos de F, $d_3, d_4, \ldots, d_n$.

Para $n \leq 3$, $\Delta_n(g_1, g_2, g_3, g_4, d)$ está definida por:

$$\Delta_3 = \begin{bmatrix} g_1 & g_2 & d_3 \\ 0 & g_3 & g_4 \\ 0 & 0 & 1 \end{bmatrix}, \ \Delta_2 = \begin{bmatrix} g_1 & g_2 \\ 0 & g_3 \end{bmatrix}, \text{ e } \Delta_1 = \begin{bmatrix} g_1 \end{bmatrix}.$$

Observe-se que nos casos $n = 1$ ou $n = 2$, $\Delta_n(g_1, g_2, g_3, g_4, d)$ não é função de todas as variáveis indicadas. A notação $d = 0$ deve ser entendida por $d_3 = d_4 = \cdots = d_n = 0$.

Lema 2.13. *Seja* $A = C(\lambda^n - a_n\lambda^{n-1} - \cdots - a_2\lambda - (-1)^{n-1}|A|) \in GL(n, F)$. *Sejam* $g_1, g_2, g_3, g_4 \in F$ *com* $g_3 \neq 0$ *e* $q(\lambda) = \lambda^n + q_n\lambda^{n-1} + \cdots + q_2\lambda + q_1 \in F[\lambda]$ *onde:*

$q_1 = (-1)^n|A|g_1g_3$ *se* $n \geq 2$;

$q_1 = -|A|g_1$ *se* $n = 1$.

$q_2 = (-1)^n|A|(g_2 + g_1g_4 + g_1g_3(n-3)) - a_2g_3$ *se* $n \geq 3$;

$q_2 = |A|g_2 - a_2g_3$ *se* $n = 2$.

Seja, ainda, $T = [g_3^{-1}] \oplus I_{n-1} \in GL(n, F)$. *Então existe* d, *uma sequência de elementos* $d_3, \cdots, d_n \in F$ *e uma matriz* $S \in SL(n, F)$ *cujas entradas satisfazem* (2) *do lema* 2.12 *e tais que*

$$STA\Delta_n(g_1, g_2, g_3, g_4, d)T^{-1}S^{-1} = C(q(\lambda)).$$

Demonstração

Se $n = 1$, tem-se que $q(\lambda) = \lambda + q_1 = \lambda - |A|g_1$, $A = C(\lambda - |A|) = [|A|]$ e $T = I_1$. Observe-se, ainda, que $\Delta_1 = [g_1]$.

Então, se $S = I_1$, tem-se que

$$STA\Delta_1 T^{-1}S^{-1} = C(q(\lambda)).$$

Se $n = 2$, tem-se que $q(\lambda) = \lambda^2 + q_2\lambda + q_1\lambda$, com $q_1 = (-1)^2|A|g_1g_3$ e $q_2 = |A|g_2 - a_2g_3$. Tem-se, ainda, que $A = C(\lambda^2 - a_2\lambda + |A|)$,

$$\Delta_2 = \begin{bmatrix} g_1 & g_2 \\ 0 & g_3 \end{bmatrix} \quad \text{e} \quad T = \begin{bmatrix} g_3^{-1} & 0 \\ 0 & 1 \end{bmatrix}.$$

Uma vez mais, se $S = I_2$ tem-se

$$STA\Delta_2 T^{-1}S^{-1} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} g_3^{-1} & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ -|A| & a_2 \end{bmatrix} \begin{bmatrix} g_1 & g_2 \\ 0 & g_3 \end{bmatrix} \begin{bmatrix} g_3 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 0 & 1 \\ -|A|g_1g_3 & -|A|g_2 + a_2g_3 \end{bmatrix} = C(\lambda^2 + q_2\lambda + q_1).$$

Portanto, se $n = 1$ ou $n = 2$ não existem elementos d_i para serem escolhidos e é, assim, suficiente considerar $S = I_n$.

Se $n \geq 3$, observe-se que o coeficiente de λ no polinómio característico $|\lambda I_n - L|$ da matriz L do lema 2.12 é $(-1)^{n-1}$ multiplicando pela soma dos menores principais de ordem $n - 1$.

Mas, o menor que se obtém retirando a primeira linha e a primeira coluna é $(-1)^n x_2$ e o menor que se obtém retirando a última linha e a última coluna é 0.

Note-se, ainda que, quando $i \in \{2, \ldots, n-1\}$, o menor que se obtém retirando a $i-$ésima linha e a $i-$ésima coluna, é $(-1)^n x_1 l_{i-1,i+1}$. Portanto, o coeficiente de λ no polinómio característico de L é

$$(-1)^{n-1}\left((-1)^n x_2 + (-1)^n x_1 l_{1,3} + +(-1)^n x_1 l_{2,4} \cdots (-1)^n x_1 l_{n-2,n} + 0\right)$$

$$= -(x_2 + x_1(l_{1,3} + l_{2,4} + \cdots l_{n-2,n})).$$

Seja agora

$$L^* = TA\Delta_n(g_1, g_2, g_3, g_4, d)T^{-1}.$$

Efectuando diversos cálculos, é possível obter-se um padrão geral para as entradas da matriz $L^* : L^* = [l^*_{i,j}]$ possui a estrutura da matriz L do lema 2.12 com

$$\begin{aligned} &l^*_{1,3} = g_4 g_3^{-1}; \\ &l^*_{i,i+2} = 1 \quad \text{para } i \in \{2, \ldots, n-2\}; \\ &x^*_1 = (-1)^{n-1} g_1 g_3 |A|; \\ &x^*_2 = (-1)^{n-1} |A| g_2 + a_2 g_3 \end{aligned}$$

e, para $i \in \{3, \ldots n\}$,

$$x^*_i = (-1)^{n-1}|A|d_i + \text{ termos não envolvendo } d_3, \ldots, d_n \tag{2.34}$$

Note-se que x_i, com $i \in \{3, \ldots n\}$, são todos os elementos de L^* que dependem de $d_3, \ldots, d_n$.

Pelo lema 2.12, existe uma matriz $S \in SL(n, F)$ que satisfaz (2) e (3) e tal que $SL^*S^{-1} = C(\lambda^n + w_n\lambda^{n-1} + \cdots + w_2\lambda + w_1)$, onde $\lambda^n + w_n\lambda^{n-1} + \cdots + w_2\lambda + w_1 \in F[\lambda]$.

Saliente-se que, sendo L^* e $C(\lambda^n + w_n\lambda^{n-1} + \cdots + w_2\lambda + w_1)$ matrizes semelhantes, os seus polinómios característicos coincidem e são $\lambda^n + w_n\lambda^{n-1} + \cdots + w_2\lambda + w_1$.

Mas, como $(-1)^n w_1 = |L^*| = |A\Delta_n| = |A| g_1 g_3$, tem-se que $w_1 = (-1)^n |A| g_1 g_3$. Seja $w_1 = q_1$. Mas uma expressão para o coeficiente de λ no polinómio característico de L^* já está determinada e, portanto, tem-se que

$$w_2 = -(x^*_2 + x^*_1(l^*_{1,3} + l^*_{2,4} + \cdots l^*_{n-2,n}))$$

$$= -\left[\left((-1)^{n-1}|A|g_2 + a_2 g_3\right) + (-1)^{n-1}|A| g_1 g_3 (g_4 g_3^{-1} + \underbrace{1 + \cdots + 1}_{n-3})\right]$$

$$= (-1)^n |A| g_2 - a_2 g_3 + (-1)^n |A| \left(g_1 g_4 + (n-3) g_1 g_3\right)$$

$$= (-1)^n |A| (g_2 + g_1 g_4 + (n-3) g_1 g_3) - a_2 g_3 = q_2.$$

Considere-se, agora, $S^{-1} = [t_{i,j}]$. Observe-se que, sendo S (e, consequentemente S^{-1}) independente dos elementos x_i, é, também, independente dos elementos d_i e, portanto, as entradas

$t_{i,j}$ são independentes de d_i e também satisfazem (2) do lema 2.12. Do produto SL^*S^{-1} é possível obter que

$$w_i = -\left(x_i^* + \sum_{j=1}^{i-1} t_{j,i}x_j^*\right), \quad i \in \{3,\ldots,n\}$$

e, fazendo, $w_i = q_i$ para $i \in \{3,\ldots,n\}$, como x_1^* e x_2^* são conhecidos, é possível resolver o sistema anterior em ordem a $x_3^*,\ldots x_n^*$. Substituindo depois em (2.34), é possível determinar $d_3,\ldots,d_n$ de forma a que $w_i = q_i$ para todo o $i \in \{1,2,\ldots,n\}$.

Fica, assim, concluída a demonstração do lema.

■

Para $n \geq 2$ seja $M = [m_{i,j}] \in F^{n\times n}$ tal que $m_{i,i+1} = 1$ para $i \in \{1,\ldots n-1\}$ e $m_{i,j} = 0$ sempre que $j \geq i+2$, ou seja, M possui a forma:

$$M = \begin{bmatrix} m_{1,1} & 1 & 0 & \cdots & \cdots & 0 \\ m_{2,1} & m_{2,2} & 1 & \ddots & & \vdots \\ \vdots & & \ddots & \ddots & \ddots & \vdots \\ \vdots & & & \ddots & \ddots & 0 \\ \vdots & & & & \ddots & 1 \\ m_{n,1} & m_{n,2} & \cdots & \cdots & \cdots & m_{n,n} \end{bmatrix}.$$

Lema 2.14. *Existe $S \in SL(n,F)$ tal que SMS^{-1} é uma matriz companheira.*

Demonstração

Para $k \in \{1,\ldots,n-1\}$, seja $S_k = S_{k+1,1}(m_{k,1})S_{k+1,2}(m_{k,2})\cdots S_{k+1,k}(m_{k,k}) \in SL(n,F)$. Então $S_kMS_k^{-1}$ possui a estrutura da matriz M nas linhas $1,2,\cdots,k-1$ e $m_{k,1} = m_{k,2} = \cdots = m_{k,k} = 0$. Note-se que a $(k+1)-$ésima linha de $S_kMS_k^{-1}$ é alterada em relação a M, assim como as colunas $1,2,\ldots,k$.

Considere-se $S_1 = S_{2,1}(m_{1,1})$, $S_k = S_{k+1,1}(m_{k,1}^*)S_{k+1,2}(m_{k,2}^*)\cdots S_{k+1,k}(m_{k,k}^*)$, para $k \in \{2,\ldots,n-1\}$, onde cada elemento $m_{k,j}^*$ presente nos factores de S_k se refere à entrada (k,j) da matriz $S_{k-1}S_{k-2}\cdots S_1MS_1^{-1}\cdots S_{k-2}^{-1}S_{k-1}^{-1}$.

Pelo que foi referido no início da demonstração, tem-se, então que

$$S_{n-1}S_{n-2}\cdots S_1MS_1^{-1}\cdots S_{n-2}^{-1}S_{n-1}^{-1}$$

é uma matriz companheira.

Considerando $S = S_{n-1}S_{n-2}\cdots S_1$, tem-se que $S \in SL(n,F)$ e SMS^{-1} é uma matriz companheira. Fica, assim, concluída a demonstração do lema.

■

Para $n \geq 3$ seja $N = [n_{i,j}] \in SL(n, GF(3))$ tal que $n_{1,1,} = n_{2,2} = -1$, $n_{i,i} = 1$ para $i \in \{3,\ldots,n\}$ e $n_{i,i+1} = 1$ para todo o $i \neq 2$. Além disso, $n_{i,j} = 0$ sempre que $i > j$. A matriz N possui a forma:

$$N = \begin{bmatrix} -1 & 1 & n_{1,3} & \cdots & \cdots & n_{1,n} \\ 0 & -1 & n_{2,3} & n_{2,4} & & \vdots \\ \vdots & \ddots & 1 & 1 & \ddots & \vdots \\ \vdots & & \ddots & \ddots & \ddots & n_{n-2,n} \\ \vdots & & & \ddots & \ddots & 1 \\ 0 & \cdots & \cdots & \cdots & 0 & 1 \end{bmatrix}.$$

Lema 2.15. *Existe $S \in SL(n,F)$ tal que $SNS^{-1} = \Delta_n(-1,1,-1,n_{2,3},d)$ onde os elementos $n_{2,3}$ e d podem ser substituídos por elementos arbitrários de F.*

Demonstração

Inicialmente será provado que é possível, sem perda de generalidade, supor que

$$n_{3,j} = n_{4,j} = \cdots = n_{j-2,j} = 0 \text{ para } j \in \{5,\ldots,n\}. \tag{2.35}$$

Suponha-se que, para qualquer $k \in \{5,\ldots,n-1\}$, as igualdades (2.35) são verificadas para $j \geq k+1$ e considere-se

$$S_k = S_{k-2,k-1}(-n_{k-2,k})S_{k-3,k-1}(-n_{k-3,k})\cdots S_{3,k-1}(-n_{3,k}) \in SL(n,F).$$

Se $k = n$, considere-se o conjunto das igualdades (2.35) como sendo o vazio e observe-se que $S_kNS_k^{-1} = [n^*_{i,j}]$ é uma matriz semelhante a N e que satisfaz as igualdades

$$n^*_{3,k} = n^*_{4,k} = \cdots = n^*_{k-2,k} = 0$$

e, portanto, (2.35) verifica-se quando $j = k$.

Seja $T = S_{n-1}S_{n-2}\cdots S_5 \in SL(n,F)$. Assim, TNT^{-1} é uma matriz semelhante a N que verificas as condições referidas em (2.35).

É possível, então, sem perda de generalidade, supor que N possui a seguinte forma:

$$N = \begin{bmatrix} -1 & 1 & n_{1,3} & n_{1,4} & \cdots & \cdots & n_{1,n} \\ 0 & -1 & n_{2,3} & n_{2,4} & \cdots & \cdots & n_{2,n} \\ \vdots & \ddots & 1 & 1 & 0 & \cdots & 0 \\ \vdots & & \ddots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & & \ddots & \ddots & \ddots & 0 \\ \vdots & & & & \ddots & \ddots & 1 \\ 0 & \cdots & \cdots & \cdots & \cdots & 0 & 1 \end{bmatrix}.$$

Para quaisquer $x_i, y_i \in F$ e $3 \leq i \leq n$ tem-se que

$$N' = [n'_{i,j}] = S_{2,i}(x_i)S_{1,i}(y_i)NS_{1,i}(x_i)^{-1}S_{2,i}(y_i)^{-1}$$

é uma matriz semelhante a N e que difere de N apenas nas entradas $(1,j)$ e $(2,j)$ para $j \geq i$. Em particular, $n'_{1,i} = n_{1,i} + 2y_i$ e $n'_{2,i} = n_{2,i} + 2x_i$.

Escolhendo x_i, y_i adequadamente é possível, para $j \geq i$ fixo, substituir em N' as entradas $n'_{1,j}$ e $n'_{2,j}$ por quaisquer elementos de F.

Seja

$$S = S_{2,n}(x_n)S_{1,n}(y_n)S_{2,n-1}(x_{n-1})S_{1,n-1}(y_{n-1})\cdots S_{2,3}(x_3)S_{1,3}(y_3) \in SL(n,F)$$

onde $x_3, \ldots, x_n, y_3, \ldots, y_n \in F$.

Tem-se então que $SNS^{-1} = \Delta_n(-1, 1, -1, n_{2,3}, d)$. Observe-se que os elementos $x_3, \ldots, x_n$ podem ser escolhidos por forma a que $n_{1,3} = d_3, n_{1,4} = d_4, \ldots, n_{1,n} = d_n$ e $n_{2,4} = n_{2,5} = \cdots = n_{2,n} = 0$.

É assim possível encontrar uma matriz $S \in SL(n,F)$ nas condições do lema. Conclui-se, assim, a demonstração.

■

Deste ponto em diante, os resultados apresentados são válidos unicamente em $GF(3)$. Usa-se também o facto de que, se $x \in GF(3)$ e $x \neq 0$, então $x^2 = 1$.

Considere-se todos os polinómios mónicos de grau dois sobre $GF(3)$ com 1 como termo constante:

$$\begin{aligned} p_1(\lambda) &= \lambda^2 + 1; \\ p_2(\lambda) &= \lambda^2 + \lambda + 1 = (\lambda - 1)^2; \\ p_3(\lambda) &= \lambda^2 - \lambda + 1 = (\lambda + 1)^2; \end{aligned} \tag{2.36}$$

e as suas respectivas matrizes companheiras,

$$C_1 = C(p_1(\lambda)) = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix};$$

$$C_2 = C(p_2(\lambda)) = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix};$$

$$C_3 = C(p_3(\lambda)) = \begin{bmatrix} 0 & 1 \\ -1 & 1 \end{bmatrix}.$$

Lema 2.16. *Seja $A \in SL(n, GF(3))$ uma matriz companheira diferente de C_1, C_2 e C_3. Então $A = SDS^{-1}D^{-1}$ para $S, D \in SL(n, GF(3))$.*

Demonstração

A hipótese de A ser uma matriz companheira diferente de C_1, C_2 e C_3 implica imediatamente que $n \neq 2$.

Para $n = 1$, então $A = [1]$ e, fazendo $S = D = I_1$, tem-se o resultado pretendido.

Suponha-se, agora, que $n \geq 3$. Seja $p(\lambda) = \lambda^n - a_n\lambda^{n-1} - \cdots - a_2\lambda - (-1)^{n-1} \in GF(3)[\lambda]$ e $A = C(p(\lambda))$.

Considere-se $g_1 = -1,\ g_2 = -1,\ g_3 = -1$ e $g_4 \in GF(3)$ tal que

$$\begin{aligned} E &= (-1)^n|A|(g_2 + g_1g_4 + g_1g_3(n-3)) - a_2g_3 \\ &= (-1)^n(-1 - g_4 + n - 3) + a_2 \end{aligned} \tag{2.37}$$

é o coeficiente de λ no polinómio $q(\lambda) = (\lambda + 1)^2(\lambda - 1)^{n-2}$ e seja

$$D = \Delta_n(-1, -1, -1, g_4, d).$$

Assim, por (2.37) e usando o lema 2.13, existem matrizes $S_1 \in SL(n, GF(3))$ e $T_1 = [g_3^{-1}] \oplus I_{n-1} = [-1] \oplus I_{n-1}$ tais que, para um determinado vector d se verifica

$$S_1 T_1 A D T_1^{-1} S_1^{-1} = C((\lambda+1)^2(\lambda-1)^{n-2}). \tag{2.38}$$

Por outro lado, tem-se que

$$T_1 D T_1^{-1} = \begin{bmatrix} -1 & 1 & -d_3 & -d_4 & \cdots & \cdots & -d_n \\ 0 & -1 & g_4 & 0 & \cdots & \cdots & 0 \\ \vdots & \ddots & 1 & 1 & \ddots & & \vdots \\ \vdots & & \ddots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & & \ddots & \ddots & \ddots & 0 \\ \vdots & & & & \ddots & 1 & 1 \\ 0 & \cdots & \cdots & \cdots & \cdots & 0 & 1 \end{bmatrix}$$

e, portanto, $T_1 D T_1^{-1}$ está nas condições do lema 2.15.

Assim, existe uma matriz $S_2 \in SL(n, GF(3))$ tal que $S_2(T_1 D T_1^{-1})S_2^{-1} = \Delta_n(-1, 1, -1, 1, 0)$.

Observe-se, ainda, que $\Delta_n(-1, 1, -1, 1, 0)$ é uma matriz com a estrutura da matriz M do lema 2.14 e, portanto, existe uma outra matriz $S_3 \in SL(n, GF(3))$ tal que

$$S_3(S_2 T_1 D T_1^{-1} S_2^{-1})S_3^{-1} = C((\lambda+1)^2(\lambda-1)^{n-2}). \tag{2.39}$$

Seja, agora, $S = T_1^{-1} S_1^{-1} S_3 S_2 T_1 \in SL(n, GF(3))$. De (2.38) e (2.39) tem-se que $A = SDS^{-1}D^{-1}$.

Mas $|S| = |D| = 1$ e, portanto, a matriz A é, então, um comutador multiplicativo de matrizes em $SL(n, GF(3))$.

Conclui-se, assim, o demonstração do lema.

■

Lema 2.17. *Seja $A \in SL(n, GF(3))$ uma matriz companheira. Então, $A = SDS^{-1}D^{-1}$ para $S, D \in GL(n, GF(3))$ e tais que $|S| = -|D| = 1$.*

Demonstração

Observe-se que, pelo lema 2.4, existe uma matriz standard $D \in GL(n, GF(3))$, com divisores elementares $(\lambda+1)$ e $(\lambda-1)^{n-1}$ e tal que os divisores elementares de AD são também $(\lambda+1)$ e $(\lambda-1)^{n-1}$.

Mas, pelo lema 2.6, tem-se que $AD = SDS^{-1}$, onde $S \in SL(n, GF(3))$.

Desta forma, $A = SDS^{-1}D^{-1}$ onde $|S| = -|D| = 1$.

■

Com o objectivo de alcançar outros resultados, note-se que pelo mesmo lema 2.6, é possível escolher $S \in GL(n, GF(3))$ tal que $|S| = -1$.

Lema 2.18. *Sejam $\pi_1(\lambda)$ e $\pi_2(\lambda)$ polinómios mónicos e irredutíveis sobre $GF(3)$ e sejam $q_1(\lambda) = \pi_1(\lambda)^u$ e $q_2(\lambda) = \pi_2(\lambda)^v$ com $u, v \in \mathbb{N}$. Sejam, ainda, $A_1 = C(q_1(\lambda))$ e $A_2 = C(q_2(\lambda))$ com $|A_1| = |A_2| = -1$.*

Seja $A = A_1 \oplus A_2$. Então $A = SDS^{-1}D^{-1}$ onde $S, D \in SL(n, GF(3))$.

Demonstração

Para $i \in \{1, 2\}$, seja $-c_i$ o coeficiente de λ em $q_i(\lambda)$, polinómio de grau $j(i)$.

Note-se que, com $A = A_1 \oplus A_2$, tem-se $n = j(1) + j(2)$ e, como $|A_i| = -1$, o termo independente de $q_i(\lambda)$ é $(-1)^{j(i)-1}$.

Observe-se, uma vez mais, que se $\pi_1(\lambda) \neq \pi_2(\lambda)$ então $q_1(\lambda)$ e $q_2(\lambda)$ são primos entre si e tem-se que A é semelhante em $GL(n, GF(3))$ a $C(q_1(\lambda)q_2(\lambda))$.

Nas condições anteriores, é válido o lema 2.16 e, portanto, $A = SDS^{-1}D^{-1}$ para $S, D \in SL(n, GF(3))$.

É, no entanto, necessário verificar que $C(q_1(\lambda)q_2(\lambda))$ não coincide com C_1, C_2 ou C_3, ou seja, tem que verificar-se que $q_1(\lambda)q_2(\lambda)$ não coincide com os polinómios $p_1(\lambda), p_2(\lambda)$ ou $p_3(\lambda)$ definidos atrás.

Se $\mathrm{gr}(q_1(\lambda)q_2(\lambda)) \geq 3$, então não se verificam as excepções.

Se $\mathrm{gr}(q_1(\lambda)q_2(\lambda)) = 2$, então, ou $q_1(\lambda)q_2(\lambda) = \lambda^2+1$, ou $q_1(\lambda)q_2(\lambda) = (\lambda-1)^2$ ou $q_1(\lambda)q_2(\lambda) = (\lambda+1)^2$.

Se $q_1(\lambda)q_2(\lambda) = \lambda^2 + 1$, então

$$q_1(\lambda) = 1 \quad \text{e} \quad q_2(\lambda) = \lambda^2 + 1 \quad \text{ou}$$

$$q_1(\lambda) = \lambda^2 + 1 \quad \text{e} \quad q_2(\lambda) = 1.$$

Qualquer um dos casos é impossível tendo em conta que $q_1(\lambda)$ e $q_2(\lambda)$ são potências de polinómios irredutíveis de expoente maior ou igual a 1.

Se $q_1(\lambda)q_2(\lambda) = (\lambda+1)^2$, então

$$q_1(\lambda) = 1 \quad \text{e} \quad q_2(\lambda) = (\lambda+1)^2 \quad \text{ou}$$

$$q_1(\lambda) = (\lambda+1)^2 \quad \text{e} \quad q_2(\lambda) = 1 \quad \text{ou}$$

$$q_1(\lambda) = \lambda+1 \quad \text{e} \quad q_2(\lambda) = \lambda+1.$$

Os dois primeiros casos são impossíveis, tendo em conta que $q_1(\lambda)$ e $q_2(\lambda)$ são potências de um polinómio irredutível de expoente maior ou igual a 1. O terceiro é, também impossível, uma vez que $q_1(\lambda)$ e $q_2(\lambda)$ são primos entre si.

Analogamente se demonstra a impossibilidade de $q_1(\lambda)q_2(\lambda) = (\lambda-1)^2$.

Suponha-se, agora, que $\pi_1(\lambda) = \pi_2(\lambda)$. Sem perda de generalidade, pode supor-se que $j(1) \geq j(2)$ e $A = A_1 \oplus A_2$.

Se $j(2) = 1$, o coeficiente do termo constante de $q_2(\lambda)$ é 1 e, portanto, $q_2(\lambda) = \pi_2^{j(2)}$ onde $\pi_2(\lambda) = \lambda + 1$.

Mas, porque $\pi_1(\lambda) = \pi_2(\lambda)$, tem-se que $A_1 = C((\lambda+1)^{j(1)})$ e, como $|A_1| = -1 = -(-1)^{j(1)-1}$, $j(1)$ é ímpar.

Se além disso se tiver $j(1) = 1$, então

$$A = C(q_1(\lambda)) \oplus C(q_2(\lambda)) = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = -I_2.$$

Neste caso, o lema 2.18 é consequência do teorema 2.1.

Note-se que após terem sido estudados os casos referidos atrás, qualquer situação não abordada, está abrangida por um dos seguintes casos:

(a) $j(1) \geq 3$ e $j(2) \geq 3$;

(b) $j(1) \geq 3$ e $j(2) = 2$;

(c) $j(1) \geq 3$ e $j(2) = 1$;

(d) $j(1) = j(2) = 2$.

Note-se que nos casos (b) e (d) se tem $c_2 \neq 0$, pois se $c_2 = 0$ ter-se-ia $q_2(\lambda) = \lambda^2 - 1$ que não é uma potência de um polinómio irredutível.

Note-se, ainda, que no caso (d), uma vez que $\pi_1(\lambda) = \pi_2(\lambda)$, tem-se $c_2 = c_1$.

Na demonstração do caso (a), sejam $g_1 = 1, g_2 = b_1, g_3 = 1, g_4 = b_2$ e escolham-se $b_1, b_2 \in GF(3)$ tais que $b_1 b_2 \neq 0$ e de forma a que

$$E_1 = (-1)^{j(2)}|A_2|(g_2 + g_1 g_4 + g_1 g_3(j(2) - 3)) - c_2 g_3$$

$$= (-1)^{j(2)+1}(b_1 + b_2 + j(2) - 3) - c_2$$

seja o coeficiente de λ no polinómio $(\lambda + 1)(\lambda - 1)^{j(2)-1}$.

Nas demonstrações dos casos (b) e (d), escolha-se $b_2 = 1$ e $b_1 = -c_2 \neq 0$.

Na demonstração do caso (c), escolha-se $b_1 = b_2 = 1$.

Sejam $g_1 = -1,\ g_2 = -b_1,\ g_3 = -1$ e seja $g_4 \in GF(3)$ a solução de

$$(-1)^{j(1)+1}(-b_1 - g_4 + j(1) - 3) + c_1 = E_2, \tag{2.40}$$

onde E_2 é o coeficiente de λ no polinómio $(\lambda + 1)(\lambda - 1)^{j(1)-1}$.

Seja $T_1 = [g_3^{-1}] \oplus I_{j(1)-1}$.

Então, porque se verifica (2.40), e porque no caso (d) se tem $b_1 = -c_2 = -c_1$, verificam-se as condições do lema 2.13 e é possível encontrar uma sequência d em $GF(3)$ e uma matriz $S_1 \in SL(j(1), GF(3))$ cujas entradas satisfazem (2) do lema 2.12 e tais que

$$S_1 T_1 A_1 \Delta_{j(1)}(g_1, g_2, g_3, g_4, d) T_1^{-1} S_1^{-1} = C((\lambda + 1)(\lambda - 1)^{j(1)-1}).$$

Mas, pela escolha de b_1 e b_2 é possível aplicar novamente o lema 2.13 e encontrar uma outra sequência d' em $GF(3)$ e uma matriz $S_2 \in SL(j(2), GF(3))$ tais que

$$S_2 A_2 \Delta_{j(2)}(1, b_1, 1, b_2, d') S_2^{-1} = C((\lambda + 1)(\lambda - 1)^{j(2)-1})$$

note-se que, neste caso, a matriz T do lema 2.13 coincide com a identidade ($g_3 = 1$).

Seja, agora,

$$D = \left[\begin{array}{c|c} \Delta_{j(1)}(-1, -b_1, -1, g_4, d) & P \\ \hline 0 & \Delta_{j(2)}(1, b_1, 1, b_2, d') \end{array}\right] \in GF(3)^{(j(1)+j(2))\times(j(1)+j(2))}$$

onde $P = [p_{i,j}] \in GF(3)^{j(1)\times j(2)}$ é tal que:

$p_{1,k} = p_k, \quad k \in \{1, \ldots, j(2)\}$ com $p_1, \ldots, p_{j(2)}$ a determinar posteriormente;

Se $j(1) = 3$, então $p_{j(1)-1,1} = b_1 b_2 g_4$ e se $j(1) \geq 3$, então $p_{j(1)-1,1} = b_1 b_2$;

$p_{j(1),1} = b_1 b_2$;

As restantes entradas de P são nulas.

Note-se que $|D| = |\Delta_{j(1)}(-1, -b_1, -1, g_4, d)||\Delta_{j(2)}(1, b_1, 1, b_2, d')| = b_1^2 = 1$ e, portanto, $D \in SL(n, F)$.

Considere-se, agora, $U_1 = S_{j(1),j(1)+1}(b_1 b_2) \in SL(n, GF(3))$ em todos os casos, excepto no caso (d). Para o caso (d) considere-se $U_1 = S_{j(1),j(1)+1}(g_3^{-1} b_1 b_2) \in SL(n, GF(3))$.

Para tornar mais ligeira a notação associem-se as matrizes seguintes:

$$\Delta_{j(1)} = \Delta_{j(1)}(-1, -b_1, -1, g_4, d), \quad \Delta_{j(2)} = \Delta_{j(2)}(1, b_1, 1, b_2, d').$$

Tem-se, então, que

$$U_1 A D U_1^{-1} = U_1 \left[\begin{array}{c|c} A_1 & 0 \\ \hline 0 & A_2 \end{array}\right] \left[\begin{array}{c|c} \Delta_{j(1)} & P \\ \hline 0 & \Delta_{j(2)} \end{array}\right] U_1^{-1} = \left[\begin{array}{c|c} A_1 \Delta_{j(1)} & Z \\ \hline 0 & A_2 \Delta_{j(2)} \end{array}\right]$$

onde a matriz $Z \in GF(3)^{j(1) \times j(2)}$ é uma matriz em que as primeiras $j(1) - 1$ linhas são nulas e se $z = \left[\begin{array}{cccc} z_1 & z_2 & \cdots & z_{j(2)} \end{array}\right]$ é a $j(1)-$ésima linha de Z tem-se que

$$z_k = (-1)^{j(1)} p_k + \text{ termos não envolvendo } p_1, \ldots, p_{j(2)}, \quad 1 \leq k \leq j(2). \tag{2.41}$$

Seja $e = \left[\begin{array}{cccc} 1 & 0 & \cdots & 0 \end{array}\right] \in GF(3)^{1 \times j(2)}$ e faça-se $z = eS_2$. Recorde-se que a matriz $S_2 = [s_{i,j}]$ possui a forma

$$\left[\begin{array}{cccccc} 1 & * & * & \cdots & * & 0 \\ 0 & 1 & * & & * & 0 \\ 0 & 0 & 1 & \ddots & \vdots & \vdots \\ \vdots & \vdots & \ddots & \ddots & * & 0 \\ 0 & 0 & \cdots & 0 & 1 & 0 \\ 0 & 0 & \cdots & 0 & 0 & 1 \end{array}\right]$$

e, portanto,

$$\left[\begin{array}{cccc} z_1 & z_2 & \cdots & z_{j(2)-1} z_{j(2)} \end{array}\right] = \left[\begin{array}{cccc} 1 & s_{1,2} & \cdots & s_{1,j(2)-1} \quad 0 \end{array}\right].$$

Uma vez que os elementos de $s_{1,2}, s_{1,3}, \ldots, s_{1,j(2)-1}$ são conhecidos, ao fazer $z = eS_2$ é possível resolver as equações (2.41) em ordem a $p_1, \ldots, p_{j(2)}$.

Com os elementos $p_1, \ldots, p_{j(2)}$ determinados desta forma, a matriz ZS_2^{-1} é uma matriz em que todas as suas entradas são nulas à excepção da entrada na posição $(j(2), 1)$ que é igual a 1. Note-se que S_2^{-1} possui a mesma estrutura de S_2.

Note-se, ainda, que, tendo em contas as estruturas de S_1, T_1 e Z, tem-se que $S_1 Z = T_1 Z = Z$. Seja $U_2 = \left[\begin{array}{c|c} S_1T_1 & 0 \\ \hline 0 & S_2 \end{array}\right]$. Então, $U_2U_1ADU_1^{-1}U_2^{-1} =$

$$\left[\begin{array}{c|c} S_1T_1A_1\Delta_{j(1)}T_1^{-1}S_1^{-1} & S_1T_1ZS_2^{-1} \\ \hline 0 & S_2A_2\Delta_{j(2)}S_2^{-1} \end{array}\right]$$

$$= \left[\begin{array}{c|c} C((\lambda+1)(\lambda-1)^{j(1)-1}) & \overbrace{ZS_2^{-1}}^{=e} \\ \hline 0 & C((\lambda+1)(\lambda-1)^{j(2)}) \end{array}\right] \tag{2.42}$$

Mas, o polinómio característico de (2.42) é $(\lambda+1)^2(\lambda-1)^{n-2}$ e, como (2.42) é uma matriz com a estrutura da matriz M do lema 2.14, existe $U_3 \in SL(n, GF(3))$ tal que

$$U_3(U_2U_1ADU_1^{-1}U_2^{-1})U_3^{-1} = C((\lambda+1)^2(\lambda-1)^{n-2}). \tag{2.43}$$

Para os casos (a), (b) e (d), seja

$$U_4 = \left[\begin{array}{c|c|c|c|c} -b_1 & 0 & \cdots & \cdots & 0 \\ \hline 0 & I_{j(1)-1} & \ddots & & \vdots \\ \hline \vdots & \ddots & b_1b_2 & 0 & 0 \\ \vdots & & 0 & b_2 & 0 \\ \hline 0 & \cdots & 0 & 0 & I_{j(2)-2} \end{array}\right].$$

Para o caso (c), seja

$$U_4 = \left[\begin{array}{c|c} -b_1 & 0 \\ \hline 0 & I_{n-1} \end{array}\right].$$

Em qualquer um dos casos $U_4DU_4^{-1}$ é uma matriz com a estrutura da matriz N do lema 2.15 e, portanto, como consequência desse lema, existe uma matriz $U_5 \in SL(n, GF(3))$ tal que

$$U_5(U_4DU_4^{-1})U_5^{-1} = \Delta_n(-1, 1, -1, 1, 0).$$

Mas, pelo lema 2.14, existe uma matriz $U_6 \in SL(n, GF(3))$ tal que

$$U_6(U_5U_4DU_4^{-1}U_5^{-1})U_6^{-1} = C((\lambda+1)^2(\lambda-1)^{n-2}) \tag{2.44}$$

Seja $S = U_1^{-1}U_2^{-1}U_3^{-1}U_6U_5U_4$ e note-se que

$|U_2| = |S_1T_1 \oplus S_2| = |T_1| = -1$;

$|U_4| = (-b_1)b_1b_2b_2 = -b_1^2b_2^2 = -1$ nos casos (a), (b) e (d);

$|U_4| = -b_1 = -1$ no caso (c) pois, nesse caso, b_1 foi escolhido sendo igual a 1;

$|U_1^{-1}| = |U_3^{-1}| = |U_6| = |U_5| = 1$.

Portanto, $|S| = 1$.

De (2.43) e (2.44) tem-se que $A = SDS^{-1}D^{-1}$ com $S, D \in SL(n, GF(3))$.

Conclui-se, assim, a demonstração do lema.

■

Lema 2.19. *Nas condições do lema anterior pode ter-se, também,* $|S| = -|D| = 1$.

Demonstração

Dada a semelhança entre os enunciados dos dois lemas anteriores, é com alguma naturalidade que essa semelhança se transporta também para as suas demonstrações. Assim, a maior parte dos elementos envolvidos nesta demonstração serão os definidos na demonstração anterior.

Para $i = 1, 2$, seja $-c_i$ o coeficiente de λ em $q_i(\lambda)$ e note-se que o termo constante de $q_i(\lambda)$ é $(-1)^{j(i)-1}$.

À semelhança do que foi escrito na demonstração anterior, se $\pi_1(\lambda) \neq \pi_2(\lambda)$, tem-se que A é semelhante em $GL(n, GF(3))$ a $C(q_1(\lambda)q_2(\lambda))$.

Mas, então a matriz A está nas condições do lema 2.17 e, portanto, existem matrizes $S, D \in GF(3)^{n\times n}$ tais que $|S| = -|D| = 1$ e $A = SDS^{-1}D^{-1}$.

É, no entanto, necessário garantir que $C(q_1(\lambda)q_2(\lambda))$ não coincide com C_1, C_2 ou C_3. Essa verificação já foi realizada na demonstração do lema 2.18.

Suponha-se, agora, que $\pi_1(\lambda) = \pi_2(\lambda)$ e, sem perda de generalidade, suponha-se, ainda, que $j(1) \geq j(2)$.

Se $j(2) = 1$, tem-se que $j(1)$ é ímpar. Se além disso se tiver $j(1) = 1$, então

$$A = C(q_1(\lambda)) \oplus C(q_2(\lambda)) = -I_2.$$

Considere-se

$$S = C(\lambda^2 + 1) \quad \text{e} \quad D = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$$

e note-se que $|S| = -|D| = 1$. Tem-se, também, que

$$SDS^{-1}D^{-1} = -I_2 = A.$$

Tem-se então o resultado pretendido, se $j(1) = j(2) = 1$.

Após a demonstração de alguns casos particulares, note-se que, uma vez mais, qualquer situação está abrangida pelo casos (a), (b), (c) e (d) da demonstração do lema anterior.

As observações a fazer são as mesmas da demonstração anterior: nos casos (b) e (d) tem-se que $c_2 \neq 0$ e no caso (d) tem-se que $c_2 = c_1$.

Para o estudo do caso (a), sejam $b_1, b_2 \in GF(3)$ tais que $b_1 b_2 \neq 0$ e tais que

$$(-1)^{j(2)+1}(b_1 + b_2 + j(2) - 3) - c_2 = E_1$$

onde E_1 é o coeficiente de λ no polinómio $(\lambda + 1)(\lambda - 1)^{j(2)-1}$.

Para os casos (b) e (d), sejam $b_2 = 1$ e $b_1 = -c_2 \neq 0$.

Quanto ao caso (c), sejam $b_1 = b_2 = 1$.

Escolham-se $g_1 = -1,\ g_3 = 1\ g_4 = 1$ e seja g_2 a solução de

$$(-1)^{j(1)+1}(g_2 - 1 - (j(1) - 3)) - c_1 = E_2 \tag{2.45}$$

onde E_3 é o coeficiente de λ no polinómio $(\lambda - 1)^{j(1)}$.

Seja $T_1 = [g_3^{-1}] \oplus I_{j(1)-1}$.

Então, porque se verifica (2.45), é possível aplicar-se o lema 2.13 e encontrar uma sequência d em $GF(3)$ e uma matriz $S_1 \in SL(j(1), GF(3))$ cujas entradas satisfazem (2) do lema 2.12 e tais que

$$S_1 T_1 A_1 \Delta_{j(1)}(g_1, g_2, g_3, g_4, d) T_1^{-1} S_1^{-1} = C((\lambda - 1)^{j(1)}).$$

Mas, tendo em conta a escolha de b_1 e b_2 é possível aplicar novamente o lema 2.13 e encontrar uma outra sequência d' em $GF(3)$ e uma matriz $S_2 \in SL(j(2), GF(3))$ tais que

$$S_2 A_2 \Delta_{j(2)}(1, b_1, 1, b_2, d') S_2^{-1} = C((\lambda + 1)(\lambda - 1)^{j(2)-1}).$$

Defina-se, agora,

$$D = \left[\begin{array}{c|c} \Delta_{j(1)}(-1, g_2, 1, 1, d) & P \\ \hline 0 & \Delta_{j(2)}(1, b_1, 1, b_2, d') \end{array}\right]$$

onde $P = [p_{i,j}] \in GF(3)^{j(1)\times j(2)}$ é a matriz definida na demonstração do lema anterior.

Observe-se que $|D| = |\Delta_{j(1)}(-1, g_2, 1, 1)||\Delta_{j(2)}(1, b_1, 1, b_2)| = -1$.

Considere-se, agora, $U_1 = S_{j(1),j(1)+1}(b_1 b_2) \in SL(n, GF(3))$ em todos os casos, excepto no caso (d). Para o caso (d) considere-se $U_1 = S_{j(1),j(1)+1}(g_3^{-1} b_1 b_2) \in SL(n, GF(3))$. Tem-se, então, que

$$U_1 A D U_1^{-1} = \left[\begin{array}{c|c} A_1 \Delta_{j(1)}(-1, g_2, 1, 1, d) & Z \\ \hline 0 & A_2 \Delta_{j(2)}(1, b_1, 1, b_2, d') \end{array}\right]$$

onde a matriz $Z \in GF(3)^{j(1)\times j(2)}$ é uma matriz em que as suas primeiras $j(1)-1$ linhas são nulas e se $z = \left[\begin{array}{cccc} z_1 & z_2 & \cdots & z_{j(2)} \end{array}\right]$ é a $j(1)-$ésima linha de Z tem-se que

$$z_k = (-1)^j(1)p_k + \text{ termos não envolvendo } p_1, \ldots, p_{j(2)}, \quad 1 \leq k \leq j(2) \tag{2.46}$$

Defina-se e como atrás: $e = \left[\begin{array}{cccc} 1 & 0 & \cdots & 0 \end{array}\right] \in GF(3)^{1\times j(2)}$

Faça-se $z = eS_2$. Tem-se, então,

$$\left[\begin{array}{cccc} z_1 & z_2 & \cdots & z_{j(2)-1} z_{j(2)} \end{array}\right] = \left[\begin{array}{cccc} 1 & s_{1,2} & \cdots & s_{1,j(2)-1} \quad 0 \end{array}\right]$$

e vez que os elementos de $s_{1,2}, s_{1,3}, \ldots, s_{1,j(2)-1}$ são conhecidos, é possível resolver as equações (2.46) em ordem a $p_1, \ldots, p_{j(2)}$.

Com $p_1, \ldots, p_{j(2)}$ determinados desta forma, a matriz ZS_2^{-1} é uma matriz em que todas as suas entradas são nulas à excepção da entrada na posição $(j(2), 1)$ que é igual a 1.

Note-se que, tendo em contas as estruturas de S_1, T_1 e Z, tem-se que $S_1 Z = T_1 Z = Z$.

Seja $U_2 = \left[\begin{array}{c|c} S_1 T_1 & 0 \\ \hline 0 & S_2 \end{array}\right]$. Então,

$$U_2 U_1 A D U_1^{-1} U_2^{-1} = \left[\begin{array}{c|c} C((\lambda-1)^{j(1)}) & ZS_2^{-1} \\ \hline 0 & C((\lambda+1)(\lambda-1)^{j(2)}) \end{array}\right]. \tag{2.47}$$

Mas, o polinómio característico de (2.47) é $(\lambda+1)(\lambda-1)^{n-1}$ e, como (2.47) é uma matriz nas condições do lema 2.14, existe $U_3 \in SL(n, GF(3))$ tal que

$$U_3(U_2 U_1 A D U_1^{-1} U_2^{-1}) U_3^{-1} = C((\lambda+1)(\lambda-1)^{n-1}). \tag{2.48}$$

Observe-se que AD é semelhante à matriz $C((\lambda+1)(\lambda-1)^{n-1})$ e, portanto, os seus divisores elementares são $(\lambda+1)$ e $(\lambda-1)^{n-1}$.

Escolha-se, agora, x tal que $(g_3-g_1)x+g_2=1$, o que equivale a $(1-(-1))x+g_2=1$, ou seja, $x=-1+g_2$.

Seja $U_7=S_{1,2}(x)\in SL(n,GF(3))$.

$$U_7DU_7^{-1}=\left[\begin{array}{cccccc|c} -1 & 1 & d_3+x & d_4 & \cdots & d_n & \\ 0 & 1 & 1 & 0 & \cdots & 0 & \\ \vdots & \ddots & 1 & 1 & \ddots & \vdots & P \\ \vdots & & \ddots & \ddots & \ddots & 0 & \\ \vdots & & & \ddots & \ddots & 1 & \\ 0 & \cdots & \cdots & \cdots & 0 & 1 & \\ \hline \multicolumn{6}{c|}{0} & \Delta_{j(2)}(1,b_1,1,b_2,d') \end{array}\right].$$

Considere-se, agora, a matriz $\lambda I_n-U_7DU_7^{-1}$. O menor de ordem $n-1$ obtido retirando a primeira linha e a primeira coluna é $(\lambda-1)^{n-1}$ e o menor de ordem $n-1$ que se obtém retirando a última linha e a primeira coluna é um polinómio em λ que não possui 1 como raiz. Assim, o máximo divisor comum dos menores de ordem $n-1$ é 1 e, portanto, D possui um único polinómio invariante não constante.

Mas isso significa que D é não derrogatória (porque $U_7DU_7^{-1}$ é não derrogatória). Assim, o polinómio característico de D coincide com o seu polinómio mínimo que, por sua vez, coincide com o último (e único) polinómio invariante não constante de D.

Mas, o polinómio característico de D é o produto dos polinómios característicos de $\Delta_{j(1)}$ e $\Delta_{j(2)}$ e que são, respectivamente, $(\lambda+1)(\lambda-1)^{j(1)-1}$ e $(\lambda-1)^{j(2)}$. Portanto o polinómio característico de D é $(\lambda+1)(\lambda-1)^{n-1}$ e os divisores elementares de D são, por decomposição do polinómio característico, $(\lambda+1)$ e $(\lambda-1)^{n-1}$.

Observe-se que, como A e AD possuem os mesmos divisores elementares (em particular um divisor elementar linear), são semelhantes e verificam as condições do lema 2.6. Tem-se, então, que existe $S\in SL(n,GF(3))$ tal que $AD=SDS^{-1}$. Mas, assim, $A=SDS^{-1}D^{-1}$ é comutador multiplicativo de matrizes, com $|S|=-|D|=1$. Conclui-se, assim, a demonstração do lema.

■

Lema 2.20. *Para $i \in \{1,2,3\}$ tem-se que $C_i \oplus C_i = S_i D_i S_i^{-1} D_i^{-1}$ onde $S_i, D_i \in GL(4, GF(3))$ e $|S_i| = -|D_i| = 1$.*

Demonstração

Seja C uma das matrizes C_1, C_2 ou C_3. Tendo em conta o comentário feito no final do lema 2.17, existem matrizes $X, Y \in GL(2, GF(3))$ com $|X| = |Y| = -1$ tais que $C = XYX^{-1}Y^{-1}$.

Utilizando, novamente, o lema 2.17, desta vez aplicado à matriz C^{-1}, que, em qualquer um dos casos é semelhante a C, existem matrizes $U, V \in GL(2, GF(3))$ com $-|U| = |V| = 1$ tais que $C = UVU^{-1}V^{-1}$.

Mas então,

$$C \oplus C = \left[\begin{array}{c|c} C & 0 \\ \hline 0 & C \end{array}\right] = \left[\begin{array}{c|c} X & 0 \\ \hline 0 & U \end{array}\right] \left[\begin{array}{c|c} Y & 0 \\ \hline 0 & V \end{array}\right] \left[\begin{array}{c|c} X^{-1} & 0 \\ \hline 0 & U^{-1} \end{array}\right] \left[\begin{array}{c|c} Y^{-1} & 0 \\ \hline 0 & V^{-1} \end{array}\right].$$

Fazendo $S = X \oplus U, \in GL(4, GF(3))$ e $D = Y \oplus V \in GL(3, GF(3))$, tem-se que $C = SDS^{-1}D^{-1}$ e $|S| = -|D| = 1$.

Fica, assim, concluída a demonstração do lema.

■

Após a apresentação dos resultados anteriores, é possível passar à apresentação e demonstração do principal resultado desta secção:

Teorema 2.4. *Se $A \in SL(2, GF(3))$ então $A = XYX^{-1}Y^{-1}$ com $X, Y \in GL(2, GF(3))$.*

Se $A \in SL(n, GF(3))$ para $n > 2$ então $A = XYX^{-1}Y^{-1}$ com $X, Y \in SL(n, GF(3))$.

Demonstração

Se $A \in SL(2, GF(3))$, então, ou A é escalar ou A é semelhante em $GL(2, GF(3))$ a uma matriz companheira.

No primeiro caso, o teorema 2.1 permite concluir que existem matrizes $X, Y \in GL(2, GF(3))$ tais que $A = XYX^{-1}Y^{-1}$. No segundo caso, o lema 2.17 permite obter a mesma conclusão: A é um comutador multiplicativo de matrizes em $GL(2, GF(3))$.

Seja, agora, $A \in SL(n, GF(3))$ com $n > 2$.

Observe-se que A é semelhante à sua forma normal invariante $F_I(A)$. Sem perda de generalidade, suponha-se que $A = F_I(A)$, e, ainda, sem perda de generalidade, aplicando uma transformação de semelhança que troque a ordem dos blocos associados a cada matriz companheira que entra na composição de $F_I(A)$, suponha-se que A possui a forma seguinte:

$$A = A_1 \oplus A_2 \oplus \cdots \oplus A_m, \tag{2.49}$$

onde para cada $i \in \{1, 2, \ldots, m\}$, $A_i \in GF(3)^{j(i)\times j(i)}$, e ou A_i é matriz companheira de uma potência de um polinómio irredutível com coeficientes em $GF(3)$ e $|A_i| = 1$, ou então, $A_i = A_{i,1} \oplus A_{i,2}$ onde $A_{i,1}$ e $A_{i,2}$ são ambas matrizes companheiras de potências de polinómios irredutíveis com coeficientes em $GF(3)$ e $|A_{i,1}| = |A_{i,2}| = -1$. Note-se que, a existir um determinado número de matrizes companheiras com determinante igual a -1, esse número será sempre par, uma vez que o determinante de A é igual a 1.

Se para todo o $i \in \{1, 2, \ldots, m\}$, A_i é diferente de C_1, C_2 e C_3, então qualquer um dos lemas 2.16 ou 2.18 permite concluir que existem matrizes $S_i, D_i \in SL(j(i), GF(3))$ tais que

$$A_i = S_i D_i S_i^{-1} D_i^{-1}.$$

Nesse caso, sejam $X = S_1 \oplus S_2 \oplus \cdots \oplus S_m$, $Y = D_1 \oplus D_2 \oplus \cdots \oplus D_m$ matrizes em $SL(n, GF(3))$. Desta forma $A = XYX^{-1}Y^{-1}$ e é, portanto, um comutador multiplicativo de matrizes em $SL(n, GF(3))$.

Se algumas das parcelas da soma directa (2.49) forem C_1, C_2 ou C_3, mas existe uma matriz A_i distinta de C_1, C_2 e C_3, então por qualquer um dos lemas 2.17 ou 2.19, para cada A_k, com $k \neq i$, existem matrizes $S_k, D_k \in GL(j(k), GF(3))$ tais que

$$A_k = S_k D_k S_k^{-1} D_k^{-1} \quad \text{e} \quad |S_k| = -|D_k| = 1.$$

Utilizando um dos lemas 2.16, 2.17, 2.18 ou 2.19 é possível encontrar matrizes $S_i, D_i \in GL(j(i), GF(3))$ tais que

$$A_i = S_i D_i S_i^{-1} D_i^{-1} \quad \text{e} \quad |S_i| = |D_1 D_2 \cdots D_m| = 1.$$

Sejam $X = S_1 \oplus S_2 \oplus \cdots \oplus S_m$, $Y = D_1 \oplus D_2 \oplus \cdots \oplus D_m$ matrizes em $SL(n, GF(3))$.

Tem-se, então, que $A = XYX^{-1}Y^{-1}$ e é, portanto, um comutador multiplicativo de matrizes em $SL(n, GF(3))$.

Suponha-se, agora, que cada matriz A_i na soma directa (2.49) é C_1, C_2 ou C_3.

Quando m é par, é possível aplicar o lema 2.17 para encontrar $S_i, D_i \in GL(j(i), GF(3))$, $i \in \{1, 2, \ldots, m\}$, tais que

$$A_i = S_i D_i S_i^{-1} D_i^{-1} \quad \text{e} \quad |S_i| = -|D_i| = 1.$$

Sejam $X = S_1 \oplus S_2 \oplus \cdots \oplus S_m$, $Y = D_1 \oplus D_2 \oplus \cdots \oplus D_m$ matrizes em $SL(n, GF(3))$.

Tem-se, então, que $A = XYX^{-1}Y^{-1}$ sendo, um comutador multiplicativo de matrizes em $SL(n, GF(3))$.

Quando m é ímpar e surgem duas matrizes C_i distintas na soma directa (2.49) (sem perda de generalidade, suponha-se que são por exemplo $A_{m-1} = C_1$ e $A_m = C_2$), então, como $A_{m-1} \oplus A_m$ é semelhante a $A'_{m-1} = C(p_1(\lambda)p_2(\lambda))$, uma vez que os polinómios $p_1(\lambda)$ e $p_2(\lambda)$ definidos em (2.36) são primos entre si, tem-se que existe $U \in SL(n, GF(3))$ tal que

$$UAU^{-1} = A_1 \oplus A_2 \oplus \cdots, \oplus A_{m-2} \oplus A'_{m-1}.$$

Mas então UAU^{-1} é soma directa de $m-1$ matrizes companheiras e $m-1$ é par. É possível, então aplicar o lema 2.17 para encontrar $S_i, D_i \in GL(j(i), GF(3))$, $i \in \{1, 2, \ldots, m-2\}$, e $S_{m-1}, D_{m-1} \in GL(j(m-1) + j(m), GF(3))$ tais que

$$A_i = S_i D_i S_i^{-1} D_i^{-1} \quad \text{e} \quad |S_i| = -|D_i| = 1, \quad i \in \{1, 2, \ldots, m-1\}.$$

Sejam $X = S_1 \oplus S_2 \oplus \cdots \oplus S_{m-1}$, $Y = D_1 \oplus D_2 \oplus \cdots \oplus D_{m-1}$ matrizes em $SL(n, GF(3))$.

Desta forma, $A = XYX^{-1}Y^{-1}$ e é, portanto, um comutador multiplicativo de matrizes em $SL(n, GF(3))$.

Finalmente, quando m é ímpar e cada $A_i = C$, onde C é uma matriz fixa de entre as matrizes C_1, C_2 ou C_3, é possível aplicar o lema 2.17 para $i \in \{1, 2, \ldots, m-2\}$ e encontrar matrizes $S_i, D_i \in GL(j(i), GF(3))$ tais que

$$A_i = S_i D_i S_i^{-1} D_i^{-1} \quad \text{e} \quad |S_i| = -|D_i| = 1.$$

Mas, pelo lema 2.20

$$A_{m-1} \oplus A_m = S_{m-1} D_{m-1} S_{m-1}^{-1} D_{m-1}^{-1}$$

onde $S_{m-1}, D_{m-1} \in GL(j(m-1)+j(m), GF(3))$ e $|S| = -|D| = 1$.

Sejam $X = S_1 \oplus S_2 \oplus \cdots \oplus S_{m-1}$, $Y = D_1 \oplus D_2 \oplus \cdots \oplus D_{m-1}$ matrizes em $SL(n, GF(3))$.

Tem-se que $A = XYX^{-1}Y^{-1}$ e é, portanto, uma vez mais, um comutador multiplicativo de matrizes em $SL(n, GF(3))$.

Conclui-se, desta forma, a demonstração do teorema.

■

Com a demonstração do teorema anterior, finaliza-se o estudo de comutadores multiplicativos em $GF(3)$, concluindo-se que, se $A \in SL(n, GF(3))$, então A é um comutador multiplicativo de matrizes em $GL(n, GF(3))$ se $n = 2$, e é um comutador multiplicativo de matrizes em $SL(n, GF(3))$ se $n > 2$.

Capítulo 3

Comutadores Multiplicativos de Matrizes com Determinantes Prescritos

A. R. Sourour em [16] demonstrou que, se F é um corpo arbitrário e $A \in F^{n\times n}$ é uma matriz não escalar e não singular e $\beta_1, \cdots, \beta_n, \gamma_1, \cdots, \gamma_n \in F$ são tais que $|A| = \beta_1 \cdots \beta_n \gamma_1 \cdots \gamma_n$, então existem matrizes $B, C \in F^{n\times n}$ com valores próprios $\beta_1, \ldots, \beta_n$ e $\gamma_1, \ldots, \gamma_n$, respectivamente, tais que $A = BC$.

R. A. Horn e C. R. Johnson em [4] demonstraram uma variante do teorema de A. R. Sourour em $\mathbb{C}$ para o caso em que exactamente $n - \text{car}(A)$ elementos de $\beta_1, \ldots, \beta_n, \gamma_1, \ldots, \gamma_n \in \mathbb{C}$ são iguais a zero. Este resultado será apresentado de seguida.

Recentemente, F. C. Silva, S. Furtado e L. Iglésias descreveram em [6] todas as possibilidades de escrever uma matriz $A \in F^{n\times n}$, onde F é um corpo arbitrário, como produto de duas matrizes com entradas em F e com valores próprios prescritos.

Pretende-se com este capítulo, utilizando por base os resultados anteriores e alguns resultados auxiliares, revelar em que condições uma matriz $A \in SL(n, F)$ pode ser escrita como $BCB^{-1}C^{-1}$, com $B, C \in GL(n, F)$ e tais que $|B| = b, |C| = c, \in F\backslash\{0\}$. À semelhança dos capítulos anteriores, F denota um corpo qualquer.

Apresenta-se, então, de seguida o resultado devido a R. A. Horn e C. R. Johnson e publicado em [4].

Teorema 3.1. *Seja $A \in \mathbb{C}^{n\times n}$ e suponha-se que* $\mathrm{car}(A) = k \leq n$. *Se $k = n$, suponha-se que A é matriz não escalar.*

Sejam $\beta_1, \ldots, \beta_n$ e $\gamma_1, \ldots, \gamma_n \in \mathbb{C}$ tais que exactamente $n - k$ deles são nulos. Se $k = n$ suponha-se que $\beta_1 \cdots \beta_n \gamma_1 \cdots \gamma_n = |A|$.

Nestas condições, existem matrizes B e C com valores próprios $\beta_1, \ldots, \beta_n$ e $\gamma_1, \ldots, \gamma_n$, respectivamente, tais que $A{=}BC$.

Demonstração Se $k = 0$ então a matriz A coincide com a matriz nula de $\mathbb{C}^{n\times n}$ e $|A| = 0$. Uma vez que $k = 0$, entre $\beta_1, \ldots, \beta_n$ e $\gamma_1, \ldots, \gamma_n$ existem n elementos nulos e é possível reordenar os elementos $\gamma_1, \cdots, \gamma_n$ por forma a que $\beta_i\gamma_{j_i} = 0$ para $i, j_i \in \{1, 2, \cdots, n\}$. Assim, $B = \mathrm{diag}(\beta_1, \cdots, \beta_n)$ e $C = \mathrm{diag}(\gamma_{j_1}, \cdots \gamma_{j_n})$ satisfazem as condições do Teorema.

Suponha-se, agora que A é não escalar e que $k \geq 1$. Como, existe pelo menos um elemento não nulo na lista $\beta_1, \cdots, \beta_n$ e um elemento não nulo na lista $\gamma_1, \cdots, \gamma_n$, suponha-se, sem perda de generalidade que esses elementos são β_1 e γ_1. Tem-se, então, que $\beta_1\gamma_1 \neq 0$. A prova será feita por indução em n.

Se $n = 1$, então a matriz A é da forma $[\alpha]$, com $\alpha \in \mathbb{C}\backslash\{0\}$. Sejam $\beta_1, \gamma_1 \in \mathbb{C}$ tais que $\beta_1\gamma_1 \neq 0$ e $\beta_1\gamma_1 = |A| = \alpha$. As matrizes $B = [\beta_1]$ e $C = [\gamma_1]$ satisfazem as condições do Teorema.

Se $n = 2$, sejam $\beta_1, \beta_2, \gamma_1, \gamma_2 \in \mathbb{C}$ tais que $\beta_1\beta_2\gamma_1\gamma_2 = |A|$. Pelo lema 1.3 a matriz A é semelhante a

$$A^{(1)} = \begin{bmatrix} \beta_1\gamma_1 & y \\ x & z \end{bmatrix} \text{ com } y, x, z \in \mathbb{C}.$$

Sem perda de generalidade, suponha-se que $A = A^{(1)}$.

Observe-se que

$$|A| = \beta_1\beta_2\gamma_1\gamma_2 = \beta_1\gamma_1 z - xy$$

e, portanto,

$$z = (|A| + xy)(\beta_1\gamma_1)^{-1} = \beta_2\gamma_2 + xy\beta_1^{-1}\gamma_1^{-1}.$$

Sejam, agora, $B, C \in \mathbb{C}^{2\times 2}$ definidas por:

$$B = \begin{bmatrix} \beta_1 & 0 \\ \gamma_1^{-1}x & \beta_2 \end{bmatrix}, \quad C = \begin{bmatrix} \gamma_1 & \beta_1^{-1}y \\ 0 & \gamma_2 \end{bmatrix}.$$

Tem-se, então que B, C satisfazem as condições do teorema.

Suponha-se, agora, que $n \geq 3$, e $\text{car}(A) = k$ e que o teorema é válido para todas as matrizes em $\mathbb{C}^{(n-1)\times(n-1)}$.

Uma vez que as hipóteses e conclusões do teorema são invariantes para a semelhança, e usando o lema 1.3, suponha-se que a matriz $A = [a_{i,j}] \in \mathbb{C}^{n\times n}$ com $a_{1,1} = \beta_1\gamma_1$ e

$$\left[\begin{array}{ccccc} a_{2,1} & a_{3,1} & \cdots & a_{n,1} \end{array}\right]^T \neq 0_{(n-1)\times 1}.$$

O objectivo é encontrar matrizes B, C com as estruturas seguintes e que satisfaçam as condições do teorema.

$$B = \left[\begin{array}{c|c} \beta_1 & 0 \\ \hline B_{2,1} & B_{2,2} \end{array}\right] \text{ e } C = \left[\begin{array}{c|c} \gamma_1 & C_{1,2} \\ \hline 0 & C_{2,2} \end{array}\right],$$

com $\beta_1, \gamma_1 \in \mathbb{C}$, $B_{2,1}, C_{1,2}^T \in \mathbb{C}^{(n-1)\times 1}$ e $B_{2,2}, C_{2,2} \in \mathbb{C}^{(n-1)\times(n-1)}$.

Tem-se que

$$BC = \left[\begin{array}{c|c} \beta_1\gamma_1 & \beta_1 C_{1,2} \\ \hline \gamma_1 B_{2,1} & B_{2,1}C_{1,2} + B_{2,2}C_{2,2} \end{array}\right],$$

e particionando A como

$$A = \left[\begin{array}{c|c} \beta_1\gamma_1 & A_{1,2} \\ \hline A_{2,1} & A_{2,2} \end{array}\right],$$

tem-se que, para B e C serem soluções do problema, é necessário que verifiquem as igualdades

$$C_{1,2} = \beta_1^{-1}A_{1,2}, \quad B_{2,1} = \gamma_1^{-1}A_{2,1} \quad \text{e } B_{2,2}C_{2,2} = A_{2,2} - (\beta_1\gamma_1)^{-1}A_{2,1}A_{1,2}\ .$$

Se $A_{2,2} - (\beta_1\gamma_1)^{-1}A_{2,1}A_{1,2} \in \mathbb{C}^{(n-1)(n-1)}$ é uma matriz não escalar, então a hipótese de indução é passível de aplicação e observe-se que

$$|A_{2,2} - (\beta_1\gamma_1)^{-1}A_{2,1}A_{1,2}| = (\beta_1\gamma_1)^{-1}|A|$$

e

$$\text{car}(A_{2,2} - (\beta_1\gamma_1)^{-1}A_{2,1}A_{1,2}) = k - 1.$$

Assim, existem matrizes $B_{2,2}, C_{2,2} \in \mathbb{C}^{(n-1)\times(n-1)}$ com valores próprios $\beta_2, \cdots, \beta_n \in \mathbb{C}$ e $\gamma_2, \cdots, \gamma_n \in \mathbb{C}$, respectivamente, e tais que

$$A_{2,2} - (\beta_1\gamma_1)^{-1}A_{2,1}A_{1,2} = B_{2,2}C_{2,2}.$$

Considere-se agora as matrizes

$$B = \left[\begin{array}{c|c} \beta_1 & 0 \\ \hline \gamma_1^{-1}A_{2,1} & B_{2,2} \end{array}\right] \quad \text{e} \quad C = \left[\begin{array}{c|c} \gamma_1 & \beta_1^{-1}A_{1,2} \\ \hline 0 & C_{2,2} \end{array}\right].$$

Tem-se, então, que $A = BC$ e os valores próprios de B e C são, respectivamente, $\beta_1, \cdots, \beta_n$ e $\gamma_1, \cdots, \gamma_n$ e, assim, a demonstração fica completa sob a hipótese de $A_{2,2} - (\beta_1\gamma_1)^{-1}A_{2,1}A_{1,2}$ ser não escalar.

Observe-se que, se $k < n$, então, $\text{car}(A_{2,2} - (\beta_1\gamma_1)^{-1}A_{2,1}A_{1,2}) = k - 1$ e, portanto, a matriz $A_{2,2} - (\beta_1\gamma_1)^{-1}A_{2,1}A_{1,2}$ possui pelo menos duas linhas linearmente dependentes. Assim, a matriz $A_{2,2} - (\beta_1\gamma_1)^{-1}A_{2,1}A_{1,2}$ é uma matriz não escalar. Tem-se, então, que se $k < n$, existem matrizes B, C nas condições do teorema.

Se $k = n$ e $A_{2,2} - (\beta_1\gamma_1)^{-1}A_{2,1}A_{1,2}$ é não escalar a conclusão é a mesma que no parágrafo anterior.

Para finalizar a demonstração, suponha-se que $k = n$ e que $A_{2,2} - (\beta_1\gamma_1)^{-1}A_{2,1}A_{1,2} = \alpha I_{n-1}$ com $\alpha \in \mathbb{C}\backslash\{0\}$. Sob estas condições a demonstração tomará um rumo diferente.

Tem-se que $\text{car}(A_{2,2} - (\beta_1\gamma_1)^{-1}A_{2,1}A_{1,2}) = k - 1$ e portanto a matriz é não singular.

Note-se que, pelo facto de A ser não singular e n ser maior que 3, então $\text{car}(A) > 2$. Isso implica que $A_{2,2}$ possui pelo menos duas linhas linearmente independentes. Sem perda de generalidade, suponha-se que são as primeiras.

Suponha-se, ainda, que

$$A_{2,1} = \begin{bmatrix} x_1 & x_2 & \cdots & x_{n-1} \end{bmatrix}^T$$

e defina-se

$$w = \begin{bmatrix} a & b & 0 & \cdots & 0 \end{bmatrix}^T \in \mathbb{C}^{(n-1)\times 1},$$

onde $a, b \in \mathbb{C}\backslash\{0\}$ são escolhidos de forma a que $ax_1 + bx_2 = 0$.

Observe-se que $w^T A_{21} = 0$ e que $w^T A_{22} \neq 0$ uma vez que as duas primeiras linhas de $A_{2,2}$ são linearmente independentes.

É, assim, possível encontrar um vector $w^T \in \mathbb{C}^{(n-1)\times 1}$ tal que $w^T A_{2,1} = 0$ mas $w^T A_{2,2} \neq 0$.

Considere-se, agora,

$$S = \left[\begin{array}{c|c} 1 & w^T \\ \hline 0 & I_{n-1} \end{array}\right] \in SL(n, \mathbb{C}),$$

e observe-se que

$$S^{-1}AS = \left[\begin{array}{c|c} \beta_1\gamma_1 & A_{1,2} + \beta_1\gamma_1 w^T - w^T A_{2,2} \\ \hline A_{2,1} & A_{2,2} + A_{2,1}w^T \end{array}\right]$$

$$= \left[\begin{array}{c|c} \beta_1\gamma_1 & 0 \\ \hline A_{2,1} & K \end{array}\right] \left[\begin{array}{c|c} 1 & \beta_1^{-1}\gamma_1^{-1}(A_{1,2} + \beta_1\gamma_1 w^T - w^T A_{2,2}) \\ \hline 0 & I_{n-1} \end{array}\right], \tag{3.1}$$

onde $K = A_{2,2} + A_{2,1}w^T - A_{2,1}(A_{1,2} + \beta_1\gamma_1 w^T - w^T A_{2,2})\beta_1^{-1}\gamma_1^{-1}$.

Note-se, agora, que

$$K = A_{2,2} + A_{2,1}w^T - A_{2,1}(A_{1,2} + \beta_1\gamma_1 w^T - w^T A_{2,2})\beta_1^{-1}\gamma_1^{-1}$$

$$= (A_{2,2} - A_{2,1}A_{1,2}\beta_1^{-1}\gamma_1^{-1}) + A_{2,1}w^T A_{2,2}\beta_1^{-1}\gamma_1^{-1}$$

$$= \alpha I_{n-1} + A_{2,1}w^T A_{2,2}\beta_1^{-1}\gamma_1^{-1}.$$

Mas, como $A_{2,1} \neq 0$ e $w^T A_{2,2} \neq 0$, tem-se que $A_{2,1}w^T A_{2,2}\beta_1^{-1}\gamma_1^{-1}$ é uma matriz de característica 1 que perturba a matriz αI_{n-1}. De facto,

$$\text{car}(A_{2,1}w^T A_{2,2}) \leq \min\{\text{car}(A_{2,1}), \text{car}(w^T A_{2,2})\} = \min\{1, n_2\} = 1,$$

para algum n_2 inteiro maior do que 1.

Assim, a matriz $K = A_{2,2} + A_{2,1}w^T - A_{2,1}(A_{1,2} + \beta_1\gamma_1 w^T - w^T A_{2,2})\beta_1^{-1}\gamma_1^{-1}$ é uma matriz não escalar e é possível aplicar a hipótese de indução.

Existem, então, matrizes $B_1, C_1 \in \mathbb{C}^{(n-1)\times(n-1)}$ com valores próprios $\beta_2, \ldots, \beta_n$ e $\gamma_2, \ldots, \gamma_n$, respectivamente e tais que $K = B_1C_1$ e $|K| = \beta_1^{-1}\gamma_1^{-1}|A| = \beta_2\gamma_2\beta_3\gamma_3\cdots\beta_n\gamma_n$.

Mas, então a expressão (3.1) toma a forma

$$S^{-1}AS = \left[\begin{array}{c|c} \beta_1\gamma_1 & 0 \\ \hline A_{2,1} & B_1C_1 \end{array}\right] \left[\begin{array}{c|c} 1 & * \\ \hline 0 & I_{n-1} \end{array}\right]$$

$$= \left[\begin{array}{c|c} \beta_1 & 0 \\ \hline \gamma_1^{-1}A_{2,1} & B_1 \end{array}\right] \left[\begin{array}{c|c} \gamma_1 & 0 \\ \hline 0 & C_1 \end{array}\right] \left[\begin{array}{c|c} 1 & * \\ \hline 0 & I_{n-1} \end{array}\right]$$

$$= \underbrace{\left[\begin{array}{c|c} \beta_1 & 0 \\ \hline \gamma_1^{-1}A_{2,1} & B_1 \end{array}\right]}_{B_2} \underbrace{\left[\begin{array}{c|c} \gamma_1 & * \\ \hline 0 & C_1 \end{array}\right]}_{C_2}.$$

Observe-se, também que os valores próprios de B_2, C_2 são $\beta_1, \beta_2, \ldots, \beta_n$ e $\gamma_1, \gamma_2, \ldots, \gamma_n$, respectivamente.

Tem-se, então que $S^{-1}AS = B_2C_2$, o que equivale a

$$A = (SB_2S^{-1})(SC_2S^{-1}).$$

Definindo $B = SB_2S^{-1}, C = SC_2S^{-1} \in \mathbb{C}^{n\times n}$, tem-se que $A = BC$ e os valores próprios de B, C são respectivamente $\beta_1,\beta_2,\ldots,\beta_n$ e $\gamma_1,\gamma_2,\ldots,\gamma_n$.

Conclui-se, assim, a demonstração do teorema.

■

Tal como referido inicialmente, A. R. Sourour demonstrou o teorema anterior quando A e B são não singulares e possuem entradas num corpo qualquer. O resultado é apenas enunciado:

Teorema 3.2. *Seja $A \in F^{n\times n}$ uma matriz não escalar e invertível. Sejam $\beta_1,\ldots,\beta_n$ e $\gamma_1,\ldots,\gamma_n$ elementos de F tais que*

$$|A| = \beta_1\cdots\beta_n\gamma_1\cdots\gamma_n,$$

então existem $B, C \in F^{n\times n}$ com valores próprios $\beta_1,\ldots,\beta_n$ e $\gamma_1,\ldots,\gamma_n$ respectivamente, tais que $A = BC$. Além disso B e C podem ser triangulares inferior e superior, respectivamente.

O resultado anterior, em conjunto com o teorema de Shoda-Thompson, a apresentar posteriormente, permite retirar conclusões bastante importantes quanto à possibilidade de escrever uma matriz como um comutador multiplicativo de matrizes com determinantes arbitrários prescritos, recorrendo apenas à cardinalidade do corpo F.

K. Shoda em [15] mostrou que, num corpo algebricamente fechado, o conjunto dos comutadores multiplicativos de matrizes em $GL(n,F)$, ou seja, $\{BCB^{-1}C^{-1} : \quad B, C \in GL(n,F)\}$ coincide com $SL(n,F)$.

No capítulo 2 apresentou-se o resultado de R. C. Thompson que revela que o resultado de K. Shoda é válido para qualquer corpo F, excepto no caso em que $n = 2$ e $F = GF(2)$ ou $F = GF(3)$. Este autor caracterizou, ainda, em [20] os comutadores multiplicativos de matrizes com determinantes prescritos.

Os resultados de K. Shoda e de R. C. Thompson referidos anteriormente seguem do teorema apresentado de seguida supondo, neste caso, que $F \neq GF(2)$, e que F possui um número de elementos suficientemente grande. O seguinte teorema é denominado teorema de Shoda-Thompson.

Teorema 3.3. *Seja $A \in SL(n, F)$.*

1. *Se F tem pelo menos $n+1$ elementos, então A é um comutador multiplicativo de matrizes em $GL(n, F)$.*
2. *Se F tem pelo menos $n+2$ elementos e A é não escalar, então A é um comutador multiplicativo de matrizes em $SL(n, F)$.*
3. *Se F tem pelo menos $n+3$ elementos e A é não escalar, então A é um comutador multiplicativo de matrizes com determinantes não nulos previamente prescritos.*

Demonstração

1. Suponha-se inicialmente que $A \in SL(n, F)$ é uma matriz não escalar.

   Suponha-se, ainda, que o corpo F possui, pelo menos, $n+1$ elementos e observe-se que isso garante que existem $\beta_1, \ldots, \beta_n \in F\backslash\{0\}$ distintos dois a dois.

   Como F é um corpo, $\beta_1^{-1}, \ldots, \beta_n^{-1}$, também pertencem a F e, além disso, $\beta_1\beta_1^{-1} \ldots \beta_n\beta_n^{-1} = 1 = |A|$.

   Mas, pelo teorema 3.2, existem matrizes $B, C \in F^{n\times n}$ com valores próprios $\beta_1, \ldots, \beta_n$ e $\gamma_1 = \beta_1^{-1}, \ldots, \gamma_n = \beta_n^{-1}$, respectivamente, tais que $A = BC$.

   Como os valores próprios de cada matriz C, B^{-1} são distintos dois a dois, então C e B^{-1} são ambas não derrogatórias e possuem os mesmos valores próprios. São, então, semelhantes e existe $U \in SL(n, F)$ tal que $C = UB^{-1}U^{-1}$.

   Mas, então, $A = BC = BUB^{-1}U^{-1}$ e é, portanto, um comutador multiplicativo de matrizes em $GL(n, F)$.

   Suponha-se, agora, que $A \in SL(n, F)$ é uma matriz escalar não nula. Então, $A = \alpha I_n$, com $\alpha \in F\backslash\{0\}$ e $|A| = \alpha^n = 1$.

   Sejam $B = \text{diag}(\alpha, \alpha^2, \cdots, \alpha^{n-1}, 1)$ e $C = \text{diag}(1, \alpha^{-1}, \cdots, \alpha^{1-n})$ e note-se que $A = BC$.

   Observe-se, ainda que, pelos mesmos motivos referidos atrás, existe $V \in SL(n, F)$ tal que $C = VB^{-1}V^{-1}$.

   Assim, $A = BC = BVB^{-1}V^{-1}$ e é, portanto, um comutador multiplicativo de matrizes em $GL(n, F)$.

2. Seja $A \in SL(n, F)$ e suponha-se que F possui pelo menos $n+2$ elementos.

   Demonstrar-se-á que a hipótese anterior permite escolher n elementos, $\beta_1, \ldots, \beta_n \in F$, distintos dois a dois tais que o seu produto é $1 = |A|$. De facto,

   - Se n é ímpar, tome-se $\beta_1 = 1$ e $\frac{n-1}{2}$ pares distintos do tipo $\{\beta_i, \beta_i^{-1}\}$, com $\beta_i \neq \pm 1$ e $i \in \{2, \cdots, \frac{n+1}{2}\}$. De notar que, como $\beta_i \neq \pm 1$, então $\beta_i \neq \beta_i^{-1}$.

     É, assim, possível escolher n elementos de F, distinto dois a dois

     $$1, \beta_2, \beta_2^{-1}, \cdots, \beta_{\frac{n+1}{2}}, \beta_{\frac{n+1}{2}}^{-1},$$

     cujo produto é $1 = |A|$.

   - Se n é par, tome-se $\frac{n}{2}$ pares distintos da forma $\{\beta_i, \beta_i^{-1}\}$ com $i \in \{1, \cdots, \frac{n}{2}\}$ e tais que $\beta_i \notin \{0, 1, -1\}$.

     A afirmação anterior parece sugerir a necessidade de que F possua pelo menos $n+3$ elementos. Se F possui mais de $n+2$ elementos isso não será um problema, pois é sempre possível escolher $\beta_1, \cdots, \beta_n$ distintos dois a dois. Se F possui exactamente $n+2$ elementos também não haverá problemas: note-se que, como F é corpo, $(F, +)$ é grupo e, se $1 \in F$, então $-1 \in F$. No entanto, como $\beta_i \neq -1$ para $i \in \{1, \cdots, n\}$, só pode ter-se $1 = -1$ e não são necessários pelo menos $n+3$ elementos.

     É, assim, possível escolher n elementos de F distintos dois a dois,

     $$\beta_1, \beta_1^{-1}, \cdots, \beta_{\frac{n}{2}}, \beta_{\frac{n}{2}}^{-1},$$

     cujo produto é $1 = |A|$.

   Para tornar mais ligeira a notação envolvida, denotem-se os n elementos distintos anteriores, quer n seja par, quer n seja ímpar, por $\beta_1, \cdots \beta_n$ e considerem-se $\gamma_1, \cdots, \gamma_n$ definidos como $\gamma_i = \beta_i^{-1}, \quad i = \{1, \cdots, n\}$.

   Pelo teorema 3.2, existem matrizes B e C em $F^{n \times n}$ com valores próprios $\beta_1, \cdots \beta_n$ e $\gamma_1, \cdots, \gamma_n$, respectivamente, tais que $A = BC$.

   Mas tendo em conta a escolha feita para os valores próprios de B e C, estas matrizes são semelhantes e, portanto, existe $W \in SL(n, F)$ tal que $C = WB^{-1}W^{-1}$.

   Conclui-se então que $A = BC = BWB^{-1}W^{-1}$ e é, portanto, um comutador multiplicativo de matrizes .

Para que A seja um comutador multiplicativo de matrizes em $SL(n,F)$ é necessário que $|B| = \beta_1, \cdots \beta_n = 1$ (já demonstrado) e que $|W| = 1$.

Para contornar esta questão é necessário ter em conta que tendo a matriz B valores próprios distintos, é diagonalizável e, então, existe uma matriz diagonalizável E que comuta com B e possui determinante não nulo arbitrário.

De facto, se B possui valores próprios distintos, existe $P \in GL(n,F)$ tal que $B = PD_1P^{-1}$, onde $D_1 \in GL(n,F)$ é uma matriz diagonal. Seja $E = PD_2P^{-1}$, onde $D_2 = \text{diag}(r, 1, \ldots, 1) \in GL(n,F)$ e $r \in F\backslash\{0\}$.

Tem-se, então, que

$$EB = (PD_2P^{-1})(PD_1P^{-1}) = PD_2D_1P^{-1}$$

$$= PD_1D_2P^{-1} = (PD_2P^{-1})(PD_1P^{-1}) = BE$$

e o determinante de E pode ser escolhido arbitrariamente de entre os elementos não nulos de F.

Pode, então, escrever-se

$$A = BWB^{-1}W^{-1} = BWE(E^{-1}B^{-1})W^{-1} = BWEB^{-1}(E^{-1}W^{-1})$$

$$= B(WE)B^{-1}(E^{-1}W^{-1}) = B(WE)B^{-1}(WE)^{-1}.$$

Como o determinante de E é arbitrário, pode ser escolhido como $|E| = |W|^{-1}$ e, assim, se se denotar WE por C, tem-se que

$$A = BCB^{-1}C^{-1} \quad \text{com } |B| = |C| = 1$$

e A é, portanto, um comutador multiplicativo de matrizes em $SL(n,F)$.

3. Seja $A \in F^{n\times n}$ uma matriz não escalar e suponha-se que F possui pelo menos $n+3$ elementos. Sejam, ainda, $b, c \in F\backslash\{0\}$.

   O objectivo deste ponto é demonstrar que é possível escrever a matriz A como $A = BCB^{-1}C^{-1}$, com $B, C \in F^{n\times n}$ tais que $|B| = b$ e $|C| = c$.

Seja $\beta_1 = b$. Tal como na alínea anterior, é possível escolher de entre os elementos $F\backslash\{-1, 0, 1, b\}$ uma lista de $n-1$ elementos distintos, $\beta_2, \cdots, \beta_n$ tais que $\beta_2\beta_3\cdots\beta_n = 1$.

Pelo teorema 3.2 é possível escrever a matriz A como $A = BC$ onde $B, C \in F^{n\times n}$ e possuem determinantes $\beta_1\beta_2\cdots\beta_n = b$ e $\beta_1^{-1}\beta_2^{-1}\cdots\beta_n^{-1}$, respectivamente.

Note-se que, tendo em conta a escolha dos valores próprios, C e B^{-1} são semelhantes e, assim, existe $Z \in GL(n, F)$ tal que $C = ZB^{-1}Z^{-1}$.

Conclui-se então que $A = BZB^{-1}Z^{-1}$ e é, portanto, um comutador multiplicativo de matrizes.

Para que A seja um comutador multiplicativo de matrizes com determinantes prescritos é necessário ter em conta que tendo a matriz B valores próprios distintos, é diagonalizável e, então, existe um matriz diagonalizável E_2 que comuta com B e possui determinante não nulo arbitrário.

Pode, então, escrever-se

$$A = BZB^{-1}Z^{-1} = BZE_2(E_2^{-1}B^{-1})Z^{-1} = BZE_2B^{-1}(E_2^{-1}Z^{-1})$$

$$= B(ZE_2)B^{-1}(E_2^{-1}Z^{-1}) = B(ZE_2)B^{-1}(ZE_2)^{-1}.$$

Como o determinante de E_2 é arbitrário, pode ser escolhido sendo $|E_2| = c|Z|^{-1}$ e, assim, se se denotar ZE_2 por C, tem-se que

$$A = BCB^{-1}C^{-1}, \quad B, C \in F^{n\times n},\ |B| = b, |C| = c.$$

e é, portanto, um comutador multiplicativo de matrizes com determinantes prescritos.

■

Com a demonstração do teorema anterior, conclui-se que uma condição suficiente para que $A \in SL(n, F)$ possa ser escrita como $A = BCB^{-1}C^{-1}$, com $|B| = b, |C| = c$, é que F possua pelo menos $n + 3$ elementos. Exclui-se o caso em que $F = GF(2)$.

Bibliografia

[1] P. M. Cohn, *Algebra, vol. 1*, University College London, 1974.

[2] A. A. Albert e B. Muckenhoupt, *On matrices with trace zero*, University of Chicago - (1956).

[3] R. A. Horn e C. R. Johnson, *Matrix analysis*, Cambridge University Press, 1985.

[4] ———, *Topics in matrix analysis*, Cambridge University Press, 1991.

[5] P. Lancaster e M. Tismenetsky, *The theory of matrizes*, Academic Press, Inc., 1985.

[6] F. C. Silva et al, *Products of matrices with prescribed spectra and ranks*, Linear Algebra and its Applications, **340(1-3)** (2002), 137–147.

[7] J. B. Fraleigh, *A first course in abstract algebra*, Addison-Wesley, 1994.

[8] S. Friedland, *Matrices with prescribed off-diagonal elements*, Israel J. Math. **11** (1972), 184–189.

[9] P. M. Gibson, *Matrix commutators over an algebraically closed field*, American Mathematical Society **52** (1975), 30–32.

[10] C. R. Johnson, *A note on matrix solutions of* $A = XY - YX$, Proc. Amer. Math. Soc **42** (1974), 351–353.

[11] E. Landau, *Über die Darstellung definiter Funktionen durch Quadrate*, Math. Ann. **62** (1906), 271–285.

[12] W. LeVeque, *Topics in number theory*, vol. 1, Addison-Wesley, 1956.

[13] T. Muir and W. H. Metzler, *A treatise on the theory of determinants*, Albany, Nova Iorque, 1930.

[14] S. Perlis, *Theory of matrices*, Cambridge, 1952.

[15] K. Shoda, *Einige sätze über matrizen*, Japan J. Math. **13** (1936), 361–365.

[16] A. R. Sourour, *A factorization theorem for matrices*, Linear Multilinear Algebra **19** (1986), 141–147.

[17] R. C. Thompson, *Commutators in the special and general linear groups*, Transactions of the American Mathematical Society **101** (1960), 16–33.

[18] ———, *Commutators of matrices with coefficients from the field of two elements*, Duke Math. J. **29** (1961), 367–374.

[19] ———, *On matrix commutators*, Portugaliae Mathematica **21** (1962), 143–153.

[20] ———, *Commutators of matrices with prescribed determinant*, Canad. J. Math. **20** (1968), 203–221.

Índice Remissivo