UNIVERSIDADE FEDERAL DE SANTA CATARINA
CURSO DE GRADUAÇÃO EM MATEMÁTICA

LUCIANO MARACCINI CHUEIRE

DEMONSTRAÇÕES EM ÁLGEBRA VIA ÁLGEBRA LINEAR

FLORIANÓPOLIS
2009

Esta monografia foi julgada adequada como **TRABALHO DE CONCLUSÃO DE CURSO** no Curso de Matemática - Habilitação Licenciatura, e aprovada em sua forma final pela Banca Examinadora designada pela Portaria nº 35/CCM/09.

Prof. Nereu Estanislau Burin
Professor da disciplina

Banca Examinadora:

Licio Hernanes Bezerra
Orientador

Danilo Royer

Paulo Rafael Bösing

Sumário

Introdução **4**

1 O corpo dos números algébricos **5**
1.1 Os números algébricos 5
1.2 Aritmética dos números algébricos 6
1.3 Corpos e subcorpos 9
1.4 Primeira demonstração 11
1.5 Segunda demonstração (via produto de Kronecker) 13

2 Decomposição de permutações em transposições **20**
2.1 Permutações 20
2.2 Fatoração em ciclos disjuntos e transposições 23
2.3 Paridade de uma permutação 28

3 O mínimo comprimento de uma permutação como produto de transposições **32**
3.1 Permutações como transformações ortogonais 32
3.2 Ação do grupo de permutação S_n sobre $\mathbb{R}^n$ 33
3.3 Transposições vistas como reflexões 37
3.4 O número mínimo de transposições 38

Conclusão **39**

Referências Bibliográficas **40**

Introdução

Este trabalho de conclusão de curso possui três capítulos, nos quais são apresentados conceitos e resultados, com a finalidade de demonstrar dois teoremas em Álgebra, via Álgebra Linear.

No primeiro capítulo, é demonstrado que o conjunto dos números algébricos forma um subcorpo do corpo dos números complexos, aplicando duas técnicas diferentes que envolvem Álgebra Linear. Para aplicar a primeira técnica, apresentamos alguns resultados sobre a aritmética dos números algébricos, essenciais para a demonstração. Para a segunda técnica, definimos o Produto de Kronecker, apresentamos alguns exemplos e algumas propriedades desse produto que, aliadas ao conceito de autovalor associado a um autovetor, permite que se conclua a demonstração.

No segundo capítulo, são apresentados exemplos, conceitos e resultados que demonstram que toda permutação pode ser escrita como produto de ciclos disjuntos, levando o leitor ao importante resultado de que toda permutação é um produto de transposições cuja paridade é invariante.

No terceiro capítulo, é visto que a ação de uma transposição sobre o espaço vetorial $\mathbb{R}^n$ é uma reflexão de Householder que é utilizada para demonstrar o seguinte teorema: uma permutação em S_n não pode ser escrita como o produto de menos que $(n - r)$ transposições, em que r é o número de ciclos disjuntos na permutação, incluindo os 1-ciclos.

Capítulo 1

O corpo dos números algébricos

Neste capítulo, introduzimos alguns conceitos de Álgebra Linear para provar de dois modos diferentes que o conjunto dos números algébricos forma um subcorpo do corpo dos números complexos. Além disso, mostramos usando as mesmas técnicas, que o conjunto dos números inteiros algébricos forma um subanel do anel dos números complexos.

1.1 Os números algébricos

O objetivo desta seção é listar alguns conceitos e resultados da teoria básica dos números algébricos que serão utilizados ao longo desse capítulo.

Definição 1.1.1. *Um número complexo que é raiz de um polinômio mônico (isto é, cujo coeficiente líder é igual a 1) com coeficientes racionais da forma*

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \qquad (1.1.a)$$

é chamado um ***número algébrico****.*

Observação 1.1.1. *Também podemos definir um número algébrico como sendo uma raiz de um polinômio com coeficientes inteiros. Pois seja α raiz de*

$$b_nx^n + b_{n-1}x^{n-1} + \cdots + b_1x + b_0 = 0 \qquad (1.1.b)\ ,$$

uma equação com coeficientes inteiros. Ao dividirmos os dois lados dessa equação pelo coeficiente líder b_n, temos

$$x^n + \frac{b_{n-1}}{b_n}x^{n-1} + \cdots + \frac{b_1}{b_n}x + \frac{b_0}{b_n} = 0 \qquad (1.1.c)$$

e tomando $a_{n-1} = \frac{b_{n-1}}{b_n}, \cdots, a_1 = \frac{b_1}{b_n}, a_0 = \frac{b_0}{b_n}$, podemos reescrever a equação (1.1.c) da forma (1.1.a). A recíproca é verdadeira, pois se α é

raiz de (1.1.a), um polinômio mônico com coeficientes racionais, supondo que $a_{n-1} = \frac{p_{n-1}}{q_{n-1}}, \cdots, a_1 = \frac{p_1}{q_1}, a_0 = \frac{p_0}{q_0}$, *multiplicando (1.1.a) por* $b_n = M.M.C.\{q_{n-1}, q_{n-2}, \cdots, q_1, q_0\}$, *obtemos (1.1.b).*

Observação 1.1.2. *Um número complexo que não seja algébrico é chamado transcendente.*

Definição 1.1.2. *Se um número complexo é raiz de um polinômio mônico*

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

em que os coeficientes $a_0, \cdots, a_{n-1}$ *são números inteiros, então ele é chamado de* ***inteiro algébrico****.*

Observação 1.1.3. *Todo inteiro algébrico é um número algébrico, pois é raiz do polinômio (1.1.b) com o coeficiente* $b_n = 1$.

Exemplo 1.1.1. $\sqrt{2}$ *e* $-\sqrt{2}$ *são inteiros algébricos, pois são raízes do polinômio* $x^2 - 2$.

Exemplo 1.1.2. $\sqrt{2+\sqrt{3}}$ *é um inteiro algébrico, pois é raiz do polinômio* $x^4 - 4x^2 + 1$.

Exemplo 1.1.3. $i = \sqrt{-1}$ *e* $-i$ *são inteiros algébricos, pois são raízes do polinômio* $x^2 + 1$.

Exemplo 1.1.4. *Todo número inteiro* z *é um inteiro algébrico, pois* z *é raiz do polinômio* $x - z$.

Exemplo 1.1.5. *Todo número racional* q *é um número algébrico: se* $q = \frac{a}{b}$, $a, b \in \mathbb{Z}$, $b \neq 0$, *então* q *é raiz do polinômio* $bx - a$.

Exemplo 1.1.6. π *é um número transcendente e a demonstração desse fato pode ser encontrada na referência [4].*

1.2 Aritmética dos números algébricos

Nesta seção veremos que as operações de adição e de multiplicação são fechadas no conjunto dos números algébricos, utilizando alguns conceitos e resultados de álgebra linear.

Lema 1.2.1. *Sejam* n *um número inteiro positivo e* δ *um número complexo. Suponha que os números complexos* $\theta_1, \theta_2, \cdots, \theta_n$, *todos não-nulos, satisfaçam as equações da forma*

$$\delta\theta_j = a_{j,1}\theta_1 + a_{j,2}\theta_2 + \cdots + a_{j,n}\theta_n \qquad (1.2.a)\ ,$$

com $j = 1, 2, \cdots, n$, *em que os* n^2 *coeficientes* $a_{j,i}$, *com* $i = 1, 2, \cdots, n$, *são racionais. Então* δ *é um número algébrico.*

Demonstração. As equações da forma (1.2.a) podem ser dispostas como um sistema de equações lineares homogêneo em $\theta_1, \theta_2, \cdots, \theta_n$:

$$\delta \cdot \begin{pmatrix} \theta_1 \\ \theta_2 \\ \vdots \\ \theta_n \end{pmatrix} = \underbrace{\begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & \cdots & a_{n,n} \end{pmatrix}}_{A} \cdot \begin{pmatrix} \theta_1 \\ \theta_2 \\ \vdots \\ \theta_n \end{pmatrix}.$$

Como $\theta_1, \theta_2, \cdots, \theta_n$ são todos não nulos, $\begin{pmatrix} \theta_1 \\ \theta_2 \\ \vdots \\ \theta_n \end{pmatrix}$ é um autovetor associado ao autovalor δ de $A = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & \cdots & a_{n,n} \end{pmatrix}$.

Logo, $det(\delta I_n - A) = 0$, isto é,

$$\begin{vmatrix} \delta - a_{1,1} & -a_{1,2} & \cdots & -a_{1,n} \\ -a_{2,1} & \delta - a_{2,2} & \cdots & -a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ -a_{n,1} & -a_{n,2} & \cdots & \delta - a_{n,n} \end{vmatrix} = 0.$$

Portanto, δ é raiz do polinômio característico de A:

$$P_A(x) = x^n + b_1 x^{n-1} + \cdots + b_{n-1}x + b_n.$$

Note que $b_1, b_2, \cdots, b_n \in \mathbb{Q}$, pois cada b_i, $i = 1, \cdots, n$, é o resultado de somas e multiplicações envolvendo os coeficientes racionais $a_{j,i}$, originadas pela operação de determinante. Assim, $P_A(x)$ é um polinômio mônico de coeficientes racionais e, como δ é raiz de $P_A(x)$, δ é número algébrico. □

Corolário 1.2.1. *No Lema 1.2.1, se supusermos que os coeficientes $a_{j,i}$ são inteiros para todo $i, j \in \{1, \cdots, n\}$, obtemos que δ é um inteiro algébrico.*

Demonstração. A demonstração é análoga à do Lema 1.2.1. □

Teorema 1.2.1. *Se α e β são números algébricos, então $\alpha + \beta$ e $\alpha \cdot \beta$ são números algébricos.*

Demonstração. Suponha que α e β satisfaçam

$$\alpha^m + a_1\alpha^{m-1} + \cdots + a_m = 0$$

e

$$\beta^r + b_1\beta^{r-1} + \cdots + b_r = 0 \quad ,$$

com coeficientes racionais, a_i e b_j.
Sejam $n = m \cdot r$ e $\theta_1, \cdots, \theta_n$ números complexos definidos como

$$\begin{array}{ccccc}
\theta_1 = 1, & \theta_2 = \alpha, & \theta_3 = \alpha^2, & \cdots, & \theta_m = \alpha^{m-1}, \\
\theta_{m+1} = \beta, & \theta_{m+2} = \alpha\beta, & \theta_{m+3} = \alpha^2\beta, & \cdots, & \theta_{2m} = \alpha^{m-1}\beta, \\
\vdots & \vdots & \vdots & \vdots & \vdots \\
\theta_{(r-1)\cdot m+1} = \beta^{r-1}, & \theta_{(r-1)\cdot m+2} = \alpha\beta^{r-1}, & \theta_{(r-1)\cdot m+3} = \alpha^2\beta^{r-1}, & \cdots, & \theta_{rm} = \alpha^{m-1}\beta^{r-1}.
\end{array}$$

Então, $\theta_1, \theta_2, \cdots, \theta_n$ são números da forma $\alpha^s\beta^t$ com $s = 0, 1, \cdots, m-1$ e $t = 0, 1, \cdots, r-1$. Logo,

$$\alpha\theta_j = \alpha\alpha^s\beta^t = \alpha^{s+1}\beta^t = \begin{cases} \theta_{j+1}, \ se\ s+1 \leq m-1 \\ \alpha^m\beta^t, \ se\ s+1 = m \end{cases} .$$

No caso de $s+1 = m$, como $\alpha^m = -a_1\alpha^{m-1} - \cdots - a_m$, temos que

$$\alpha^m\beta^t = (-a_1\alpha^{m-1} - \cdots - a_m)\beta^t = -a_1\alpha^{m-1}\beta^t - \cdots - a_m\beta^t =$$

$$= -a_1\theta_j - a_2\theta_{j-1} - \cdots - a_m\theta_{j-m+1}.$$

Constatamos, então, que existem constantes racionais, digamos $h_{j,1}, \cdots, h_{j,n}$ tal que

$$\alpha\theta_j = h_{j,1}\theta_1 + \cdots + h_{j,n}\theta_n.$$

E, similarmente, existem constantes racionais $k_{j,1}, \cdots, k_{j,n}$ tal que

$$\beta\theta_j = k_{j,1}\theta_1 + \cdots + k_{j,n}\theta_n.$$

Então, temos

$$(\alpha+\beta)\theta_j = (h_{j,1} + k_{j,1})\theta_1 + \cdots + (h_{j,n} + k_{j,n})\theta_n$$

que é uma equação do mesmo tipo da equação (1.2.a) do Lema 1.2.1. Portanto, $\alpha + \beta$ é um número algébrico.

Agora, como $\beta\theta_j = k_{j,1}\theta_1 + \cdots + k_{j,n}\theta_n$, temos que

$$\alpha\beta\theta_j = \alpha(k_{j,1}\theta_1 + \cdots + k_{j,n}\theta_n) = k_{j,1}\alpha\theta_1 + \cdots + k_{j,n}\alpha\theta_n.$$

Como $(\forall j)\ \alpha\theta_j = h_{j,1}\theta_1 + \cdots + h_{j,n}\theta_n$,

$$\alpha\beta\theta_j = k_{j,1}\sum_{k=1}^{n} h_{1,k}\theta_k + \cdots + k_{j,n}\sum_{k=1}^{n} h_{n,k}\theta_k.$$

Logo, distribuindo as operações de soma e multiplicação, obtemos que

$$(\forall j)\ \ \alpha\beta\theta_j = \sum_{k=1}^{n} r_k\theta_k,\ r_k \in \mathbb{Q}\ ,$$

que é uma equação com a mesma forma da equação (1.2.a) do Lema 1.2.1. Portanto, $\alpha \cdot \beta$ é um número algébrico.

□

Corolário 1.2.2. *Se α e β são inteiros algébricos, então $\alpha + \beta$ e $\alpha \cdot \beta$ são inteiros algébricos.*

Demonstração. A demonstração é análoga à do Teorema 1.2.1. □

1.3 Corpos e subcorpos

O objetivo desta seção é listar alguns conceitos e resultados de Álgebra que serão utilizados ao longo desse capítulo.

Definição 1.3.1. *Um **corpo** $(K, +, \cdot)$ é um conjunto K, com pelo menos dois elementos, munido de uma operação $+$ (chamada adição) e de uma outra operação $\cdot$ (chamada multiplicação) que satisfazem as condições seguintes:*

1. *A adição é associativa, isto é,*

$$(\forall x, y, z \in K) \quad (x + y) + z = x + (y + z).$$

2. *Existe um elemento neutro com respeito à adição, isto é,*

$$(\forall x \in K)(\exists 0 \in K) \quad 0 + x = x \quad e \quad x + 0 = x.$$

3. *Todo elemento de K possui um inverso com respeito à adição, isto é,*

$$(\forall x \in K)(\exists z \in K) \quad x + z = 0 \quad e \quad z + x = 0.$$

4. *A adição é comutativa, isto é,*

$$(\forall x, y \in K) \quad x + y = y + x.$$

5. *A multiplicação é associativa, isto é,*

$$(\forall x, y, z \in K) \quad (x \cdot y) \cdot z = x \cdot (y \cdot z).$$

6. *Existe um elemento neutro com respeito à multiplicação, dito a unidade do corpo, isto é,*

$$(\forall x \in K)(\exists 1 \in K) \quad 1 \cdot x = x \quad e \quad x \cdot 1 = x.$$

7. $1 \neq 0$.

8. *A multiplicação é comutativa, isto é,*

$$(\forall x, y \in K) \quad x \cdot y = y \cdot x.$$

9. *A adição é distributiva relativamente à multiplicação, isto é,*

$$(\forall x, y, z \in K) \quad x \cdot (y + z) = x \cdot y + x \cdot z.$$

10. *Todo elemento diferente de zero de K possui um inverso com respeito à multiplicação, isto é,*

$$(\forall x \in K \backslash \{0\})(\exists y \in K) \quad x \cdot y = 1.$$

Observação 1.3.1. *Se todas as condições acima são satisfeitas com exceção da 10^a, então K é chamado de anel comutativo com unidade. A partir de agora, quando nos referirmos a um anel, consideraremos que o anel é sempre um anel comutativo com unidade.*

Observação 1.3.2. *Como todo corpo satisfaz as nove primeiras condições acima, todo corpo é um anel.*

Exemplo 1.3.1. $(\mathbb{Z}, +, \cdot)$ *é um anel.*

Exemplo 1.3.2. $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ *são corpos.*

Definição 1.3.2. *Seja $(K, +, \cdot)$ um corpo. Um subconjunto não vazio H de K é um* ***subcorpo*** *de K quando, com as operações de K, o conjunto H é um corpo.*

Exemplo 1.3.3. *Com $+$ e $\cdot$ denotando respectivamente a adição e a multiplicação em $\mathbb{C}$, temos que $(\mathbb{Q}, +, \cdot)$ e $(\mathbb{R}, +, \cdot)$ são subcorpos de $(\mathbb{C}, +, \cdot)$.*

Observação 1.3.3. *Seguindo o raciocínio da definição acima, se* $(A, +, \cdot)$ *é um anel, um subconjunto não vazio* B *de* A *é um subanel de* A *quando, com as operações de* A*, o conjunto* B *é um subanel.*

Observação 1.3.4. *Para facilitar o enunciado da proposição a seguir, denotamos* $-x$ *como inverso com respeito à adição e denotamos* x^{-1} *como inverso com respeito à multiplicação.*

Proposição 1.3.1. *Seja* H *um subconjunto não-vazio do corpo* K*. Então* H *é um subcorpo de* K *se, e somente se, as quatro condições seguintes são satisfeitas:*

1. $(\forall x, y \in H)\ x + y \in H$*. (a adição é uma operação fechada em* H*)*
2. $(\forall x, y \in H)\ x \cdot y \in H$*. (a multiplicação é uma operação fechada em* H*)*
3. $(\forall x \in H)\ -x \in H$*.*
4. $(\forall x \in K \backslash \{0\})\ x^{-1} \in H$*.*

Demonstração. A demonstração dessa proposição é simples e pode ser encontrada na referência [2]. □

Observação 1.3.5. *Note que se* B *for um subconjunto não-vazio de um anel* A*, tal que* B *satisfaça apenas as três primeiras condições da proposição acima, temos que* B *é um subanel de* A*.*

1.4 Primeira demonstração

Para esta seção, já temos todas as ferramentas necessárias para provarmos que o conjunto dos números algébricos forma um subcorpo do corpo dos números complexos.

Teorema 1.4.1. *O conjunto dos números algébricos forma um subcorpo do corpo dos números complexos.*

Demonstração. Seja $\mathbb{X}$ o conjunto dos números algébricos.

Para demonstrarmos este teorema, vamos provar que as quatro condições seguinte são satisfeitas:

1. $(\forall \alpha, \beta \in \mathbb{X}) \quad \alpha + \beta \in \mathbb{X}$.

   Já foi provado no Teorema 1.2.1.

2. $(\forall \alpha, \beta \in \mathbb{X}) \quad \alpha \cdot \beta \in \mathbb{X}$.

   Já foi provado no Teorema 1.2.1.

3. $(\forall \alpha \in \mathbb{X}) \quad -\alpha \in \mathbb{X}$.

   Prova: Seja $\alpha \in \mathbb{X}$. Então temos que α é raiz do polinômio com coeficientes inteiros

   $$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \ ,$$

   ou seja,

   $$a_n \alpha^n + a_{n-1} \alpha^{n-1} + \cdots + a_1 \alpha + a_0 = 0.$$

   Então, temos que $-\alpha$ é raiz do polinômio com coeficientes inteiros

   $$(-1)^n a_n x^n + (-1)^{n-1} a_{n-1} x^{n-1} + \cdots + (-1) a_1 x + a_0 \ ,$$

   pois

   $$(-1)^n a_n (-\alpha)^n + (-1)^{n-1} a_{n-1} (-\alpha)^{n-1} + \cdots + (-1) a_1 (-\alpha) + a_0 =$$

   $$= a_n \alpha^n + a_{n-1} \alpha^{n-1} + \cdots + a_1 \alpha + a_0 = 0.$$

4. $(\forall \alpha \in \mathbb{X})(\alpha \neq 0) \quad \alpha^{-1} \in \mathbb{X}$.

   Prova: Seja $\alpha \in \mathbb{X}$. Então, α^{-1} é raiz do polinômio com coeficientes inteiros

   $$a_0 x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n \ ,$$

   pois,

   $$\alpha^n [a_0 (\alpha^{-1})^n + a_1 (\alpha^{-1})^{n-1} + \cdots + a_{n-1} \alpha^{-1} + a_n] =$$

   $$= a_0 (\alpha^{-1})^n \alpha^n + a_1 (\alpha^{-1})^{n-1} \alpha^n + \cdots + a_{n-1} \alpha^{-1} \alpha^n + a_n \alpha^n =$$

   $$= a_n \alpha^n + a_{n-1} \alpha^{n-1} + \cdots + a_1 \alpha + a_0 = 0.$$

□

Proposição 1.4.1. *Um inteiro algébrico real é inteiro ou irracional.*

Demonstração. Seja α um inteiro algébrico. Suponha, por contradição, que $\alpha = \frac{p}{q}$, em que $p \in \mathbb{Z}$, $q \in \mathbb{N}$ e $q > 1$, p e q primos entre si. Isto é, α é um número racional que não é inteiro. Como α é uma raiz de um polinômio mônico com coeficientes inteiros do tipo

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \ ,$$

substituindo x por $\frac{p}{q}$ temos:

$$p^n = -a_{n-1}p^{n-1}q - \cdots - a_0 q^n \ ,$$

ou ainda

$$p^n = q(-a_{n-1}p^{n-1} - \cdots - a_0 q^{n-1}) \ .$$

Logo, q divide p^n. Seja r um fator primo de q, $r \neq 1$ ($r = q$ se q for primo). Assim, r divide p^n e logo, r divide p. Consequentemente r divide p e q, o que é um absurdo, pois contradiz o fato deles serem primos entre si. Portanto, um inteiro algébrico real é inteiro ou irracional.

□

Corolário 1.4.1. *O conjunto dos inteiros algébricos forma um subanel do anel dos números complexos.*

Demonstração. Tomando α e β inteiros algébricos, já vimos no Corolário 1.2.2 que as duas primeiras condições do Proposição 1.3.1 são satisfeitas. E tomando $a_n = 1$, fácilmente vemos que a terceira condição também é satisfeita. □

1.5 Segunda demonstração (via produto de Kronecker)

Novamente, vamos demonstrar que as operações de adição e multiplicação são fechadas no conjunto dos números algébricos e que o conjunto dos números algébricos forma um subcorpo do corpo dos números complexos, fatos que serão abordados nesta seção por meio de uma demonstração alternativa, via Álgebra Linear. Primeiramente listamos alguns resultados essenciais.

Definição 1.5.1. *Seja $A \in \mathbb{C}^{n\times n}$. Definimos $\lambda(A)$ como o conjunto dos autova-lores de A.*

Exemplo 1.5.1. $A = I_2 \Rightarrow \lambda(A) = \{1, 1\}$.

Lema 1.5.1. *Seja* $A = \begin{pmatrix} B & 0 \\ 0 & C \end{pmatrix}_{n\times n}$, $B \in \mathbb{C}^{r\times r}$, $C \in \mathbb{C}^{(n-r)\times(n-r)}$. *Então* $\lambda(A) = \lambda(B) \cup \lambda(C)$.

Demonstração. $|A - \lambda I| = \begin{vmatrix} B - \lambda I & 0 \\ 0 & C - \lambda I \end{vmatrix} = |B - \lambda I||C - \lambda I|$. Note que $\lambda \in \lambda(A) \Leftrightarrow |A - \lambda I| = 0 \Leftrightarrow |B - \lambda I| = 0$ *ou* $|C - \lambda I| = 0 \Leftrightarrow \lambda \in \lambda(B)$ *ou* $\lambda \in \lambda(C)$.

□

Definição 1.5.2. *Sejam* $c_1, \cdots, c_n \in \mathbb{C}$. *Então a matriz companheira* $C(c_1, \cdots, c_n)$ *é a matriz*

$$\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 1 \\ -c_n & -c_{n-1} & \cdots & -c_2 & -c_1 \end{pmatrix}_{n\times n}.$$

Exemplo 1.5.2. $C(1,2,3) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -3 & -2 & -1 \end{pmatrix}$.

Lema 1.5.2. *Seja* $A = C(c_1, \cdots, c_n)$ *uma matriz companheira. Então o polinômio característico de* A, $P_A(x)$, *é igual a*

$$x^n + c_1x^{n-1} + \cdots + c_{n-1}x + c_n.$$

Demonstração. (por indução em n)
Para n=2, temos

$$det(xI_2 - C(c_1, c_2)) = \begin{vmatrix} x & -1 \\ c_2 & x + c_1 \end{vmatrix} = x(x + c_1) + c_2 = x^2 + c_1x + c_2.$$

Vamos supor que, para $n \geq 2$,

$$det(xI_n - C(c_1, \cdots, c_n)) = x^n + c_1x^{n-1} + \cdots + c_{n-1}x + c_n.$$

Sejam $c_1, \cdots, c_{n+1} \in \mathbb{C}$. Usando a expansão do cofator com respeito à primeira coluna, obtemos

$$det(xI_{n+1} - C(c_1, \cdots, c_{n+1})) = \begin{vmatrix} x & -1 & 0 & \cdots & 0 \\ 0 & x & -1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & x & -1 \\ c_{n+1} & c_n & \cdots & c_2 & x + c_1 \end{vmatrix} =$$

$$= (-1)^2 x \begin{vmatrix} x & -1 & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & x & -1 \\ c_n & \cdots & c_2 & x + c_1 \end{vmatrix} + (-1)^{1+n+1} c_{n+1} \begin{vmatrix} -1 & 0 & \cdots & 0 \\ x & -1 & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & x & -1 \end{vmatrix} =$$

$$= x(x^n + c_1 x^{n-1} + \cdots + c_{n-1}x + c_n) + (-1)^{2+n} c_{n+1}(-1)^n =$$

$$= x^{n+1} + c_1 x^n + \cdots + c_{n-1}x^2 + c_n x + (-1)^{2+2n} c_{n+1} =$$

$$= x^{n+1} + c_1 x^n + \cdots + c_{n-1}x^2 + c_n x + c_{n+1}.$$

□

Corolário 1.5.1. *$C(c_1, \cdots, c_n)$ é inversível se, e somente se, $c_n \neq 0$.*

Demonstração. ($\Rightarrow$)

Suponha, por contradição, que $c_n = 0$. Usando a expansão do cofator com respeito à primeira coluna, obtemos

$$det(\, C(c_1, \cdots, c_n)\,) = det(\, C(c_1, \cdots, c_{n-1}, 0)\,) = \begin{vmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 1 \\ 0 & -c_{n-1} & \cdots & -c_2 & -c_1 \end{vmatrix} = 0.$$

Logo, $C(c_1, \cdots, c_n)$ não é inversível, o que contradiz a hipótese.

($\Leftarrow$)

Pelo Lema 1.5.2, $P_{C(c_1,\cdots,c_n)}(x) = x^n + c_1 x^{n-1} + \cdots + c_{n-1}x + c_n$. Como $c_n \neq 0$, temos que $P_{C(c_1,\cdots,c_n)}(0) = c_n \neq 0$. Então, 0 não é autovalor de $C(c_1, \cdots, c_n)$. Portanto, $C(c_1, \cdots, c_n)$ é uma matriz inversível (pois uma matriz $n \times n$ é inversível se, e somente se, 0 não é um autovalor dessa matriz). □

Proposição 1.5.1. *Seja λ um número complexo. Temos que λ é um número algébrico se, e somente se, λ é um autovalor de uma matriz quadrada com entradas racionais.*

Demonstração. ($\Rightarrow$)

Seja λ um número algébrico. Seja $f(x)$ um polimônio mônico em $\mathbb{Q}[x]$, digamos $f(x) = x^n + c_1x^{n-1} + \cdots + c_{n-1}x + c_n$, tal que $f(\lambda) = 0$. Seja $A \in \mathbb{Q}^{n\times n}$ a matriz companheira $C(c_1, \cdots, c_n)$, isto é,

$$A = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 1 \\ -c_n & -c_{n-1} & \cdots & -c_2 & -c_1 \end{pmatrix}.$$

Então, pelo Lema anterior, temos que $P_A(x) = f(x)$. Logo,

$$P_A(\lambda) = f(\lambda) = 0.$$

Portanto, λ é raiz de $P_A(x)$, ou seja, é autovalor de uma matriz quadrada com coeficientes racionais.

($\Leftarrow$)

Seja λ um autovalor de $A \in \mathbb{Q}^{n\times n}$. Então λ é raiz de $P_A(x)$ que é o polinômio mônico $det(xI_n - A)$. Como os coeficientes de $P_A(x)$ são racionais (são o resultado de somas e multiplicações originadas pela operação determinante), λ é um número algébrico.

□

Corolário 1.5.2. *Seja λ um número complexo. Temos que λ é um inteiro algébrico se, e somente se, λ é um autovalor de uma matriz quadrada com entradas inteiras.*

Demonstração. A demonstração é análoga a demonstração da Proposição 1.5.1, trocando: $\mathbb{Q}[x]$ por $\mathbb{Z}[x]$ e $\mathbb{Q}^{n\times n}$ por $\mathbb{Z}^{n\times n}$.

□

Definição 1.5.3. *Sejam $A \in \mathbb{C}^{m\times n}$ e $B \in \mathbb{C}^{p\times q}$. O **produto de Kronecker** (ou produto tensorial) de A e B é definido como a matriz*

$$A \otimes B = \begin{pmatrix} a_{1,1}B & \cdots & a_{1,n}B \\ \vdots & \ddots & \vdots \\ a_{m,1}B & \cdots & a_{m,n}B \end{pmatrix} \in \mathbb{C}^{mp\times nq}.$$

Exemplo 1.5.3. *Sejam $A = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ e $B = \begin{pmatrix} 2 & 1 \\ 2 & 3 \end{pmatrix}$. Então,*

$$A \otimes B = \begin{pmatrix} B & 2B & 3B \\ 3B & 2B & B \end{pmatrix} = \begin{pmatrix} 2 & 1 & 4 & 2 & 6 & 3 \\ 2 & 3 & 4 & 6 & 6 & 9 \\ 6 & 3 & 4 & 2 & 2 & 1 \\ 6 & 9 & 4 & 6 & 2 & 3 \end{pmatrix}.$$

$$B \otimes A = \begin{pmatrix} 2A & A \\ 2A & 3A \end{pmatrix} = \begin{pmatrix} 2 & 4 & 6 & 1 & 2 & 3 \\ 6 & 4 & 2 & 3 & 2 & 1 \\ 2 & 4 & 6 & 3 & 6 & 9 \\ 6 & 4 & 2 & 9 & 6 & 3 \end{pmatrix}.$$

Note que, em geral, $A \otimes B \neq B \otimes A$.

Exemplo 1.5.4. $(\forall B \in \mathbb{C}^{p\times q}) \quad I_2 \otimes B = \begin{pmatrix} B & 0 \\ 0 & B \end{pmatrix}$.

Note que, trocando I_2 *por* I_n*, teríamos* B *se repetindo na diagonal principal da matriz resultante* n *vezes.*

Exemplo 1.5.5. *Seja* $B = \begin{pmatrix} b_{1,1} & b_{1,2} \\ b_{2,1} & b_{2,2} \end{pmatrix}$. *Então,*

$$B \otimes I_2 = \begin{pmatrix} b_{1,1} & 0 & b_{1,2} & 0 \\ 0 & b_{1,1} & 0 & b_{1,2} \\ b_{2,1} & 0 & b_{2,2} & 0 \\ 0 & b_{2,1} & 0 & b_{2,2} \end{pmatrix}.$$

Exemplo 1.5.6. *Sejam* $x = \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} \in \mathbb{C}^m$ *e* $y = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} \in \mathbb{C}^n$. *Então,*

$$x \otimes y = \begin{pmatrix} x_1 y^T, & \cdots, & x_m y^T \end{pmatrix}^T = \begin{pmatrix} x_1 y_1, & \cdots, & x_1 y_n, & x_2 y_1, & \cdots, & x_m y_n \end{pmatrix}^T \in \mathbb{C}^{mn}.$$

Exemplo 1.5.7. *Seja* $a \in \mathbb{C}$.

$$a(A \otimes B) = a \begin{pmatrix} a_{1,1}B & \cdots & a_{1,n}B \\ \vdots & \ddots & \vdots \\ a_{m,1}B & \cdots & a_{m,n}B \end{pmatrix} =$$

$$= \begin{pmatrix} aa_{1,1}B & \cdots & aa_{1,n}B \\ \vdots & \ddots & \vdots \\ aa_{m,1}B & \cdots & aa_{m,n}B \end{pmatrix} = \begin{pmatrix} a_{1,1}aB & \cdots & a_{1,n}aB \\ \vdots & \ddots & \vdots \\ a_{m,1}aB & \cdots & a_{m,n}aB \end{pmatrix}.$$

Assim,

$$a(A \otimes B) = (aA) \otimes B = A \otimes (aB).$$

Proposição 1.5.2. *Sejam* $A \in \mathbb{C}^{m\times n}$, $B \in \mathbb{C}^{r\times s}$, $C \in \mathbb{C}^{n\times p}$ *e* $D \in \mathbb{C}^{s\times t}$. *Então,*

$$(A \otimes B)(C \otimes D) = AC \otimes BD \ \in \mathbb{C}^{mr\times pt}.$$

Demonstração. Simplesmente verificamos que

$$(A \otimes B)(C \otimes D) = \begin{pmatrix} a_{1,1}B & \cdots & a_{1,n}B \\ \vdots & \ddots & \vdots \\ a_{m,1}B & \cdots & a_{m,n}B \end{pmatrix} \begin{pmatrix} c_{1,1}D & \cdots & c_{1,p}D \\ \vdots & \ddots & \vdots \\ c_{n,1}D & \cdots & c_{n,p}D \end{pmatrix} =$$

$$= \begin{pmatrix} \sum_{k=1}^{n} a_{1,k}c_{k,1}BD & \cdots & \sum_{k=1}^{n} a_{1,k}c_{k,p}BD \\ \vdots & \ddots & \vdots \\ \sum_{k=1}^{n} a_{m,k}c_{k,1}BD & \cdots & \sum_{k=1}^{n} a_{m,k}c_{k,p}BD \end{pmatrix} = AC \otimes BD.$$

□

Proposição 1.5.3. *Considere $A \in \mathbb{C}^{n\times n}$, $B \in \mathbb{C}^{m\times m}$, λ um autovalor de A e δ um autovalor de B. Então:*

1. *$\lambda + \delta$ é um autovalor de $(A \otimes I_m) + (I_n \otimes B)$.*
2. *$\lambda\delta$ é um autovalor de $A \otimes B$.*

Demonstração. Seja x um autovetor de A associado a λ e seja y um autovetor de B associado a δ. Então, pela proposição anterior:

1. $((A \otimes I_m) + (I_n \otimes B))(x \otimes y) = (A \otimes I_m)(x \otimes y) + (I_n \otimes B)(x \otimes y) =$
$$= Ax \otimes I_m y + I_n x \otimes By = (\lambda x) \otimes y + x \otimes (\delta y) =$$
$$= \lambda(x \otimes y) + \delta(x \otimes y) = (\lambda + \delta)(x \otimes y).$$
2. $(A \otimes B)(x \otimes y) = Ax \otimes By = \lambda x \otimes \delta y = \lambda\delta(x \otimes y)$.

□

Teorema 1.5.1. *O conjunto dos números algébricos forma um subcorpo do corpo dos números complexos.*

Demonstração. Seja $\mathbb{X}$ o conjunto dos números algébricos.

Para demonstrarmos este teorema, vamos provar que as quatro condições seguintes são satisfeitas:

1. $(\forall \lambda, \delta \in \mathbb{X}) \quad \lambda + \delta \in \mathbb{X}$.

   Prova: Sejam λ e δ números algébricos.

   Então, pela Proposição 1.5.1, λ é um autovalor de uma matriz quadrada com entradas racionais, digamos A, e δ é um autovalor de uma matriz quadrada com entradas racionais, digamos B.

   Logo, pela Proposição 1.5.3, $\lambda+\delta$ é um autovalor de $(A\otimes I_m)+(I_n\otimes B)$.

   Como $(A \otimes I_m) + (I_n \otimes B)$ é uma matriz com entradas racionais, pela Proposição 1.5.1, temos que $\lambda + \delta$ é um número algébrico.

2. $(\forall \lambda, \delta \in \mathbb{X}) \quad \lambda \cdot \delta \in \mathbb{X}$.

   Prova: Sejam λ e δ números algébricos.

   Então, pela Proposição 1.5.1, λ é um autovalor de uma matriz quadrada com entradas racionais, digamos A e δ é um autovalor de uma matriz quadrada com entradas racionais, digamos B.

   Logo, pela Proposição 1.5.3, $\lambda\delta$ é um autovalor de $A \otimes B$, que é uma matriz com entradas racionais.

   Portanto, pela Proposição 1.5.1, temos que $\lambda \cdot \delta$ é um número algébrico.

3. $(\forall \lambda \in \mathbb{X}) \quad -\lambda \in \mathbb{X}$.

   Prova: $\lambda \in \mathbb{X} \Rightarrow (\exists A \in \mathbb{Q}^{n\times n})$ λ é autovalor de A (pela Proposição 1.5.1). Pela Proposição 1.5.3, $(-\lambda)$ é autovalor de $A \otimes (-I)$ que é uma matriz com entradas racionais. Portanto, pela Proposição 1.5.1, temos que $-\lambda$ é um número algébrico.

4. $(\forall \lambda \in \mathbb{X}) \quad \lambda \neq 0,\ \lambda^{-1} \in \mathbb{X}$.

   Prova: Seja $\lambda \neq 0$ um número algébrico. Então, existe uma matriz companheira $A = C(c_1, \cdots, c_n)$ com entradas racionais, tal que λ é autovalor de A (pela Proposição 1.5.1). Sem perda de generalidade, podemos supor que $c_n \neq 0$, pois se $c_n = 0$,

$$C(c_1, \cdots, 0) = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 1 \\ 0 & -c_{n-1} & \cdots & -c_2 & -c_1 \end{pmatrix},$$

   $\lambda(A) = \{0\} \cup \lambda(C(c_1, \cdots, c_{n-1}))$ (pelo Lema 1.5.1) e, como $\lambda \neq 0$, existe $j \in \{2, n-1\}$ tal que $c_k \neq 0$ para $k \leq j$. Assim, λ é um autovalor de $A = C(c_1, \cdots, c_n)$, A inversível (pelo Corolário 1.5.1). Logo, λ^{-1} é autovalor de A^{-1}. Como $A^{-1} = \frac{(cofatora\ de\ A)^T}{detA}$, $A^{-1} \in \mathbb{Q}^{n\times n}$, pois suas entradas resultam de somas e multiplicações envolvendo racionais. Portanto, λ^{-1} é um número algébrico.

□

Corolário 1.5.3. *O conjunto dos inteiros algébricos forma um subanel do anel dos números complexos.*

Demonstração. Basta tomar λ *e* δ inteiros algébricos, para que as três primeiras condições da demonstração do Teorema 1.5.1 sejam satisfeitas de forma análoga. □

Capítulo 2

Decomposição de permutações em transposições

Neste capítulo, demonstramos um teorema clássico de Álgebra: toda permutação de S_n pode ser escrita como um produto de transposições.

2.1 Permutações

O objetivo desta seção é definir permutação e apresentar alguns conceitos que serão necessários ao longo deste capítulo.

Definição 2.1.1. *Se X é um conjunto finito não-vazio, uma* ***permutação*** *de X é uma bijeção $\alpha : X \to X$. Denotamos o conjunto de permutações de X por S_X.*

Quando $X = \{1, \cdots, n\}$, denotamos S_X por S_n. Uma permutação de $X = \{1, \cdots, n\}$ pode ser vista como um rearranjo de todos os termos de X, formando uma lista $i_1, i_2, \cdots, i_n$, sem repetições. Dado um rearranjo $i_1, i_2, \cdots, i_n$, definimos uma função $\alpha : X \to X$, com $\alpha(j) = i_j$, para todo $j \in X$. Esta função é uma injeção, porque a lista não tem repetições, e ela é uma sobrejeção, porque todos os elementos de X aparecem na lista. Então, essa função é uma bijeção.

Consequentemente, qualquer bijeção α pode ser representada por duas fileiras:

$$\alpha = \begin{pmatrix} 1 & 2 & \cdots & n \\ \alpha(1) & \alpha(2) & \cdots & \alpha(n) \end{pmatrix},$$

em que a fileira de baixo é um rearranjo de $\{1, \cdots, n\}$.

Exemplo 2.1.1. $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ *e* $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ *são permutações em S_3.*

Exemplo 2.1.2. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}$ *e* $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix}$ *são permutações em* S_5.

Definição 2.1.2. *Uma* ***transposição*** *é uma permutação que troca dois elementos, um pelo outro, e mantém os demais fixos.*

Exemplo 2.1.3. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 2 & 4 & 5 & 6 \end{pmatrix}$ *e* $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}$ *são transposições.*

Definição 2.1.3. *A* ***identidade****, denotada por id, é uma permutação tal que* $id(i) = i$*, para todo* $i = 1, \cdots, n$.

Exemplo 2.1.4. $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ *e* $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}$ *são identidades.*

Definição 2.1.4. *Definimos o* ***produto entre permutações*** *como a composição das bijeções associadas às permutações (que resulta em outra bijeção):*

$$\alpha = \begin{pmatrix} 1 & 2 & \cdots & n \\ \alpha(1) & \alpha(2) & \cdots & \alpha(n) \end{pmatrix} \; e \;\; \beta = \begin{pmatrix} 1 & 2 & \cdots & n \\ \beta(1) & \beta(2) & \cdots & \beta(n) \end{pmatrix}$$

$$\Rightarrow \alpha\beta = \begin{pmatrix} 1 & 2 & \cdots & n \\ \alpha(\beta(1)) & \alpha(\beta(2)) & \cdots & \alpha(\beta(n)) \end{pmatrix}.$$

Exemplo 2.1.5. $\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ *e* $\beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$. *O produto* $\alpha\beta$ *é* $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$*; computamos este produto, primeiro aplicando* β *e depois aplicando* α*:*

$$\alpha\beta(1) = \alpha(\beta(1)) = \alpha(2) = 2 \ ,$$
$$\alpha\beta(2) = \alpha(\beta(2)) = \alpha(3) = 1 \ ,$$
$$\alpha\beta(3) = \alpha(\beta(3)) = \alpha(1) = 3 \ .$$

Observação 2.1.1. *Note que* $\alpha\beta \neq \beta\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$.

Exemplo 2.1.6.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 5 & 3 & 2 & 4 & 1 & 6 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 4 & 6 & 1 & 3 & 5 & 7 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 2 & 1 & 7 & 3 & 4 & 6 \end{pmatrix}.$$

Observação 2.1.2. *S_n com a operação de produto, $(S_n, \cdot)$, é um grupo não abeliano (não-comutativo).*

Proposição 2.1.1. *Se α é uma permutação de S_n, então $\alpha\ id = \alpha = id\ \alpha$.*

Demonstração. Seja $\alpha \in S_n$. Então,

$$\alpha\ id = \begin{pmatrix} 1 & 2 & \cdots & n \\ \alpha(1) & \alpha(2) & \cdots & \alpha(n) \end{pmatrix} \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix} =$$

$$= \underbrace{\begin{pmatrix} 1 & 2 & \cdots & n \\ \alpha(1) & \alpha(2) & \cdots & \alpha(n) \end{pmatrix}}_{\alpha} = \begin{pmatrix} 1 & 2 & \cdots & n \\ id(\alpha(1)) & id(\alpha(2)) & \cdots & id(\alpha(n)) \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix} \begin{pmatrix} 1 & 2 & \cdots & n \\ \alpha(1) & \alpha(2) & \cdots & \alpha(n) \end{pmatrix} = id\ \alpha$$

□

Exemplo 2.1.7.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 4 & 5 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 4 & 5 & 2 \end{pmatrix}.$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 4 & 5 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 4 & 5 & 2 \end{pmatrix}.$$

Definição 2.1.5. *Se $x \in X$ e $\alpha \in S_X$ então α **fixa** x, se $\alpha(x) = x$ e α **move** x, se $\alpha(x) \neq x$.*

Definição 2.1.6. *Sejam $i_1, i_2, \cdots, i_r$ números inteiros distintos entre 1 e n. Se $\alpha \in S_n$ fixa os restantes $n - r$ inteiros e se*

$$\alpha(i_1) = i_2\ ,\ \alpha(i_2) = i_3\ ,\ \cdots\ ,\ \alpha(i_{r-1}) = i_r\ ,\ \alpha(i_r) = i_1\ ,$$

*então α é um **ciclo** de comprimento r (ou, α é um r-ciclo). Denotamos α como $(i_1\ i_2\ \cdots\ i_r)$.*

Exemplo 2.1.8. *A identidade* $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = (1) = (2) = (3) = (4)$, *é um 1-ciclo.*

Exemplo 2.1.9. *As transposições* $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 2 & 4 & 5 & 6 \end{pmatrix} = (2\ 3)$ *e* $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix} = (3\ 4)$, *são exemplos de 2-ciclo.*

Exemplo 2.1.10. *A permutação* $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = (1\ 2\ 3\ 4)$, *é um um ciclo de comprimento 4 (4-ciclo).*

Exemplo 2.1.11. $(1\ 2\ 3\ \cdots\ n)$ *é um n-ciclo.*

Exemplo 2.1.12. *A permutação* $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix} = (1\ 2\ 3)(4)(5) = (1\ 2\ 3)$*, é um 3-ciclo. Note que* $(1\ 2\ 3)$*,* $(2\ 3\ 1)$ *e* $(3\ 1\ 2)$ *representam o mesmo ciclo (um r-ciclo, com* $r > 1$*, pode ser representado por r modos diferentes).*

Exemplo 2.1.13. *A permutação* $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix} = (1\ 3\ 5)(2\ 4)$ *não é um ciclo.*

Definição 2.1.7. *Duas permutações* $\alpha, \beta \in S_X$ *são* ***disjuntas*** *se todo elemento movido por uma é fixo pela outra, ou seja, se* $\alpha(x) \neq x$*, então* $\beta(x) = x$ *e se* $\beta(y) \neq y$*, então* $\alpha(y) = y$*. Uma família de permutações* $\alpha_1, \cdots, \alpha_m$ *é* ***disjunta*** *se cada par delas é disjunto.*

Exemplo 2.1.14. *Os ciclos* $(1\ 3\ 5)$ *e* $(2\ 5)$ *não são disjuntos, pois o elemento 5 é movido por ambos.*

Exemplo 2.1.15. *Os ciclos* $(1\ 3\ 4)$ *e* $(2\ 5)$ *são disjuntos.*

2.2 Fatoração em ciclos disjuntos e transposições

Nesta seção vamos demonstrar que podemos escrever uma permutação, com exceção da id, como um produto de ciclos disjuntos com comprimentos ≥ 2 *e que essa fatoração é única a menos da ordem dos fatores. Também vamos demonstrar que toda permutação de* S_n *pode ser expressa como um produto de transposições.*

Definição 2.2.1. *O processo que transforma uma permutação em um produto de ciclos disjuntos é chamado de* ***fatoração em ciclos disjuntos****.*

Exemplo 2.2.1. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 5 & 4 & 1 & 2 & 6 & 7 \end{pmatrix} = (1\,3\,4)(2\,5)(6)(7) = (1\,3\,4)(2\,5).$

Exemplo 2.2.2. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 4 & 1 & 2 & 5 & 3 & 8 & 9 & 7 \end{pmatrix} = (1\ 6\ 3)(2\ 4)(7\ 8\ 9).$

Proposição 2.2.1. *Sejam* α *e* β *ciclos disjuntos. Então* $\alpha\beta = \beta\alpha$*.*

Demonstração. Sejam $\alpha = (i_1 \cdots i_r)$ e $\beta = (j_1 \cdots j_k)$ dois ciclos disjuntos. Logo

$$\alpha\beta = (i_1 \cdots i_r)(j_1 \cdots j_k) =$$

$$= \begin{pmatrix} i_1 & \cdots & i_r & j_1 & \cdots & j_k \\ i_2 & \cdots & i_1 & j_1 & \cdots & j_k \end{pmatrix} \begin{pmatrix} i_1 & \cdots & i_r & j_1 & \cdots & j_k \\ i_1 & \cdots & i_r & j_2 & \cdots & j_1 \end{pmatrix} =$$

$$= \begin{pmatrix} i_1 & \cdots & i_r & j_1 & \cdots & j_k \\ i_2 & \cdots & i_1 & j_2 & \cdots & j_1 \end{pmatrix} =$$

$$= \begin{pmatrix} i_1 & \cdots & i_r & j_1 & \cdots & j_k \\ i_1 & \cdots & i_r & j_2 & \cdots & j_1 \end{pmatrix} \begin{pmatrix} i_1 & \cdots & i_r & j_1 & \cdots & j_k \\ i_2 & \cdots & i_1 & j_1 & \cdots & j_k \end{pmatrix} =$$

$$= (j_1 \cdots j_k)(i_1 \cdots i_r) = \beta\alpha.$$

□

Observação 2.2.1. *Consideramos nesse trabalho que* α^k ($\alpha \in S_n$ *e* $k \in \mathbb{Z}^+$) *corresponde ao produto* $\underbrace{\alpha\alpha\alpha\cdots\alpha}_{k \text{ vezes}}$. *Notemos que as seguintes propriedades são satisfeitas:*

- ($\alpha \in S_n$ *e* $j, k \in \mathbb{Z}$) $\alpha^j\alpha^k = \alpha^{j+k}$.
- ($\alpha, \beta, \cdots, \gamma$ *ciclos disjuntos de* S_n) $(\alpha\beta \ldots \gamma)^k = \alpha^k\beta^k \cdots \gamma^k$.

Observação 2.2.2. *Um corolário do Teorema de Lagrange (ver [6]) é o seguinte: se* G *é um grupo finito com* n *elementos* ($\forall a \in G$) a^n *é a identidade. Assim, faz sentido a definição seguinte.*

Definição 2.2.2. *Seja* $\alpha \in S_n$. *A* ***ordem*** *de* α *é o menor inteiro positivo* k *que satisfaz* $\alpha^k = id$.

Exemplo 2.2.3. *A ordem de* $\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ *é 3, pois* $\alpha \neq id$, $\alpha^2 \neq id$ *e*

$$\alpha^3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = id.$$

Exemplo 2.2.4. *A ordem de* $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix}$ *é 2, pois* $\alpha \neq id$ *e*

$$\alpha^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = id.$$

Proposição 2.2.2. *Seja* $\alpha \in S_n$ *um r-ciclo. Então a ordem de* α *é igual a* r.

Demonstração. O r-ciclo $\alpha = (a_1 a_2 \cdots a_r)$ move a_i para a_{i+1}. Então, α^2 tem o efeito dobrado de mover cada a_i para a_{i+2}. Generalizando, α^k move a_i para a_{i+k}, em que todos subscritos são reduzidos módulo r. Agora, α^k é a identidade id se, e somente se, $(\forall i)\ a_{i+k} = a_i$. Isso ocorre se, e somente se, $k \equiv 0(mod\ r)$. O menor k positivo tal que $\alpha^k = id$ é o próprio r. Então α tem ordem r. □

Corolário 2.2.1. *Seja $\alpha \in S_n$ um r-ciclo. Então a ordem de α é menor ou igual a n.*

Lema 2.2.1. *Sejam $\alpha_1, \alpha_2, \cdots, \alpha_k$ ciclos disjuntos de S_n. Se $\phi = \alpha_1 \alpha_2 \cdots \alpha_k$, então*

$$(\exists m \in \mathbb{Z}^+)\ \phi^m = id \Leftrightarrow (\forall i)\ \alpha_i^m = id\ .$$

Demonstração. ($\Rightarrow$) Suponha, por contradição, que $(\exists i)\ \alpha_i^m \neq id$. Sem perda de generalidade, vamos supor $i = 1$. Assim, existe $j \in \{1, \cdots, n\}$ tal que $\alpha_1^m(j) \neq j$. Logo, $\alpha_1(j) \neq j$. Então, $(\forall i \neq 1)\ \alpha_i(j) = j$, pois $\alpha_1, \alpha_2, \cdots, \alpha_k$ são disjuntos. Assim, $\alpha_i^m(j) = j$ para todo $i > 1$. Agora, $id = \alpha_1^m \alpha_2^m \cdots \alpha_k^m$, então

$$j = id(j) = \alpha_1^m(j)\alpha_2^m(j) \cdots \alpha_k^m(j) = \alpha_1^m(j) id(j) = \alpha_1^m(j)\ ,$$

que é um absurdo, pois contradiz o fato de $\alpha_1(j) \neq j$.

($\Leftarrow$)

$$\phi = \alpha_1 \alpha_2 \cdots \alpha_k \Rightarrow \phi^m = (\alpha_1 \alpha_2 \cdots \alpha_k)^m \Rightarrow$$
$$\Rightarrow \phi^m = \alpha_1^m \alpha_2^m \cdots \alpha_k^m = id\ id\ \cdots\ id = id.$$

□

Proposição 2.2.3. *Sejam $\alpha_1, \cdots, \alpha_r \in S_n$ ciclos disjuntos de comprimentos $r_1, \cdots, r_t$, respectivamente. Então, o produto $\phi = \alpha_1 \cdots \alpha_r$ tem ordem igual ao M.M.C. de $\{r_1, \cdots, r_t\}$.*

Demonstração. Para todo $i \neq j$, como α_i e α_j são ciclos disjuntos, $\alpha_i \alpha_j = \alpha_j \alpha_i$. Assim, $\phi^m = \alpha_1^m \cdots \alpha_r^m$ para todo m. Logo, $\phi^m = id$ se, e somente se, $\alpha_i^m = id$ (pelo Lema 2.2.1). Pela Proposição 2.2.2, se $\alpha_i^m = id$, então m é múltiplo de r_i. Logo, $\phi^m = id$ se, e somente se, m é um múltiplo comum de $\{r_1, \cdots, r_t\}$. Portanto, a ordem de $\phi = \alpha_1 \cdots \alpha_r$ é o M.M.C. de $\{r_1, \cdots, r_t\}$. □

Teorema 2.2.1. *Seja $\alpha \in S_n$, $\alpha \neq id$. Então a permutação α é igual a um produto de ciclos disjuntos de comprimentos ≥ 2 e essa fatoração é única a menos da ordem dos fatores.*

Demonstração. Como α é diferente de id, existe i_1 tal que $\alpha(i_1) \neq i_1$. Considere a sequência $i_1, \alpha(i_1), \alpha^2(i_1), \cdots$. Como α é uma bijeção em $\{1, \cdots, n\}$, esta sequência começa a se repetir a partir de um expoente r_1, $2 \leq r_1 \leq n$. Logo, $i_1, \alpha(i_1), \cdots, \alpha^{r_1-1}(i_1)$ são todos distintos e $\alpha^{r_1}(i_1) = i_1$. Portanto, a restrição de α ao conjunto $\{i_1, \alpha(i_1), \cdots, \alpha^{r_1-1}(i_1)\}$ é tal que

$$\alpha|_{\{i_1, \alpha(i_1), \cdots, \alpha^{r_1-1}(i_1)\}} = (i_1 \alpha(i_1) \ \cdots \ \alpha^{r_1-1}(i_1)).$$

Denotaremos este r_1-ciclo $(i_1 \alpha(i_1) \ \cdots \ \alpha^{r_1-1}(i_1))$ por σ_1. Se a restrição de α ao complementar de $\{i_1, \alpha(i_1), \cdots, \alpha^{r_1-1}(i_1)\}$ é a id, então $\alpha = \sigma_1$. Se não, tomamos um elemento $i_2 \in \{1, 2, \cdots, n\} \backslash \{i_1, \alpha(i_1), \cdots, \alpha^{r_1-1}(i_1)\}$ tal que $\alpha(i_2) \neq i_2$; de maneira similar à etapa anterior, vai existir um número inteiro $r_2 \geq 2$ tal que

$$\alpha|_{\{i_2, \alpha(i_2), \cdots, \alpha^{r_2-1}(i_2)\}} = (i_2 \alpha(i_2) \ \cdots \ \alpha^{r_2-1}(i_2)).$$

Denotaremos este r_2-ciclo $(i_2 \alpha(i_2) \ \cdots \ \alpha^{r_2-1}(i_2))$ por σ_2. Observamos que σ_1 e σ_2 são disjuntos. Se a restrição de α ao complementar do conjunto $\{i_1, \alpha(i_1), \cdots, \alpha^{r_1-1}(i_1), i_2, \alpha(i_2), \cdots, \alpha^{r_2-1}(i_2)\}$ é a identidade, então $\alpha = \sigma_1\sigma_2 = \sigma_2\sigma_1$. Se não, seja $i_3 \in \{1, 2, \cdots, n\} \backslash \{i_1, \alpha(i_1), \cdots, \alpha^{r_1-1}(i_1), i_2, \alpha(i_2), \cdots, \alpha^{r_2-1}(i_2)\}$ tal que $\alpha(i_3) \neq i_3$ e continuamos o processo. Claramente este processo vai ter que parar depois de um número finito de etapas e vamos obter que $\alpha = \sigma_1\sigma_2 \cdots \sigma_t$, em que $\sigma_1, \sigma_2, \cdots, \sigma_t$ são ciclos disjuntos de comprimentos ≥ 2.

Agora, para provar a unicidade, suponha que temos também $\alpha = \tau_1\tau_2 \cdots \tau_u$, com $\tau_1, \tau_2, \cdots, \tau_u$ ciclos disjuntos, cada um deles de comprimento ≥ 2. Como $\tau_1\tau_2 \cdots \tau_u(i_1) = \alpha(i_1) \neq i_1$ e como os τ's são ciclos disjuntos, existe um único τ_j tal que $\tau_j(i_1) = \alpha(i_1)$. Como os τ's comutam entre si, podemos supor que $j = 1$ e então $\tau_1(i_1) = \alpha(i_1)$. Vamos mostrar que $\tau_1 = \sigma_1$. O ciclo τ_1 não pode deixar $\alpha(i_1)$ fixo, isto é, τ_1 não pode mandar $\alpha(i_1)$ sobre $\alpha(i_1)$, pois τ_1 já manda i_1 sobre $\alpha(i_1)$. Como os τ's são ciclos disjuntos, então, $(\forall j \geq 2)$, τ_j deixa $\alpha(i_1)$ fixo e, portanto, $\alpha(\alpha(i_1)) = \tau_1(\alpha(i_1))$; assim $\tau_1(\alpha(i_1)) = \alpha^2(i_1)$. De maneira similar obtemos que $\tau_1(\alpha^{k-1}(i_1)) = \alpha^k(i_1)$, para todo $k \geq 0$ e, portanto, $\tau_1 = \sigma_1$. Similarmente, trabalhando com i_2 no lugar de i_1, vamos obter que $\tau_2 = \sigma_2$; continuando assim, obteremos que $u = t$ e que, a menos de ordem, $\sigma_j = \tau_j$, para cada $j = 1, \cdots, t$.

□

Teorema 2.2.2. *Toda permutação de S_n pode ser expressa como um produto de transposições.*

Demonstração. Seja $\alpha \in S_n$ ($\alpha \neq id$). Pelo Teorema 2.2.1, podemos reescrever α como um produto de ciclos disjuntos com comprimentos ≥ 2. Então, basta provarmos que qualquer r-ciclo possa ser expresso como um produto de transposições, para que α possa ser expressa como um produto de transposições.
Seja $\beta = (1\ 2\ \cdots\ r)$ um r-ciclo de S_n. Vamos demonstrar que

$$(1\ 2\ \cdots\ r) = (1\ r)(1\ \ r-1)\cdots(1\ 2)\ .$$

Para $r = 2$: $(1\ 2) = (1\ 2)$.

Suponha, por indução, que para $r = k \geq 2$

$$(1\ 2\ \cdots\ k) = (1\ k)(1\ \ k-1)\cdots(1\ 2)\ .$$

Tomando $r = k+1$, temos

$$(1\ 2\ \cdots\ k\ \ k+1) = \begin{pmatrix} 1 & 2 & \cdots & k & k+1 \\ 2 & 3 & \cdots & k+1 & 1 \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & 2 & \cdots & k & k+1 \\ k+1 & 2 & \cdots & k & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & \cdots & k & k+1 \\ 2 & 3 & \cdots & 1 & k+1 \end{pmatrix} =$$

$$= (1\ \ k+1)(1\ 2\ 3\ \cdots\ k) = (1\ \ k+1)(1\ k)(1\ \ k-1)\cdots(1\ 2)\ .$$

□

Corolário 2.2.2. *Todo r-ciclo pode ser expresso como um produto de transposições da forma*

$$(1\ 2\ \cdots\ r) = (1\ r)(1\ \ r-1)\cdots(1\ 2)\ .$$

Exemplo 2.2.5. *Vamos expressar a permutação* $\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ *como um produto de transposições.*

$$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1\ 2\ 3) = (1\ 3)(1\ 2) =$$

$$= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \alpha\ .$$

Observação 2.2.3. *Note que* $(1\ 3)(1\ 2) = (1\ 2\ 3) \neq (1\ 3\ 2) = (1\ 2)(1\ 3)$.

2.3 Paridade de uma permutação

Vamos demonstrar, que toda permutação fatorada como produto de transposições possui a mesma paridade no número de fatores, para toda fatoração possível.

Lema 2.3.1. *Se $g, h \geq 1$, então*

$$(a\ b)(a\ c_1\ \cdots\ c_g\ b\ d_1\ \cdots\ d_h) = (a\ c_1\ \cdots\ c_g)(b\ d_1\ \cdots\ d_h) \qquad (2.3.a)$$

e

$$(a\ b)(a\ c_1\ \cdots\ c_g)(b\ d_1\ \cdots\ d_h) = (a\ c_1\ \cdots\ c_g\ b\ d_1\ \cdots\ d_h) \qquad (2.3.b)\ .$$

Demonstração.

$$(a\ b)(a\ c_1\ \cdots\ c_g\ b\ d_1\ \cdots\ d_h) =$$

$$= \begin{pmatrix} a & c_1 & \cdots & c_g & b & d_1 & \cdots & d_h \\ b & c_1 & \cdots & c_g & a & d_1 & \cdots & d_h \end{pmatrix} \begin{pmatrix} a & c_1 & \cdots & c_g & b & d_1 & \cdots & d_h \\ c_1 & c_2 & \cdots & b & d_1 & d_2 & \cdots & a \end{pmatrix} =$$

$$= \begin{pmatrix} a & c_1 & \cdots & c_g & b & d_1 & \cdots & d_h \\ c_1 & c_2 & \cdots & a & d_1 & d_2 & \cdots & b \end{pmatrix} =$$

$$= \begin{pmatrix} a & c_1 & \cdots & c_g & b & d_1 & \cdots & d_h \\ c_1 & c_2 & \cdots & a & b & d_1 & \cdots & d_h \end{pmatrix} \begin{pmatrix} a & c_1 & \cdots & c_g & b & d_1 & \cdots & d_h \\ a & c_1 & \cdots & c_g & d_1 & d_2 & \cdots & b \end{pmatrix} =$$

$$= (a\ c_1\ \cdots\ c_g)(b\ d_1\ \cdots\ d_h)\ .$$

$$(a\ b)(a\ c_1\ \cdots\ c_g)(b\ d_1\ \cdots\ d_h) =$$

$$= \begin{pmatrix} a & c_1 & \cdots & c_g & b & d_1 & \cdots & d_h \\ c_1 & c_2 & \cdots & b & d_1 & d_2 & \cdots & a \end{pmatrix} =$$

$$= (a\ c_1\ \cdots\ c_g\ b\ d_1\ \cdots\ d_h)\ .$$

□

Definição 2.3.1. *Se $\alpha \in S_n$ e $\alpha = \sigma_1 \cdots \sigma_k$ é uma fatoração em ciclos disjuntos (considerando os 1-ciclos), o* ***sinal*** *de α é definido por*

$$sgn(\alpha) = (-1)^{n-k}\ .$$

Observação 2.3.1. *A função sgn está bem definida, pois pelo Teorema 2.2.1 a fatoração em ciclos disjuntos é única a menos da ordem dos fatores.*

Observação 2.3.2. *Se τ é uma transposição, então ela move dois números, digamos, i e j, e fixa cada um dos outros $n-2$ números. Logo, $k = (n-2)+1 = n-1$, e então*

$$sgn(\tau) = (-1)^{n-(n-1)} = -1 \ .$$

Exemplo 2.3.1. *Seja* $\alpha = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} = (1\ 2)$. *Então,* $k = 1$. *Logo,* $sgn(\alpha) = (-1)^{2-1} = -1$.

Exemplo 2.3.2. *Seja* $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 4 & 5 \end{pmatrix} = (1\ 3\ 2)(4)(5) = (1\ 2)(1\ 3)$.

Então, $k = 3$. *Logo,* $sgn(\alpha) = (-1)^{5-3} = 1$.

Exemplo 2.3.3. *Seja* $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 1 & 2 & 5 & 4 & 6 & 7 \end{pmatrix} = (1\ 3\ 2)(4\ 5)(6)(7) = (1\ 2)(1\ 3)(4\ 5)$.

Então, $k = 4$. *Logo,* $sgn(\alpha) = (-1)^{7-4} = -1$.

Lema 2.3.2. *Se $\alpha \in S_n$ e τ é uma transposição, então*

$$sgn(\tau\alpha) = -sgn(\alpha) \ .$$

Demonstração. Seja $\tau = (a\ b)$ uma transposição. Seja $\alpha = \sigma_1 \cdots \sigma_k$ a fatoração completa de α em ciclos disjuntos (existe um 1-ciclo para cada i fixo por α, e todo número entre 1 e n ocorre em um único ciclo). Se a e b ocorrem no mesmo ciclo, digamos, sem perda de generalidade, em σ_1, então $\sigma_1 = (a\ c_1\ \cdots\ c_g\ b\ d_1\ \cdots\ d_h)$, em que $g, h \geq 0$. Pelo Lema 2.3.1,

$$\tau\sigma_1 = (a\ c_1\ \cdots\ c_g)(b\ d_1\ \cdots\ d_h) \ ,$$

e então $\tau\alpha = (\tau\sigma_1)\sigma_2 \cdots \sigma_k$ é uma fatoração completa com um ciclo extra ($\tau\sigma_1$ separa-se em dois ciclos disjuntos). Logo, $sgn(\tau\alpha) = (-1)^{n-(k+1)} = -sgn(\alpha)$. A outra possibilidade é que a e b ocorram em ciclos diferentes, digamos, sem perda de generalidade, $\sigma_1 = (a\ c_1\ \cdots\ c_g)$ e $\sigma_2 = (b\ d_1\ \cdots\ d_h)$, em que $g, h \geq 0$. E, agora, $\tau\alpha = (\tau\sigma_1\sigma_2)\sigma_3 \cdots \sigma_k$, e pelo Lema 2.3.1,

$$\tau\sigma_1\sigma_2 = (a\ c_1\ \cdots\ c_g\ b\ d_1\ \cdots\ d_h) \ .$$

Logo, a fatoração completa de $\tau\alpha$ tem um ciclo a menos que α, e então $sgn(\tau\alpha) = (-1)^{n-(k-1)} = -sgn(\alpha)$. □

Teorema 2.3.1. *Para todo $\alpha, \beta \in S_n$, $sgn(\alpha\beta) = sgn(\alpha)sgn(\beta)$.*

Demonstração. Seja $\alpha \in S_n$, tal que $\alpha = \tau_1 \cdots \tau_m$, τ's são transposições e m mínimo. Suponha, por indução em m, que $sgn(\alpha\beta) = sgn(\alpha)sgn(\beta)$, para todo $\beta \in S_n$. O primeiro passo é garantido pelo Lema 2.3.2. Se $m > 1$, então a fatoração $\tau_2 \cdots \tau_m$ também é mínima, pois se $\tau_2 \cdots \tau_m = \sigma_1 \cdots \sigma_q$, em que cada σ_j é uma transposição e $q < m - 1$, temos a fatoração $\alpha = \tau_1\sigma_1 \cdots \sigma_q$ que contradiz o fato de m ser mínimo. Portanto,

$$sgn(\alpha\beta) = sgn(\tau_1 \cdots \tau_m\beta) = -sgn(\tau_2 \cdots \beta) \qquad \text{(pelo Lema 2.3.2)}$$

$$= -sgn(\tau_2 \cdots \tau_m)sgn(\beta) \qquad \text{(pela indução)}$$

$$= sgn(\tau_1 \cdots \tau_m)sgn(\beta) \qquad \text{(pelo Lema 2.3.2)}$$

$$= sgn(\alpha)sgn(\beta)\ . \qquad \square$$

Teorema 2.3.2. *(i) Se $\alpha \in S_n$ e $sgn(\alpha) = 1$, então α é um produto de um número par de transposições.*
(ii) Se $\alpha \in S_n$ e $sgn(\alpha) = -1$, então α é um produto de um número ímpar de transposições.

Demonstração. (i) Pela Observação 2.3.2, temos que $sgn(\tau) = -1$ para toda transposição τ. Logo, se $\alpha = \tau_1 \cdots \tau_q$ é uma fatoração de α em transposições, pelo Teorema 2.3.1, $sgn(\alpha) = sgn(\tau_1) \cdots sgn(\tau_q) = (-1)^q$. Então, $sgn(\alpha) = 1$ se, e somente se, q é par.

(ii) Como $sgn(\tau) = -1$ para toda transposição τ, se $\alpha = \tau_1 \cdots \tau_q$ é uma fatoração de α em transposições, pelo Teorema 2.3.1, $sgn(\alpha) = sgn(\tau_1) \cdots sgn(\tau_q)$ $= (-1)^q$. Então, $sgn(\alpha) = -1$ se, e somente se, q é ímpar. $\square$

Exemplo 2.3.4. *A permutação $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$, possui $sgn(\alpha) = 1$, note que ela pode ser escrita como o produto de um número par de transposições:*
$\alpha = (1\ 3)(1\ 2) = (2\ 3)(1\ 3) = (1\ 3)(4\ 2)(1\ 2)(1\ 4) =$
$= (1\ 3)(4\ 2)(1\ 2)(1\ 4)(2\ 3)(2\ 3)$.

Definição 2.3.2. *Seja $\alpha \in S_n$. Se $sgn(\alpha) = 1$, ou seja, se α é o produto de um número par de transposições, então α é **par**. E, se $sgn(\alpha) = -1$, ou seja, se α é o produto de um número ímpar de transposições, então α é **ímpar**.*

Exemplo 2.3.5. $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 2 & 5 & 1 & 4 \end{pmatrix} = (1\ 5)(1\ 4)(1\ 6)(2\ 3)$ *é um produto de um número par de transposições, então α é par.*

Exemplo 2.3.6. $\alpha = (2\ 6)$, *é uma transposição, então* $sgn(\alpha) = -1$, *assim* α *é ímpar.*

Observação 2.3.3. *Toda transposição é ímpar.*

Capítulo 3

O mínimo comprimento de uma permutação como produto de transposições

Neste capítulo, demonstramos via Álgebra Linear, que uma permutação em S_n não pode ser escrita como um produto de menos que $(n-r)$ transposições, em que r é o número de ciclos disjuntos na permutação, incluindo os 1-ciclos.

3.1 Permutações como transformações ortogonais

Inicialmente, vamos apresentar alguns conceitos e resultados importantes.

Definição 3.1.1. *Uma* ***matriz de permutação*** *é uma matriz obtida permutando-se as colunas da matriz identidade. Logo, existem $n!$ matrizes de permutação de ordem n.*

Exemplo 3.1.1. $\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ *é uma matriz de permutação de ordem 3.*

Definição 3.1.2. *Uma* ***matriz ortogonal*** *é uma matriz real quadrada cujas colunas formam um conjunto ortonormal de vetores.*

Observação 3.1.1. *Note que a definição acima é equivalente à seguinte afirmação: $Q \in \mathbb{R}^{n\times n}$ é uma matriz ortogonal $\Leftrightarrow QQ^T = Q^TQ = I$.*

Exemplo 3.1.2. *A matriz de permutação é um exemplo simples de uma matriz ortogonal, pois suas colunas formam a base canônica do $\mathbb{R}^n$.*

3.2 Ação do grupo de permutação S_n sobre $\mathbb{R}^n$

Definição 3.2.1. *Seja σ uma permutação de S_n. Seja $\{e_1, e_2, \cdots, e_n\}$ a base canônica de $\mathbb{R}^n$. Definimos a transformação linear $f_\sigma : \mathbb{R}^n \to \mathbb{R}^n$ tal que $f_\sigma(e_i) = e_{\sigma(i)}$. Essa transformação linear f_σ é dita ser a ação de permutação σ sobre $\mathbb{R}^n$.*

Exemplo 3.2.1. *Seja* $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1\ 2\ 3)$. *Então,* $f_\sigma : \mathbb{R}^3 \to \mathbb{R}^3$ *é definida por:*

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \mapsto \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} ,$$

pois

$$f_\sigma(e_1) = e_{\sigma(1)} = e_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} ,$$

$$f_\sigma(e_2) = e_{\sigma(2)} = e_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} ,$$

$$f_\sigma(e_3) = e_{\sigma(3)} = e_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} .$$

Exemplo 3.2.2. *Seja* $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 5 & 2 & 4 & 3 & 1 & 7 \end{pmatrix} = (2\ 5\ 3)(1\ 6)(4)(7) = (2\ 5\ 3)(1\ 6)$. *Então,* $f_\sigma : \mathbb{R}^7 \to \mathbb{R}^7$ *é definida por:*

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{pmatrix} \mapsto \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{pmatrix} ,$$

pois

$$f_\sigma(e_1) = e_{\sigma(1)} = e_6 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \; f_\sigma(e_2) = e_{\sigma(2)} = e_5 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix},$$

$$f_\sigma(e_3) = e_{\sigma(3)} = e_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \; f_\sigma(e_4) = e_{\sigma(4)} = e_4 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

$$f_\sigma(e_5) = e_{\sigma(5)} = e_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \; f_\sigma(e_6) = e_{\sigma(6)} = e_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix},$$

$$f_\sigma(e_7) = e_{\sigma(7)} = e_7 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}.$$

Observação 3.2.1. *Como podemos notar nos exemplos anteriores, a matriz associada a f_σ é uma matriz ortogonal, pois é uma matriz de permutação.*

Definição 3.2.2. *Seja f_σ a ação da permutação $\sigma \in S_n$ sobre $\mathbb{R}^n$. O* ***Espaço de ponto fixo*** *de f_σ é o subespaço de $\mathbb{R}^n$ definido por*

$$V_\sigma = \{x \in \mathbb{R}^n \mid f_\sigma(x) = x\}.$$

Proposição 3.2.1. *Seja $\sigma \in S_n$. Então, $V_\sigma \neq \{0\}$.*

Demonstração. Se $\sigma = id$, então $V_\sigma = \mathbb{R}^n$. Se $\sigma \neq id$, pelo Teorema 2.2.1, $\sigma = \tau_1 \cdots \tau_r$, $r \geq 1$, em que $\tau_1, \cdots, \tau_r$ são ciclos disjuntos de ordem ≥ 2. Suponha $\tau_1 = (i_1, \cdots, i_k)$. Logo, $e_{i_1} + \cdots + e_{i_k} \in V_\sigma$. □

Observação 3.2.2. *V_σ é o autoespaço de f_σ associado ao autovalor 1.*

Exemplo 3.2.3. *Seja $\sigma = (1\ 2)$ em S_3. Temos que*

$$f_\sigma(e_1) = e_{\sigma(1)} = e_2 \ ,$$

$$f_\sigma(e_2) = e_{\sigma(2)} = e_1 \ ,$$

$$f_\sigma(e_3) = e_{\sigma(3)} = e_3 \ ,$$

$$f_\sigma(e_1 + e_2) = f_{\sigma(e_1)} + f_{\sigma(e_2)} = e_2 + e_1 = e_1 + e_2 \ ,$$

$$f_\sigma(e_1 + e_3) = f_{\sigma(e_1)} + f_{\sigma(e_3)} = e_2 + e_3 \ ,$$

$$f_\sigma(e_2 + e_3) = f_{\sigma(e_2)} + f_{\sigma(e_3)} = e_1 + e_3 \ .$$

Então, $e_1 + e_2$ e e_3 são fixos. Logo, $V_\sigma = [e_1 + e_2 \ , \ e_3]$.

Observação 3.2.3. *De modo geral, se $(i\ j) \in S_n$ então uma base para V_σ é*

$$\{e_k \mid k \neq i, j\} \cup \{e_i + e_j\} \ .$$

Exemplo 3.2.4. *Seja $\sigma = (1\ 2\ 3)$ em S_5. Temos que*

$$f_\sigma(e_1) = e_{\sigma(1)} = e_2 \ ,$$

$$f_\sigma(e_2) = e_{\sigma(2)} = e_3 \ ,$$

$$f_\sigma(e_3) = e_{\sigma(3)} = e_1 \ ,$$

$$f_\sigma(e_4) = e_{\sigma(4)} = e_4 \ ,$$

$$f_\sigma(e_5) = e_{\sigma(5)} = e_5 \ .$$

Então, $e_1 + e_2 + e_3$, e_4 e e_5 são fixos. Assim, $V_\sigma = [e_1 + e_2 + e_3 \ , \ e_4 \ , \ e_5]$.

Proposição 3.2.2. *Se σ é um r-ciclo, $\sigma = (i_1 \ \cdots \ i_r)$, então uma base de V_σ é $\{e_k \mid k \notin \{i_1, \cdots, i_r\}\} \cup \{e_{i_1} + \cdots + e_{i_r}\}$.*

Demonstração. Pela definição de f_σ, $f_\sigma(e_k) = e_k$, se $k \notin \{i_1, \cdots, i_r\}$. Então, $f_\sigma(e_{i_k}) = e_{i_{k+1}}$, se $k = 1, \cdots, r-1$, e $f_\sigma(e_{i_r}) = e_{i_1}$. Seja β a base ordenada $\{e_{i_1}, \cdots, e_{i_r}\} \cup \{e_k \mid k \notin \{i_1, \cdots, i_r\}\}$. Seja A a matriz de f_σ em relação à base β, isto é,

$$[f_\sigma]_\beta = \begin{bmatrix} [f_\sigma(e_{i_1})]_\beta & \cdots & [f_\sigma(e_{i_r})]_\beta & \cdots \end{bmatrix} = \begin{bmatrix} 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \\ 1 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & & \vdots \\ 0 & \cdots & 1 & 0 & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & 1 & \cdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 1 \end{bmatrix}.$$

Então, temos que

$$det[xI - A] = \begin{vmatrix} x & \cdots & 0 & -1 & 0 & \cdots & 0 \\ -1 & \ddots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots & \vdots & & \vdots \\ 0 & \cdots & -1 & x & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & x-1 & \cdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & x-1 \end{vmatrix} =$$

$$= \begin{vmatrix} x & \cdots & 0 & -1 \\ -1 & \ddots & 0 & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & -1 & x \end{vmatrix} \cdot \begin{vmatrix} x-1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & x-1 \end{vmatrix} =$$

$$= \left(x \begin{vmatrix} x & \cdots & 0 & 0 \\ -1 & \ddots & 0 & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & -1 & x \end{vmatrix} + (-1)^{1+r}(-1) \begin{vmatrix} -1 & x & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \ddots & x \\ 0 & 0 & \cdots & -1 \end{vmatrix} \right) \cdot (x-1)^{n-r} =$$

$$= (x^r - (-1)^{1+r+r-1})(x-1)^{n-r} = (x^r - 1)(x-1)^{n-r}$$

$$= (x-1)^{n-r+1}(x^{r-1} + x^{r-2} + \cdots + x + 1).$$

Logo, 1 tem multiplicidade algébrica $n - r + 1$. Mas, a multiplicidade geométrica de 1 também é $n-r+1$, pois $\{e_k \mid k \notin \{i_1, \cdots, i_r\}\} \cup \{e_{i_1} + \cdots + e_{i_k}\}$ é um conjunto linearmente independente de $n - r + 1$ autovetores de A associados a 1.

□

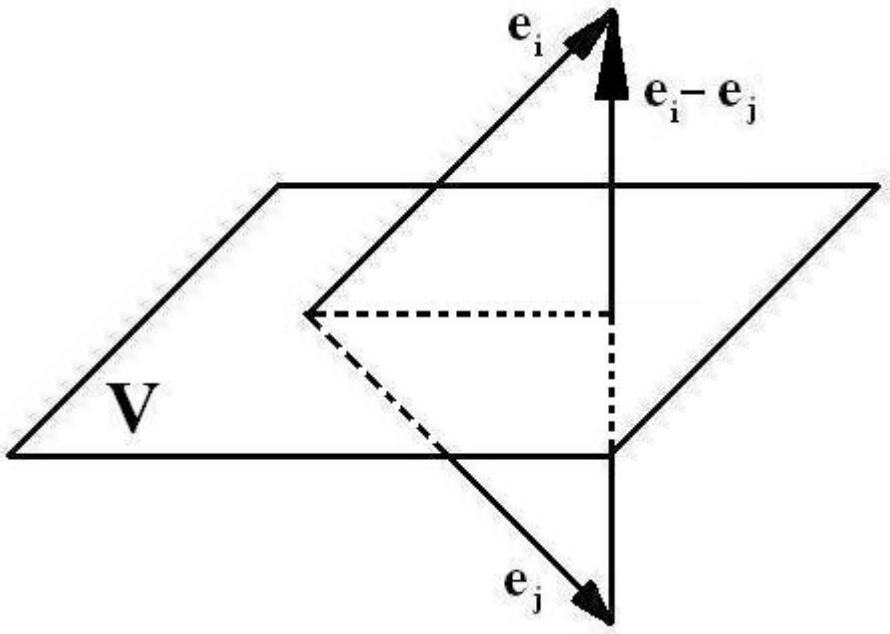
Observação 3.2.4. *Como podemos notar, os vetores da base de V_σ podem ser formados de acordo com os ciclos disjuntos na decomposição da permutação.*

Se uma permutação pode ser escrita como produto de r ciclos disjuntos, incluindo os 1-ciclos, temos que dim $V_\sigma = r$, pois cada ciclo contribui com um elemento na base que forma V_σ.

3.3 Transposições vistas como reflexões

Proposição 3.3.1. *A ação de uma transposição sobre $\mathbb{R}^n$ é uma reflexão de Householder (uma reflexão em relação a um subespaço de dimensão $n-1$).*

Demonstração. Seja $\sigma = (i\ j)$, $i < j$. Seja V o hiperplano ortogonal ao vetor $e_i - e_j$. Logo, $V^\perp = [e_i - e_j]$. Notemos que $e_i + e_j \in V$ e $(\forall k \neq i, j)$ e_k é ortogonal a $e_i - e_j$, ou seja, $e_k \in V$. Logo, $\{e_k \mid k \neq i, j\} \cup \{e_i + e_j\}$ é base de V. Assim, $V = V_\sigma$.



Logo, como $\mathbb{R}^n = V \oplus V^\perp$, para todo $x \in \mathbb{R}^n$, existe um único $x_V \in V$ e existe um único $x_{V^\perp} \in V^\perp$ tais que $x = x_V + x_{V^\perp}$. Como f_σ é uma transformação linear,

$$f_\sigma(x) = f_\sigma(x_V) + f_\sigma(x_{V^\perp}) =$$
$$= x_V + (-x_{V^\perp}) = x_V + x_{V^\perp} - x_{V^\perp} - x_{V^\perp} = x - 2x_{V^\perp}\ .$$

A projeção de x sobre o hiperplano $V^\perp = [e_i - e_j]$ é $x_{V^\perp} = (e_i - e_j)\dfrac{(e_i - e_j)^T}{||e_i - e_j||^2}x$.

Então,

$$f_\sigma(x) = x - \left[\frac{2(e_i - e_j)(e_i - e_j)^T}{2}\right] x = [I - (e_i - e_j)(e_i - e_j)^T]x\ .$$

Logo, a matriz de permutação associada a uma transposição $(i\ j)$ é a matriz da reflexão dada por $I - (e_i - e_j)(e_i - e_j)^T$. □

3.4 O número mínimo de transposições

A permutação $\sigma \in S_5$, $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix}$, *pode ser escrita como o produto de no mínimo duas transposições:* $(1\ 2\ 3)(4)(5) = (1\ 3)(1\ 2)$. *Note que quem fica fixo são os vetores* $e_1 + e_2 + e_3$, e_4 *e* e_5, *contidos na interseção dos hiperplanos cujos vetores normais são* $(e_1 - e_3)$ *e* $(e_1 - e_2)$, *respectivamente. Como* $V_\sigma = [e_1 + e_2 + e_3\ ,\ e_4\ ,\ e_5]$, *temos que dim* $V_\sigma = 3$. *Pela Observação 3.2.4, temos que dim* $V_\sigma = r$, *em que* r *denota o número de ciclos disjuntos presentes em* σ, *incluindo os 1-ciclos. No caso,* $r = 3$. *Note que dim* $V_\sigma = 3 \geq n - k$, *em que* $n = 5$ *e* $k = 2$, *o número de transposições.*

Será que esse fato se generaliza para todas as permutações em S_n*? A resposta é sim e a demonstração se encontra no teorema a seguir:*

Teorema 3.4.1. *Uma permutação em* S_n *não pode ser escrita como um produto de menos que* $(n - r)$ *transposições, em que* r *é o número de ciclos disjuntos na permutação, incluindo os 1-ciclos.*

Demonstração. Seja $\sigma \in S_n$ tal que $\sigma = \tau_1\tau_2\cdots\tau_k$, em que $\tau's$ são transposições. Como demonstramos na Proposição 3.3.1, transposições podem ser vistas como reflexões em relação a hiperplanos. Tomamos, então, v_i, $i = 1, 2, \cdots, k$, vetores associados a essas transposições, vetores ortogonais aos hiperplanos V_{τ_i} determinados por τ_i. Logo, $V_{\tau_1} \cap \cdots \cap V_{\tau_k} = [v_1, \cdots, v_k]^\perp$. Notemos que $V_{\tau_1} \cap \cdots \cap V_{\tau_k} \subseteq V_\sigma$, pois os elementos de $V_{\tau_1} \cap \cdots \cap V_{\tau_k}$ ficam fixos por cada reflexão τ_i, $i = 1, \cdots, k$. Assim, $V_\sigma^\perp \subseteq [v_1, \cdots, v_k]$ e, logo, dim $V_\sigma^\perp \leq k$. Então, $dim\ V_\sigma = n - dim\ V_\sigma^\perp \geq n - k$. Portanto, como $dim\ V_\sigma = r$, o número de ciclos disjuntos (incluindo os 1-ciclos) em σ, temos que $k \geq n - r$.

□

Conclusão

As disciplinas de Álgebra e de Álgebra Linear, durante minha graduação, foram apresentadas de maneira que ambas me pareciam ser isoladas. Elaborar este Trabalho de Conclusão de Curso, me deu a chance de aprender que existem vínculos entre essas duas diferentes áreas da Matemática. Além disso, pude aplicar alguns conceitos que aprendi durante o curso, aprender outros que eu não conhecia, ter meu primeiro contato com um orientador e com a confecção de uma monografia. Graças a essa experiência, sinto-me mais seguro para iniciar um curso de pós-graduação.

Referências Bibliográficas

[1] *BIRKHOFF, Garret, MAC LANE, Saunders.* ***A Survey of Modern Algebra****. 4.ed. New York: Macmillan, 1977. 500p.*

[2] *DOMINGUES, Hygino H., IEZZI, Gelson.* ***Álgebra Moderna****. 2.ed. São Paulo: Atual Editora, 1982. 263p.*

[3] *FALLAT, Shaun M. (1996).Algebraic Integers and Tensor Products of Matrices. In* ***Linear Algebra Gems: Assets for Undergraduate Mathematics****, Washington: The Mathematical Association of America, p.231-233, 2002.*

[4] *FIGUEIREDO, Djairo Guedes de.* ***Números Irracionais e Transcendentes****. 3.ed. Rio de Janeiro: Sociedade Brasileira de Matemática, 2002. 60p.*

[5] *GARCIA, Arnaldo, LEQUAIN, Yves.* ***Elementos de Álgebra****. 3.ed. Rio de Janeiro: IMPA, 2005. 326p.*

[6] *HERNSTEIN, I. N..* ***Tópicos de Álgebra****. 1.ed. São Paulo: Editora Polígono, 1970. 414p.*

[7] *LANG, Serge.* ***Álgebra Linear****. 3.ed. Rio de Janeiro: Editora Ciência Moderna, 2003. 405p.*

[8] *LAY, David C..* ***Álgebra Linear e Suas Aplicações****. 2.ed. Rio de Janeiro: Editora LTC, 1999. 504p.*

[9] *LEON, Steve J..* ***Álgebra Linear Com Aplicações****. 4.ed. Rio de Janeiro: Editora LTC, 1999. 390p.*

[10] *MACKIW, George.The Minimum Length of a Permutation as a Product of Transpositions. In* ***Linear Algebra Gems: Assets for Undergraduate Mathematics****, Washington: The Mathematical Association of America, p.255-257, 2002.*

[11] *ROTMAN, Joseph J..* ***An Introduction to the Theory of Groups****. 4.ed. New York: Springer-Verlag, 1990. 268p.*