2020: Trabalho de Conclusão de Curso do Mestrado Profissional em Matemática em Rede Nacional
Universidade Federal de São João del-Rei - UFSJ
Sociedade Brasileira de Matemática - SBM

Teorema de Kontsevich e os Intercâmbios Polinomiais

Adailton José da Silva[1]

Amanda Gonçalves Saraiva Ottoni[2]

José Eloy Ottoni[3]

Resumo: Depois de receber um bilhete de metrô de seu colega Maxim Kontsevich com alguns rabiscos, Étienne Gys mal pôde acreditar que este queria compartilhar com ele um novo teorema sobre posição relativa de polinômios. Este trabalho tem por objetivo apresentar o Teorema de Kontsevich, cujo resultado são algumas restrições para a posição relativa dos gráficos de quatro polinômios reais.

Palavras-chave:

Teorema de Kontsevich, Intercâmbios Polinomiais, Permutações Separáveis.

[1]Aluno de Mestrado Profissional em Matemática em Rede Nacional, Turma 2019

Instituição: Universidade Federal de São João Del-Rei - UFSJ

E-mail: ajsgalan@yahoo.com.br

[2]Orientadora do Trabalho de Conclusão de Curso

Departamento de Estatística, Física e Matemática - Defim, CAP-UFSJ

E-mail: amandagso@ufsj.edu.br

[3]Coorientador do Trabalho de Conclusão de Curso

Departamento de Estatística, Física e Matemática - Defim, CAP-UFSJ

E-mail: jeottoni@ufsj.edu.br

Sumário

.

1 Introdução

A Matemática sempre esteve em constante evolução. Esse desenvolvimento ocorre graças às pessoas que dedicam (dedicaram) suas vidas a investigar os fenômenos dessa área tão apaixonante.

Permutações e teoria de polinômios sempre foram temas de grande investigação e interesse acadêmico. Grandes matemáticos como Pascal, Fermat, Leibniz, Cardano, Gauss entre outros se dedicaram a essas áreas, desenvolvendo-as e deixando uma base sólida para que toda humanidade pudesse usufruir e seguir seus passos.

Esse trabalho tem a finalidade de compreender a relação entre as configurações dos gráficos de n polinômios que se intersectam na origem e as permutações de n elementos. Em particular, quando $n = 4$, essa relação é descrita pelo Teorema de Kontesevich. Os resultados do teorema de Kontsevich são essenciais para compreender o caso geral para n polinômios.

Como o tema central deste trabalho envolve permutação de polinômios, o capítulo 2 apresenta uma breve introdução a Grupo de Permutações. No capítulo 3 serão apresentados diversos resultados sobre polinômios, destacando-se o conceito de valuação e configurações de polinômios afins. O capítulo 4 enuncia e demonstra o Teorema de Kontsevich, além de apresentar as definições de intercâmbios polinomiais e permutações separáveis para, posteriormente, apresentar uma generalização do Teorema de Kontsevich. Com o intuito de divulgar o resultado do Teorema de Kontsevich para o ensino médio, o capítulo 5 finaliza este trabalho com uma proposta de atividade em sala de aula.

2 Grupo de Permutações

Nesta seção será estudado o conceito de permutações de um conjunto X. Apenas o caso em que X é finito será abordado, em especial quando $X = \{1, 2, 3, \ldots, n\}$, pois apenas as permutações deste conjunto serão utilizadas nos problemas propostos nesta dissertação.

A seção 2.1 apresenta uma maneira de se representar permutações por meio de matrizes. Já na seção 2.2, uma forma auxiliar bastante útil e sucinta será introduzida: a representação por ciclos. A seção 2.3 expõe algumas propriedades básicas do conjunto das permutações de n elementos. Finalmente, a seção 2.4 define e exemplifica os Grupos de Rotações e o Grupo Diedral.

Os resultados e definições apresentados nesta seção foram fundamentados nas referências

(Santos und Bovo, 2004), (Marques, 2019) e (Firmo und Ottoni, 2020).

O conceito de permutação será a base fundamental deste trabalho. Para todo número $n \in \mathbb{N}$ será utilizada a notação $[n]$ para indicar o conjunto finito $\{1, 2, 3, \ldots n\}$.

Definição 2.1. *Dado um número natural n, diz-se que um conjunto A tem n elementos, ou que A tem cardinalidade n, se podemos estabelecer uma bijeção entre A e o conjunto dos números $\{1, 2, \ldots, n\}$. Denota-se por $|A| = n$ ou $\#A = n$. Em vez de dizer que A tem **cardinalidade** n também se diz-se, com o mesmo sentido, que A tem ordem n.*

Definição 2.2. *Uma **permutação** f do conjunto X é uma função de X em X bijetiva, ou seja:*

$f : X \to X$: f bijetiva.

Seja $S(X)$ o conjunto de todas as permutações do conjunto X. Sendo X um conjunto finito, tal que $[X] = n$, dessa forma existem $n!$ permutações do conjunto X. Sendo n possibilidades para a primeira posição da sequência, $n - 1$ possibilidades para a segunda posição, $n - 2$ para a terceira posição, e assim por diante dependendo do valor de n. Logo, pelo princípio multiplicativo, existem $n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot 2 \cdot 1 = n! = [S(X)]$, permutações distintas. Como os principais casos estudados neste trabalho serão para $X = [n]$, denotaremos por S_n o conjunto das permutações $S(X)$.

Exemplo 2.3. *(Morgado und Carvalho, 2015) De quantos modos podemos ordenar em fila n objetos distintos? A escolha do objeto que ocupará o primeiro lugar pode ser feita de n modos; a escolha do objeto que ocupará o segundo lugar pode ser feita de $n - 1$ modos; a escolha do objeto que ocupará o terceiro lugar pode ser feita de $n-2$ modos, etc...; a escolha do objeto que ocupará o último lugar pode ser feita de 1 modo. Ou seja, $P_n = n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot 1 = n!$*

2.1 Representação Matricial de Permutações

A função bijetora $\sigma \in S_n$ e $i \in [n]$ definida por:

$$\begin{aligned} 1 &\mapsto \sigma(1) \\ 2 &\mapsto \sigma(2) \\ 3 &\mapsto \sigma(3) \\ &\vdots \\ n &\mapsto \sigma(n) \end{aligned}$$

a notação $\sigma(i)$ representa o valor da função bijetora σ no número i. Assim, a permutação σ, pode ser representada pelo diagrama:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n) \end{pmatrix}$$

A primeira linha exibe cada elemento do domínio e a segunda linha os elementos de suas respectivas imagens por σ. Dessa forma a identidade de S_n será a bijeção

$$e = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 1 & 2 & 3 & \cdots & n \end{pmatrix}$$

Exemplo 2.4. *O diagrama* $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 3 & 4 & 2 & 1 & 8 & 7 & 6 \end{pmatrix}$ *representa uma permutação de* S_8*, sendo o número* 7 *o único que não mudou de posição pois* $\sigma(7) = 7$.

2.2 Notação de Permutação por Ciclos

Para simplificar a representação de uma permutação, podemos utilizar uma notação por ciclos que será vista a seguir.

Definição 2.5. *Sejam os números inteiros distintos* $a_1, a_2, \ldots, a_r \in [n]$. *Se* $\alpha \in S_n$ *é uma permutação tal que:*

$$\alpha(a_1) = a_2$$

$$\alpha(a_2) = \alpha^2(a_1) = a_3$$

$$\vdots$$

$$\alpha(a_{r-1}) = \alpha^{r-1}(a_1) = a_r$$

$$\alpha(a_r) = \alpha^r(a_1) = a_1.$$

Então a permutação $\begin{pmatrix} a_1 & a_2 & a_3 & \ldots & a_r \\ a_2 & a_3 & a_4 & \ldots & a_1 \end{pmatrix}$ *chama-se* ***ciclo de comprimento*** r ***de*** α *e é denotada por* $(a_1, a_2, a_3, \ldots, a_r)$.

Proposição 2.6. *Se* $\alpha \in S_n$*, para todo* $j \in \{1, 2, \ldots, n\}$*, existe* $l_j \in \{1, 2, \ldots, n\}$ *tal que:*

$$\alpha^{l_j}(j) = \underbrace{(\alpha \circ (\alpha \circ (\ldots \circ \alpha(j)) \ldots)))}_{l_j \text{ vezes}} = j.$$

Demonstração. Se não existisse um l_j, então, depois de fazer n iterações, o valor resultante estaria fora do conjunto $[n]$, o que é um absurdo, já que α é uma bijeção definida em $[n]$. Portanto, há um ciclo de α de comprimento l_j determinado por $(j, \alpha(j), \alpha^2(j), \ldots, \alpha^{l_j-1}(j))$. □

Acompanhando a demonstração acima, no ciclo $(j, \alpha(j), \alpha^2(j), \ldots, \alpha^{l_j-1}(j))$ foram utilizados l_j elementos, restam outros $n-l_j$ elementos de $[n]$, dos quais há l_k elementos formando outro ciclo, disjunto do primeiro, de comprimento l_k determinado por $(k, \alpha(k), \alpha^2(k), \ldots, \alpha^{l_j-1}(k))$. Dessa forma, todos os elementos de $[n]$ serão utilizados. Sendo assim, obtemos por meio de ciclos disjuntos, uma representação da permutação de $[n]$. Para simplificar, dada uma permutação α, chama-se um ciclo de tamanho r de α, um r-ciclo. Chama-se de **ponto fixo** de α um r-ciclo com $r = 1$. Já para $r = 2$ diz-se que o r-ciclo é uma **transposição**.

Exemplo 2.7. *Temos* $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 5 & 2 & 3 & 6 \end{pmatrix} \in S_6$. *Pelo diagramas de setas temos:*

$$1 \to 4 \to 2 \to 1$$

$$3 \to 5$$

$$6 \to 6$$

Em notação de ciclos, α *pode ser escrito na forma* $\alpha = (1,4,2)(3,5)(6)$ *ou* $\alpha = (1,4,2)(3,5)$.

Exemplo 2.8. *Temos que* $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$ *denota a permutação* $\beta : \{1,2,3,4\} \to \{1,2,3,4\}$ *definida por* $\beta(1) = 3$, $\beta(2) = 4$, $\beta(3) = 2$ *e* $\beta(4) = 1$. *Em notação de ciclos,* β *pode ser escrito na forma* $\beta = (1,3,2,4)$.

2.3 Propriedades

Nesta seção serão apresentadas três propriedades do conjunto $S(X)$ que fornecerão a este conjunto uma estrutura algébrica bastante conhecida e que será definida na seção 2.4.

Seja X um conjunto não vazio. Em diversos resultados nessa seção, X será considerado o conjunto $[n]$.

Lema 2.9. *O conjunto* $S(X)$ *é fechado por composição de permutações, isto é, se* $\alpha_1, \alpha_2 \in S(X)$, *então* $\alpha_1\alpha_2 \in S(X)$.

Demonstração. Sejam $\alpha_1, \alpha_2 \in S(X)$. Para que $\alpha_1\alpha_2$ pertença a $S(X)$ deve-se ter que $\alpha_1\alpha_2$ é uma função bijetiva de X em X.

Injetividade: Considere $x, y \in X$, com $x \neq y$. Como α_2 é injetiva, tem-se que $\alpha_2(x) \neq \alpha_2(y)$. Como α_1 também é injetiva, então $\alpha_1(\alpha_2(x)) \neq \alpha_1(\alpha_2(y))$. Portanto, $\alpha_1\alpha_2$ é injetiva.

Sobrejetividade: Seja $z \in X$. Sabe-se que α_1 e α_2 são sobrejetivas. Logo, existe $y \in X$ com $\alpha_1(y) = z$. Além disso existe $x \in X$ com $\alpha_2(x) = y$. Assim, $\alpha_1(\alpha_2(x)) = z$, para todo $x \in X$. Portanto, $\alpha_1\alpha_2$ é sobrejetiva.

Como $\alpha_1\alpha_2$ é injetiva e sobrejetiva, então ela é bijetiva, logo conclui-se que $S(X)$ é fechado por composição de permutações. □

Lema 2.10. *A função $e : X \longrightarrow X$ denida por $e(x) = x$ para todo $x \in X$ é uma bijeção e funciona como o elemento neutro de $S(X)$, isto é, $\forall \alpha \in S(X)$ temos que $\alpha e = e\alpha = \alpha$. Além disso, dada qualquer permutação $\alpha \in S(X)$, existe uma permutação inversa $\alpha^{-1} \in S(X)$ tal que $\alpha\alpha^{-1} = \alpha^{-1}\alpha = e$.*

Demonstração. É imediato verificar que a função identidade e é uma permutação e que funciona como elemento neutro de $S(X)$. Como toda função bijetiva possui inversa, esta inversa também é bijetiva e, portanto, pertence a $S(X)$. □

Lema 2.11. *Dadas as permutações α_1, α_2 e α_3 em $S(X)$, tem-se que $\alpha_1(\alpha_2\alpha_3) = (\alpha_1\alpha_2)\alpha_3$.*

A demonstração do Lema 2.11 é imediata e, portanto, será omitida.

2.4 Grupo de Permutações

As propriedades descritas na seção anterior fazem com que o conjunto das permutações $S(X)$ tenha uma estrutura algébrica chamada grupo. Esta estrutura algébrica e alguns exemplos estão descritos brevemente nesta seção.

Definição 2.12. *Seja $*$ uma operação fechada no conjunto não vazio G, ou seja,*

$$\forall a, b \in G \Rightarrow a * b \in G.$$

*Dizemos que $(G, *)$ é um **grupo** quando satisfaz os seguintes axiomas:*

(i) $a * (b * c) = (a * b) * c$, $\forall a, b, c \in G$. *(Associatividade)*

(ii) Existe $e \in G$ tal que $a * e = e * a = a, \forall a \in G$. (Existência de elemento neutro)

(iii) Dado $a \in G$, existe $a' \in G$ tal que $a * a' = a' * a = e$. (Existência de simétrico)

Antes de apresentar exemplos de grupos as definições 2.13 e 2.14 definem uma função muito especial entre dois grupos.

Definição 2.13. *(Janesch, 2008) Sejam $(G, \cdot)$ e $(H, *)$ grupos. Um **homomorfismo** de G em H é uma função $f : G \to H$ que satisfaz*

$$f(ab) = f(a) * f(b), \ \forall \ a, b \in G.$$

Definição 2.14. *Um homomorfismo bijetor é chamado **isomorfismo**.*

Como consequência dos lemas 2.9, 2.10 e 2.11, descritos na seção anterior, o conjunto S(X) é um grupo com a operação de composição de funções, chamado de **grupo de permutações** de X. Este é resultado do Teorema 2.15 descrito abaixo.

Teorema 2.15. *Se X é um conjunto não-vazio, $(S(X), \circ)$ é um grupo.*

$(S(X), \circ)$ será denotado simplesmente por $S(X)$. Desde que a composição de bijeções é uma bijeção, temos que a composição é uma operação em $S(X)$.

Exemplo 2.16. *Como exemplos básicos, temos que os seguintes conjuntos, munidos com as respectivas operações, são grupos:*

$$(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +).$$

O elemento neutro de todos eles é $e = 0$.

Exemplo 2.17. *Todos os conjuntos do exemplo acima são fechados por multiplicação, tendo $e = 1$ como identidade. No entanto, apenas os elementos não-nulos dos conjuntos $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ possuem inversos. Assim temos mais três exemplos de grupos,*

$$(\mathbb{Q}^*, \times), (\mathbb{R}^*, \times), (\mathbb{C}^*, \times).$$

Definição 2.18. *O grupo $S(X)$ é chamado de grupo de permutações (ou grupo simétrico) do conjunto X.*

Quando X é um conjunto finito com n elementos, indicamos a notação $S(X)$ por S_n.

Se $X = 1, 2, \ldots, n$ denota-se $S(X)$ por S_n e este é chamado de grupo simétrico de grau n. A ordem de S_n é $n!$.

Existem diversos exemplos de grupos e subgrupos de simetria. Dois exemplos bastante conhecidos são o grupo de rotação e o grupo diedral. A subseção 2.4.1 defini e ilustra com mais detalhes estes dois grupos.

2.4.1 Grupos de Rotações

Esta subseção apresenta uma breve introdução aos Grupos de Rotações e, posteriormente, ao estudo do Grupo Diedral. O objetivo desta seção é apenas ilustrar com mais detalhes dois exemplos de grupos de simetria que possuem aplicações em diversas áreas. A teoria aqui descrita não possui relação direta com o tema deste trabalho, entretanto, por sua beleza ela ganho espaço nesta dissertação. Os resultados apresentados foram baseados em (Andretti, 2011).

Considere $\{1, 2, \ldots n\}$, o conjunto dos vértices de um polígono regular com n lados. Cada uma das rotações em relação a ângulo, $0, \frac{2\pi}{n}, 2\frac{2\pi}{n}, \ldots, (n-1)\frac{2\pi}{n}$, no sentido anti-horário, mantém o polígono invariante (move apenas os vértices) ver figura 1. Dessa forma, notamos do grupo simétrico $S_n = S(X)$, $X = \{1, 2, \ldots n\}$, que estas rotações podem ser identificadas com elementos distintos de S_n.

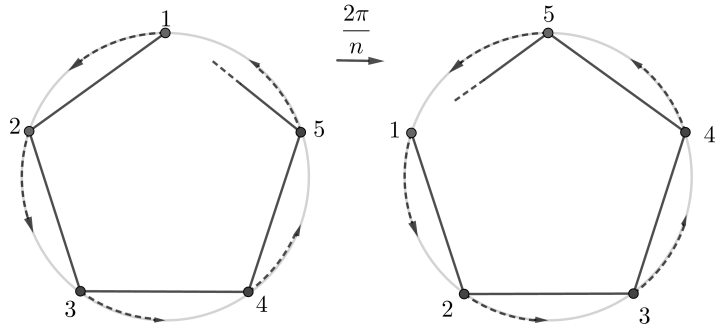

Figura 1: Rotação de polígono regular com n lados.

Sejam e a rotação de 0 radianos e a a rotação de $\frac{2\pi}{n}$ radianos. Estes elementos correspondem às seguintes funções de S_n:

$$e = \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ 1 & 2 & \cdots & n-1 & n \end{pmatrix} \text{ e } a = \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ 2 & 3 & \cdots & n & 1 \end{pmatrix}.$$

Usando a notação $a^j = a \circ a \circ \ldots \circ a$, j vezes, e a convenção $a^0 = id = e$, é fácil perceber que as potências de a produzem todas as rotações. De fato,

a^2 é a rotação de ângulo $2\frac{2\pi}{n}$.

$\vdots$

a^{n-1} é a rotação de ângulo $(n-1)\frac{2\pi}{n}$.

$a_n = a_0 = e$ é a rotação de ângulo 0.

Denomina-se R_n **o conjunto das rotações do polígono regular de** n **lados**, isto é,

$$R_n = \{e = a^0, a, a^2, \ldots, a^{n-1}\} \subseteq S_n.$$

Note que, dados $a^i, a^j \in R_n$, vale $a^i \circ a^j = a^{i+j}$. Dividindo $i + j$ por n obtemos $q, r \in \mathbb{N}$ tais que $i + j = nq + r$, com $0 \leq r < n$. Assim,

$$a^i \circ a^j = a^{i+j} = a^{nq+r} = (a^n)^q \circ a^r = e^q \circ a^r = e \circ a^r = a^r \in R_n.$$

Portanto,

$$\begin{array}{rccc} \circ: & R_n \times R_n & \longrightarrow & R_n \\ & (a^i, a^j) & \longmapsto & a^{i+j} \end{array}$$

é uma operação em R_n.

Definição 2.19. *(Hefez, 2002) Os grupos nos quais dois elementos quaisquer comutam são chamados* ***abelianos****.*

Proposição 2.20. $(R_n, \circ)$ *é grupo abeliano com* n *elementos.*

Demonstração. Como os elementos de R_n são rotações de $\dfrac{2\pi}{n}k$, com $0 \leq k < n$, temos que R_n tem exatamente n elementos. Vamos verificar que $(R_n, \circ)$ é grupo abeliano.

Associatividade.

$$a^i \circ (a^j \circ a^k) = a^i \circ a^{j+k} = a^{i+(j+k)} = a^{i+j} \circ a^k = (a^i \circ a^j) \circ a^k.$$

É fácil perceber que $a_0 = e$ é o elemento neutro de R_n. Todo elemento tem simétrico.

$$a^i \circ a^{n-i} = a^n = a^0 = e, \ \forall i \in R_n.$$

Logo, o simétrico de $a^i \in R_n$ é $a^{n-i} \in R_n$.

Comutatividade.

$$a^i \circ a^j = a^{i+j} = a^{j+i} = a^j \circ a^j.$$

Portanto, $(R_n, \circ)$ é um grupo abeliano. □

Definição 2.21. *O grupo* $(R_n, \circ)$ *é chamado grupo de rotações de um polígono regular de* n *lados.*

Exemplo 2.22. *O grupo* $R_3 = \{e, a, a^2\}$ *é o grupo de rotações do triângulo equilátero de vértices* 1, 2 *e* 3. *O elemento neutro é* $e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$, $a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ *é a rotação de* $\frac{2\pi}{3}$, *e o elemento* $a^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ *é a rotação de* $\frac{4\pi}{3}$, *ver figura 2.*

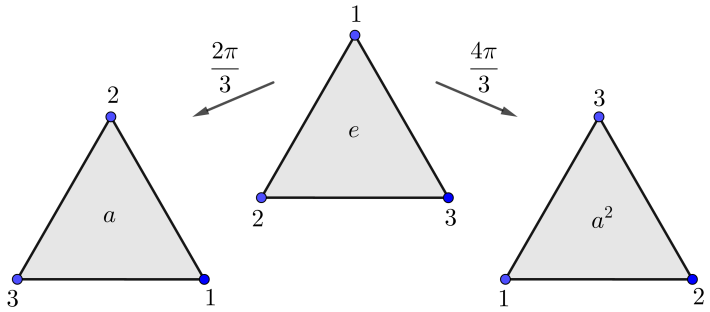

Figura 2: Representação do grupo R_3.

Exemplo 2.23. *O grupo* $R_4 = \{e, a, a^2, a^3\}$ *é o grupo de rotações do quadrado de vértices* 1, 2, 3 *e* 4. *O elemento neutro é* $e = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$, *o elemento* $a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ *é a rotação de* $\frac{\pi}{2}$, *e o elemento* $a^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$ *é a rotação de* π *e o elemento* $a^3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$ *é a rotação de* $\frac{3\pi}{2}$, *ver figura 3.*

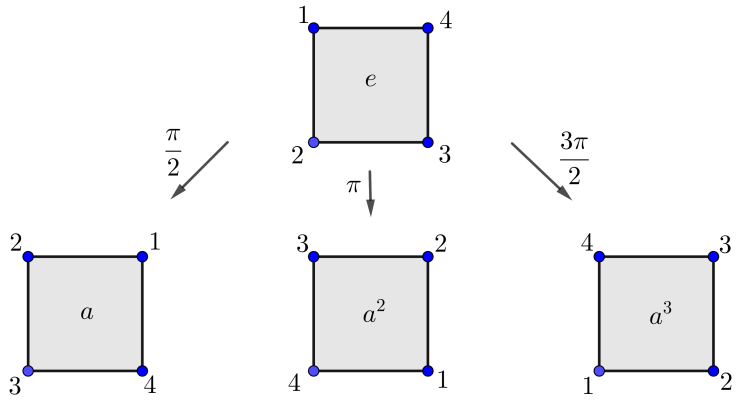

Figura 3: Representação do grupo R_4.

Além das rotações, existem outras transformações que levam um polígono regular nele mesmo. Essas transformações serão definidas e estudadas a seguir.

2.4.2 Grupo Diedral

Um grupo diedral é o grupo de simetrias de um polígono regular de n lados, veja (Andretti, 2011). Com o objetivo de enriquecer este trabalho e finalizar o capítulo 2 de forma elegante e interessante, esta seção exibe algumas definições e exemplos do grupo diedral.

Considere o conjunto $\{1, 2, \ldots, n\}$, $n \geq 3$, dos vértices de um polígono regular de n lados. Seja $b \in S_n$ a reflexão em relação ao eixo que passa pelo vértice 1 e pelo centro da circunferência em que o polígono está inscrito.

Note que $b = \begin{pmatrix} 1 & 2 & 3 & \ldots & n-1 & n \\ 1 & n & n-1 & \ldots & 3 & 2 \end{pmatrix}$ não é uma rotação, e que $b^2 = \begin{pmatrix} 1 & 2 & \ldots & n \\ 1 & 2 & \ldots & n \end{pmatrix}$.

Veja que o conjunto das rotações é $R_n = \{e, a, a^2, \ldots, a^{n-1}\}$, onde $a = \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ 2 & 3 & \cdots & n & 1 \end{pmatrix}$.

Ao conjunto R_n, vamos acrescentar a reflexão b e também todos as composições $a^i b$ tal que $i \in \{1, 2, \ldots, n-1\}$, obtendo o seguinte conjunto:

$$D_n = \{e, a, a^2, \ldots, a^{n-1}, b, ab, a^2b, \ldots, a^{n-1}b\} \subseteq S_n,$$

que tem $2n$ elementos. Cada um destes elementos representa uma simetria do polígono, isto é, um movimento que deixa o polígono invariante (move apenas os vértices). Na verdade, D_n é conjunto de todas as simetrias de um polígono de n lados.

D_n é um grupo com a operação de composição, chamado de *Grupo Diedral*. Para demonstrar que D_n é um grupo, inicialmente será mostrado que

$$\begin{aligned} \circ : \ D_n \times D_n &\longrightarrow D_n \\ (a^i b, a^j b) &\longmapsto a^i b \circ a^j b \end{aligned}$$

é uma operação em D_n, ou seja, $a^i b \circ a^j b \in D_n, \forall i, j \in \{0, 1, \cdots, n-1\}$. Para isso, considere o lema a seguir.

Lema 2.24. *Em D_n, vale a igualdade $ba^r = a^{n-r}b, \forall\ r \in \{1, 2, \ldots, n-1\}$.*

Demonstração. Vamos provar este fato utilizando o Princípio de Indução sobre r.

(i) Para r = 1:

$$ba = \begin{pmatrix} 1 & 2 & 3 & \ldots & n-1 & n \\ 1 & n & n-1 & \ldots & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & \ldots & n-1 & n \\ 2 & 3 & 4 & \ldots & n & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & \ldots & n-1 & n \\ n & n-1 & n-2 & \ldots & 2 & 1 \end{pmatrix}.$$

(ii) Para calcular $a^{n-1}b$, note que

$$a^{n-1} = a^n \circ a^{-1} = e \circ a^{-1} = a^{-1}.$$

Assim, $a^{n-1} = a^{-1}$ corresponde à rotação de $\dfrac{2\pi}{n}$ no sentido horário.

$$a^{-1}b = \begin{pmatrix} 1 & 2 & 3 & \dots & n-1 & n \\ n & 1 & 2 & \dots & n-2 & n-1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & \dots & n-1 & n \\ 1 & n & n-1 & \dots & 3 & 2 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & \dots & n-1 & n \\ n & n-1 & n-2 & \dots & 2 & 1 \end{pmatrix}.$$

De (i) e (ii) segue que $ba = a^{n-1}b$.

Suponha que $ba^k = a^{n-k}b$, para $k > 1$. Deseja-se mostrar que $ba^{k+1} = a^{n-(k+1)}b$. É possivel observar que

$$ba^{k+1} = a^{n-k}ba.$$

Como mostrado acima, $ba = a^{n-1}b$, logo

$$ba^{k+1} = a^{n-k}a^{n-1}b = a^n a^{n-(k+1)}b = ea^{n-(k+1)}b = a^{n-(k+1)}b.$$

□

Proposição 2.25. *A composição é uma operação em D_n.*

Demonstração. Deseja-se provar que se $a^ib, a^jb \in D_n$, então $a^ib^ua^jb^v \in D_n$, para $i, j \in \{0, 1, \dots, n-1\}$ e $u, v \in \{0, 1\}$.

(i) $u = 0$:

$$a^ib^ua^jb^v = a^iea^jb^v = a^{i+j}b^v \in D_n$$

.

Lembrando que $a^{i+j} \in \{e, a, a^2, \dots, a^{n-1}\}$ para quaisquer i e j.

(ii) $u = 1$:

$$a^ib^ua^jb^v = a^iba^jb^v = a^ia^{n-j}bb^v = a^{i+j}b^{v+1} \in D_n.$$

Lembrando que $b^2 = e$ e, portanto, qualquer potência de b pode ser reduzida a e ou b.

□

Proposição 2.26. *$(D_n, \circ)$ é grupo não abeliano, com $2n$ elementos.*

Demonstração. • Associatividade.

Como $D_n \subseteq S_n$, a associatividade em D_n é consequência da associatividade em S_n.

- e é o elemento neutro de D_n.

- Todo elemento tem simétrico.

  Para provar que $a^i b^u \in D_n$ tem inverso em D_n, separamos em dois casos.

  (i) $u = 0$:

  Neste caso, $a^i b^u = a^i$, e seu inverso é $a^{n-i} \in D_n$.

  (ii) $u = 1$:

  Neste caso, $a^i b^u = a^i b$ cujo inverso é o próprio $a^i b \in D_n$, pois

$$a^i b a^i b = a^i a^{n-i} bb = a^n b^2 = ee = e.$$

- É um grupo não comutativo.

  Basta notar que, pelo lema 2.24, $ba = a^{n-1}b \neq ab$.

  Portanto, $(D_n, \circ)$ é grupo não abeliano.

- Falta verificar que D_n tem exatamente $2n$ elementos. Para isso vamos mostrar que os elementos do conjunto $\{e, a, a^2, \ldots, a_{n-1}, b, ab, a^2b, \ldots, a^{n-1}b\}$ são distintos dois a dois.

  Sejam $i, j \in \{0, 1, 2, \ldots, n-1\}$ e $u, v \in \{0, 1\}$ tais que $a^i b^u = a^j b^v$.

  Devemos verificar que i = j e u = v:
  Multiplicando à esquerda por $(a^j)^{-1}$ e à direita por $(b^u)^{-1}$ ficamos com

$$a^i b^u = a^j b^v \Rightarrow (a^j)^{-1} a^i = b^v (b^u)^{-1} = b^{-u+v} \in \{e, a, \ldots, a^{n-1}\},$$

  pois $(a^j)^{-1} a^i$ é uma rotação.

  Se $u \neq v$ então $b^{-u+v} \notin \{e, a, \ldots, a^{n-1}\}$. Absurdo.

  Logo, $u = v$ e a igualdade $a^i b^u = a^j b^v$ leva a $a^i = a^j$, e daí $i = j$.

  Portanto, D_n tem $2n$ elementos.

□

Definição 2.27. *O grupo $(D_n, \circ)$ é chamado* ***grupo diedral de ordem*** $2n$*, ou* ***grupo das simetrias do polígono regular de*** n ***lados****.*

Exemplo 2.28. *$D_3 = \{e, a, a^2, b, ab, a^2b\}$ é o grupo das simetrias do triângulo equilátero de vértices 1, 2 e 3, onde $a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ é a rotação de ângulo $\frac{2\pi}{3}$ e $b = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ é a reflexão em relação ao eixo horizontal e a mediatriz que passa pelo vértice 1, ver figura 4.*

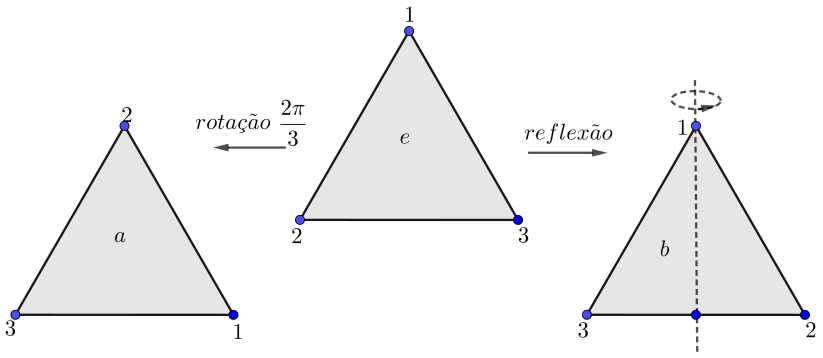

Figura 4: Rotação e reflexão dos vértices do triângulo equilátero.

Exemplo 2.29. *D_4 é o grupo das simetrias do quadrado. Um quadrado desenhado no plano possui 8 simetrias: a identidade, 3 rotações de ângulos $\frac{\pi}{2}, \pi, \frac{3\pi}{2}, 2$ reflexões através de suas mediatrizes e 2 reflexões através de suas diagonais.*

Veremos a seguir um exemplo de Grupo Diedral, destacaremos o grupo de simetrias do triângulo equilátero, ver (Cançado, 2016).

Exemplo 2.30. *Seja D_3 o conjunto de simetrias do triângulo equilátero de vértices $1, 2$ e 3. (Figura 5).*

(i) Transformações Planas:

Denotadas por e, r_1 e r_2, as rotações de 0, $\frac{2\pi}{3}$ e $\frac{4\pi}{3}$ radianos em torno do centro O, no sentido anti-horário. Representadas pelas permutações:
$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$, $r_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ e $r_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$.

(ii) Transformações Espaciais:

Denotadas por s_1, s_2 e s_3, as reflexões espaciais de π radianos em torno das retas t_1, t_2 e t_3. Representadas pelas seguintes permutações:
$s_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$, $s_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ e $s_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$.

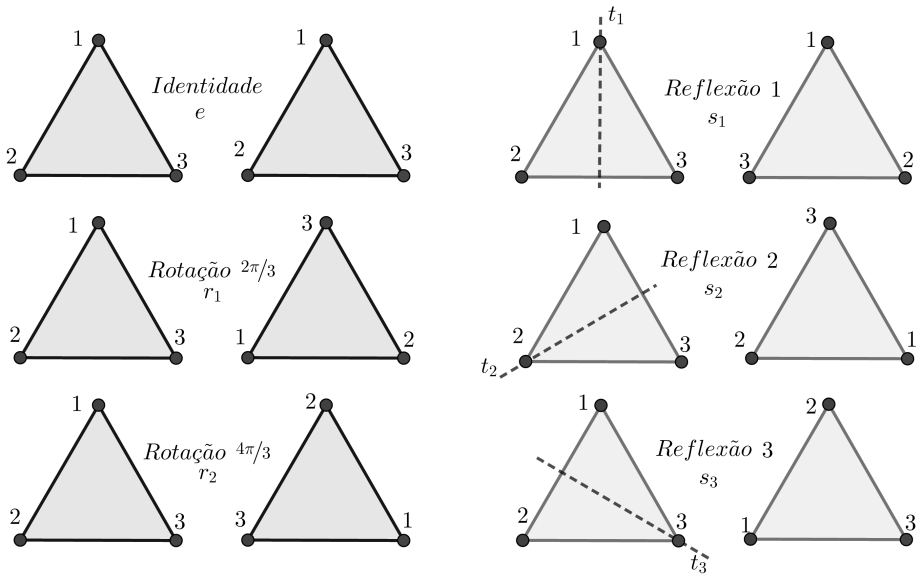

Figura 5: Simetrias em D_3

Segue que $D_3 = \{e, r_1, r_2, s_1, s_2, s_3\} = \{e, r_1, r_1^2, s, s \circ r_1, s \circ r_1^2\}$. *Em seguida, faremos a construção da tábua de* D_3. *Temos que:*

$$r_1 \circ s_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = s_2;$$

$$s_1 \circ s_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = r_2.$$

Realizando-se todas as possíveis composições, temos a seguinte tábua:

$\circ$	e	r_1	r_2	s_1	s_2	s_3
e	e	r_1	r_2	s_1	s_2	s_3
r_1	r_1	r_2	e	s_2	s_3	s_1
r_2	r_2	e	r_1	s_3	s_1	s_2
s_1	s_1	s_3	s_2	e	r_2	r_1
s_2	s_2	s_1	s_3	r_1	e	r_2
s_3	s_3	s_2	s_1	r_2	r_1	e

Podemos observar que $(D_3, \circ)$ *é grupo (não abeliano). Através da tábua, verificamos a existência do elemento neutro* $e = r_0$ *e dos inversos de* $r_1^{-1} = r_2, s_1^{-1} = s_1, s_2^{-1} = s_2, s_3^{-1} = s_3, r_2^{-1} = r_1$. *Além disso, vale a associatividade por se tratar da composição*

de aplicações. Contudo, não vale a comutatividade, pois $s_3 \circ s_1 \neq s_1 \circ s_3$. *Como já havíamos demonstrado anteriormente.*

Observação 2.31. $D_3 = S_3 = 3! = 6$ *elementos, que corresponde a ordem de* D_3.

Exemplo 2.32. *Os grupos* S_3 *e* D_3 *são isormorfos. Podemos observar a seguir que, de fato, existe uma bijeção* f *de* S_3 *em* D_3*:*

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \quad e \longmapsto e$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \quad r_1 \longmapsto r_1$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \quad r_1^2 \longmapsto r_2$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \quad s \longmapsto s_1$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \quad s \circ r_1 \longmapsto s_2$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \quad s \circ r_1^2 \longmapsto s_3$$

Agora, verificaremos se f *é homomorfismo. Para isso, tomaremos* $s_1, r_1 \in D_3$. *Mostremos que* $f(s_1 \circ r_1) = f(s_1) \circ f(r_1)$.

Segue que $f(s_1 \circ r_1) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = s_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = f(s_1) \circ f(r_1)$.

Procedimentos análogos podem ser aplicados aos demais elementos de D_3. *Portanto, temos um isomorfismo.*

3 Polinômios

O objetivo deste capítulo é apresentar algumas definições e resultados básicos a respeito da teoria de polinômios. Alguns desses resultados serão necessários para o desenvolvimento do conteúdo exposto no capítulo 4 deste trabalho.

Será exibida a definição de polinômio, seu grau e sua valuação, entre outros conceitos. Alguns resultados do capítulo 2 serão utilizados para a descrição das configurações dos gráficos de polinômios afins, próximos da origem. Os resultados, definições e exemplos apresentados neste capítulo foram baseados essencialmente nas referências (Vieira, 2011), (Ghys, 2017) e (Coelho, 2019).

3.1 Definições e Operações

Nesta seção, serão apresentadas algumas definições, propriedades e exemplos sobre polinômios até alcançar famoso Algoritmo da Divisão de Euclides.

Definição 3.1. *Seja F um corpo, **um polinômio na variável x sobre F** é uma expressão da forma:*

$$p(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$$

onde $a_i \in F$ para qualquer $i = 1, \ldots, n$ e $n \in \mathbb{N}$.

O conjunto de todos os polinômios na variável x com coeficientes em um corpo F é denotado por $F[x]$. O conjunto $F[x]$ é um anel, chamado de anel de polinômios na variável x sobre F, veja Hefez (2002). Os elementos $a_i \in F$ são chamados de coeficientes do polinômio p.

Definição 3.2. *Dizemos que dois polinômios $p(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ e $g(x) = b_n x^n + b_{n-1}x^{n-1} + \ldots + b_1 x + b_0$ sobre F são **iguais** se, e somente se, $a_i = b_i$ em F, $\forall i \in \mathbb{N}$.*

Uma função $p : \mathbb{R} \to \mathbb{R}$ é chamada de função polinomial, se existirem $a_0, a_1, \ldots, a_n \in \mathbb{R}$ tais que $p(x) = a_0 + a_1 x + \ldots + a_n x^n$, para todo $x \in \mathbb{R}$.

A correspondência que associa a cada polinômio $P(X)$, uma função polinomial $p(x)$, isto é, $P(X) = a_0 + a_1 X + \ldots + a_n X^n \longmapsto p(x) = a_0 + a_1 x + \ldots + a_n x^n$ é uma função sobrejetiva por definição e injetiva (logo bijetiva) porque funções polinomiais são iguais se, e somente se possuem os mesmos coeficientes, portanto os polinômios no domínio serão iguais. Por este

motivo, não será feita distinção entre o polinômio $P(X)$ e a função polinomial $p(x)$, neste texto.

A notação $p(x)$ será utilizada para representar o polinômio p, como um elemento do anel $F[x]$, bem como (por abuso de notação) para representar a imagem da função polinomial $p(x)$, pertencente ao corpo F.

Exemplo 3.3. *Sabendo que os polinômios* $p(x) = ax^4 + 3x^3 - 2ix^2 + 4(b-2)x + 5$ *e* $q(x) = -3x^4 + (c-1)x^3 + dx^2 - x + 5$ *são iguais em* $\mathbb{C}$*, determine os valores de a, b, c e d.*
Pela Definição 3.2, se os polinômios são idênticos devemos ter:

$$a = -3,\ c - 1 = 3,\ d = -2i \text{ e } b - 2 = -1$$

ou seja,

$$a = -3,\ b = 1,\ c = 4 \text{ e } d = -2i.$$

Observações:

1. Se $p(x) = 0x^n + 0x^{n-1} + \ldots + 0x + 0$, indicaremos $p(x)$ por 0 e o chamamos de **polinômio identicamente nulo sobre** F. Assim, um polinômio $p(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ sobre F é identicamente nulo se, e somente se, $a_i = 0 \in F, \forall i \in \mathbb{N}$.

2. Se $a \in F$, indicaremos por a ao polinômio $p(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ onde $a_0 = a$, e $a_i = 0, \forall i \geq 1$. Chamamos ao polinômio $p(x) = a$, de **polinômio constante** igual a a.

3. Se $p(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ é tal que $a_n \neq 0$, dizemos que n é o grau do polinômio $p(x)$. Vamos usar a notação $\partial p(x)$ para denotar o **grau do polinômio** $p(x)$.

4. O grau do polinômio 0 não está definido e ∂ pode ser interpretada como uma função do conjunto de todos os polinômios diferentes de zero no conjunto $\mathbb{N}$. Assim,

$$\begin{aligned} \partial : F[x] - 0 &\longrightarrow \mathbb{N} \\ p(x) &\longrightarrow \partial p(x) = \textit{grau de } p(x) \end{aligned}$$

Proposição 3.4. *Se* $p(x)$ *e* $g(x)$ *são polinômios não-nulos em* $F[x]$*, então o produto* $p(x)g(x)$ *é não-nulo e*

$$\partial(p(x)g(x)) = \partial(p(x) + \partial(g(x))$$

.

Demonstração. Considerando $p(x) = a_n x^n + \ldots + a_1 x + a_0$ e $g(x) = b_m x^m + \ldots + b_1 x + b_0$ de graus n e m respectivamente, temos $a_n \neq 0$ e $b_m \neq 0$. Assim, ao fazer o produto, obtemos o coeficiente de $x^{n+m} = a_n b_m \neq 0$.

Portanto, $p(x)g(x) \neq 0$. Por outro lado, o coeficiente de x^k no produto $p(x)g(x)$ é

$$a_0 b_k + a_1 b_{k-1} + \ldots + a_{k-1} b_1 + a_k b_0,$$

e assim, para $k > n + m$, temos que este coeficiente é nulo, pois $a_i = 0$, para $i > n$ e $b_j = 0$, para $j > m$.

Logo, $\partial(p(x)g(x)) = n + m$. □

Exemplo 3.5. *O polinômio $p(x) = 3x^4 - x^3 + 5x^2 - 2$ tem coeficientes racionais com $a_4 = 3, a_3 = -1, a_2 = 5, a_1 = 0$ e $a_0 = -2$, ou seja, $p(x) \in \mathbb{Q}[x]$. Podemos dizer que $p(x) \in \mathbb{R}[x]$ ou $p(x) \in \mathbb{C}[x]$, pois $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.*

Exemplo 3.6. *O polinômio $q(x) = (-3 + i)x^3 + (-7 + 11i)x + 4$ tem coeficientes complexos com $a_3 = -3 + i, a_2 = 0, a_1 = -7 + 11i$ e $a_0 = 4$, ou seja, $q(x) \in \mathbb{C}[x]$.*
É claro que $q(x) \notin \mathbb{R}[x]$, pois $a_3, a_1 \notin \mathbb{R}$.

Pode-se definir as operações de soma e produto no conjunto $F[x]$ da seguinte maneira: considere dois elementos do conjunto $F[x]$, $p(x) = a_n x^n + \ldots + a_1 x + a_0$ e $g(x) = b_r x^r + \ldots + b_1 x + b_0$, então $p(x) + g(x) = c_k x^k + \cdots + c_0$, em que $c_i = (a_i + b_i) \in F$, e $p(x) \cdot g(x) = d_k x^k + \cdots + d_0$, em que $d_0 = a_0 b_0$, $d_1 = a_0 b_1 + a_1 b_0$, $d_2 = a_0 b_2 + a_1 b_1 + a_2 b_0, \ldots,$ $d_k = a_0 b_k + a_1 b_{k-1} + \ldots + a_{k-1} b_1 + a_k b_0$.

A arimética de $F[x]$ é semelhante à de $\mathbb{Z}$, pois os conjuntos são fechados em relação às operações de soma e de multiplicação. Além disso, ambos não possuem inverso multiplicativo.

Pode-se observar, ainda, que a definição de produto de polinômios justifica-se pela propriedade $x^n \cdot x^r = x^{n+r}$ e pela propriedade distributiva dos números reais. Por convenção, as seguintes notações são utilizadas: $x^0 = 1$ e $x^1 = x$.

Pode-se verificar em (Garcia und Lequain, 2003), que $(F[x], +, \cdot)$ é um domínio de integridade em que o polinômio 0 é o elemento neutro de $F[x]$ e o polinômio constante 1 é sua unidade.

Da função $\partial p(x)$, tem-se as seguintes propriedades:

(i) $\partial(p(x) + g(x)) \leq max\{\partial p(x), \partial g(x)\}$, quaisquer que sejam os polinômios não nulos $p(x), g(x) \in F[x]$ tais que $p(x) + g(x) \neq 0$.

(ii) $\partial(p(x)\cdot g(x)) = \partial p(x)+\partial g(x)$, quaisquer que sejam os polinômios não nulos $p(x), g(x) \in F[x]$.

O inverso multiplicativo de um polinômio $p(x)$ em $F[x]$ é um polinômio $g(x) \in F[x]$ tal que $p(x)g(x) = 1$.

Exemplo 3.7. *O polinômio* $p(x) = 2x^6 - x^5 + x^4 - x^3 + 5x^2 + 7x$ *é um polinômio de grau 6 e denotamos o grau de p como* $\partial(p) = 6$.

Exemplo 3.8. *O polinômio* $g(x) = -\frac{2}{3}$, *é um polinômio de grau* 0, *pois temos* $g(x) = -\frac{2}{3}x^0$ *denotamos o grau de g como* $\partial(g) = 0$.

Exemplo 3.9. *(Iezzi u. a., 2002) Sendo* $p(x) = 4x^3 - x^2 + 5x - 6$ *e* $q(x) = -4x^2 + 3x + 2$, *vamos determinar o polinômio correspondente a:*

(a) $p(x) + q(x)$

Para isso, basta reduzir termos semelhantes, isto é, operar separadamente com potências de mesmo grau:

$$\begin{aligned} p(x) + q(x) &= (4x^3 - x^2 + 5x - 6) + (-4x^2 + 3x + 2) \\ &= 4x^3 - 5x^2 + 8x - 4 \end{aligned}$$

(b) $p(x) - q(x)$

Realizando o mesmo procedimento da adição, temos:

$$\begin{aligned} p(x) - q(x) &= (4x^3 - x^2 + 5x - 6) - (-4x^2 + 3x + 2) \\ &= 4x^3 + 3x^2 + 2x - 8 \end{aligned}$$

(c) $p(x) \cdot q(x)$

Basta aplicar a propriedade distributiva, lembrando as propriedades de potenciação:

$$\begin{aligned} p(x) \cdot q(x) &= (4x^3 - x^2 + 5x - 6) \cdot (-4x^2 + 3x + 2) \\ &= -16x^5 + 12x^4 + 8x^3 + 4x^4 - 3x^3 - 2x^2 - 20x^3 + 15x^2 + 10x \\ &\quad + 24x^2 - 18x - 12 \\ &= 16x^5 + 16x^4 - 15x^3 + 37x^2 - 8x - 12 \end{aligned}$$

Para efetuar a divisão entre dois polinômios, utiliza-se o Algoritmo da Divisão de Euclides. Neste procedimento, temos uma analogia entre a divisão de polinômios e a divisão de números inteiros: no caso de números inteiros, o processo de divisão é finalizado quando o resto for menor que o divisor; já no caso de polinômios, a finalização da divisão acontece quando o grau do polinômio do resto for menor do que o grau do polinômio do divisor.

Teorema 3.10 (Algoritmo da Divisão de Euclides)**.** *Sejam* $p(x), g(x) \in F[x]$ *e* $g(x) \neq 0$*, então existem únicos* $q(x), r(x) \in F[x]$ *tais que* $p(x) = q(x) \cdot g(x) + r(x)$*, em que* $r(x) = 0$ *ou* $\partial r(x) < \partial g(x)$*.*

Demonstração. (Gonçalves, 1979) Sejam $p(x) = a_0 + a_1x + \ldots + a_nx^n$ e $g(x) = b_0 + b_1x + \ldots + b_mx^m$.

Existência:

Se $p(x) = 0$, basta tomar $q(x) = r(x) = 0$. Suponha $p(x) \neq 0$ e que o grau de p vale n. Se $n < m$, basta tomar $q(x) = 0$ e $r(x) = p(x)$. Se $n \geq m$, seja $p_1(x)$ o polinômio definido por

$$p(x) = \frac{a_n}{b_m}x^{n-m} \cdot g(x) + p_1(x).$$

É fácil percebermos que $\partial p_1 < \partial p$: Vamos demonstrar o teorema por indução sobre o grau $\partial p(x) = n$.

Primeiramente, devemos mostrar que o resultado é verdadeiro para $n = 0$. Nesse caso $\partial p(x) \geq \partial g(x)$ temos $\partial g(x) = 0$ e, portanto, $p(x) = a_0 \neq 0$, $g(x) = b_0 \neq 0$. Dessa forma $a_0 = \frac{a_0}{b_0}b_0 + 0$, isto é $p(x) = \frac{a_0}{b_0}g(x)$ e basta tomar $q(x) = \frac{a_0}{b_0}$ e $r(x) = 0$, o que mostra que a divisão de $p(x)$ por $g(x)$ é possível.

Pela igualdade

$$p_1(x) = p(x) - \frac{a_n}{b_m}x^{n-m}g(x)$$

Considerando $n \geq 1$ e $\partial p_1(x) < \partial p(x)$ temos pela hipótese de indução que: existem $q_1(x), r_1(x)$ tais que:

$$p_1(x) = q_1(x) \cdot g(x) + r_1(x)$$

onde $r_1(x) = 0$ ou $\partial r_1(x) < \partial g(x)$. Daí segue imediatamente que:

$$p(x) = \left(q_1(x) + \frac{a_n}{b_m}x^{n-m}\right) g(x) + r_1(x)$$

e, portanto, tomando $q(x) = q_1(x) + \frac{a_n}{b_m}x^{n-m}$ e $r_1(x) = r(x)$ provamos a existência dos polinômios $q(x)$ e $r(x)$ tais que $p(x) = q(x) \cdot g(x) + r(x)$, e $r(x) = 0$ ou $\partial r(x) < \partial g(x)$.

Unicidade:

Sejam $q_1(x), q_2(x), r_1(x)$ e $r_2(x)$ tais que: $p(x) = q_1(x) \cdot g(x) + r_1(x) = q_2(x) \cdot g(x) + r_2(x)$ onde $r_i(x) = 0$ ou $\partial r_i(x) < \partial g(x),\ i = 1, 2$. Daí segue:

$$(q_1(x) - q_2(x)) \cdot g(x) = r_2(x) - r_1(x).$$

Mas se $q_1(x) \neq q_2(x)$ o grau do polinômio do lado esquerdo da igualdade acima é maior ou igual a $\partial g(x)$, enquanto que o grau $\partial(r_2(x) - r_1(x)) < \partial g(x)$, o que é uma contradição. Logo, $q_1(x) = q_2(x)$ e daí segue $r_1(x) = p(x) - q_1(x)g(x) = p(x) - q_2(x)g(x) = r_2(x)$, verificando o resultado. □

Claramente a demonstração do Teorema de Euclides fornece um método construtivo para a realização da divisão de um polinômio por outro, e só será válida para polinômios com coeficientes em um corpo, pois os inversos dos coeficientes são utilizados nos cálculos do algoritmo da divisão de polinômios.

Vamos resolver um exemplo que descreve o algoritmo da divisão de polinômios de Euclides para um caso particular.

Exemplo 3.11. *Mostre que o polinômio* $p(x) = 2x^4 - 6x^2 + 2x - 4$ *é divisível por* $d(x) = x^3 - 2x^2 + x - 1$ *em* $\mathbb{R}[x]$.

Sejam $n = \partial(p(x)) = 4$, $m = \partial(d(x)) = 3$, $a_n = 2$ *e* $b_m = 1$. *Dai,* $\frac{a_n}{b_m}x^{n-m} = 2x$, $\frac{a_n}{b_m}x^{n-m}d(x) = 2x^4+4x^3-2x^2+2x$ *e, portanto,* $h(x) = p(x)-\frac{a_n}{b_m}x^{n-m}d(x) = 4x^3-8x^2+4x-4$. *Continuando o processo das divisões sucessivas, até que tenhamos o grau de h(x) menor que o grau de* $d(x)$, *obtemos quociente* $q(x) = 2x + 4$ *e o* $r(x) = 0$. *Como nesse caso o resto* $r(x) = 0$, *concluímos que* $p(x)$ *é divisível por* $d(x)$.

3.2 Raízes

Encontrar as raízes de um polinômio é de grande utilidade para a decomposição deste em produto de polinômios de graus menores, bem como para a construção do seu gráfico, haja visto que a raízes correspondem aos pontos onde a função intersecta o eixo das abscissas.

Definição 3.12. *Se* $p(x) = a_0 + a_1x + \ldots + a_nx^n$ *é um polinômio não nulo em* $F(x)$ *e* $\alpha \in F$ *é tal que* $p(\alpha) = a_0 + a_1\alpha + \ldots + a_n\alpha^n = 0$, *dizemos que* α *é uma* ***raiz*** *de* $p(x)$ *em* F.

No Algoritmo da Divisão de Euclides, se $\partial q(x) = 1$, então $\partial(r) < 1$, ou seja, $\partial(r) = 0$, logo o resto r é uma constante ou $r = 0$.

Teorema 3.13. *[Teorema do resto] Se* F *é um corpo,* $a \in F$ *e* $p(x) \in F[x]$, *então* $p(a)$ *é o resto da divisão de* $p(x)$ *por* $x - a$.

Demonstração. Se o quociente e o resto da divisão de $p(x)$ por $x - a$ em $F[x]$ são, respectivamente, $q(x)$ e $r(x)$, então:

$$p(x) = (x - a) \cdot q(x) + r(x).$$

em que $\partial(r) < \partial(x - a) = 1$ ou $r = 0$, pelo Teorema 3.10. Substituindo-se a variável x por a na equação acima, obtêm-se $p(a) = (a - a) \cdot q(a) + r(a) = r(a)$: e, como r é um polinômio constante, então $r(a) = r$. De onde, $r = p(a)$. □

Convém observar que, nas condições do Teorema 3.13, o grau do polinômio quociente $q(x)$ é uma unidade a menos que o grau de $p(x)$. De fato, como $r = 0$ ou $\partial(r) = 0$, então $\partial(p) = \partial((x - a) \cdot q) = \partial(x - a) + \partial(q) = 1 + \partial(q)$ e, portanto $\partial(q) = \partial(p) - 1$. Além disso, pode ser facilmente demonstrado que os polinômios $p(x)$ e $q(x)$ têm o mesmo coeficiente dominante.

Além disso, cabe notar que um polinômio pode ter coeficientes em um corpo F e não possuir raízes neste corpo, como por exemplo $f(x) = x^2 + 3 \in \mathbb{R}[x]$ não possui raízes em $\mathbb{R}$. A Proposição 3.14, descrita abaixo, limita o número de raízes de um polinômio em um corpo.

Seja F um corpo. Se $K \supset F$ é um corpo, dizemos que K é uma **extensão** de F. Dessa forma, o polinômio $x^2 + 3$ não possui raízes na extensão $\mathbb{R}$, visto que $\sqrt{-3} \notin \mathbb{R}$, mas possui duas raízes em $\mathbb{C}$ pois $\pm i\sqrt{3} \in \mathbb{C}$, dado que $\mathbb{C} \supset \mathbb{R}$.

Proposição 3.14. *Seja F um corpo e seja $p(x) = a_0 + a_1x + \ldots + a_nx^n$ um polinômio não nulo em $F[x]$ de grau n, então o número de raízes de $p(x)$ em F é no máximo igual a $\partial p(x) = n$.*

Demonstração. Esta demonstração será feita por indução sobre o grau $\partial p(x) = n$.

Se $n = 1$, então $p(x)$ é um polinômio de grau 1 e portanto, tem apenas uma raiz em F . Agora, vamos supor que o resultado é verdadeiro para $n = k \geq 1$ e vamos mostrar que ele é verdadeiro para $k + 1$, ou seja, nossa hipótese de indução é que polinômios em $F[x]$ de grau $n = k$ possuem no máximo k raízes em F .

Suponhamos que $\partial p(x) = k + 1$. Se $p(x)$ não tem raízes em F, não temos nada para mostrar. Caso contrário, $p(x)$ tem uma raiz $a \in F$ e assim, pelo teorema 3.13, $p(x) = (x - a)g(x)$, para $g(x) \in F[x]$, $\partial g(x) = k$. Logo, $g(x)$ possui no máximo k raízes em F e, portanto, $p(x)$ possui no máximo $k + 1$ raízes em F, como queríamos mostrar. □

Observação 3.15. *As raízes consideradas na proposição anterior podem ser iguais, ou seja, estamos levando em consideração a repetição de raízes. O número de vezes que uma mesma raiz aparece, indica a sua multiplicidade, conforme a Definição 3.17 logo a seguir.*

Exemplo 3.16. *O polinômio* $x^3 - 1$ *possui apenas uma raiz em* $\mathbb{R}$*, pois* $1 \in \mathbb{R}$*, mas* $\frac{-1-\sqrt{-3}}{2}$*,* $\frac{-1+\sqrt{-3}}{2} \notin \mathbb{R}$*. Em contrapartida, possui* 3 *raízes em* $\mathbb{C}$ *por* $1, \frac{-1-i\sqrt{3}}{2}, \frac{-1+i\sqrt{3}}{2} \in \mathbb{C}$*, ou seja, o polinômio* $x^3 - 1$ *se fatora completamente em* $\mathbb{C}[x]$*.*

Definição 3.17. *Seja um polinômio* $p(x) \in F[x]$*,* $\alpha \in F$*, e um inteiro* $s \geq 1$*. Dizemos que* α *é uma raiz de* $p(x)$ *de* ***multiplicidade*** s *se* $(x-\alpha)^s$ *divide* $p(x)$*, mas* $(x-\alpha)^{s+1}$ *não divide* $p(x)$*.*
As raízes de multiplicidade 1 *são ditas* ***raízes simples*** *e as de multiplicidade maior ou igual a* 2 *são ditas* ***raízes múltiplas****.*

Definição 3.18. *(Vieira, 2011) Um polinômio* $p(x) = a_n x^n + \ldots + a_1 x + a_0$ *em* $F[x]$ *de grau* n *é dito mônico se* $a_n = 1$*.*

Teorema 3.19. *Seja* F *um corpo,* $p(x) \in F[x]$*,* $\alpha \in F$*, e seja* $s \geq 1$ *um inteiro. Então as afirmações seguintes são equivalentes:*

(i) α *é uma raiz de* $p(x)$ *de multiplicidade* s*.*

(ii) Existe um polinômio $q(x) \in F[x]$ *tal que* $p(x) = (x-\alpha)^s q(x)$ *com* $q(\alpha) \neq 0$*.*

Demonstração. $(i) \Rightarrow (ii)$. Temos que $p(x) \in F[x]$, e $\alpha \in F$. Então $p(\alpha) = 0$ se, e somente se existe um polinômio $q(x) \in F[x]$ tal que $p(x) = (x-\alpha) \cdot q(x)$. Aplicando o mesmo raciocínio s vezes, obtêm-se o resultado.

$(ii) \Rightarrow (i)$. Deseja-se mostrar que $(x-\alpha)^{s+1}$ não divide $p(x)$. Para isso, suponha por absurdo que $(x-\alpha)^{s+1}$ divida $p(x)$. Neste caso, $(x-\alpha)^s q(x) = p(x) = (x-\alpha)^{s+1} h(x)$ para algum $h(x) \in F[x]$, logo $(x-\alpha)^s [q(x) - (x-\alpha)h(x)] = 0$. Como $(x-\alpha)^s$ é um polinômio mônico, segue que $q(x) = (x-\alpha)h(x)$ e, portanto, $q(\alpha) = 0$, o que contradiz a hipótese. □

Suponha que $p(x)$ se fatore completamente em $F[x]$ e que ele possua n raízes distintas α_1, α_2, ..., α_n. Se α_1 é uma raiz de $p(x)$ de multiplicidade s_1, α_2 é um raiz de $p(x)$ de multiplicidade s_2, ..., α_n é um raiz de $p(x)$ de multiplicidade s_n, então a soma das multiplicidades das raízes é igual ao grau do polinômio $p(x)$, ou seja, $\partial p(x) = s_1 + s_2 + \ldots + s_n$.

Exemplo 3.20. *Determine as raízes do polinômio* $p(x) = x^3 + x^2 - 5x + 3 \in \mathbb{Q}[x]$*.*
Pode-se verificar que 1 *é uma raiz de* $p(x)$*:*

$$p(1) = 1 + 1 - 5 + 3 = 0.$$

Assim, $x-1$ divide $p(x)$, logo $p(x) = (x-1)\cdot q(x)$, em que $q(x) = x^2+2x-3 \in \mathbb{Q}[x]$. Além disso, 1 também é raiz de $q(x)$:

$$q(1) = 1+2-3 = 0.$$

Mas o polinômio $q(x)$ se fatora da seguinte maneira: $q(x) = (x-1)\cdot(x+3)$. Dessa forma, concluí-se que -3 também é raiz de $p(x)$ e que $p(x) = (x-1)^2(x+3)$.
Neste exemplo, $p(x)$ tem 3 raízes em $\mathbb{Q}$, onde 1 é uma raiz múltipla. Note que $(x-1)^2$ divide $p(x) = x^3+x^2-5x+3$ em $\mathbb{Q}[x]$, mas $(x-1)^3$ não divide $p(x)$. Logo, 1 é raiz de multiplicidade 2, enquanto -3 é raiz simples de $p(x)$.

Teorema 3.21. *[Teorema Fundamental da Álgebra] Todo polinômio $p(x) \in \mathbb{C}[x]$ de grau $n \geq 1$ possui pelo menos uma raiz complexa.*

O Teorema Fundamental da Álgebra garante que todos os polinômios com coeficientes em $\mathbb{C}$ possuem todas as suas raízes em $\mathbb{C}$. O mesmo pode não ocorrer com polinômios que possuem coeficientes em $\mathbb{Q}$ e este resultado foi provado por Gauss em sua tese de doutorado em 1798, ver (Vieira, 2011).

Além disso, o Teorema 3.21 garante que $\mathbb{C}$ é algebricamente fechado, isto é, qualquer polinômio de uma variável e grau maior ou igual a 1, com coeficientes em $\mathbb{C}$, terá uma raiz em $\mathbb{C}$. O Teorema 3.21 possui muitas demonstrações, nenhuma delas, porém, se faz com métodos puramente algébricos, devendo-se usar também ferramentas de análise ou considerações geométricas. Por este motivo, a demonstração será omitida neste trabalho, podendo ser encontrada em (Monteiro, 1969).

Dado um polinômio em $F[x]$ com $F \subset \mathbb{C}$, este polinômio tem raízes em $\mathbb{C}$. Mas é claro que este polinômio pode ter raízes em um corpo contido em $\mathbb{C}$, como mostram os exemplos a seguir:

Exemplo 3.22. *O polinômio $p(x) = x^2 - 7 \in \mathbb{Q}[x]$ mas não tem raízes em $F = \mathbb{Q}$.*

Exemplo 3.23. *O polinômio $p(x) = x^2 + 2 \in \mathbb{R}[x]$ mas não possui raízes em $\mathbb{R}$, embora possua raízes em $\mathbb{C}$.*

Exemplo 3.24. *O polinômio $p(x) = (x^2+1)(x^2-2) \in \mathbb{Q}[x]$ não possui raízes em $\mathbb{Q}$, possui as seguintes raízes em $\mathbb{C}$: $\pm\sqrt{2}$, $\pm i$.*

A partir do Teorema Fundamental da Álgebra, pode-se concluir que um polinômio $p(x) \in \mathbb{C}[x]$ de grau $n \geq 1$ possui n raízes em $\mathbb{C}$. De fato, o Teorema 3.21 garante que existe uma

raiz $z \in \mathbb{C}$ de $p(x)$. Pelo Teorema 3.13, $p(x) = (x - z)q(x)$, em que $q(x) \in \mathbb{C}[x]$ possui grau $n - 1$ e o resultado pode ser demonstrado por indução em n.

Teorema 3.25. *Seja $p(x) = a_n x^n + \ldots + a_1 x + a_0$ um polinômio em $\mathbb{R}[x]$. Se $z = \alpha + \beta i \in \mathbb{C}$ é uma raiz de $p(x)$, então seu conjugado $\overline{z} = \alpha - \beta i$ também é raiz de $p(x)$.*

Demonstração. Considere $p(x) = a_n x^n + \ldots + a_1 x + a_0 \in \mathbb{R}[x]$ e suponha que $z = \alpha + \beta i \in \mathbb{C}$ seja uma raiz de $p(x)$. Desse modo,

$$p(z) = a_n z^n + \ldots + a_1 z + a_0 = 0.$$

Como $a_i \in \mathbb{R}$, $\overline{a_i} = a_i, \forall i = 1, \ldots n$. Dessa forma,

$$p(\overline{z}) = a_n \overline{z}^n + \ldots + a_1 \overline{z} + a_0$$

$$p(\overline{z}) = \overline{a_n}\overline{z^n} + \ldots + \overline{a_1}\ \overline{z} + \overline{a_0}$$

$$p(\overline{z}) = \overline{a_n z^n + \ldots + a_1 z + a_0}$$

Portanto, $\overline{z} = \alpha - \beta i$ também é raiz de $p(x)$. □

O exemplo a seguir mostra que o Teorema 3.25 não pode ser aplicado a um polinômio $p(x) \in \mathbb{C}[x]$.

Exemplo 3.26. *O polinômio $p(x) = x^2 + 2ix + 3 \in \mathbb{C}[x]$ possui $z = i$ como raiz, pois:*

$$p(i) = i^2 + 2i \cdot i + 3 = -1 - 2 + 3 = 0$$

mas o conjugado $\overline{z} = -i$ não é raiz de $p(x)$, pois:

$$p(-i) = (-i)^2 + 2i(-i) + 3 = -1 + 2 + 3 = 4 \neq 0.$$

Corolário 3.27. *Todo polinômio $p(x) \in \mathbb{R}[x]$ de grau ímpar possui pelo menos uma raiz real.*

Demonstração. Pelo Teorema Fundamental da Álgebra, $p(x)$ tem uma raiz em $\mathbb{C}$. Como as raízes complexas aparecem em pares (z e $\overline{z}$) e como $p(x)$ tem grau ímpar, não é possível que todas as raízes de $p(x)$ sejam da forma $\alpha + \beta i \in \mathbb{C}$, com $\beta \neq 0$. Portanto, pelo menos uma das raízes deve ser real. □

3.3 Gráficos

Esta seção aborda o comportamento de gráficos de polinômios. Uma atenção especial é dada para polinômios que passam pela origem.

Seja $P(x)$ uma função polinomial de coeficientes reais e variável real x da forma

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0.$$

Se $y = P(x)$ então podemos associar a cada par ordenado (x, y) da função um ponto do plano cartesiano e, assim, obter o seu gráfico (Iezzi, 1977). É importante observar que uma função polinomial está definida para todos os números reais, ou seja, $D(P) = \mathbb{R}$, e também é contínua para todo número real (Thomas, 2009). O comportamento final de uma função descreve a tendência do gráfico se olharmos para a extremidade direita do eixo x (conforme x tende a $+\infty$) e para a extremidade esquerda do eixo x (conforme x tende a $-\infty$).

O comportamento final de qualquer função polinomial é $+\infty$ ou $-\infty$. A figura 6 ilustra esse comportamento ao mostrar o gráfico de função polinomial P. Observe que, conforme x aumenta, $P(x)$ também aumenta, isto é, quando x tende ao infinito, $P(x)$ tende ao infinito (Khan, 2020).

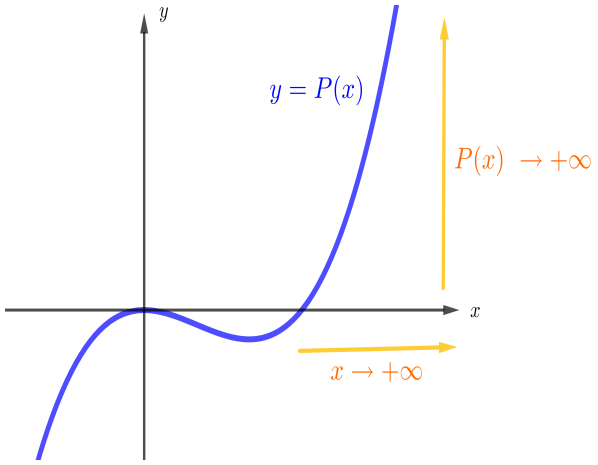

Figura 6: Valores de $P(x)$ aumentam quando os valores de x aumentam.

Na outra extremidade do gráfico, à medida que se avança para a esquerda ao longo do eixo x (x se aproximando de $-\infty$), o gráfico de P avança para baixo. Isto significa que quando x diminui, $P(x)$ também diminui, isto é, $P(x)$ tende a menos infinito quando x tende a menos infinito, veja figura 7.

De uma maneira geral, para determinar o comportamento final de um polinômio P devemos fazer as duas perguntas a seguir:

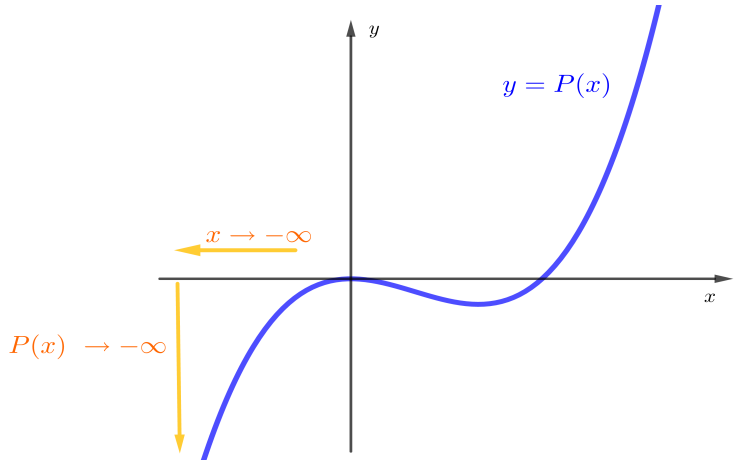

Figura 7: Valores de $P(x)$ diminuem quando os valores de x diminuem.

- Conforme $x \longrightarrow +\infty, P(x)$ qual o comportamento de $P(x)$?
- Conforme $x \longrightarrow -\infty, P(x)$ qual o comportamento de $P(x)$?

Note que quando x aumenta em valor absoluto, o termo $a_n x^n$ do polinômio $P(x)$ assume valor absoluto muito maior que os demais termos e, por isso, o comportamento do gráfico de $P(x)$ é o mesmo comportamento do gráfico de $P_n(x) = a_n x^n$. Os gráficos das figuras 8 e 9 ilustram o comportamento da função polinomial $P_n(x) = a_n x^n$, em termos da paridade de n e do sinal de a_n, em que a_n é um número real e n é um número inteiro não negativo.

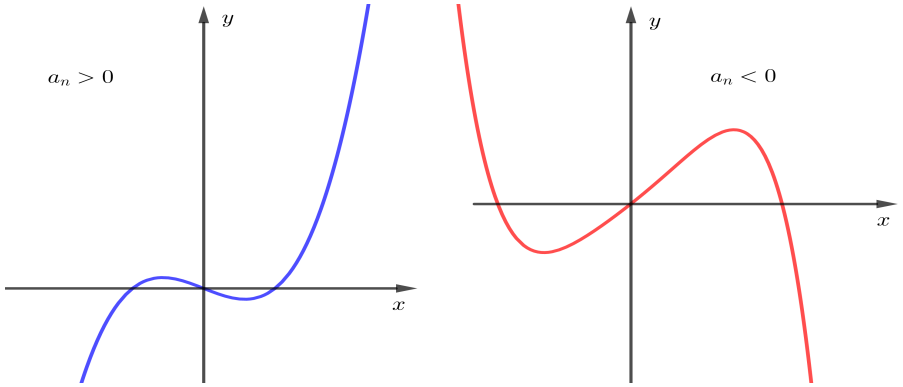

Figura 8: Gráficos de polinômios com o termo de maior grau ímpar.

Observe como o grau do polinômio, n, e o sinal do coeficiente principal, a_n, afetam o comportamento final do polinômio $P(x)$.

Quando n é par, o comportamento da função nas duas extremidades é igual. O sinal do coeficiente principal determina se ambas tendem a $+\infty$ $(a > 0)$ ou se ambas tendem a $-\infty$ $(a < 0)$.

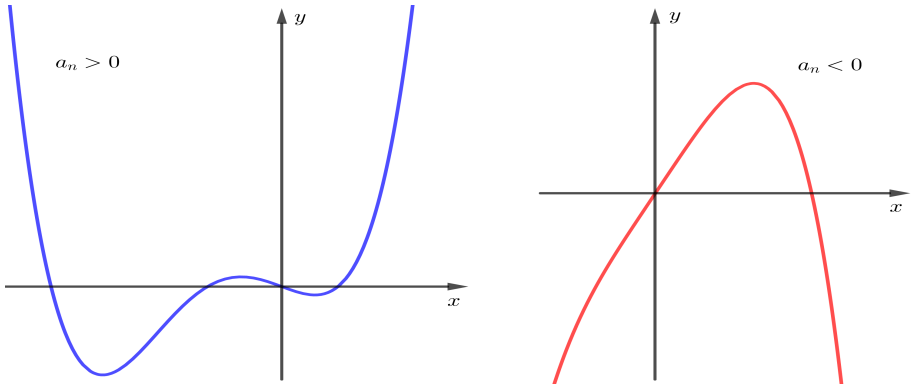

Figura 9: Gráficos de polinômios com o termo de maior grau par.

Por outro lado, quando n é ímpar, o comportamento da função nas duas extremidades é o oposto. O sinal do coeficiente principal determina o comportamento: Se $a > 0$, o gráfico "sai de $-\infty$ e chega em $+\infty$". Já se $a < 0$ o gráfico de P sai de $+\infty$ e chega em $-\infty$.

Suponha, agora, que $P(x)$ seja um polinômio que passa pela origem. De forma análoga ao raciocino anterior, pode-se verificar que quando x assume valores próximos da origem, o termo dominante passa a ser o termo de menor grau. É ele que determina o comportamento da função polinomial $P(x)$ perto da origem. O exemplo 3.28, a seguir, ilustra esse fato.

Exemplo 3.28. *Considere os polinômios $P_1(x) = x^2$ e $P_2(x) = x^4$. Para $|x| > 1$, x^4 supera x^2 e, quando $0 < |x| < 1$, x^4 é menor do que x^2 (veja figura 10). Além disso, $P_2(x)$ se aproxima mais rapidamente de 0 quando comparado a $P_1(x)$, quando x tende a zero por valores positivos.*

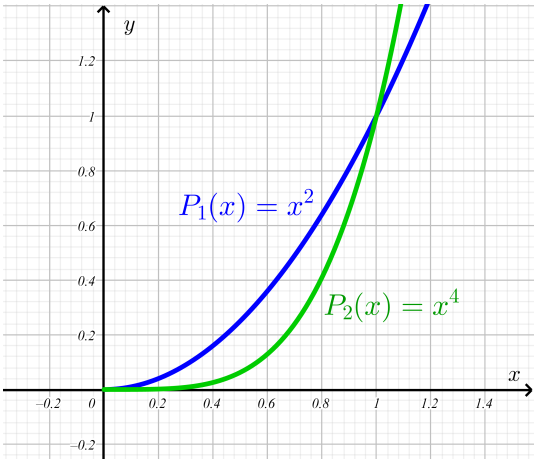

Figura 10: Gráficos dos polinômios $P_1(x) = x^2$ e $P_2(x) = x^4$.

Exemplo 3.29. *Considere os polinômios $P_1(x) = x + x^2$ e $P_2(x) = x^2 + x^3$. Estão descritos*

na Tabela 1 abaixo os valores de P_1 e P_2 quando x assume valores próximos da origem.

x	-1	$-0,5$	0	$0,5$	1
$P_1(x) = x + x^2$	0	$-0,25$	0	$0,75$	2
$P_2(x) = x^2 + x^3$	0	$0,125$	0	$0,375$	2

Tabela 1: Valores de P_1 e P_2 próximos da origem

Comparando os valores das funções polinomiais $P_1(x)$ e $P_2(x)$, descritos acima, pode-se perceber que $|P_2(x)| < |P_1(x)|$ para valores de x tendendo a zero. Note que o termo dominante de $P_2(x)$ possui maior grau que o termo dominante de $P_1(x)$, o que justifica este comportamento. Observe os gráficos da figura 11.

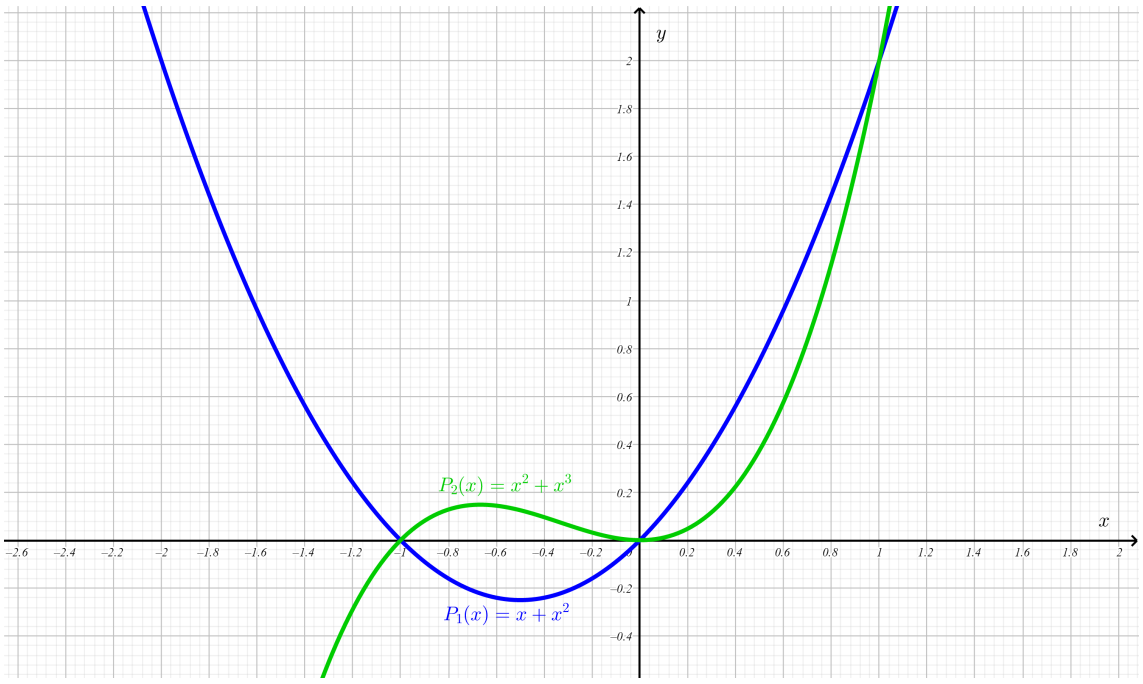

Figura 11: Gráficos dos polinômios $P_1(x) = x + x^2$ e $P_2(x) = x^2 + x^3$.

3.4 Fatoração

Fatorar significa escrever na forma de produto. A fatoração é uma grande ferramenta utilizada em diversas áreas da matemática. Existem, por exemplo, diversos problemas envolvendo números primos que utilizam a fatoração de números inteiros. Esta seção apresenta resultados e exemplos sobre a fatoração polinomial.

Se $u \in F - \{0\}$ e se $p_1(x), \ldots, p_m(x)$ são polinômios irredutíveis sobre F, a expressão $p(x) = u \cdot p_1(x) \ldots p_m(x)$ será utilizada para significar que $p(x) = u$ no caso de $m = 0$.

Teorema 3.30. *Seja F um corpo, então todo polinômio $p(x) \in F[x] - \{0\}$ pode ser escrito na forma,*

$$p(x) = u \cdot p_1(x) \ldots p_m(x),$$

em que $u \in F - \{0\}$ e $p_1(x), p_2(x), \ldots, p_m(x)$ são polinômios irredutíveis sobre $F[x]$ (não necessariamente distintos). Essa expressão é única a menos da constante u e da ordem dos polinômios $p_1(x), \ldots, p_m(x)$.

Demonstração. Seja $p(x) \in F[x] - \{0\}$. O teorema será demonstrado por indução sobre $\partial p(x) = n$. Se $n = 0$, então $p(x) = u$ é uma constante não nula e o resultado é imediato.

Suponha que $n > 1$ e que todo polinômio não nulo de grau menor que n possa ser escrito na expressão desejada. Deseja-se demonstrar que $p(x)$ também pode ser escrito naquela expressão.

Se $p(x)$ é irredutível, o resultado está demonstrado. Suponha que $p(x)$ seja redutível sobre $F[x]$, isto é, existem polinômios (não necessariamente irredutíveis) $g(x), h(x) \in F[x]$, $1 \leq \partial g(x) < n$, $1 \leq \partial h(x) < n$, tais que $p(x) = g(x) \cdot h(x)$.

Por hipótese de indução, existem $a, b \in F - \{0\}$ e $p_1(x), \ldots, p_r(x), p_{r+1}(x), \ldots, p_m(x)$ polinômios irredutíveis sobre $F[x]$, tais que

$$g(x) = a \cdot p_1(x) \ldots p_r(x),\ a \in F - \{0\} \text{ e } p_1(x), \ldots, p_r(x),$$

e

$$h(x) = b \cdot p_{r+1}(x) \ldots p_m(x), b \in F - \{0\} \text{ e } p_{r+1}(x), \ldots, p_m(x).$$

Logo, $p(x) = u \cdot p_1(x) \ldots p_m(x)$, em que $u = ab \in F - \{0\}$ e $p_1(x), \ldots, p_m(x)$ são polinômios irredutíveis sobre F.

Para demonstrar a unicidade da expressão, suponha que

$$p(x) = u \cdot p_1(x) \ldots p_m(x) = u' \cdot p'_1(x) \ldots p'_s(x)$$

em que $u, u' \in F - \{0\}$ e $p_1(x), \ldots, p_m(x), p'_1(x), \ldots, p'_s(x)$ são polinômios irredutíveis sobre $F[x]$.

Assim,

$$p_1(x) \mid p'_1(x) \ldots p'_s(x)$$

e daí segue que existe $u_i' \in F - \{0\}$ tal que $p_i'(x) = u_i' \cdot p_1(x)$ (nesse caso $p_i'(x)$ e $p_1(x)$ são ditos associados em $F[x]$).

Para concluir a demonstração da unicidade, será feita indução sobre m.

Se $m = 1$ e $p_1(x)$ irredutível, então $s = 1$ e $p_1(x)$ e $p_i'(x)$ são associados em $F[x]$.

Suponha $m > 1$. De $p_i'(x) = u_i' \cdot p_1(x)$ e sendo $F[x]$ um domínio (veja (Hefez, 1993)) segue que:

$$u \cdot p_2(x) \dots p_m(x) = u' \cdot u_i \cdot p_1'(x) \dots p_{i-1}(x) \cdot p_{i+1}(x) \dots p_s(x).$$

Pela hipótese de indução $m - 1 = s - 1$ (isto é, $m = s$), além disso, cada $p_j'(x)$ está associado com algum $p_i(x)$ através de uma constante. A partir dessas conclusões, termina-se a demonstração do teorema. □

Ao pensar em polinômios irredutíveis é inevitável não fazer uma analogia entre eles e inteiros primos. Esta seção deixa claro esta analogia e mostra que a irredutibilidade de um polinômio depende do anel sobre o qual ele é considerado.

Definição 3.31. *Um polinômio não-nulo p(x) é dito* ***irredutível*** *em F[x] se valem as seguintes afirmações:*

i) $\partial(p(x)) > 0$

ii) Ao escrever $p(x)$ *como um produto* $p(x) = d(x)h(x)$*, em que* $d(x), h(x) \in F[x]$*, então* $\partial(d(x)) = 0$ *ou* $\partial(h(x)) = 0$.

Um polinômio não constante que não é irredutível será chamado de **redutível**. Logo, se um polinômio $p(x)$ de grau maior ou igual a 1 é redutível sobre $F[x]$, ele pode ser escrito como um produto $p(x) = d(x)h(x)$, com $d(x), h(x) \in F[x]$ e $\partial(d(x)) > 0$ e $\partial(h(x)) > 0$.

Independente do corpo F, qualquer polinômio $p(x)$ de grau 1 em $F[x]$ é irredutível. De fato, suponha $p(x) = d(x) \cdot h(x)$, com $d(x), h(x) \in F[x]$, então $\partial(p(x)) = \partial(d(x)h(x)) = \partial(d(x)) + \partial(h(x))$, pela proposição 3.4. Como $\partial(p(x)) = 1$, segue que $\partial(d(x)) = 0$ e $\partial(h(x)) = 1$ ou $\partial(d(x)) = 1$ e $\partial(h(x)) = 0$.

Dados dois corpos F e G, com $F \subset G$, o exemplo 3.32 a seguir, mostra que um polinômio pode ser irredutível em $F[x]$, mas redutível em $G[x]$.

Exemplo 3.32. *O polinômio $p(x) = x^4 - 1$ é irredutível em $\mathbb{Q}[x]$ e irredutível em $\mathbb{R}[x]$, pois $x^4 - 1 = (x^2 - 1)(x^2 + 1)$ e o fator $(x^2 + 1)$ é irredutível em $\mathbb{Q}[x]$ e em $\mathbb{R}[x]$, mas é redutível em $\mathbb{C}[x]$, já que $x^4 + 1 = (x - 1)(x + 1)(x - i)(x + i)$.*

Definição 3.33. *Um polinômio $p(x) \in \mathbb{Z}[x]$ é dito **primitivo** se o máximo divisor comum (MDC) de seus coeficientes é igual a 1.*

Exemplo 3.34. *(Biazzi, 2014) Seja $p(x) = x^4 - x^2 + 1 \in \mathbb{Z}[x]$. Vamos mostrar que $p(x)$ é irredutível em $\mathbb{Z}[x]$. Basta mostrar que $P(x)$ não é um produto de dois fatores de grau maior ou igual a 1 em $\mathbb{Z}[x]$.*

- *$p(x)$ não tem fator de grau 1 em $\mathbb{Z}[x]$. Com efeito, se ele tivesse, este fator seria do tipo $x - a$, com $a \in \mathbb{Z}$, isto é, teríamos $x^4 - x^2 + 1 = (x - a)g(x)$ com $g(x) \in \mathbb{Z}[x]$; olhando para o termo constante, teríamos $1 = am$ com $m \in \mathbb{Z}$; logo $a = \pm 1$, isto é, ± 1 seria raiz de $x^4 - x^2 + 1$, no entanto, é imediato verificar que ± 1, não são raízes de $x^4 - x^2 + 1$.*

  Observe que se tivéssemos trabalhando em $\mathbb{Q}[x]$ no lugar de $\mathbb{Z}[x]$; a priori a poderia ser qualquer elemento diferente de zero pertencente a $\mathbb{Q}$ e logo não daria para verificar, um por um, que nenhum a de $\mathbb{Q}$ é raiz de $p(x)$.

- *$p(x)$ não tem fator $g(x)$ de grau 3 em $\mathbb{Z}[x]$. Com efeito, se ele tivesse, teríamos $p(x) = g(x)h(x)$, onde $h(x) \in \mathbb{Z}[x]$ teria necessariamente grau 1, mas isto é impossível pelo caso precedente.*

- *$p(x)$ não tem fator de grau 2 em $\mathbb{Z}[x]$, com efeito, se ele tivesse, teríamos*
  $x^4 - x^2 + 1 = (x^2 + ax + b)(x^2 + cx + d)$ com $a, b, c, d \in \mathbb{Z}$

$$\begin{aligned} \textit{(termo constante)} \quad 1 &= bd, \textit{ logo } b = d = \pm 1; \\ \textit{(termo em } x\textit{)} \quad 0 &= ad + bc \\ &= b(a + c), \textit{ logo } a = -c; \\ \textit{(termo em } x^2\textit{)} \quad -1 &= d + ac + b \\ &= 2b - a^2, \textit{ logo } a^2 - 1 = 2b = \pm 2; \end{aligned}$$

  assim $a^2 = 3$ ou $a^2 = -1$, o que é impossível.

Lema 3.35. *O produto de dois polinômios primitivos $f(x), g(x) \in \mathbb{Z}[x]$ também é primitivo.*

Demonstração. Se tal produto não for primitivo, então existe um número primo p que divide todos os coeficientes de $f(x) \cdot g(x)$ e, portanto, este produto será nulo no anel $\mathbb{Z}_P[x]$ (a definição

e propriedades desse conjunto podem ser encontrados na referência (Araujo, 2009)). Dessa forma, um dos polinômios deverá ser nulo em $\mathbb{Z}_P[x]$. Suponha, sem perda de generalidade, que $f(x)$ é nulo em $\mathbb{Z}_P[x]$. Isso quer dizer que todos os seus coeficientes são divisíveis por p, o que é um absurdo. Conclui-se que um produto de polinômios primitivos deve ser primitivo. □

Lema 3.36. *[Lema de Gauss] Seja $p(x) \in \mathbb{Z}[x]$ tal que $p(x)$ é um polinômio irredutível sobre $\mathbb{Z}[x]$, então $p(x)$ também é irredutível sobre $\mathbb{Q}[x]$.*

Demonstração. Suponha que $p(x)$ possa ser fatorado sobre $\mathbb{Q}[x]$ da seguinte forma: $p(x) = q(x) \cdot h(x)$, com $\partial(q(x)) > 0$ e $\partial(h(x)) > 0$.

Seja m_1 o mínimo múltiplo comum dos denominadores dos coeficientes de $q(x)$, então $m_1 \cdot q(x) \in \mathbb{Z}[x]$ é primitivo. Analogamente, se m_2 é o mínimo múltiplo comum dos denominadores dos coeficientes de $h(x)$, $m_2 \cdot h(x) \in \mathbb{Z}[x]$ é primitivo. Logo,

$$m_1 m_2 p(x) = m_1 q(x) m_2 h(x).$$

Como o lado direito é primitivo, o lado esquerdo também é primitivo. Mas isso só é possível se m_1 e m_2 são ± 1, o que faz com que a fatoração inicial já fosse em $\mathbb{Z}[x]$, gerando, assim, um absurdo.

Portanto, $p(x)$ é irredutível sobre $\mathbb{Q}[x]$. □

Exemplo 3.37. *(Biazzi, 2014) Mostre que o polinômio $p(x) = x^4 - 2x^2 + 8x + 1$ é redutível sobre $\mathbb{Q}[x]$.*

Pelo Lema de Gauss, é suficiente mostrar que o polinômio é irredutível sobre $\mathbb{Z}[x]$. Uma fatoração de $p(x)$ pode ser de dois tipos: produto de um polinômio linear por um polinômio de grau 3, ou então o produto de dois polinômios quadráticos.

Se existe um polinômio linear que divide $p(x)$ isso quer dizer que $p(x)$ tem uma raiz inteira. As únicas possíveis raízes inteiras de p(x) são ± 1, e podemos ver facilmente que nenhuma dela é raiz, pois $p(1) = 8$ e $p(-1) = -8$. Logo uma possível fatoração de $p(x)$ só poderia ser um produto de dois polinômios quadráticos. Seja então $p(x) = (x^2 + ax + b)(x^2 + cx + d)$, com $a, b, c, d \in \mathbb{Z}$. Fazendo a distributiva e comparando coeficientes, temos $bd = 1, ad + bc = 8, ac + b + d = -2$ e $a + c = 0$

De $bd = 1$ temos $b = d = 1$ ou $b = d = -1$. Se $b = d = 1$, ficamos com $ac = -4$ e portanto $a = -c = \pm 2$ e não podemos ter $ad + bc = 8$. Se $b = d = -1$, obtemos $ac = 0$; logo $a = c = 0$ e novamente não temos $ad + bc = 8$. Portanto a fatoração como dois polinômios quadráticos também é impossível, e concluímos que o polinômio $p(x)$ é irredutível sobre $\mathbb{Q}$.

Proposição 3.38. *Se $p(x) \in F[x]$ é polinômio de grau $n > 2$ e possui pelo menos uma raiz em F, então $p(x)$ é redutível em $F[x]$.*

Demonstração. Se $a \in F$ é raiz de $p(x)$ então, pelo Teorema 3.13, $(x-a)$ divide $p(x)$. Dessa forma, $p(x) = (x-a)d(x)$, em que $d(x) \in F[x]$. Note que $p(x)$ tem grau n, $(x-a)$ tem grau 1 e $d(x)$ tem grau $n-1$. Como $n > 2$, então $n-1 > 1$, o que implica em $p(x)$ ser redutível em $F[x]$. □

Teorema 3.39. *Se $p(x) \in F[x] - \{0\}$, $\partial(p(x)) = 2$ ou 3, então p é redutível em $F[x]$ se, e somente se, p possui raízes em F.*

Demonstração. Seja $p(x) \in F[x]$ com grau 2 ou 3, assuma primeiramente que $p(x)$ é redutível sobre F, tal que $p(x) = g(x)h(x)$ para algum polinômio não constante $g(x), h(x) \in F[x]$. Como o grau de $g(x)$ e $h(x)$ somados é 2 ou 3, segue que, um ou ambos os polinômios devem ter grau 1. Assim, pelo menos um deles deve ter raiz em F, logo $p(x)$ deve ter uma raiz em F.

Reciprocamente, suponhamos que $p(x)$ tem raiz em F. Então, $p(x)$ têm um fator de grau 1, logo temos que $p(x) \in F[x]$ é redutível sobre F.

□

Teorema 3.40. *Um polinômio $p(x)$ em $\mathbb{C}[x]$ é irredutível sobre $\mathbb{C}$ se, e somente se, $p(x)$ tem grau 1.*

Demonstração. Se $\partial(p(x)) = 1$, claramente $p(x)$ é irredutível sobre $\mathbb{C}$. Reciprocamente, suponha que $p(x)$ seja irredutível sobre $\mathbb{C}$ e tenha grau $n > 1$. Pelo Teorema 3.21, existe uma raiz α de $p(x)$ em $\mathbb{C}$ e pelo Teorema 3.13, segue que $(x-\alpha)$ divide $p(x)$. Logo, $p(x)$ pode ser escrito da forma $p(x) = (x-\alpha)q(x)$, em que $\partial(q) = n-1 \geq 1$, o que é absurdo, pois $p(x)$ é irredutível. Logo, $n = 1$. □

3.5 Valuação

Para a apresentação dos resultados expostos no capítulo 4, faz-se necessária a apresentação de diversas definições. Algumas destas definições, bem como alguns exemplos ilustrativos, estão descritos nesta seção.

Definição 3.41 (Polinômio Afim)**.** *O polinômio $P(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in F[x]$ é dito **afim** se $P(0) = 0$.*

Note que $P(0) = 0$ se, e somente se, o seu termo independente $a_0 = 0$. Além disso, o gráfico de qualquer polinômio afim em $F[x]$ passa pela origem.

Definição 3.42 (Valuação)**.** *Seja $P(x) = a_0 + a_1x + a_2x^2 + \cdots$ um polinômio (ou uma série formal). A* ***valuação*** *$v(P)$ de P é o menor número inteiro k tal que $a_k \neq 0$. Por convenção, a valuação do polinômio zero é ∞.*

Exemplo 3.43. *Os polinômios $P(x) = 3x + 5x^2$ e $Q(x) = 5x^3 + x^4 - 3x^7$ são afins e suas valuações valem $v(P) = 1$ e $v(Q) = 3$, respectivamente.*

Exemplo 3.44. *O polinômio $P_1(x) = x^2$ tem a mesma valuação que o polinômio $P_2(x) = x^2 + x^3$, entretanto $|P_1(x)| \geq |P_2(x)|$ para x pequeno e $x < 0$ e $|P_1(x)| \leq |P_2(x)|$ para x pequeno e $x > 0$, na vizinhança da origem, o que pode ser verificado na figura 12.*

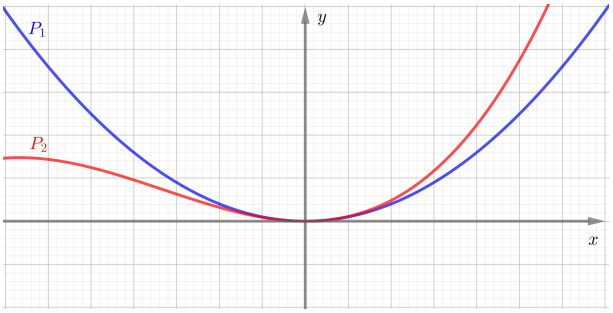

Figura 12: $P_1(x) > P_2(x)$, para x pequeno e $x < 0$ e $P_1(x) < P_2(x)$, para x pequeno e $x > 0$

Seja $P(x) = a_1x + a_2x^2 + \cdots + a_nx^n$ um polinômio afim com valuação $k = v(P)$. Em uma vizinhança da origem, $P(x) \approx a_kx^k$. Dessa forma é possível concluir que o gráfico de P cruza o eixo x em $(0, 0)$ se, e somente se, a valuação $k = v(P)$ é um inteiro ímpar.

Além disso, ao considerar dois polinômios distintos P_1, P_2, o sinal de $P_1(x) - P_2(x)$ muda em 0 se, e somente se, $v(P_1 - P_2)$ for ímpar. Os Exemplos 3.45, 3.46 e 3.47 ilustram essa situação.

Exemplo 3.45. *Seja $P_1(x) = x^2$ e $P_2(x) = x^2 + x^3$. Temos que $P_1(x) - P_2(x) = x^2 - (x^2 + x^3) = x^2 - x^2 - x^3 = -x^3$. Dessa forma a valuação $v(P_1(x) - P_2(x)) = 3$. Como 3 é um número ímpar os gráficos de $P_1(x)$ e $P_2(x)$ se cruzam na origem como está representado na figura 13.*

Exemplo 3.46. *Seja $P_1(x) = x^2$ e $P_2(x) = x^2 + x^4$. Temos que $P_1(x) - P_2(x) = x^2 - (x^2 + x^4) = x^2 - x^2 - x^4 = -x^4$. Dessa forma a valuação $v(P_1(x) - P_2(x)) = 4$. Como 4*

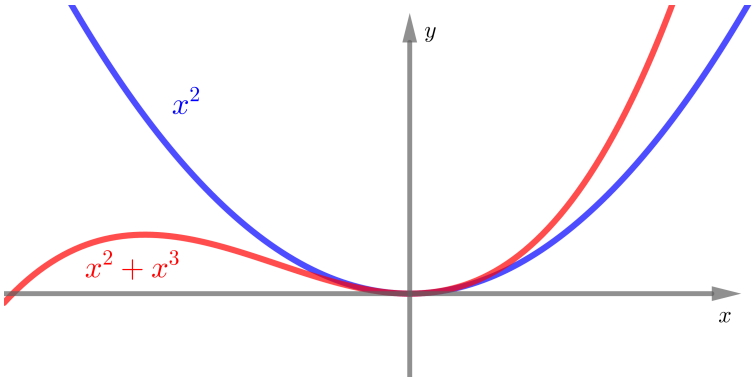

Figura 13: As curvas que representam os gráficos de $P_1(x)$ e $P_2(x)$ se cruzam na origem.

é um número par os gráficos de $P_1(x)$ e $P_2(x)$ se tocam na origem sem se cruzar como está representado na Figura 14.

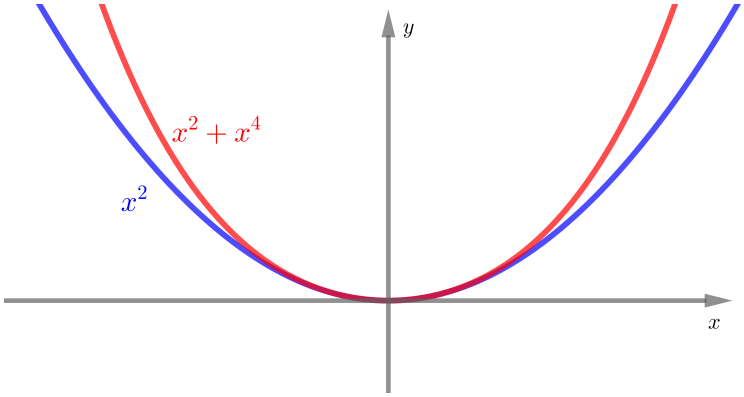

Figura 14: As curvas que representam os gráficos de $P_1(x)$ e $P_2(x)$ se tocam na origem sem se cruzar.

Exemplo 3.47. *Considere os polinômios $P_1(x) = \frac{1}{2}x^3, P_2(x) = x^2$ e $P_3(x) = x^3 - 3x$. Temos que:*

$P_1(x) - P_2(x) = \frac{1}{2}x^3 - x^2 = -x^2 + \frac{1}{2}x^3$;

$P_1(x) - P_3(x) = \frac{1}{2}x^3 - (x^3 - 3x) = \frac{1}{2}x^3 - x^3 + 3x = 3x - \frac{1}{2}x^3$

$P_2(x) - P_3(x) = x^2 - (x^3 - 3x) = x^2 - x^3 + 3x = 3x + x^2 - x^3$

De onde obtém-se as valuações v_1, v_2 e v_3, tais que $v_1(P_1(x) - P_2(x)) = 2$, $v_2(P_1(x) - P_3(x)) = 1$ e $v_3(P_2(x) - P_3(x)) = 1$ o que significa graficamente que $P_1(x)$ e $P_2(x)$ não se cruzam na origem, somente se tocam pois $v_1 = 2$ é par. $P_1(x)$ e $P_3(x)$ se cruzam na origem pois $v_2 = 1$ é ímpar. Por fim, $P_2(x)$ e $P_3(x)$ se cruzam na origem visto que $v_3 = 1$ é ímpar. Ver Figura 15 .

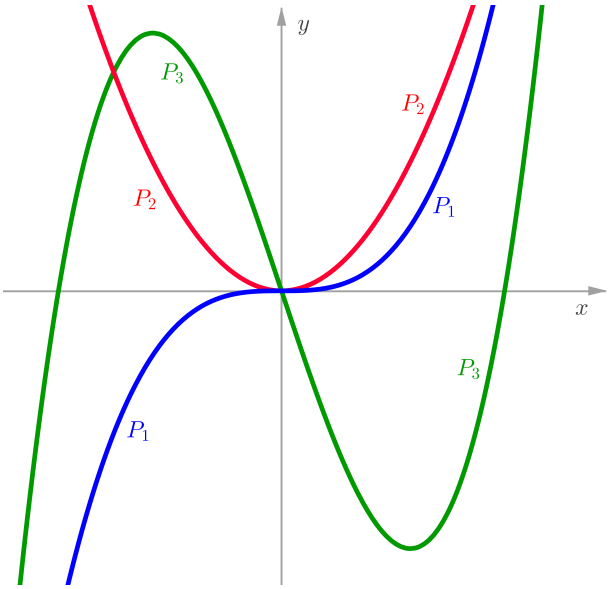

Figura 15: Comportamento entre os polinômios $P_1(x)$, $P_2(x)$ e $P_3(x)$ na vizinhança da origem.

3.6 Configurações de Polinômios Afins

O objetivo desta seção é estudar as possíveis configurações dos gráficos de n polinômios afins perto da origem. Mais claramente, ao considerar n polinômios afins $P_1,\ P_2,\ \cdots,\ P_n$ tais que para x pequeno e $x < 0$, $P_1(x) < P_2(x) < \cdots < P_n(x)$, deseja-se conhecer as possíveis ordens em que esses polinômios podem assumir, se x for pequeno e $x > 0$.

Para o caso de dois polinômios P_1 e P_2, por exemplo, com $P_1(x) < P_2(x)$ para x pequeno e negativo, pretende-se saber qual o número total de possíveis configurações dos seus gráficos para x pequeno e positivo. Existem $2! = 2$ possíveis configurações, ambas ilustradas na figura 16, sendo elas:

1- $P_1(x) < P_2(x)$ para x pequeno e $x > 0$.

2- $P_1(x) > P_2(x)$ para x pequeno e $x > 0$.

Para ilustrar o caso 1, os polinômios $P_1(x) = x^2$ e $P_2(x) = -x^2$ podem ser usados. Exemplos de polinômios que se encaixam na configuração 2 são $Q_1(x) = x$ e $Q_2(x) = -x$.

A mesma análise pode ser feita para três polinômios P_1, P_2 e P_3, em condições idênticas às citadas anteriormente. Ou seja, se $P_1(x) < P_2(x) < P_3(x)$ para x pequeno e negativo, qual o número total de possíveis configurações dos gráficos para x pequeno e positivo?

Neste caso, existem $3! = 6$ possíveis configurações dos gráficos, todas ilustradas na figura 17. Exemplos de polinômios que satisfazem essas seis configurações podem ser facilmente elaborados.

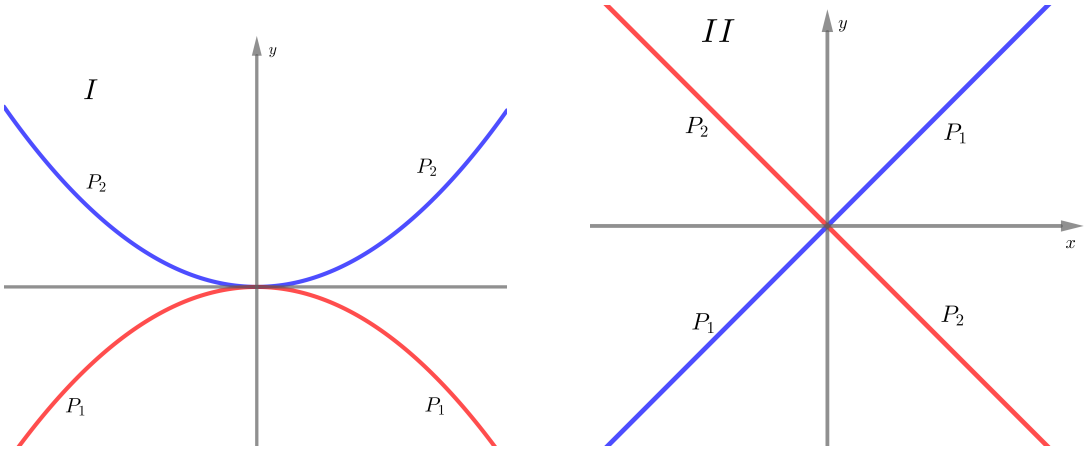

Figura 16: Em I: $P_1(x) < P_2(x)$, para x pequeno e $x < 0$ e $P_1(x) < P_2(x)$, para x pequeno e $x > 0$. Em II: $P_1(x) < P_2(x)$, para x pequeno e $x < 0$ e $P_2(x) < P_1(x)$, para x pequeno e $x > 0$.

Para o caso de quatro polinômios algo diferente acontece. Dados quatro polinômios afins em $\mathbb{R}[x]$, P_1, P_2, P_3 e P_4, tais que $P_1(x) < P_2(x) < P_3(x) < P_4(x)$, se $x < 0$ em uma vizinhança de 0, poderia-se esperar $4! = 24$ possíveis configurações dos gráficos dos mesmos para $x > 0$ e pequeno. Estas configurações esperadas estão descritas abaixo, utilizando-se a notação de permutação dos elementos do conjunto $\{P_1, P_2, P_3, P_4\}$.

$(P_1, P_2, P_3, P_4), (P_1, P_2, P_4, P_3), (P_1, P_3, P_2, P_4), (P_1, P_3, P_4, P_2), (P_1, P_4, P_2, P_3), (P_1, P_4, P_3, P_2),$
$(P_2, P_1, P_3, P_4), (P_2, P_1, P_4, P_3), (P_2, P_3, P_1, P_4), (P_2, P_3, P_4, P_1), (P_2, P_4, P_1, P_3), (P_2, P_4, P_3, P_1),$
$(P_3, P_1, P_2, P_4), (P_3, P_1, P_4, P_2), (P_3, P_2, P_1, P_4), (P_3, P_2, P_4, P_1), (P_3, P_4, P_1, P_2), (P_3, P_4, P_2, P_1),$
$(P_4, P_1, P_2, P_3), (P_4, P_1, P_3, P_2), (P_4, P_2, P_1, P_3), (P_4, P_2, P_3, P_1), (P_4, P_3, P_1, P_2), (P_4, P_3, P_2, P_1).$

Entretanto, duas dessas permutações, (P_2, P_4, P_1, P_3) e (P_3, P_1, P_4, P_2), são impossíveis de se obter. Esse é o resultado do teorema de Kontsevich que será apresentado e demonstrado no capítulo 4, descrito a seguir.

O caso das possíveis configurações dos gráficos de n polinômios afins em uma vizinhança da origem é bem mais complicado e também será abordado no capítulo 4.

4 O Teorema de Kontsevich e as Configurações Proibidas

Começamos a estudar álgebra no segundo ano do ensino fundamental quando aprendemos a encontrar raízes para um polinômio do primeiro grau e não paramos mais. No final do ensino fundamental estudamos a equação polinomial do segundo grau e algumas maneiras de resolvê-

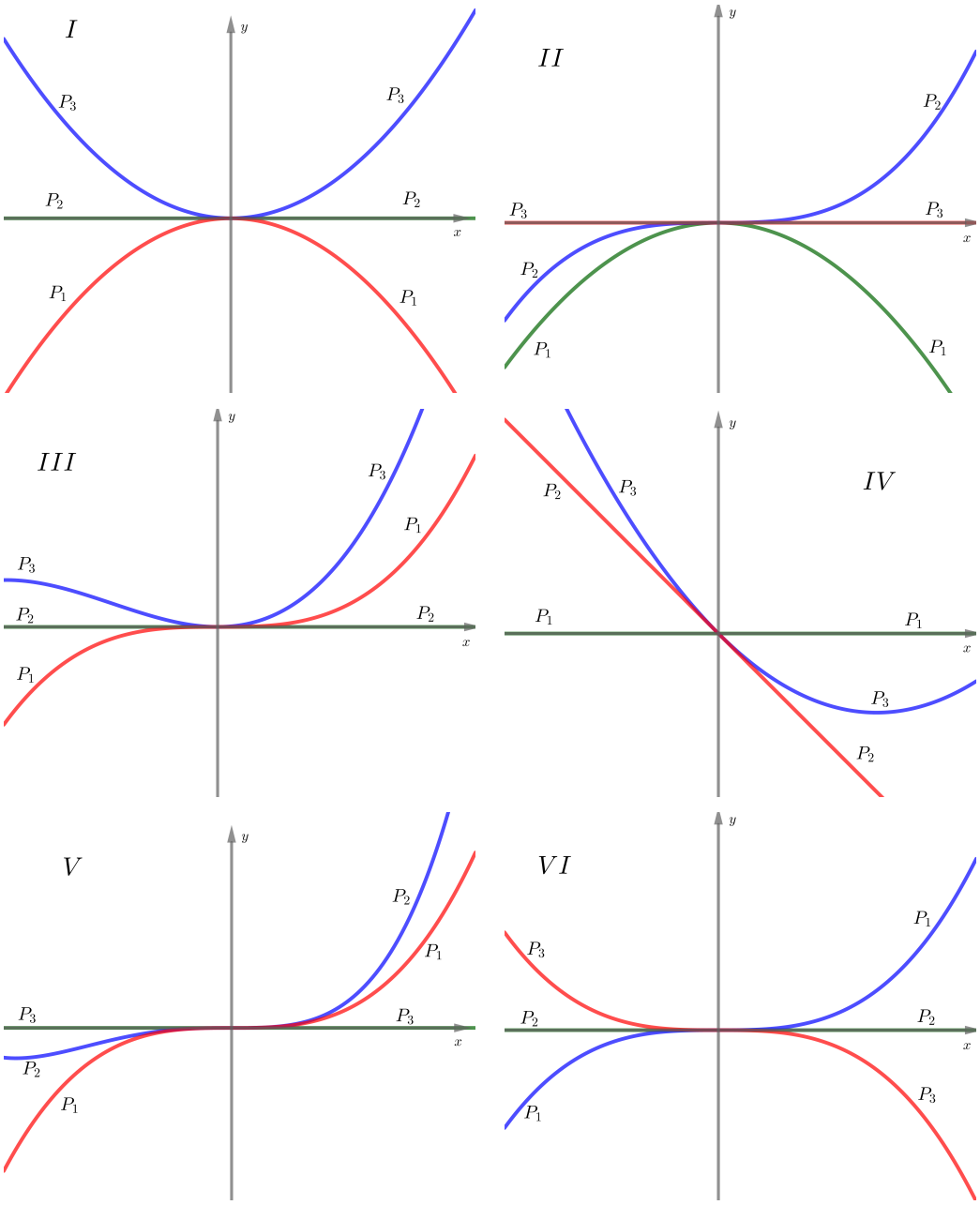

Figura 17: Em I: $P_1(x) < P_2(x) < P_3(x)$, para x pequeno e $x < 0$ e $P_1(x) < P_2(x) < P_3(x)$, para x pequeno e $x > 0$. Em II: $P_1(x) < P_2(x) < P_3(x)$, para x pequeno e $x < 0$ e $P_1(x) < P_3(x) < P_2(x)$, para x pequeno e $x > 0$. Em III: $P_1(x) < P_2(x) < P_3(x)$, para x pequeno e $x < 0$ e $P_2(x) < P_1(x) < P_3(x)$, para x pequeno e $x > 0$. Em IV: $P_1(x) < P_2(x) < P_3(x)$, para x pequeno e $x < 0$ e $P_2(x) < P_3(x) < P_1(x)$, para x pequeno e $x > 0$. Em V: $P_1(x) < P_2(x) < P_3(x)$, para x pequeno e $x < 0$ e $P_3(x) < P_1(x) < P_2(x)$, para x pequeno e $x > 0$. Em VI: $P_1(x) < P_2(x) < P_3(x)$, para x pequeno e $x < 0$ e $P_3(x) < P_2(x) < P_1(x)$, para x pequeno e $x > 0$.

la. Estudamos também polinômios do quarto grau que não possuem termos de grau ímpar, chamados de equações biquadradas. Neste mesmo ano também é visto, de forma introdutória, as funções polinomiais do primeiro e segundo grau. No terceiro ano do ensino médio o assunto polinômios volta a ser visto agora com números complexos e um grau maior do que dois. O estudo envolve operações elementares entre polinômios e encontrar suas raízes (são utilizadas as famosas Relações de Girard). Visto todas essas ferramentas envolvendo polinômios, fica a pergunta: O que acontece quando dois ou mais polinômios se cruzam? A resposta a essa pergunta pode parecer simples, mas coisas inesperadas podem acontecer. Este capítulo busca jogar uma luz sobre estes fenômenos misteriosos, mais especificamente para o caso em que quatro ou mais polinômios afins se cruzam na origem.

Na Seção 3.6 foram apresentadas as configurações dos gráficos de polinômios afins de grau n, próximos da origem, entretanto mencionou-se a possibilidade de exemplificar todas as possibilidades de configurações apenas para os casos $n = 2$ e $n = 3$. O caso $n = 4$ apresenta uma particularidade. Particularidade esta que vai se propagar para os demais valores de $n > 4$, como será mostrado neste capítulo. Os resultados apresentados foram baseados em (Ghys, 2017).

4.1 O Teorema de Kontsevich

Ao buscar por exemplos de polinômio afins, cujos gráficos obedeçam todas as configurações expostas na seção 3.6 (caso n=4 polinômios), duas configurações ficarão sem os exemplos desejados. Este é o tema do Teorema de Kontsevich, que será enunciado a seguir.

Teorema 4.1 (Teorema de Kontsevich)**.** *(Ghys, 2017) Quatro polinômios* $P_1, P_2, P_3, P_4 \in \mathbb{R}[x]$ *não podem satisfazer*

I. $P_1(x) < P_2(x) < P_3(x) < P_4(x)$ *para* x *pequeno e* $x < 0$,

$P_2(x) < P_4(x) < P_1(x) < P_3(x)$ *para* x *pequeno e* $x > 0$, *ou analogamente*

II. $P_1(x) < P_2(x) < P_3(x) < P_4(x)$ *para* x *pequeno e* $x < 0$,

$P_3(x) < P_1(x) < P_4(x) < P_2(x)$ *para* x *pequeno e* $x > 0$.

Demonstração. I. Por contradição, assuma que existem quatro polinômios P_1, P_2, P_3, P_4 satisfazendo: $P_1(x) < P_2(x) < P_3(x) < P_4(x)$ para x pequeno e $x < 0$, $P_2(x) < P_4(x) <$

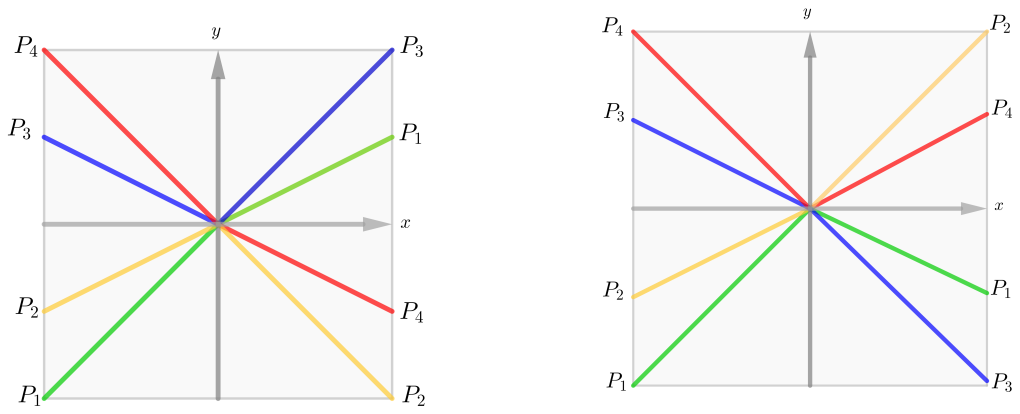

Figura 18: As duas permutações proibidas do Teorema de Kontsevich.

$P_1(x) < P_3(x)$ para x pequeno e $x > 0$. Substituindo cada P_i por $P_i - P_1$, pode-se que assumir que $P_1 = 0$.

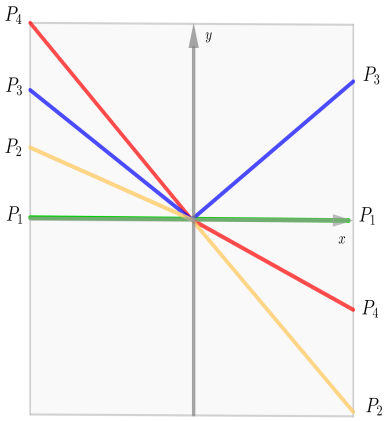

Figura 19: Configuração $(2, 4, 1, 3)$ de quatro polinômios com $P_1(x) = 0$.

Ao analisar a Figura 19, pode-se observar que P_2 e P_4 mudam de sinal na origem, logo as suas valuações $v(P_2)$ e $v(P_4)$ são ímpares. Além disso, a Figura 19 também mostra que P_3 não muda de sinal na origem, o que implica que a sua valuação $v(P_3)$ é par.

Como $0 < P_2(x) < P_3(x) < P_4(x)$ para x negativo pequeno, pode-se concluir que $v(P_2) \geq v(P_3) \geq v(P_4)$ (basta notar que $P_i(x) \approx a_{v(P_i)}x^{v(P_i)}$ para x pequeno). Da mesma forma, $|P_4(x)| < |P_2(x)|$ para x pequeno positivo implica que $v(P_4) \geq v(P_2)$. Isso forçaria as três valuações a serem iguais, mas duas delas são ímpares e uma delas é par. Contradição!

II. Novamente, por contradição, assuma que existem quatro polinômios P_1, P_2, P_3, P_4 sa-

tisfazendo: $P_1(x) < P_2(x) < P_3(x) < P_4(x)$ para x pequeno $x < 0$, $P_3(x) < P_1(x) < P_4(x) < P_2(x)$ para x pequeno $x > 0$. Substituindo cada P_i por $P_i - P_1$ (como foi feito no caso $(I.)$), pode-se que assumir que $P_1 = 0$.

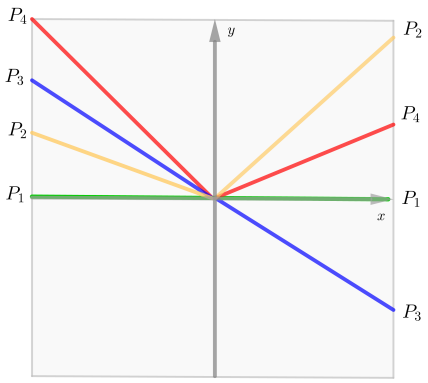

Figura 20: Configuração $(3, 1, 4, 2)$ de quatro polinômios com $P_1(x) = 0$.

Ao analisar a Figura 20, pode-se observar que P_3 muda de sinal na origem, logo as sua valuação $v(P_3)$ é ímpar. Além disso, a Figura 20 também mostra que P_2 e P_4 não mudam de sinal na origem, o que implica que as suas valuações $v(P_2)$ e $v(P_4)$ são pares.

Como $0 < P_2(x) < P_3(x) < P_4(x)$ para x negativo pequeno, pode-se concluir que $v(P_2) \geq v(P_3) \geq v(P_4)$ (mesmo raciocínio do caso I). Da mesma forma, $|P_4(x)| < |P_2(x)|$ para x pequeno positivo implica que $v(P_4) \geq v(P_2)$. Isso forçaria as três valuações a serem iguais, mas duas delas são pares e uma delas é ímpar. Contradição!

□

Dados quatro polinômios afins, o Teorema 4.1 mostra duas configurações de seus gráficos que são proibidas perto da origem. Será que existem outras configurações proibidas? O exemplo 4.2 mostra que não.

As duas configurações descritas no teorema 4.1 serão chamadas de **configurações proibidas** ou **configurações de Kontsevich**. Elas (e todas as demais) podem ser descritas pela notação por ciclos das permutações que as geraram, a saber: $(2, 4, 1, 3)$ e $(3, 1, 4, 2)$. Serão chamadas de **configurações permitidas** aquelas que não são proibidas.

Exemplo 4.2. *Os 22 quartetos de polinômios afins descritos abaixo possuem gráficos que satisfazem todas configurações permitidas (todas as configurações descritas na seção 3.6 menos as configurações proibidas de Kontsevich). As 22 configurações podem ser observadas na figura 21.*

$I:$	$P_1(x) = -x^2,$	$P_2(x) = -x^4,$	$P_3(x) = x^4,$	$P_4(x) = x^2,$
$II:$	$P_1(x) = -x^2,$	$P_2(x) = 0,$	$P_3(x) = x^2,$	$P_4(x) = x^2 - x^3,$
$III:$	$P_1(x) = -x^2,$	$P_2(x) = 0,$	$P_3(x) = -x^3,$	$P_4(x) = x^2,$
$IV:$	$P_1(x) = -x^2,$	$P_2(x) = 0,$	$P_3(x) = 2x^3,$	$P_4(x) = x^4,$
$V:$	$P_1(x) = -x^2,$	$P_2(x) = x^3,$	$P_3(x) = x^3 + x^4,$	$P_4(x) = -x^3,$
$VI:$	$P_1(x) = -x^2,$	$P_2(x) = x^3,$	$P_3(x) = 0,$	$P_4(x) = -x^3,$
$VII:$	$P_1(x) = -x^2 + x^3,$	$P_2(x) = -x^2,$	$P_3(x) = 0,$	$P_4(x) = x^2,$
$VIII:$	$P_1(x) = -x^2,$	$P_2(x) = -x^2 - x^3,$	$P_3(x) = x^3 + x^4,$	$P_4(x) = -x^3,$
$IX:$	$P_1(x) = x^3 + 3x^5,$	$P_2(x) = -2x^4,$	$P_3(x) = 0,$	$P_4(x) = 2x^2,$
$X:$	$P_1(x) = x^3 - x^5,$	$P_2(x) = x^2 + x^4,$	$P_3(x) = -x^5,$	$P_4(x) = -x^3,$
$XI:$	$P_1(x) = x,$	$P_2(x) = -x^2,$	$P_3(x) = 0,$	$P_4(x) = x^2,$
$XII:$	$P_1(x) = x + x^2,$	$P_2(x) = -x^2 - x^3,$	$P_3(x) = x^3 + x^4,$	$P_4(x) = -x^3,$
$XIII:$	$P_1(x) = -2x^4,$	$P_2(x) = x^5 + x^6,$	$P_3(x) = -3x^3,$	$P_4(x) = 2x^2,$
$XIV:$	$P_1(x) = x,$	$P_2(x) = 2x^3,$	$P_3(x) = -2x^3,$	$P_4(x) = -x,$
$XV:$	$P_1(x) = x^3,$	$P_2(x) = 0,$	$P_3(x) = -x^3,$	$P_4(x) = x^2,$
$XVI:$	$P_1(x) = x,$	$P_2(x) = x^3,$	$P_3(x) = 0,$	$P_4(x) = x^2,$
$XVII:$	$P_1(x) = 2x^3 - 2x^4,$	$P_2(x) = 2x^3 + 2x^5,$	$P_3(x) = -x^4,$	$P_4(x) = x^4,$
$XVIII:$	$P_1(x) = 2x^3,$	$P_2(x) = x^3,$	$P_3(x) = 0,$	$P_4(x) = x^4,$
$XIX:$	$P_1(x) = -x^2,$	$P_2(x) = 0,$	$P_3(x) = x^2,$	$P_4(x) = -x,$
$XX:$	$P_1(x) = -x^2,$	$P_2(x) = x^3,$	$P_3(x) = x^4,$	$P_4(x) = -x,$
$XXI:$	$P_1(x) = x^3,$	$P_2(x) = 0,$	$P_3(x) = x^2,$	$P_4(x) = -x,$
$XXII:$	$P_1(x) = x,$	$P_2(x) = x^3,$	$P_3(x) = x^2,$	$P_4(x) = -x.$

4.2 Configurações Proibidas para Cinco ou Mais Polinômios

Para o caso de $n = 2$ e $n = 3$ polinômios, foi mostrado que todas as $n!$ permutações geram configurações possíveis. Para o caso $n = 4$, o teorema de Kontsevich garante que existem duas, das 24 permutações, que são configurações proibidas. Mas o que acontece para n polinômios quando $n \geq 5$? Esta seção vai apresentar definições e resultados que objetivam responder a esta pergunta.

Inicialmente, serão apresentadas algumas definições envolvendo polinômios e permutações. Por se tratarem de definições pouco usuais elas serão acompanhadas de alguns exemplos ilustrativos.

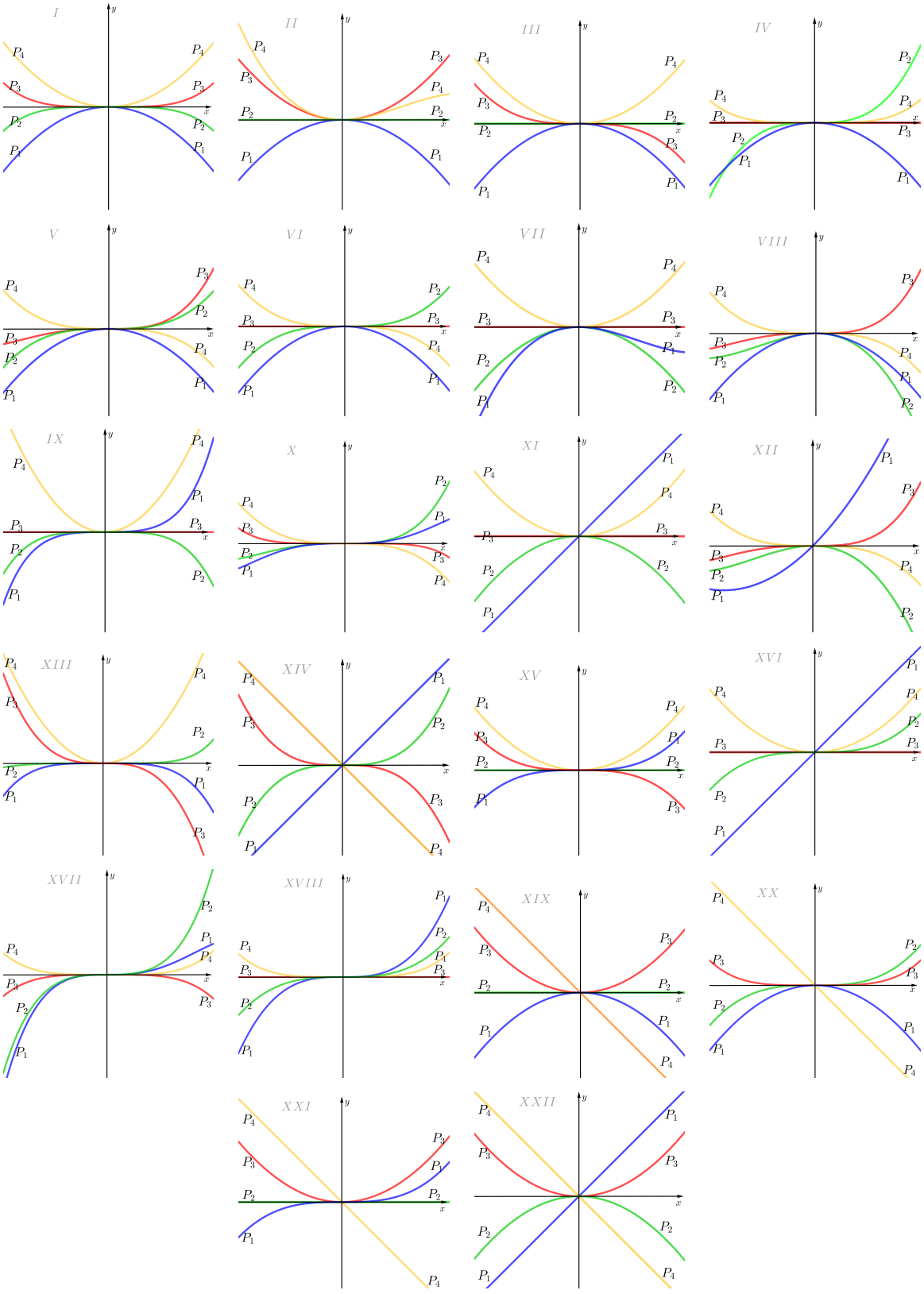

Figura 21: Configurações permitidas para 4 polinômios.

Definição 4.3 (Intercâmbio Polinomial)**.** *Seja $n \geq 2$ um número inteiro e π alguma permutação de $\{1, 2, \ldots, n\}$. Dizemos que π é um* ***intercâmbio polinomial*** *se existirem n polinômios $P_1, \ldots, P_n$ de modo que: $P_1(x) < P_2(x) < \ldots < P_n(x)$ para x pequeno e negativo e $P_{\pi(1)}(x) < P_{\pi(2)}(x) < \ldots < P_{\pi(n)}(x)$ para x pequeno e positivo.*

Exemplo 4.4. *Seja $n = 3$ e $\pi = (1, 2, 3)$ a permutação identidade. π é um intercâmbio polinomial, de fato, considere os polinômios $P_1(x) = x^2$, $P_2(x) = 2x^2$ e $P_3(x) = 3x^2$. Claro que $P_1(x) < P_2(x) < P_3(x)$ para x pequeno e negativo e $P_1(x) < P_2(x) < P_3(x)$ para x pequeno e positivo, como mostra a figura 22.*

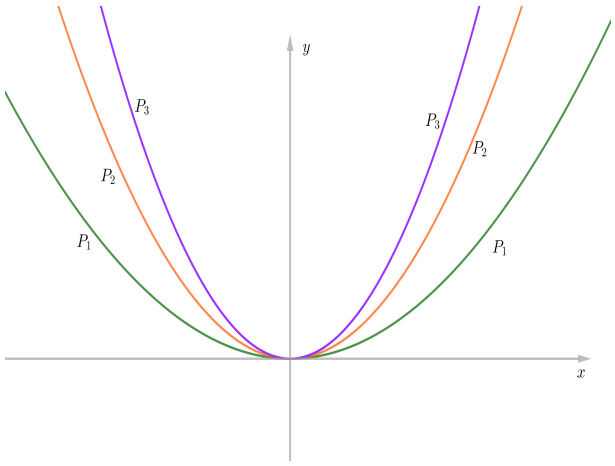

Figura 22: P_1,P_2 e P_3 formam um intercâmbio polinomial

Exemplo 4.5. *Vamos considerar os dez polinômios a seguir, escolhidos ao acaso.*

$$P_1(x) = 2x + 2x^2 - x^3 - x^4 + x^5 + x^6 \qquad P_6(x) = 2x^2 + 2x^3 - x^4 + 2x^5 + x^7 - x^8$$
$$P_2(x) = \tfrac{1}{2}x - x^2 + x^3 + 2x^4 + x^6 + x^7 - x^8 \qquad P_7(x) = -\tfrac{1}{2}x + x^2 + x^3 + x^4 + x^6 - 2x^8$$
$$P_3x = -x^2 - x^3 + x^4 - 2x^5 + 2x^6 \qquad P_8(x) = -x + x^3 + x^4 + x^5 - x^6 + x^7$$
$$P_4(x) = x^2 + x^3 + x^4 - 2x^5 + x^6 - x^7 + x^8 \qquad P_9(x) = -x + 2x^2 + 2x^3 + x^4 - x^5 + x^6 + x^7$$
$$P_5(x) = x^2 - x^3 + x^5 - x^6 + x^8 \qquad P_{10}(x) = -2x + x^2 + x^4 + 2x^5 + x^6 + x^7$$

Esses polinômios representam a configuração $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 10 & 8 & 9 & 7 & 3 & 5 & 4 & 6 & 2 & 1 \end{pmatrix}$ *das* 10! *possíveis de um intercâmbio polinomial com dez polinômios. A Figura 23 mostra seus gráficos.*

Definição 4.6. *Seja $n \geq 2$ um número inteiro e π alguma permutação de $\{1, 2, \ldots, n\}$. É dito que a permutação π contém a permutação $(2, 4, 1, 3)$ se existem inteiros $1 \leq i_1 < i_2 <$*

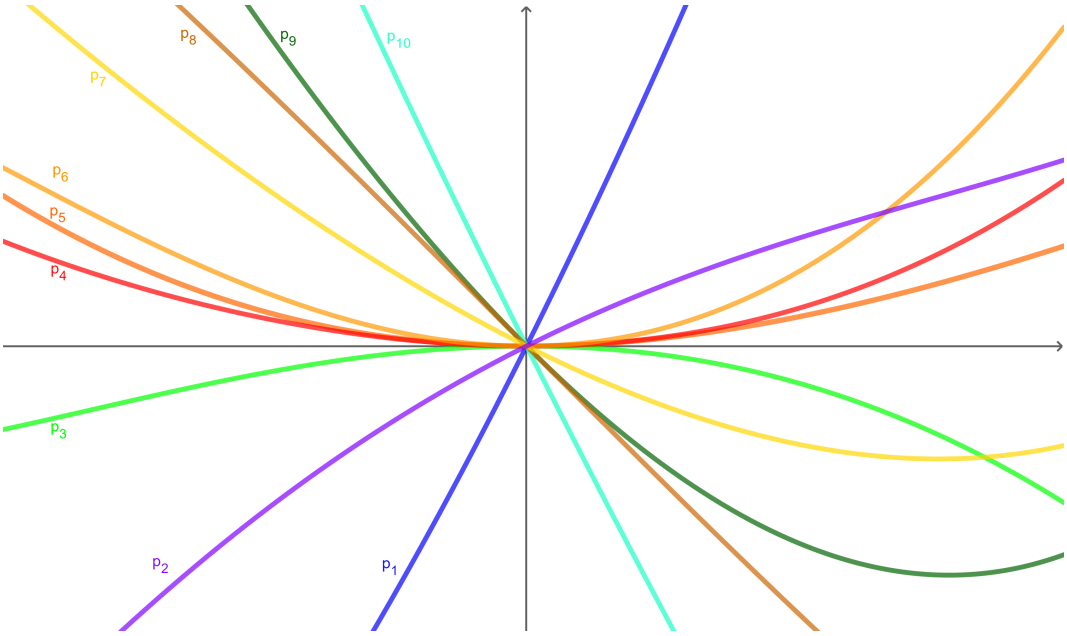

Figura 23: Representação gráfica de dez polinômios.

$i_3 < i_4 \leq n$ *tais que* $\pi(i_2) < \pi(i_4) < \pi(i_1) < \pi(i_3)$. *A definição é análoga se* π *contém a outra permutação proibida* $(3, 1, 4, 2)$.

Definição 4.7 (Permutação Separável)**.** *Seja* $n \geq 2$ *um número inteiro e* π *alguma permutação de* $\{1, 2, \ldots, n\}$. *A permutação* π *é dita separável se não contém uma das duas permutações proibidas de Kontesevich.*

Exemplo 4.8. *(Sorea, 2018) A permutação* $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 6 & 8 & 1 & 7 & 5 & 4 \end{pmatrix}$ *não é separável uma vez que contém a sub-permutação* $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$. *De fato, existem quatro índices* $i_1 = 2$, $i_2 = 3$, $i_3 = 5$ *e* $i_4 = 8$ *tais que:* $i_1 < i_2 < i_3 < i_4$ *e* $\sigma(i_3) < \sigma(i_1) < \sigma(i_4) < \sigma(i_2)$. *Veja figura 24.*

No contexto de permutações representando configurações de polinômios afins perto da origem, surge a necessidade de uma definição diferente para intervalo. A definição 4.9 apresenta uma definição de intervalo em um conjunto discreto que possui uma analogia com a definição de intervalo real.

Definição 4.9 (Intervalo)**.** *Considere o conjunto* $[n] = \{1, 2, \cdots, n\}$, *um* ***intervalo*** *de* $[n]$ *é um subconjunto* J *contendo uma sequência com dois ou mais inteiros consecutivos, isto é,* $J = \{i, i+1, \cdots, i+l\}$.

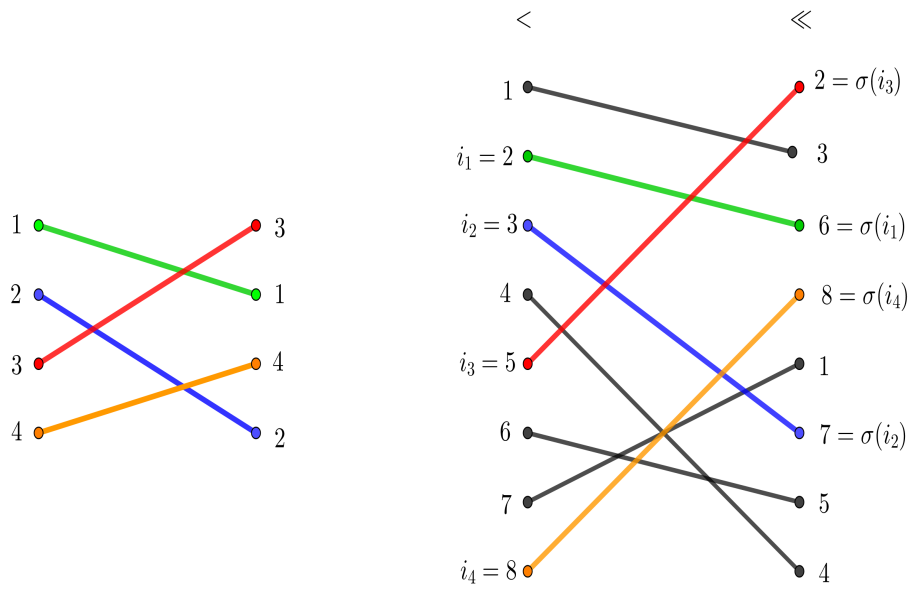

Figura 24: A permutação não separável contém uma das duas permutações proibidas.

O objetivo central desta seção é caracterizar os intercâmbios polinomiais para um valor qualquer de n. Essa caracterização é feita por meio do teorema 4.3, descrito ao final da seção. Para demonstrar o Teorema 4.3 são necessários os resultados dos Lemas 4.10 e 4.11.

Lema 4.10. *Seja π uma permutação separável de $\{1, 2, \ldots, n\}$ para $n \geq 3$. Então existe um intervalo próprio I de $[n]$ (I não pode ter apenas um elemento e $I \neq [n]$) cuja imagem $\pi(I)$ também é um intervalo de $[n]$.*

Demonstração. Sem perda de generalidade, pode-se assumir que $\pi(1) < \pi(2)$ pois, caso contrário, basta substituir π pela permutação $\overline{\pi}(k) = n + 1 - \pi(k)$.

Se $\pi(2) = \pi(1)+1$ o resultado do teorema será obtido pois a imagem de $\{1, 2\}$ é o intervalo $\{\pi(1), \pi(2)\}$.

Suponha, então, que $\pi(2) > \pi(1) + 1$. Seja k o menor número inteiro tal que a imagem do intervalo $J = \{1, 2, \ldots, k\}$, $\pi(J)$, contenha o intervalo $S = \{\pi(1), \cdots, \pi(2)\}$ (observe que podem haver elementos de $\pi(J)$ fora de S).

Se a imagem $\pi(J)$ for exatamente igual ao intervalo S, o teorema está demonstrado. Caso contrário, escolha um elemento l entre 1 e k ($1<l<k$), cuja imagem por π está fora de S. Veja a figura 25.

Se $\pi(l) < \pi(1)$, os quatro elementos $1 < 2 < l < k$ satisfazem $\pi(l) < \pi(1) < \pi(k) < \pi(2)$ e isso quer dizer que π contém uma das permutações proibidas. Mas isso é um absurdo, pois π é separável. Portanto, todos os elementos de $\pi(\{1, \ldots, k\})$ são maiores ou iguais a $\pi(1)$.

Suponha que $\pi(J)$ não é um intervalo, pois caso contrário, a demonstração está concluída. Neste caso, há pelo menos uma lacuna em $\pi(J)$, isto é, existe $m > k$ tal que $\pi(2) < \pi(m) < \pi(l)$. Mas os elementos $2 < l < k < m$ satisfazem $\pi(k) < \pi(2) < \pi(m) < \pi(l)$, o que gera uma permutação proibida em π, que é impossível. □

O Lema 4.10 será utilizado como ferramenta para demonstração do Lema 4.11. O Lema 4.11 afirma que existe um intervalo, cuja existência é garantida pelo Lema 4.10, de comprimento 2, cuja imagem é um intervalo de comprimento 2. Ele será utilizado para se demonstrar o Teorema 4.12, que apresenta uma caracterização para permutações que são intercâmbios polinomiais.

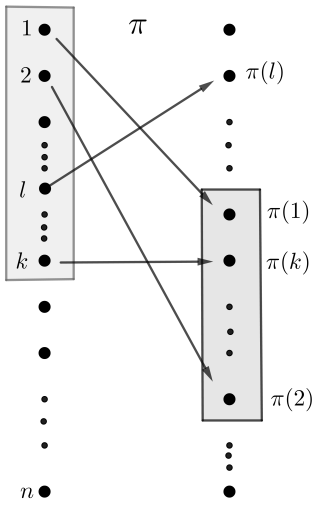

Figura 25: Esquema para facilitar a visualização do resultado do lema 4.1.

Lema 4.11. *Seja π uma permutação separável de $\{1, 2, \ldots, n\}$. Então existem dois números inteiros consecutivos cujas imagens são consecutivas.*

Demonstração. Pelo Lema 4.10 existe um intervalo J_1 tal que a imagem $\pi(J_1)$ também é um intervalo.

Seja π_1 a permutação induzida π restrita a J_1. Obviamente π_1 também é separável e, portanto, pode-se aplicar o Lema 4.10 na permutação π_1. Logo, existe um intervalo $J_2 \subset J_1$ tal que $\pi(J_2)$ é um intervalo.

Ao repetir esse procedimento recursivamente, pode-se garantir a existência de um inteiro k tal que J_k tem comprimento 2 e $\pi(J_k)$ é um intervalo. □

Observe que o Lema 4.11 garante que existe um inteiro a tal que $1 \leq a < a+1 \leq n$ e $\pi(\{a, a+1\})$ é um intervalo.

Será enunciado agora o Teorema 4.12, um dos principais resultados deste trabalho (juntamente com o Teorema 4.1). Ele faz uma caracterização das permutações que são intercâmbios polinomiais, ou seja, ele poderá responder se uma dada configuração de n polinômios afins, numa vizinhança da origem, é ou não proibida. Até o momento essa resposta é clara apenas se $n = 2$, 3 ou 4. Além disso, ele mostra que as permutações proibidas de Kontsevich são a chave para responder se uma dada configuração de n polinômios é ou não permitida.

Teorema 4.12. *Uma permutação é um intercâmbio polinomial se, e somente se, for separável.*

Demonstração. ($\Rightarrow$) Seja π um intercâmbio polinomial e suponha que π não seja separável, o que quer dizer que existem índices $i_1 < i_2 < i_3 < i_4$ tais que $\pi(i_2) < \pi(i_4) < \pi(i_1) < \pi(i_3)$. Na configuração de polinômios gerada por π apague todos os polinômios P_j, em que $j \neq i_k$, para $k = 1, 2, 3, 4$. Isso geraria uma configuração proibida, o que é absurdo. A demonstração é análoga para a outra permutação proibida.

($\Leftarrow$) Seja π uma permutação separável de $[n]$. Deseja-se mostrar que existem n polinômios $P_1(x) < \cdots < P_n(x)$ se $x < 0$ e pequeno tais que $P_{\pi(1)}(x) < \cdots < P_{\pi(n)}(x)$ se $x > 0$ e pequeno. Para isso será feita indução em n.

Se $n = 4$ o resultado é válido a partir da aplicação direta do teorema 4.1. Suponha o resultado válido para $n-1$. O Lema 4.11 garante que existe um inteiro a, $1 \leq a < n$, tal que $\{\pi(a), \pi(a+1)\}$ é um intervalo. Se $\{a, a+1\}$ e $\{\pi(a), \pi(a+1)\}$ forem colapsados em um único ponto, será produzida uma permutação $\pi^{'}$ de $n-1$ elementos. A permutação π' é obviamente separável e, portanto, um intercâmbio polinomial por hipótese de indução. Logo existem $n-1$ polinômios afins

$$P_1, \ldots, P_{n-1}$$

que se interceptam na origem de acordo com π'.

O i-ésimo polinômio P_i de $P_1, \ldots, P_{n-1}$ pode ser dividido em dois a fim de produzir n polinômios

$$P_1, \ldots, P_{i-1}, P_i', P_i'', P_{i+1}, \ldots, P_{n-1}$$

que se cruzam de acordo com π. Para isso, basta definir $P_i'(x) = P_i(x)$ e $P_i''(x) = P_i(x) + (-x)^N$ para um valor suficientemente grande de N tal que $N \gg max\{v(P_k)\}$, $k = 1, \cdots, n-1$, onde $v(P_k)$ denota a valuação do polinômio P_k. Note que, perto da origem P_i' e P_i'' são muito próximos. Além disso, se N for par, segue que $\pi(i+1) > \pi(i)$ e, se N for ímpar, $\pi(i+1) < \pi(i)$. Com isso, conclui-se que é um intercâmbio polinomial, como desejado.

□

O Lema 4.11 juntamente com o Teorema 4.12 fornecem um simples algoritmo para responder se uma dada configuração de n polinômios afins é proibida ou permitida, como pode ser visto abaixo.

Algoritmo 1:

Seja π a permutação de $[n]$ associada a configuração de polinômios dada.

(1) Procure por dois inteiros consecutivos cujas imagens sejam consecutivas.

(2) Encontrou?

   i. Sim $\rightarrow$ Colapse esses dois pontos, gerando uma sequência de $n-1$ elementos e volte ao passo (1).

   ii. Não $\rightarrow$ π não é um intercâmbio polinomial.

Responder se uma dada configuração de n polinômios na origem é ou não permitida parecia ser um processo complicado. Entretanto o algoritmo 1, de complexidade quadrática, exibe uma forma simples e eficiente de se resolver o problema.

Para finalizar este trabalho vale destacar a importância das permutações proibidas de Kontsevich, $(2,4,1,3)$ e $(3,1,4,2)$ no estudo das configurações de polinômios na origem. A partir de duas permutações particulares de [4] pode-se concluir resultados sobre configurações de um número qualquer de polinômios. Mas, o quê essas permutações têm de tão especial? Isso, sem dúvidas, é um dos extraordinários mistérios da matemática.

5 Aplicação do Teorema de Kontsevich no Ensino Médio

Esse capítulo finaliza este trabalho com duas propostas de atividades em sala de aula e tem o intuito de divulgar o resultado do Teorema de Kontsevich para o ensino médio prezando pela excelência no ensino da matemática.

5.1 Proposta 1: Permutações e as Configurações de Polinômios

São propostos cinco exercícios envolvendo permutações e configurações de polinômios afins. A ideia é aplicar essa proposta logo após o tema Permutações ser abordado aos alunos. Esses exercícios podem ser todos propostos em uma única aula, sendo que do 5.1 ao 5.4 os alunos são capazes de resolver em sala de aula. Após essa etapa, deve-se enunciar e dar a ideia da demonstração do Teorema de Kontsevich e, em seguida, enunciar o Teorema 4.12. Os exercícios 5.5 e 5.6 devem ser deixados com atividade para fazer em casa. Espera-se uma dificuldade maior para a realização do exercício 5.6. Na aula seguinte o professor deve fazer alguns exemplos propostos do exercício 5.5 e apresentar o algoritmo 1 como ferramenta para resolver o exemplo 5.6.

Exercício 5.1 (Situação problema)**.** *Três pessoas entram em uma lanchonete que só tem uma porta de acesso.*

Elas têm garantia de sair do outro lado da mesma maneira?

Podemos permutá-las?

E se pudermos permutá-las, todas as permutações são possíveis?

Quantas são possíveis?

E se fossem três polinômios passando pela origem, se aproximando-se de $(0, 0)$ *pela esquerda: geometricamente, um polinômio deve estar no topo, um na parte inferior e um no meio. Quantas configurações são possíveis ao lado direito da origem?*

Exercício 5.2. *(a) Quantas permutações são possíveis para os elementos* P_1 *e* P_2*?*

(b) Quantas permutações são possíveis para os elementos P_1*,* P_2 *e* P_3*?*

(c) Quantas permutações são possíveis para os elementos P_1*,* P_2*,* P_3 *e* P_4*?*

Exercício 5.3. *(a) Sejam* P_1 *e* P_2 *dois polinômios afins, isto é, polinômios que passam pela origem. Podemos associar as possíveis configurações desses polinômios na origem*

com as permutações de P_1 e P_2 (explicar essa associação verbalmente e com o uso do quadro).

Quantas são as configurações possíveis dos polinômios P_1 e P_2?

(b) Encontre exemplos de polinômios afins que satisfazem as configurações encontradas em (a).

Exercício 5.4. *(a) Sejam P_1, P_2 e P_3 três polinômios afins. Quantas são as possíveis configurações na origem?*

(b) Para cada uma das configurações encontrada em (a), encontre exemplos de três polinômios que as satisfaçam.

Exercício 5.5. *(a) Considere quatro polinômios afins P_1, P_2, P_3 e P_4. Quantas são as possíveis configurações na origem?*

(b) Existe alguma configuração impossível de se obter (Enunciar e dar a ideia da demonstração do Teorema de Kontesevich)?

(c) Mostre que as 22 permutações restantes de $1, 2, 3, 4$ ocorrem para escolhas adequadas de 4 polinômios P_1, P_2, P_3 e P_4.

Exercício 5.6. *(a) Quantas são as permutações de 5 elementos? Dessas será que todas representam configurações de polinômios na origem?*

(b) Dada uma permutação de cinco elementos, como detectar se ela é ou não possível de obter? (Explicar o algoritmo 1 apresentado ao final do capítulo 4)?

5.2 Proposta 2: Permutações Ordenadas por Pilha

No capítulo 4, permutações em S_n foram associadas a configurações de polinômios na origem e, nesse contexto, o teorema de Kontsevich exibe, quando $n = 4$, duas permutações ditas proibidas. A partir do resultado obtido para $n = 4$, pode-se deduzir um resultado mais geral para qualquer valor de $n > 4$.

Algo semelhante acontece ao associar permutações em S_n a sorteios de pilhas. Entretanto, neste caso, ocorrem permutações proibidas para o caso $n = 3$ e essas permutações permitem deduzir resultados para o caso geral $n > 3$. Devido a semelhança desse fenômeno com o

fenômeno de Kontsevich, este problema é proposto, neste capítulo, como divulgação e motivação da teoria desenvolvida neste trabalho. Além disso, trata-se de um problema bastante interessante e belo, havendo, dessa forma, grande chance de despertar grande interesse por parte de alunos do ensino médio.

A teoria dos padrões de permutação recebeu um forte impulso de um exercício no volume 1 de A arte da programação de computadores de Donald Knuth. O exercício está rotulado como $M28$. O M significa que ele é destinado a leitores matematicamente inclinados e o 28 é uma indicação do tempo necessário para resolvê-lo. Este exercício teve uma influência duradoura sobre combinatória e sua ideia será explicada em seguida.

Uma permutação ordenada por pilha, ou por sorteio de pilhas, é obtida por meio do seguinte método:

(1) Posicione os elementos do conjunto $1, 2, \ldots, n$, em uma linha horizontal, nesta ordem da esquerda para a direita. Suponha que a direita de n, há uma pilha, isto é, um tipo de poço estreito e fundo, em que os objetos podem ser empilhados uns sobre os outros. As figuras 26 e 27 podem ajudar a compreender melhor a definição de pilha. Inicialmente, a pilha está vazia. O primeiro passo consiste em alocar o elemento n dentro da pilha.

(2) O passo seguinte consiste em aplicar na sequência de números um dos movimentos: *Push* ou *Pop*.

- Push: Termo do inglês que significa empurre. Essa aplicação consiste em empurrar os números da esquerda para a direita, de modo que o elemento mais próximo da pilha, à esquerda, caia sobre a pilha, empilhado sobre os demais elementos lá existentes.
- Pop: Termo do inglês que significa estoure ou estale. Essa aplicação consiste em retirar o elemento do topo da pilha e colocá-lo na linha horizontal a direita da pilha.

(3) Volte ao passo 2 até que os n elementos estejam sobre a linha horizontal, ao lado direito da pilha.

Definição 5.7. *Uma permutação p é dita ordenada por pilha se for o resultado de uma sequência de Push e Pop aplicada a $\{1, 2, \ldots, n\}$.*

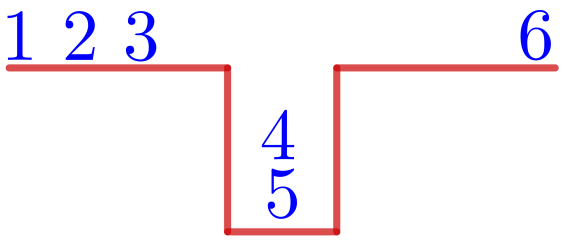

Figura 26: Sorteio de pilha com 6 números.

O seguinte exemplo ilustra o procedimento de se obter uma permutação ordenada por pilha.

Exemplo 5.8. *Considere o conjunto* $[6] = \{1, 2, ..., 6\}$. *A permutação* $p = (3, 2, 1, 6, 4, 5) \in S_6$ *é ordenada por pilha, pois ela pode ser obtida a partir da seguinte sequência: Push, Push, Pop, Push, Pop, Pop, Push, Push, Push, Pop, Pop, Pop. Confira na figura 27.*

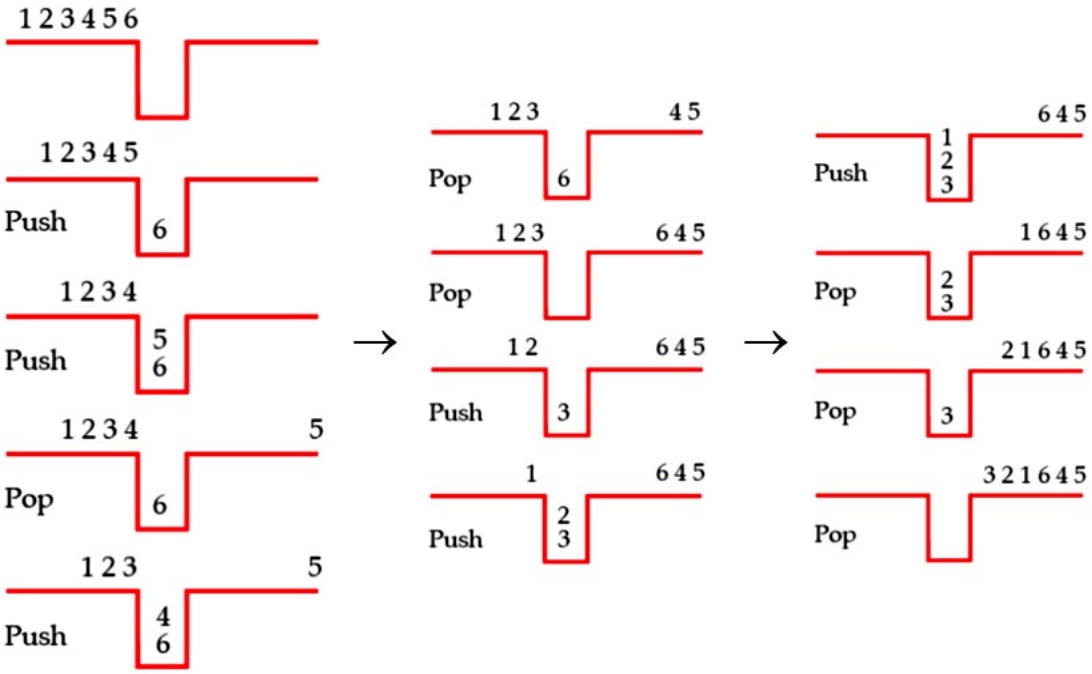

Figura 27: Sorteio de pilha.

Exercício 5.9. *(a) Quantos sorteios de pilha podemos obter da sequência de números* $\{1, 2, 3\}$*?*

(b) Existe alguma permutação impossível?

Exercício 5.10. *(a) Quantos sorteios de pilha podemos obter da sequência de números* $\{1, 2, 3, 4\}$*?*

(b) Quantas e quais são as permutações impossíveis?

Exercício 5.11. *(a) Quantos sorteios de pilha podemos obter da sequência de números* $\{1, 2, .., n\}$*?*

(b) Quando que uma permutação pode ser considerada impossível?

6 Conclusão

Essa dissertação apresentou o Teorema de Kontsevich, que exibe duas configurações impossíveis para os gráficos de quatro polinômios afins, em uma vizinhança da origem. As configurações proibidas de Kontsevich são usadas para classificar configurações impossíveis para os gráficos de cinco ou mais polinômios afins, perto da origem. Um algoritmo simples foi proposto para detectar as configurações proibidas dos gráfico de $n >= 4$ polinômios afins. Alguns conceitos sobre grupos de Permutações e polinômios foram introduzidos para uma melhor compreensão dos assuntos estudados. Foram elaboradas duas proposta de atividades para alunos do ensino médio: a primeira envolve conceitos de permutações, polinômios e o Teorema Kontsevich; e a segunda apresenta as permutações ordenadas por pilhas, tema lúdico que apresenta analogia ao Teorema de Kontesevich.

7 Agradecimentos

A Deus, pela oportunidade e que esteve presente em todos os momentos, auxiliando-me com força de vontade e dedicação para produzir este trabalho.

A minha família, em especial a minha mãe, por suas orações, e a minha namorada Edna, por sua força e paciência.

Aos amigos José Geraldo e Carlos, por tornarem o percurso mais leve e a distância menor, com muitas trocas de ideias e discussões proveitosas sobre tudo.

Aos colegas do PROFMAT, pelos momentos de descontração e companheirismo diante desse grande desafio.

A todos os professores do PROFMAT UFSJ, que contribuíram com minha formação pessoal compartilhando os seus conhecimentos.

À minha orientadora, Professora Amanda Gonçalves Saraiva Ottoni, pela paciência, dedicação, compromisso, presteza, pelos ensinamentos que contribuíram decisivamente para a

conclusão desta dissertação e meu ao coorientador Professor José Eloy Ottoni, pelas dicas tão preciosas que fizeram a diferença na construção deste trabalho.

Referências

[Andretti 2011] Andretti, Cinthia Marques V.: Ações de Grupos e Contagem: Teorema de Burnside. Monografia. In: *Universidade Federal de Santa Catarina* (2011)

[Araujo 2009] Araujo, Kalasas V.: Estruturas Algébricas II. In: *Universidade Federal de Sergipe* (2009)

[Biazzi 2014] Biazzi, Ricardo N.: Polinômios Irredutíveis: Critérios e Aplicações. In: *Universidade Estadual Paulista* (2014)

[Cançado 2016] Cançado, Ana P.: Grupo Diedral: O Estudo de Grupos de Simetrias em Polígonos Regulares. In: *Universidade Federal de São João del Rei* (2016)

[Coelho 2019] Coelho, Leonardo A.: Congruências e Aplicações em Polinômios. In: *Universidade Federal de São João del Rei* (2019)

[Firmo und Ottoni 2020] Firmo, Teresa ; Ottoni, Amanda: Problemas de Contagem: Os Teoremas de Burnside e Pólya. In: *Universidade Federal de São João del Rei* (2020)

[Garcia und Lequain 2003] Garcia, A ; Lequain, Y: *Elementos de Álgebra.* Rio de Janeiro, IMPA, 2003

[Ghys 2017] Ghys, Étienne: *A singular mathematical promenade.* ENS Éditions Lyon, 2017

[Gonçalves 1979] Gonçalves, Adilson: *Introdução à Álgebra.* IMPA, 1979

[Hefez 1993] Hefez, Abramo: *Curso de Álgebra, vol. 1.* Coleção Matemática Universitária, IMPA/CNPq, RJ, 1993

[Hefez 2002] Hefez, Abramo: *Curso de Álgebra, vol. 2.* 2002

[Iezzi 1977] Iezzi, Gelson: *Fundamentos de Matemática Elementar, vol. 6: Complexos.* Atual, São Paulo, 1977

[Iezzi u. a. 2002] Iezzi, Gelson ; Dolce, Osvaldo ; Degenszajn, David M. ; Périgo, Roberto: *Matemática: volume único*. Atual, 2002

[Janesch 2008] Janesch, Oscar R.: *Álgebra II*. UFSC/EAD, 2008

[Khan 2020] Khan, Academy: *Comportamento Final de Polinômios*. https://pt.khanacademy.org/math/algebra2. Novembro 2020. – Acesso: 16 de Novembro de 2020

[Marques 2019] Marques, Davi de S.: Teorema de Burnside e Algumas Aplicações de Contagem. In: *Universidade Federal de Viçosa* (2019)

[Monteiro 1969] Monteiro, Jacy: Elementos de Álgebra. In: *Rio de Janeiro, Livro Técnico e Científico* (1969)

[Morgado und Carvalho 2015] Morgado, Augusto C. ; Carvalho, Paulo Cezar P.: *Matemática Discreta*. Rio de Janeiro: Sociedade Brasileira de Matemática, Coleção PROFMAT, 2015

[Santos und Bovo 2004] Santos, José P. ; Bovo, Eduardo: O Teorema de Burnside e Aplicações. In: *Texto para minicurso na 2a. Bienal da SBM, Salvador* (2004)

[Sorea 2018] Sorea, Miruna S.: *The Shapes of Level Curves of Real Polynomials Near Strict Local Minima*, Dissertation, 2018

[Thomas 2009] Thomas, George B.: *Cálculo, vol. 1*. São Paulo: Addison Wesley, 2009

[Vieira 2011] Vieira, Ana C.: *Fundamentos de Álgebra, vol. 2*. CAED-UFMG, 2011