Álgebra Linear Avançada

Anéis de Polinômios

Daniel Miranda Machado

18 de Setembro

UFABC

Anel dos Polinômios

Anel

Um anel R é um conjunto com menos dois elementos, juntamente com duas operações: adição, denotada por $+$ e multiplicação, denotada por $\cdot$ ou pela concatenação, que satisfaz os três seguintes axiomas

- R1 o conjunto R forma um grupo abeliano em relação à adição e com elemento neutro o denominado **zero**,
- R2 é fechado em relação à multiplicação (por ser uma operação), a multiplicação é associativa, e existe um elemento **identidade**, denotado por 1, satisfazendo
  $1 \neq 0$ e
  $a1 = 1a = a$, para todos os $a \in R$.

R3 a multiplicação distribui sobre a adição, ou seja, se $a, b, c \in R$,

$$a(b+c) = ab + ac \quad \text{e} \quad (a+b)c = ac + b$$

Um anel R é dito **commutativo** se $ab = ba$ para todos os $a, b \in R$

Observe que diversos autores usam uma definição mais fraca de anel não exigindo a associatividade e a existência do elemento identidade para multiplicação.

Um elemento $a \in R$, diferente de zero, é dito divisor de zero caso exista $b \in R$, diferente de zero, tal que $ab = 0$.

Um **domínio de integridade** é um anel comutativo (com identidade) e sem divisores de zero.

Exemplos

1. Os **inteiros** com adição e multiplicação formam um anel comutativo indicado por $\mathbb{Z}$.
2. O conjunto das matrizes 2×2 com entradas reais, $M(2, \mathbb{R})$, com adição e multiplicação de matrizes, é um anel.

Consideramos brevemente dois subsistemas num anel: **subanel** e **ideal**, que desempenham apenas um papel menor neste livro.

Definição (Subanel e Ideal)

- *Dado um anel R, um subconjunto não vazio S de R é denominado **subanel** se for um anel com as operações de R.*
- *Um subconjunto não vazio I de R é denominado **ideal** de R*
  - *se $a, b \in I$, então $a + b \in I$*
  - *se $a \in R$ e $c \in I$, então $ac \in I$ e $ca \in I$ e*

Exemplos

- Se R é o anel de todas as matrizes reais de 2×2 e S é o subconjunto de matrizes triangulares superiores, então S é uma subanel;
- Se R é $\mathbb{Z}$ e $I = 7\mathbb{Z}$, I é o ideal de todos os números inteiros divisíveis por 7.
- O conjunto $\{0\}$ é ideal para todos os anéis R e 0 pertence a todos os ideais I.
- Se R for um corpo, os únicos ideais de R serão $\{0\}$ e R [se o I ideal contiver um elemento diferente de zero a, por exemplo, então $1 = aa^{-1} \in I$ e, portanto, $c = 1c \in I$ para todos os $c \in R$].

Definição (Ideal Gerado)

Se A é um conjunto qualquer de R, então definimos o ***ideal gerado*** *por A como o menor ideal de R contendo A. Ele está bem definido como a interseção de todos ideais que contém A e será denotado por $\langle A \rangle$.*

Pode-se provar que $\langle A \rangle$ é composto de todas as somas finitas da forma $r_1 a_1 + \ + r_n a_n$ com $r_i \in R$ e $a_i \in A$.

Definição (Domínio de Ideais Principais)

*Um **domínio de ideais principais** é um domínio de integridade no qual todo ideal é principal, ou seja, gerado por um único elemento.*

Definição (Polinômio)

Seja $\mathbb{K}$ um corpo. Por um ***polinômio*** *$p(x)$ com coeficientes em $\mathbb{K}$, queremos dizer uma expressão da forma $a_m x^m + a_{m-1} x^{m-1} + \cdots + a_1 x + a_0$, em que $a_i \in \mathbb{K}$ e x é um símbolo abstrato denominado variável. Os escalares a_i são os* ***coeficientes do polinômio*** *$p(x)$. O polinômio zero é o polinômio cujos coeficientes são zero. Denotamos esse polinômio por 0.*

Suponha $f(x) \neq 0$. O maior número natural k, de modo que o coeficiente a_k não seja zero, é chamado de **grau** de $f(x)$, denotado $\deg f(x)$ e o termo $a_k x^k$ é chamado de termo principal. Se o coeficiente do termo inicial for 1, diremos que o polinômio $f(x)$ é **mônico**.

Denotaremos por $\mathbb{K}[x]$ a coleção de todos os polinômios com entradas em $\mathbb{K}$ e por $\mathbb{K}_m[x]$ todos os polinômios de grau no máximo m.

O grau do polinômio zero é deixado indefinido ou então é definido como negativo (geralmente -1 ou $-\infty$).

Soma de Polinômios

Definição (Soma de Polinômios)

Seja $f(x)$ e $g(x)$ sejam dois polinômios de grau k e l, respectivamente. Defina $m = \max\{k, l\}$ e desta forma $f(x)$ e $g(x)$ estão em $\mathbb{K}_{(m)}[x]$. Podemos então escrevê-los como $f(x) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0$ e $g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0$. Então a soma de $f(x)$ e $g(x)$ é

$$f(x) + g(x) = (a_m + b_m)x^m + (a_{m-1} + b_{m-1})x^{m-1} + \cdots + (a_1 + b_1)x + (a_0 + b_0).$$

Multiplicação por Escalar

Definição (Multiplicação por Escalar)

Seja $f(x) = a_m x^m + a_{m-1} x^{m-1} + \cdots + a_1 x + a_0 \in \mathbb{K}[x]$ *e* $c \in \mathbb{K}$ *sejam escalares. Então* $c \cdot f(x) = (ca_m)x^m + (ca_{m-1})x^{m-1} + \cdots + (ca_1)x + (ca_0)$.

Multiplicação

Definição (Produto de Polinômios)

Seja $f(x) = a_m x^m + a_{m-1} x^{m-1} + \cdots + a_1 x + a_0$ *e* $g(x) = b_n x^n + b_{n-1} x^{n-1} + \cdots + b_1 x + b_0$ *seja polinômio com entradas em* $\mathbb{K}$. *Então o produto* $f(x)g(x)$ *é definido por*

$$f(x)g(x) = \sum_{l=0}^{m+n} \left(\sum_{j+k=l} a_j b_k \right) x^l.$$

Ou seja, para obter o coeficiente de x^l no produto, você multiplica todos os termos $a_j x^j$ e $b_k x^k$, onde $j + k = l$ e soma.

Suponha que $f(x) \neq 0$ tenha o termo inicial $a_m x^m$ e $g(x) \neq 0$ tenha o termo inicial $b_n x^n$. Então $f(x)g(x)$ tem o termo inicial $a_m b_n x^{m+n}$. Portanto, $f(x)g(x)$ é diferente de zero e possui um grau $m + n$.

Teorema

Seja $f, g, h \in \mathbb{K}[x]$. Então, vale o seguinte:

a. $(fg)h = f(gh)$. *A multiplicação de polinômios é associativa.*

b. $fg = gf$. *A multiplicação de polinômios é comutativa.*

c. *O polinômio* 1 *é uma identidade multiplicativa:* $1 \cdot f = f \cdot 1 = f$.

d. $(f + g)h = fh + gh$. *Multiplicação distribui sobre adição.*

e. *Se* $f(x)g(x) = 0$, *então* $f(x) = 0$ *ou* $g(x) = 0$

Como consequência dos teorema anteriores, podemos concluir $\mathbb{K}[x]$ é um anel comutativo com identidade sobre $\mathbb{K}$.

Proposição

Suponha que $f(x) \neq 0$ *e* $f(x)g(x) = f(x)h(x)$. *Então* $g(x) = h(x)$.

Teorema (Teorema da Divisão Euclidiana)

Sejam $\mathbb{K}$ um corpo, $f(x)$ e $g(x)$ dois polinômios em $\mathbb{K}[x]$, com $g(x) \neq 0$. Então existem $q(x), r(x) \in \mathbb{K}[x]$ unicamente determinados, tais que $f(x) = g(x)q(x) + r(x)$ onde $r(x) = 0$ ou $\deg r(x) < \deg g(x)$.

Corolário

Seja $\mathbb{K}$ um corpo. Então $\mathbb{K}[x]$ é um domínio de ideais principais.

Máximo Divisor Comum

Definição (Máximo Divisor Comum)

Dados $f(x), g(x) \in \mathbb{K}[x]$ definimos o ***máximo divisor comum*** *entre $f(x)$ e $g(x)$ como um gerador do ideal $\langle f(x), g(x) \rangle$.*

É imediato que dois mdc entre polinômios diferem por um produto por uma constante, isto é, se $d_1(x) = \text{mdc}(f(x), g(x))$ e $d_2(x) = \text{mdc}(f(x), g(x))$, então existe $u \in \mathbb{K}$ tal que $d_1(x) = ud_2(x)$. Portanto, para obtermos uma unicidade do mdc entre polinômios, podemos dizer que o mdc entre dois polinômios $f(x)$ e $g(x)$ é o gerador do ideal $\langle f(x), g(x) \rangle$, com termo líder unitário. Cabe aqui observar que um polinômio com termo líder unitário é dito **mônico**.

Identidade de Bezout

Lema (Identidade de Bézout)

Seja $d(x) = \text{mdc}(f(x), g(x))$ *em* $\mathbb{K}[x]$. *Então existem polinômios* $r(x)$ *e* $s(x)$ *tais que*

$$d(x) = f(x)r(x) + g(x)s(x)$$

Demonstração.

Todo elemento do ideal $d(x) \in \langle f(x), g(x) \rangle$ é da forma $d(x) = f(x)r(x) + g(x)s(x)$, em particular o gerador.

Raiz

Muitas vezes, queremos resolver equações polinomiais em um corpo, mas em muitos casos isso é impossível. Por exemplo, a equação polinomial $x^2 - 2 = 0$ não é solúvel em $\mathbb{Q}$, mas é solúvel em $\mathbb{R}$.

Definição (Raiz)

Seja $\mathbb{K}$ um corpo e $p(x)$ seja um polinômio com coeficientes em $\mathbb{K}$. Dizemos que $a \in \mathbb{K}$ é raiz de $p(x)$ se $p(a) = 0$.

O próximo resultado faz a conexão entre o problema de obter soluções de equações polinomiais e a teoria de fatoração polinômios:

Proposição

Sejam $\mathbb{K}$ um corpo, $f(x) \in \mathbb{K}[x]$ e $\alpha \in \mathbb{K}$. Então α é uma raiz de $f(x)$ se, e somente se, $(x - \alpha)$ divide $f(x)$.

Demonstração. Do Teorema da divisão Euclidiana segue que existem polinômios $q(x)$ e $r(x)$ em $\mathbb{K}[x]$ tais que $f(x) = (x - \alpha)q(x) + r(x)$, onde $r(x) = 0$ ou $\deg r(x) < \deg(x - \alpha) = 1$. Portanto, podemos escrever $f(x) = (x - \alpha)q(x) + r_0$, onde $r_0 \in \mathbb{K}$. Calculando $f(x)$ em α, temos $f(\alpha) = (\alpha - \alpha)q(\alpha) + r_0$, de onde segue que $r_0 = f(\alpha)$. Assim, se $x - \alpha$ divide $f(x)$, então $f(\alpha) = 0$, e reciprocamente. $\triangleleft$

Definição (Multiplicidade da Raiz)

Um elemento $\alpha \in \mathbb{K}$ é dito uma ***raiz de multiplicidade*** *k de $p(x)$ se houver um polinômio $s(x)$ tal que $s(\alpha) \neq 0$ e $p(x) = (x - \alpha)^k s(x)$. Quando $k = 1$, α é dito* ***raiz simples*** *e quando $k \geq 2$ α é dito* ***raiz múltipla****.*

Podemos definir uma derivada formal em $\mathbb{K}[x]$. Se $p(x) = \sum_{i=0}^{n} a_i x^i$, fazemos $= p'(x) = \sum_{i=1}^{n} i a_i x^{i-1}$.

Proposição

Seja $p(x) \in \mathbb{K}[x]$. Então α é uma raiz de multiplicidade m de $p(x)$ se e somente se $p^{(m-1)}(\alpha) = 0$ mas $p^{(m)}(\alpha) \neq 0$, onde $p^{(k)}(x)$ denota a k-ésima derivada de $p(x)$.

Teorema

Sejam $\mathbb{K}$ um corpo e $f(x) \in \mathbb{K}[x]$ um polinômio de grau n. Então $f(x)$ possui no máximo n raízes em $\mathbb{K}$.

Definição (Algebricamente Fechado)

Dizemos que um corpo$\mathbb{K}$ é algebricamente fechado se todo polinômio $f(x)$ em $\mathbb{K}[x]$ possui uma raiz em $\mathbb{K}$.

Teorema (Teorema Fundamental da Álgebra)

Todo polinômio $f(x) \in \mathbb{C}[x]$ possui uma raiz em $\mathbb{C}$.

Teorema

Sejam $\mathbb{K}$ um corpo algebricamente fechado e $f(x) \in \mathbb{K}[x]$ um polinômio de grau n. Então $f(x)$ se fatora em um produto de fatores lineares:

$$f(x) = c(x - \alpha_1)(x - \alpha_2)...(x - \alpha_n)$$

onde $\alpha i \in \mathbb{K}$ são as raízes de $f(x)$ em $\mathbb{K}$, e $c \in \mathbb{K}$ é o coeficiente líder do polinômio $f(x)$.

Comentários Finais.

Sejam D um domínio e $f(x) \in D[x]$ um polinômio não invertível. Dizemos que $f(x)$ é irredutível em $D[x]$, se $f(x)$ só admite fatoração trivial, isto é, se $f(x) = g(x)h(x)$, então $h(x)$ é invertível em $D[x]$ ou $g(x)$ é invertível em $D[x]$.

Caso contrário, dizemos que $f(x)$ é redutível em $D[x]$.

No caso particular em que o domínio D é um corpo, podemos dizer que $f(x)$ é um polinômio irredutível em $D[x]$, se o fato de $f(x) = g(x)h(x)$, implicar em $\deg g(x) = 0$ ou $\deg h(x) = 0$, pois os únicos elementos invertíveis nestes anéis são exatamente os polinômios de grau zero.

Se $\mathbb{K}$ é um corpo algebricamente fechado, então segue do Teorema Fundamental da álgebra que todo polinômio se fatora em produto de polinômios irredutíveis.

Lema

Seja D um domínio de ideais principais. Se $p, a, b \in D$ são tais que p é irredutível em D e $p|ab$, então $p|a$ ou $p|b$.

Demonstração. Suponhamos $p|ab$, isto é, $ab \in pD$. Se $p|a$, então $a \in pD$ e, como p é irredutível em D, segue que pD é um ideal maximal, ou seja, $pD + aD = D$. Portanto, existem elementos $x, y \in D$ tais que $px + ay = 1$. Multiplicando agora esta última igualdade por b, obtemos $b = b.1 = b(px + ay) = pbx + aby$ de onde segue que $b \in pD$, pois $pbx, aby \in pD$. Logo, temos que $p|b$. ◁

Teorema (Teorema de Fatoração Única)

Dado $f(x) \in \mathbb{K}[x]$, onde $\mathbb{K}$ é um corpo e $\deg f(x) \geq 1$. Então existem polinômios irredutíveis mônicos $p_1(x), p_2(x), ..., p_t(x)$ unicamente determinados e $u \in \mathbb{K}$ tais que

$$f(x) = up_1(x)p_2(x)...p_t(x)$$

com $\deg p_1(x) \leq \deg p_2(x) \leq \cdots \leq \deg p_t(x)$.

Proposição

Sejam $\mathbb{K}$ um corpo e $f(x)$ um polinômio em $\mathbb{K}[x]$ de grau igual a dois ou três. Então $f(x)$ é irredutível se, e somente se, $f(x)$ não possui raízes em $\mathbb{K}$.

Demonstração. Consideremos inicialmente $\deg f(x) = 2$. Suponhamos $f(x) = g(x)h(x)$, onde $g(x), h(x) \in \mathbb{K}[x]$. Assim, temos $\deg g(x) + \deg h(x) = 2$, de onde decorre que $\deg g(x) = 0$ e $\deg h(x) = 2$, ou $\deg g(x) = 1$ e $\deg h(x) = 1$ ou $\deg g(x) = 2$ e $\deg h(x) = 0$. Se ocorrer o caso em que $\deg g(x) = \deg h(x) = 1$, então estes polinômios possuem raízes em$\mathbb{K}$ e estas são raízes de $f(x)$. As outras duas situações produzem fatorações triviais. Suponhamos agora que $\deg f(x) = 3$. Pelo mesmo tipo de argumento acima, $f(x) = g(x)h(x)$ é uma fatoração não trivial em $\mathbb{K}[x]$ se, e somente se, $\deg g(x) = 1$ ou $\deg h(x) = 1$, isto é, se, e somente se, $g(x)$ tem uma raiz em $\mathbb{K}$ ou $h(x)$ tem uma raiz em $\mathbb{K}$. Isto completa a prova da Proposição. ◁

O critério acima não funciona em grau 4, como mostra o exemplo dado pelo polinômio $f(x) = x^4 + 3x^2 + 2$, que não possui raízes em $\mathbb{R}$, mas se fatora como $f(x) = (x^2 + 1)(x^2 + 2)$.

Passaremos a analisar separadamente a irredutibilidade em $\mathbb{R}[x]$, Para este caso, temos um teorema de classificação dos polinômios irredutíveis.

Teorema

Os únicos polinômios irredutíveis em $\mathbb{R}[x]$ são os lineares e os de grau dois que não possuem raízes em $\mathbb{R}$.

Pelo exposto acima, já sabemos que os polinômios lineares e os polinômios de grau dois que não possuem raízes em $\mathbb{R}$ são irredutíveis em $\mathbb{R}[x]$. O que temos que mostrar então é que estes são os únicos tais polinômios. Vamos fazer isto através de dois resultados auxiliares.

Primeiro observemos que se α é raiz de um polinômio de coeficientes reais então $\overline{\alpha}$ também é

Lema

Seja $f(x) = ax^2 + bx + c \in \mathbb{R}[x]$, com $a \neq 0$. Se $\alpha \in \mathbb{C}$ é uma raiz de $f(x)$, então $\overline{\alpha}$ também é uma raiz de $f(x)$.

Como consequência imediata deste lema, segue que as raízes complexas aparecem aos pares e, sendo assim, todo polinômio de grau ímpar com coeficientes reais tem pelo menos uma raiz real, de onde concluímos que são polinômios redutíveis em $\mathbb{R}[x]$. Falta então apenas analisar o caso dos polinômios de grau par e maior que dois. Para estes, temos o seguinte resultado.

Lema

Seja $f(x) \in \mathbb{R}[x]$ um polinômio com $\deg f(x)$ par e maior que 2, sem raízes em R. Então $f(x)$ possui pelo menos um fator irredutível de grau dois.

Demonstração. Seja $f(x)$ um polinômio como no enunciado deste Lema. Pelo Lema anterior, fatorando este polinômio em $\mathbb{C}[x]$, obtemos

$$f(x) = c(x - \alpha_1)(x - \alpha_1)...(x - \alpha k)(x - \alpha k)$$

Observamos agora que o produto $(x - \alpha)(x - \alpha)$, onde $\alpha = a + bi \in \mathbb{C}$, produz um polinômio com coeficientes reais, a saber,

$$(x - \alpha)(x - \alpha) = (x - (a + bi))(x - (a - bi)) = x^2 - 2ax + (a^2 + b^2)$$

Logo, o resultado segue. ◁

Supondo $f(x) = ax^2 + bx + c \in \mathbb{R}[x]$, com $a \neq 0$, chamamos $\Delta = b2 - 4ac$ o discriminante de $f(x)$. Assim, $f(x)$ não possui raízes em R se, e somente se, $\Delta < 0$. Resumindo tudo isto, podemos enunciar o seguinte

Teorema

Seja $f(x) \in \mathbb{R}[x]$. Então $f(x)$ é irredutível em $\mathbb{R}[x]$ se, e somente se, $\deg f(x) = 1$ *ou,* $\deg f(x) = 2$ *e o discriminante de $f(x)$ é negativo.*

Comentários Finais.