Corpos e Álgebra Linear Complexa

Álgebra Linear – Videoaula 23

Luiz Gustavo Cordeiro

Universidade Federal de Santa Catarina
Centro de Ciências Físicas e Matemáticas
Departamento de Matemática

Escalares diferentes?

- Por que consideramos números reais?
- Daria de fazer (quase) tudo com números racionais.
- Não dá da fazer tudo com números inteiros (pois dividimos).

Álgebra Linear pode ser feita com diferentes tipos de “escalares”.

Corpos

Um **corpo** é uma estrutura algébrica $(\mathbb{F}, +, \cdot, 0, 1)$ que satisfaz diversos axiomas: (como de costume, denota-se "$x \cdot y = xy$")

1. $x + (y + z) = (x + y) + z$
2. $x + y = y + x$
3. $x + 0 = x$
4. Para todo $x \in \mathbb{F}$, existe $-x \in \mathbb{F}$ com $x + (-x) = 0$
5. $x(yz) = (xy)z$
6. $xy = yx$
7. $x1 = x$
8. Para todo $x \neq 0$, existe x^{-1} tal que $xx^{-1} = 1$
9. $x(y + z) = xy + xz$.

Exemplos e contra-exemplos simples

Com as operações usuais:

- O conjunto $\mathbb{R}$ dos números reais é um corpo.
- O conjunto $\mathbb{Q}$ dos números racionais é um corpo.
- O conjunto $[0, \infty)$ dos números reais não-negativos não é um corpo: Falha a existência de opostos aditivos
- O conjunto $\mathbb{Z}$ dos inteiros não é um corpo: Fala a existência de inversos multiplicativos.

Exemplos legais

Com as operações usuais, $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ é um corpo.

O problema é verificar a existência de inversos multiplicativos:

$$\begin{aligned}
(a+b\sqrt{2})^{-1} &= \frac{1}{a+b\sqrt{2}} \\
&= \frac{1}{a+b\sqrt{2}} \cdot \frac{a-b\sqrt{2}}{a-b\sqrt{2}} \\
&= \frac{a-b\sqrt{2}}{a^2-2b^2} \\
&= \left(\frac{a}{a^2-2b^2}\right) + \left(\frac{-b}{a^2-2b^2}\right)\sqrt{2}
\end{aligned}$$

e $\frac{a}{a^2-2b^2}, \frac{-b}{a^2-2b^2} \in \mathbb{Q}$.

Contra-exemplos legais

O corpo com dois elementos é

$$\mathrm{GF}(2) = \{0, 1\}$$

Com as tabelas de operação:

$$\begin{array}{c|cc} + & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 0 \end{array} \qquad \begin{array}{c|cc} \cdot & 0 & 1 \\ \hline 0 & 0 & 0 \\ 1 & 0 & 1 \end{array}$$

(são quase as operações normais, mas pomos $1 + 1 = 0$).

Este corpo é relacionado com "tabelas verdade": Se reescrevermos $0 = F$ e $1 = V$, podemos ver a multiplicação o produto como conjunção lógica ("$\ldots \mathrm{e} \ldots$") e a soma como disjunção lógica exclusiva ("$\mathrm{ou} \ldots \mathrm{ou} \ldots$")

Contra-exemplos legais

ou . . . ou . . .	F	V
F	F	V
V	V	F

. . . e . . .	F	V
F	F	F
V	F	V

A definição correta de um espaço vetorial

Definição

Se $\mathbb{F}$ é um corpo, então um **espaço vetorial** SOBRE $\mathbb{F}$ consiste de um espaço conjunto V com duas operações (soma e produto por escalar)

$$+: \begin{array}{ccc} V \times V & \longrightarrow & V \\ (u, v) & \longmapsto & u + v \end{array} \qquad \cdot: \begin{array}{ccc} \mathbb{F} \times V & \longrightarrow & V \\ (\alpha, v) & \longmapsto & \alpha v \end{array}$$

satisfazendo aos mesmos axiomas de espaços vetoriais como vimos na primeira aula.

Nós temos visto espaços vetoriais sobre $\mathbb{R}$, também chamados de espaços vetoriais reais.

Exercício

Verifique que toda a teoria desenvolvida antes da parte de produtos internos pode ser feita para espaços vetoriais sobre corpos arbitrários.

Um número complexo é uma expressão da forma

$$z = a + bi,$$

onde $a, b \in \mathbb{R}$ e i é a **unidade imaginária**.

- a é a parte real de z, denotada $a = \mathrm{Re}(z)$
- b é a parte imaginária de z, denotada $b = \mathrm{Im}(z)$.

O conjunto de todos os números complexos é $\mathbb{C}$.

- Se $\mathrm{Im}(z) = 0$, então $z = a + 0i = a$ é real.
- Se $\mathrm{Re}(z) = 0$, então $z = 0 + bi = bi$ é imaginário puro.

Números complexos
Operações simbólicas: soma e produto

A soma e multiplicação de números complexos são feitas como se fossem números reais (com distributividade, associatividade, etc.), e com a seguinte regra:

$$i^2 = -1.$$

Então, se $z = a + bi$, $w = c + di$,

$$\begin{aligned} z + w &= (a + di) + (c + di) \\ &= (a + c) + (b + d)i \end{aligned}$$

$$\begin{aligned} zw &= (a + bi)(c + di) \\ &= ac + adi + bic + bidi \\ &= ac + adi + bci + bdi^2 \\ &= ac + (ad + bc)i - bd \\ &= (ac - bd) + (ad + bc)i \end{aligned}$$

Se $z = 2 + 3i$ e $w = 1 - i$, então

$$\begin{aligned} z + w &= (2 + 3i) + (1 - i) \\ &= (2 + 1) + (3 - 1)i \\ &= 3 + 2i \end{aligned}$$

$$\begin{aligned} zw &= (2 + 3i)(1 - i) \\ &= 2 - 2i + 3i - 3i^2 \\ &= 2 + i - 3(-1) \\ &= 2 + 3 + i \\ &= 5 + i \end{aligned}$$

Se $z = a + bi$ e $w = c + di$, então

$$\begin{aligned} z - w &= (a + bi) - (c + di) \\ &= (a - c) + (b - d)i \end{aligned}$$

$$\begin{aligned} \frac{z}{w} &= \frac{a + bi}{c + di} \cdot \frac{c - di}{c - di} \\ &= \frac{(ac - bd) + (ad + bc)i}{c^2 - (id)^2} \\ &= \frac{(ac - bd) + (ad + bc)i}{c^2 + d^2} \\ &= \left(\frac{ac - bd}{c^2 + d^2}\right) + \left(\frac{ad + bc}{c^2 + d^2}\right) i \end{aligned}$$

Se $z = 2 + 3i$ e $w = 1 - i$, então

$$\begin{aligned} z - w &= (2 + 3i) - (1 - i) \\ &= 1 + 4i \end{aligned}$$

$$\begin{aligned} \frac{z}{w} &= \frac{2 + 3i}{1 - i} \cdot \frac{1 + i}{1 + 1} \\ &= \frac{(2 - 3) + (2 + 3)i}{1^2 - i^2} \\ &= \frac{-1 + 5i}{2} \\ &= -\frac{1}{2} + \frac{5}{2}i \end{aligned}$$

Formalmente, $\mathbb{C} = \mathbb{R}^2$ com operações

$$\begin{aligned}(a, b) + (c, d) &= (a + c, b + d)\\ (a, b)(c, d) &= (ac - bd, ad + bc)\end{aligned}$$

e utilizamos a notação $a + bi = (a, b)$.

$$\begin{aligned}(a + bi) + (c + di) &= (a + c) + (b + d)i\\ (a + bi)(c + di) &= (ac - bd) + (ad + bc)i\end{aligned}$$

Fato

$\mathbb{C}$ é um corpo.

Conjugação

Definição

O **conjugado** de um número complexo $z = a + bi$ (onde $a, b \in \mathbb{R}$) é o número complexo

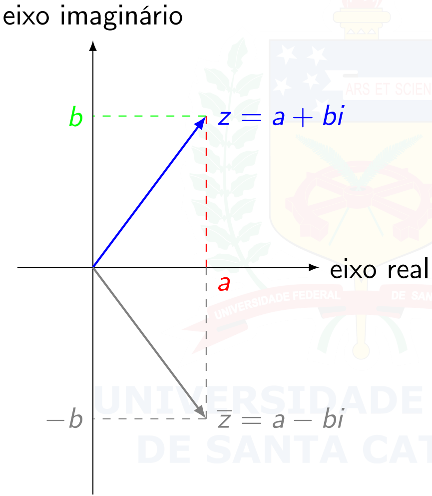
$$\overline{z} = a - bi.$$

Exemplo

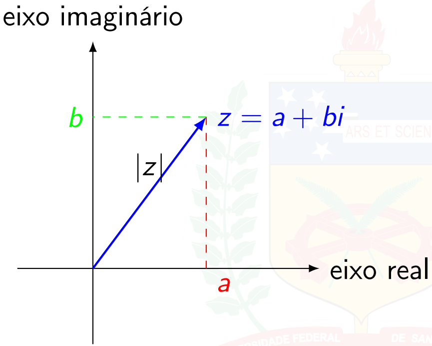
- $\overline{-3 + 4i} = -3 - 4i$
- $\overline{2 - 5i} = 2 + 5i$

Geometria de $\mathbb{C}$

Formalmente, $\mathbb{C} \approx \mathbb{R}^2$, o que dá uma geometria:



Geometria de $\mathbb{C}$



Definição

O **módulo** ou **valor absoluto** de um número complexo $z = a + bi$ é

$$|z| = \sqrt{a^2 + b^2}$$

Proposição (Propriedades algébricas de $\mathbb{C}$)

Se $z, w \in \mathbb{C}$, então are complex numbers, then

- $z = \overline{z} \iff z \in \mathbb{R}$
- $z = -\overline{z} \iff z$ é imaginário puro
- $z + \overline{z} = 2\,\mathrm{Re}(z)$
- $z - \overline{z} = 2i\,\mathrm{Im}(z)$
- $\overline{z + w} = \overline{z} + \overline{w}$
- $\overline{zw} = \overline{z} \cdot \overline{w}$
- $|zw| = |z| \cdot |w|$
- (desigualdade triangular) $|z + w| \leq |z| + |w|$
- $\overline{z}z = z\overline{z} = |z|^2 \geq 0$

Álgebra Linear complexa

Toda a parte puramente algébrica (sem produtos internos) podem $\mathbb{C}$ no lugar de $\mathbb{R}$

- Equações com coeficientes complexos
- Matrizes complexas
- $\mathbb{C}^n$ no lugar de $\mathbb{R}^n$
- etc.

O Teorema Fundamental da Álgebra

Teorema (Teorema fundamental da Álgebra, versão 1)

Todo polinômio complexo tem raiz.

Teorema (Teorema fundamental da Álgebra, versão 2)

Todo polinômio complexo não-nulo pode ser completamente fatorado, na forma

$$p(x) = C(x - \lambda_1)(x - \lambda_2)\cdots(x - \lambda_n)$$

onde $C, \lambda_1, \ldots, \lambda_n \in \mathbb{C}$.

Exemplo

O polinômio real $p(x) = x^2 + 1 = (x - i)(x + i)$ pode ser fatorado em $\mathbb{C}$, mas não em $\mathbb{R}$.

Espaços vetoriais complexos

Definição

Um espaço vetorial **complexo** consiste de um espaço conjunto V com duas operações (soma e produto por escalar)

$$+: \begin{array}{ccc} V \times V & \longrightarrow & V \\ (u, v) & \longmapsto & u + v \end{array} \qquad \cdot: \begin{array}{ccc} \mathbb{C} \times V & \longrightarrow & V \\ (\alpha, v) & \longmapsto & \alpha v \end{array}$$

satisfazendo aos mesmos axiomas de espaços vetoriais como vimos na primeira aula.

Importante

Todo espaço vetorial complexo pode ser visto como espaço vetorial real, restringindo a multiplicação por escalar.

Mas as noções de conjuntos linearmente dependentes/independentes/geradores, bases e dimensão mudam!

Exemplo

Seja $\mathbb{C}$ como espaço complexo com a estrutura usual. Então $\{1, i\}$ é LD sobre $\mathbb{C}$, pois $i = i \cdot 1$.
Mas com $\mathbb{C}$ como espaço real, $\{1, i\}$ é LI.

Transformações conjugado-lineares

Um isomorfismo linear $T\colon V \to W$ entre espaços vetoriais complexos é linear se

$$T(v + \alpha w) = T(v) = \alpha T(w).$$

Mas dizemos que T é **conjugado-linear** ou **anti-linear** se

$$T(v + \alpha w) = T(v) + \overline{\alpha} T(w)$$

Produtos internos complexos

Definição

Um **produto interno** em um espaço vetorial complexo V é uma função

$$\langle \cdot, \cdot \rangle \colon V \times V \to \mathbb{R}, \qquad (v, w) \mapsto \langle v, w \rangle$$

satisfazendo às seguinte propriedades:

- (Linearidade na primeira entrada) Para todos $u, v, b \in V$ e $\lambda \in \mathbb{R}$,
$$\langle u + \lambda v, b \rangle = \langle u, b \rangle + \lambda \langle v, b \rangle.$$
- (Simetria conjugada) Para todos $u, v \in V$,
$$\langle u, v \rangle = \overline{\langle v, u \rangle}.$$
- (Positividade estrita) Para qualquer $v \neq 0_V$,
$$\langle v, v \rangle > 0.$$

Linearidade entrada-a-entrada

Um produto interno $\langle \cdot, \cdot \rangle$ complexo é

- Linear na primeira entrada:

$$\langle u + \alpha v, w \rangle = \langle u, w \rangle + \alpha \langle v, w \rangle.$$

- Conjugado-linear na segunda entrada:

$$\langle w, u + \alpha v \rangle = \langle w, u \rangle + \overline{\alpha} \langle w, v \rangle.$$

Exemplo

Em $\mathbb{C}^n$, o produto escalar usual é

$$(z_1, \ldots, z_n)(w_1, \ldots, w_n) = \sum_{i=1}^{n} z_i \overline{w_i}$$

Norma

A **norma** em um EPI complexo é definida do modo normal:

$$\|v\| = \sqrt{\langle v, v\rangle}.$$

Mas no caso complexo, a norma de uma soma satisfaz

$$\|u+v\|^2 = \|u\|^2 + 2\,\mathrm{Re}(\langle u, v\rangle) + \|v\|^2.$$

Representação de Riesz

Dado um espaço complexo V, definimos $V^* = \mathrm{L}(V, \mathbb{C})$ o espaço dos funcionais lineares $V \to \mathbb{C}$.

Teorema (Representação de Riesz complexa)

Seja V um EPI complexo de dimensão finita. A transformação

$$\tau\colon V \to V^*, \qquad \tau(v) = \langle \cdot, v \rangle$$

é um isomorfismo conjugado-linear.

Adjuntas complexas

Se $T \in \mathrm{L}(V, W)$ é uma transformação linear entre EPIs complexos, a **adjunta** $T^* \in \mathrm{L}(W, V)$ também existe e satisfaz à mesma igualdade que no caso real:

$$\langle T(v), w \rangle = \langle v, T^*(w) \rangle$$

para quaisquer $v \in V$ e $w \in W$.

A única diferença é que a associação $T \mapsto T^*$ é conjugado-linear:

$$(T + \alpha S)^* = T^* + \overline{\alpha} S^*.$$

Matrizes adjuntas

Se $A \in \mathrm{M}_{m\times n}(\mathbb{C})$ é uma matriz complexa, a **adjunta** ou **Hermitiana** A^* de A é sua conjugada transposta:

$$\text{Se } A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}, \text{ então } A^* = \overline{A}^t = \begin{bmatrix} \overline{a_{11}} & \overline{a_{21}} & \cdots & \overline{a_{m1}} \\ \overline{a_{12}} & \overline{a_{22}} & \cdots & \overline{a_{m2}} \\ \vdots & \vdots & \ddots & \vdots \\ \overline{a_{1n}} & \overline{a_{2n}} & \cdots & \overline{a_{mn}} \end{bmatrix}.$$

Teorema

Com respeito a bases ortonormais em EPIs complexos, matrizes adjuntas correspondem a transformações adjuntas.

Matrizes adjuntas são o análogo correto para "transpostas" no caso complexo.

Transformações unitárias

Uma transformação linear $T \in \mathrm{L}(V, W)$ entre EPIs complexos é uma **isometria** se

$$\|T(v)\| = \|v\|$$

para todo $v \in V$, ou equivalentemente se

$$\langle T(v), T(w)\rangle = \langle v, w\rangle$$

para todos $v, w \in V$.

Isso equivale a dizer que $T^*T = \mathrm{id}_V$.

Isometrias inversíveis são chamadas de transformações **unitárias**.

Transformações unitárias

Uma matriz quadrada complexa $U \in \mathrm{M}_n(\mathbb{C})$ é **unitária** se $U^* = U^{-1}$.

Teorema

Para EPIs complexos de mesma dimensão finita, matrizes unitárias correspondem a transformações unitárias.

Teorema

Para EPIs complexos, matrizes unitárias são matrizes de mudança entre bases ortonormais.

Autovalores complexos

Corolário

Todo endomorfismo linear T em um espaço vetorial complexo de dimensão finita tem autovalor.

De fato, o polinômio característico $p_T(x)$ tem raiz.