Complementos de Matemática I

— Prof. Adriano Cattai —

Corpos Numéricos

(*Atualizada em 8 de março de 2016*)

Nome: ____ Data: ____/____/_______

> "Não há ciência que fale das harmonias da natureza com mais clareza do que a matemática"
> (Paulo Carus)

1 Definição de Corpo

Seja $\mathbb{K}$ um conjunto não vazio munido de duas operações,

$$\begin{array}{rccc} +: & \mathbb{K}\times\mathbb{K} & \to & \mathbb{K} \\ & (x,y) & \mapsto & x+y \end{array} \quad \text{e} \quad \begin{array}{rccc} \cdot: & \mathbb{K}\times\mathbb{K} & \to & \mathbb{K} \\ & (x,y) & \mapsto & x\cdot y \end{array}$$

chamadas *adição* e *multiplicação*, respectivamente. Diz-se que $\mathbb{K}$, em relação a estas operações, ou simplesmente $(\mathbb{K},+,\cdot)$, é um *corpo* se, e somente se, satisfazem os seguintes axiomas:

(i) A adição e a multiplicação são operações fechadas, ou seja,

$$x+y\in\mathbb{K} \ \text{ e } \ x\cdot y\in\mathbb{K}, \ \ \forall\, x,y\in\mathbb{K};$$

(ii) A adição e a multiplicação são comutativas, ou seja,

$$x+y=y+x \ \text{ e } \ x\cdot y=y\cdot x, \ \ \forall\, x,y\in\mathbb{K};$$

(iii) A adição e a multiplicação são associativas, ou seja,

$$x+(y+z)=(x+y)+z \ \text{ e } \ x\cdot(y\cdot z)=(x\cdot y)\cdot z, \ \ \forall\, x,y,z\in\mathbb{K};$$

(iv) Existe um único elemento 0 (zero) em $\mathbb{K}$ tal que

$$x+0=0+x=x, \ \ \forall\, x\in\mathbb{K}$$

denominado elemento neutro da adição;

(v) A cada elemento $x\in\mathbb{K}$ exixte um único elemento $-x$ (oposto) em $\mathbb{K}$, tal que

$$x+(-x)=-x+x=0, \ \ \forall\, x\in\mathbb{K};$$

(vi) Existe um único elemento 1 (um) em $\mathbb{K}$ tal que

$$1\cdot x=x\cdot 1=x, \ \ \forall\, x\in\mathbb{K}$$

denominado elemento neutro da multiplicação;

(vii) A cada elemento $x \in \mathbb{K} - \{0\}$ exixte um único elemento x^{-1} ou $\dfrac{1}{x}$ em $\mathbb{K} - \{0\}$, tal que

$$x \cdot x^{-1} = x^{-1} \cdot x = 1, \;\; \forall\, x \in \mathbb{K} - \{0\};$$

denominado inverso multiplicativo;

(viii) A multiplicação é distributiva em relação à adição, ou seja,

$$x \cdot (y + z) = x \cdot y + x \cdot z, \;\; \forall\, x, y, z \in \mathbb{K}.$$

A respeito da notação $(\mathbb{K}, +, \cdot)$ para definir um corpo, quando não houver dúvidas em relação as operações $+$ e $\cdot$, estas serão excluídas da notação, assim usa-se-á a notação $\mathbb{K}$ para definir corpo.

2 Exemplos e Contra-Exemplos de Corpos

Exemplo 1
Os conjuntos $\mathbb{N}$, $\mathbb{Z}$ e $\mathbb{Q}'$, com as operações usuais de adição e multiplicação, não são corpos.

De fato:

(i) Para cada natural $x \neq 0$, não existe $-x \in \mathbb{N}$;

(ii) Para cada inteiro $x \neq \pm 1$, não existe $x^{-1} \in \mathbb{Z}$;

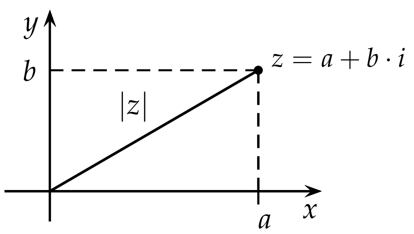
(iii) Note que $\mathbb{Q}'$ não é fechado para a adição, pois $\pm\sqrt{2} \in \mathbb{Q}'$ mas $-\sqrt{2} + \sqrt{2} = 0 \notin \mathbb{Q}'$.

Exemplo 2
Os conjuntos $(\mathbb{Q}, +, \cdot)$ e $(\mathbb{R}, +, \cdot)$ são corpos, ou seja, $\mathbb{Q}$ e $\mathbb{R}$, com as operações usuais são corpos.

De fato, com as operações usuais de adição e multiplicação esses conjuntos são fechados, ou seja, $\forall\, x, y \in \mathbb{R}$ e $\forall\, a, b \in \mathbb{Q}$, $x + y, x \cdot y \in \mathbb{R}$ e $a + b, a \cdot b \in \mathbb{Q}$. Além disso, os demais axiomas de corpo são satisfeitos, verifique!

Exemplo 3
Um *número complexo* é um número z que pode ser escrito na forma $z = a + b \cdot i$, sendo a e b números reais e i denota a unidade imaginária com a propriedade $i^2 = -1$. Os números a e b são chamados, respectivamente, *parte real* e *parte imaginária* de z. O conjunto $\mathbb{C} = \{a + b \cdot i; a, b \in \mathbb{R}\}$ é denominado de *conjunto dos números complexos*.

Este conjunto também pode ser entendido como o espaço bidimensional euclidiano $\mathbb{R}^2$, identificando $z = a + b \cdot i$ como o par (a, b), ou seja, $z = a + b \cdot i = (a, b)$. Desta forma, a cada número complexo podemos atribuir um número real positivo chamado módulo, dado por $|z| = \sqrt{a^2 + b^2}$.



Note que $\mathbb{R} \subset \mathbb{C}$.

Se z e w são dois números complexos dados por $z = a + b \cdot i$ e $w = c + d \cdot i$, então definem-se as relações e operações elementares como segue:

(i) Identidade: $z = w$ se, e somente se, $a = c$ e $b = d$;

(ii) Adição: $z + w = (a + b \cdot i) + (c + d \cdot i) = (a + c) + (b + d) \cdot i \in \mathbb{C}$;

(iii) Multiplicação: $z \cdot w = (a + b \cdot i) \cdot (c + d \cdot i) = (ac - bd) + (ad + bc) \cdot i \in \mathbb{C}$.

Com estas operações, $(\mathbb{C}, +, \cdot)$ é um corpo, em que $0 = 0 + 0 \cdot i$ é o elemento neutro da adição, $1 = 1 + 0 \cdot i$ é o elemento neutro da multiplicação, $-z = -a - b \cdot i$ é o elemento oposto e, o inverso multiplicativo é dado por

$$z^{-1} = \frac{1}{z} = \frac{1}{a + b \cdot i} \cdot \frac{a - b \cdot i}{a - b \cdot i} = \frac{a - b \cdot i}{a^2 - (b \cdot i)^2} = \frac{a - b \cdot i}{a^2 + b^2} = \frac{\overline{z}}{|z|^2},$$

em que $\overline{z} = a - b \cdot i$ é o conjugado de z.

Exemplo 4

Vamos definir um conjunto numérico bem interessante. Neste conjunto, diremos que dois elementos serão considerados iguais se possuirem o mesmo resto na divisão por um determinado número. Para motivar, considere os conjuntos $A = \{0, 2, 4, 6, \ldots\}$ e $B = \{1, 3, 5, 7, \ldots\}$, isto é, os conjuntos dos números naturais pares e dos naturais ímpares, respectivamente. Note que, para todo elemento de A, a divisão por 2 deixa resto 0 e, para todo elemento em B, a divisão por 2 deixa resto 1. Desta forma, iremos dizer que A é composto por um único número $\overline{0}$ (que representa todos os outros em A) e que, B é composto por um único número $\overline{1}$ (que representa todos os outros em B). Definimos assim o conjunto $\mathbb{Z}_2 = \{\overline{0}, \overline{1}\}$, e as operações de adição e de multiplicação dadas pelas tabelas abaixo:

$$\begin{array}{c|c|c} + & \overline{0} & \overline{1} \\ \hline \overline{0} & \overline{0} & \overline{1} \\ \overline{1} & \overline{1} & \overline{0} \end{array} \quad \text{e} \quad \begin{array}{c|c|c} \cdot & \overline{0} & \overline{1} \\ \hline \overline{0} & \overline{0} & 0 \\ \overline{1} & \overline{0} & \overline{1} \end{array}$$

Por exemplo, neste conjunto $\overline{1} + \overline{1} + \overline{1} + \overline{1} = \overline{0}$, pois $1 + 1 + 1 + 1 = 4$ que, na divisão por 2 deixa resto 0. Já, $\overline{1} + \overline{1} + \overline{1} = \overline{1}$, pois $1 + 1 + 1 = 3$ que, na divisão por 2 deixa resto 1.

Afirmamos que $\mathbb{Z}_2$ é um corpo, ou seja, $(\mathbb{Z}_2, +, \cdot)$ é corpo. De fato,

(i) $\mathbb{Z}_2$ é fechado para estas operações;

(ii) Estas operações são comutativas e associativas (verifique!)

(iii) Existe o elemento neutro da adição, que é $\overline{0}$;

(iv) Cada elemento admite oposto em $\mathbb{Z}_2$: $-\overline{0} = \overline{0}$ e $-\overline{1} = \overline{1}$;

(v) Existe o elemento neutro da multiplicação, que é $\overline{0}$;

(vi) O elemento não nulo admite inverso em $\mathbb{Z}_2$: $(\overline{1})^{-1} = \overline{1}$, pois $\overline{1} \cdot \overline{1} = \overline{1}$;

(vii) A multiplicação é distributiva em relação à adição, verifique!

Observação 1

Vejamos duas situações reais em que podemos ver conjuntos dessa natureza.

(a) Nos relógios de ponteiros, no qual o dia é divido em dois períodos de 12 horas cada, podemos ver esse tipo de conjunto, neste caso o $\mathbb{Z}_{12}$. Se, por exemplo, a hora é 5 horas agora, então daqui a 9 horas serão 2 horas e não 14 horas. A adição usual sugere que o tempo futuro deveria ser $5 + 9 = 14$, mas não é assim, pois o relógio "reinicia" a cada 12 horas, assim não existe "14 horas" nele. Dizemos então que, em $\mathbb{Z}_{12}$, 2 é congruente a 14, pois 14 deixa resto 2 na divisão por 12 ou, simplimente, $14 - 2 = 12$ que é um múltiplo de 12. Agora, suponha que decorreram 16 horas, daí $5 + 16 = 21 = 9$, pois $21 - 9 = 12$ ou 21 deixa resto 9 na por 12. Note que, a hora chamada "12 : 00" pode ser chamada "0 : 00", pois $12 - 0 = 12$ que é múltiplo de 12. $\mathbb{Z}_{12} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}, \overline{8}, \overline{9}, \overline{10}, \overline{11}\}$.

(b) Nos ônibus convencionais interurbanos, que contamos atualmente, podemos identificar o $\mathbb{Z}_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$. Nestes ônibus, as cadeiras que são janelas atrás do motorista são identificados por $\overline{1}$ e a sua vizinha (no corredor) por $\overline{2}$. As cadeiras que são janelas do lado da porta são identificadas por $\overline{3}$ e sua vizinha (no corredor) por $\overline{0}$. Desta forma, se o ônibus for extenso o suficiente para ter a cadeira de número 1.153, esta estará localizada na janela atrás mo do motorista pois, 1.153 deixa resto 1 na divisão por 4 ou, $1.153 - 1 = 1.152 = 4 \cdot 288$, múltiplo de 4.

Para concluir o Exemplo 4, dizemos que dois inteiros a e b são *congruentes módulo* n se $a - b$ é múltiplo de n. Simbolicamente, temos:

$$a \equiv b \pmod{n} \;\Leftrightarrow\; a - b = n \cdot k,\ k \in \mathbb{Z}.$$

Outra notação usual para $a \equiv b \pmod{n}$ é $a \equiv_n b$.

Vejamos alguns exemplos:

(i) $17 \equiv 2 \pmod{5}$, pois $17 - 2 = 15$, múltiplo de 5;

(ii) $20 \equiv 0 \pmod{4}$, pois $20 - 0 = 20$, múltiplo de 4;

(iii) $-9 \equiv_6 3$, pois $-9 - 3 = -12$, múltiplo de 6;

(iv) $2 \equiv_5 -3$, pois $2 - (-3) = 5$, múltiplo de 5;

(v) $-13 \equiv -5 \pmod{4}$, pois $-13 - (-5) = -8$, múltiplo de 4;

Se a e b são os dois positivos ou os dois negativos, então $a \equiv b \pmod{n}$ pode ser visto como a afirmação de que a e b possuem o mesmo resto na divisão por n. Por exemplo, $47 \equiv 32 \pmod{15}$ pois 37 e 32 tem o mesmo resto 2, quando dividos por 15. Observe ainda que $47 - 32 = 15$, que é múltiplo de 15.

Seja $n > 1$ um número natural. Denotamos por $\mathbb{Z}_n$ o conjunto dos inteiros módulo n. Ou seja, se $a \in \mathbb{Z}$, então

$$\overline{a} = \{a + k \cdot n;\ k \in \mathbb{Z}\}.$$

Em particular, $\overline{0}$ é o conjunto dos múltiplos de n e

$$\mathbb{Z}_n = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \ldots, \overline{n-1}\}.$$

Observação 2

(i) Algoritmo da divisão de Euclides: dados a e n inteiros positivos, $a > n$, existem inteiros q e r tais que

$$a = n \cdot q + r \qquad 0 \leq r \leq n - 1.$$

Ou seja, $a - r \equiv 0 \pmod{n}$ e, portanto, $a \equiv r \pmod{n}$.

(ii) Adição e Multiplicação em $\mathbb{Z}_n$:

$\overline{a}+\overline{b}=\overline{a+b}$. Ex. $\overline{6}+\overline{3}=\overline{6+3}=\overline{9}=\overline{1}$, em $\mathbb{Z}_8$;

$\overline{a}\cdot\overline{b}=\overline{a\cdot b}$. Ex. $\overline{5}\cdot\overline{4}=\overline{5\cdot 4}=\overline{20}=\overline{2}$, em $\mathbb{Z}_6$.

(iii) Propriedades da Adição e da Multiplicação:

$A1$	$(\overline{a}+\overline{b})+\overline{c}=\overline{a}+(\overline{b}+\overline{c})$	$M1$	$(\overline{a}\cdot\overline{b})\cdot\overline{c}=\overline{a}\cdot(\overline{b}\cdot\overline{c})$
$A2$	$\overline{a}+\overline{b}=\overline{b}+\overline{a}$	$M2$	$\overline{a}\cdot\overline{b}=\overline{b}\cdot\overline{a}$
$A3$	$\overline{a}+\overline{0}=\overline{a}$	$M3$	$\overline{a}\cdot\overline{1}=\overline{a}$
$A4$	$\overline{a}+\overline{-a}=\overline{0}$	$M4$	$\overline{a}(\overline{b}+\overline{c})=\overline{a}\overline{b}+\overline{a}\overline{c}$

(iv) Em $\mathbb{Z}_4$, vemos que $\overline{2}\cdot\overline{1}=\overline{2}$, $\overline{2}\cdot\overline{2}=\overline{0}$ e $\overline{2}\cdot\overline{3}=\overline{2}$, ou seja, não existe um elemento em $\mathbb{Z}_4$ que seja inverso de $\overline{2}$. Logo, afirmamos que $\mathbb{Z}_n$, em geral, não é corpo;

(v) Afirmação: $\mathbb{Z}_p$ é corpo se p é um natural primo.

Questão 1 Contrua as tabelas de adição e de multiplicação para $\mathbb{Z}_4$, $\mathbb{Z}_5$ e $\mathbb{Z}_6$. Verifique que, dentre esses três, apenas $\mathbb{Z}_5$ é corpo.

Exemplo 5
Seja $\mathbb{K}=\{a+b\sqrt{2}; a,b\in\mathbb{Q}\}$. Afirmamos que $(\mathbb{K},+,\cdot)$ é corpo.

De fato:

(i) Adição e Multiplicação são fechadas:

$$(a+b\sqrt{2})+(c+d\sqrt{2})=(a+c)+(b+c)\sqrt{2}\in\mathbb{K}$$

$$(a+b\sqrt{2})\cdot(c+d\sqrt{2})=ac+2bd+(ad+cd)\sqrt{2}\in\mathbb{K}, \text{ pois } a+c, b+c, ac+2bd, ad+cd\in\mathbb{Q};$$

(ii) Comutatividade ...

(iii) Associatividade ...

(iv) Elemento neutro da adição $0=0+0\cdot\sqrt{2}$;

(v) Para cada $x=a+b\sqrt{2}\in\mathbb{K}$, existe o elemento (oposto) $-x=-a-b\sqrt{2}\in\mathbb{K}$:

$$x+(-x)=a+b\sqrt{2}+(-a-b\sqrt{2})=0;$$

(vi) Elemento neutro da multiplicação $1=1+0\cdot\sqrt{2}\in\mathbb{K}$;

(vii) Para cada elemento $x=a+b\sqrt{2}\in\mathbb{K}-\{0\}$, o elemento inverso é dado por

$$x^{-1}=\frac{1}{a+b\sqrt{2}}=\frac{1}{a+b\sqrt{2}}\cdot\frac{a-b\sqrt{2}}{a-b\sqrt{2}}=\frac{a-b\sqrt{2}}{a^2-2b^2};$$

(viii) Distributividade...

Questão 2 Considere o conjunto $M_2(\mathbb{R})$ de todas as matrizes 2×2 da forma

$$M=\begin{bmatrix} x & -y \\ y & x \end{bmatrix}$$

em que x e y são números reais. A soma e de multiplicação de matrizes são as usuais. Sejam os elementos neutros da soma e da multiplicaçao:

$$0 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \quad \text{e} \quad 1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Verifique que $(M_2(\mathbb{R}), +, \cdot)$ é corpo.

3 Propriedades de Corpo

Sejam $a, b, x \in \mathbb{K}$, então:

1. Os neutros são únicos e indicamos com 0 e 1;
2. O oposto e o inverso são únicos e indicamos com $-x$ e x^{-1};
3. Se $a + x = a$, então $x = 0$;
4. Cancelamento da soma: $a + x = b + x$ implica $a = b$;
5. Cancelamento do produto: $a \cdot x = b \cdot x$ implica $a = b$, se $x \neq 0$;
6. Anulamento do produto: $a \cdot b = 0$ implica $a = 0$ e/ou $b = 0$;
7. Se $b \neq 0$ e $b \cdot x = b$, então $x = 1$;
8. Se $a + b = 0$, então $b = -a$;
9. A única solução da equação $a + x = b$ é $x = -a + b$;
10. Se $a \neq 0$, a equação $a \cdot x = b$ tem uma única solução $x = a^{-1} \cdot b = \dfrac{b}{a}$;
11. $x \cdot 0 = 0$;
12. $-x = (-1) \cdot x$;
13. $-(a + b) = (-a) + (-b)$;
14. $-(-x) = x$;
15. $(-1) \cdot (-1) = 1$.

4 Referências

1. ???;

Texto composto em $\LaTeX\,2_\varepsilon$, Cattai, 8 de março de 2016