MC358 - Fundamentos matemáticos da computação

Prof. Dr. Hilder Vitor Lima Pereira

Instituto de computação

UNICAMP

04 de outubro de 2023

1. Construindo conjuntos a partir de relações de equivalências

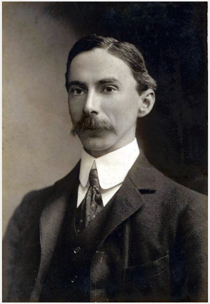
2. Perguntas, observações, comentários?

Construindo conjuntos a partir de relações de equivalências

Construindo os números racionais

Até agora, definimos o conjunto dos números racionais, $\mathbb{Q}$, e trabalhamos com ele...

No entanto, como podemos garantir que ele existe (ou seja, que nossos axiomas e os resultados obtidos deles nos permitem construir tal conjunto)?



Defina o seguinte conjunto M, cujos elementos são conjuntos A que não pertencem a si mesmos:

$$M = \{A : A \notin A\}$$

Podemos definir M, mas M existe?

Voltando à construção dos racionais

Defina a seguinte relação sobre $A = \mathbb{Z} \times \mathbb{Z}^*$:

$$\mathcal{R} = \{((a, b), (c, d)) \in A \times A : ad = bc\}$$

Note que essa relação relaciona pares ordenados!

Voltando à construção dos racionais

Defina a seguinte relação sobre $A = \mathbb{Z} \times \mathbb{Z}^*$:

$$\mathcal{R} = \{((a, b), (c, d)) \in A \times A : ad = bc\}$$

Note que essa relação relaciona pares ordenados!

Podemos ver que $\mathcal{R}$ é uma relação de equivalência:

- Reflexividade: ?
- Simetria: ?
- Transitividade: ?

Temos que

$$\mathcal{R} = \{((a,b),(c,d)) \in A \times A : ad = bc\}$$

é uma relação de equivalência sobre $A = \mathbb{Z} \times \mathbb{Z}^*$.
Então, podemos definir as classes de equivalência:

$$[(a,b)]_{\mathcal{R}} = \{(c,d) \in A \times A : (a,b) \equiv (c,d)\}$$

Temos que

$$\mathcal{R} = \{((a,b),(c,d)) \in A \times A : ad = bc\}$$

é uma relação de equivalência sobre $A = \mathbb{Z} \times \mathbb{Z}^*$.
Então, podemos definir as classes de equivalência:

$$[(a,b)]_{\mathcal{R}} = \{(c,d) \in A \times A : (a,b) \equiv (c,d)\}$$

Vamos identificar as seguintes classes de equivalência:

- $[(1,1)]_{\mathcal{R}}$

Temos que

$$\mathcal{R} = \{((a,b),(c,d)) \in A \times A : ad = bc\}$$

é uma relação de equivalência sobre $A = \mathbb{Z} \times \mathbb{Z}^*$.
Então, podemos definir as classes de equivalência:

$$[(a,b)]_{\mathcal{R}} = \{(c,d) \in A \times A : (a,b) \equiv (c,d)\}$$

Vamos identificar as seguintes classes de equivalência:

- $[(1,1)]_{\mathcal{R}}$
- $[(1,2)]_{\mathcal{R}}$

Temos que

$$\mathcal{R} = \{((a,b),(c,d)) \in A \times A : ad = bc\}$$

é uma relação de equivalência sobre $A = \mathbb{Z} \times \mathbb{Z}^*$.
Então, podemos definir as classes de equivalência:

$$[(a,b)]_{\mathcal{R}} = \{(c,d) \in A \times A : (a,b) \equiv (c,d)\}$$

Vamos identificar as seguintes classes de equivalência:

- $[(1,1)]_{\mathcal{R}}$
- $[(1,2)]_{\mathcal{R}}$
- $[(6,2)]_{\mathcal{R}}$

Lembrando que o conjunto das classes de equivalência é

$$B = A/\mathcal{R} = \{[(a,b)]_{\mathcal{R}} : (a,b) \in A\}$$

Lembrando que o conjunto das classes de equivalência é

$$B = A/\mathcal{R} = \{[(a,b)]_{\mathcal{R}} : (a,b) \in A\}$$

Note que se a e b não são coprimos, i.e., $\texttt{mdc}(a,b) = d > 1$, então definindo $a' = (a/d) \in \mathbb{Z}$ e $b' = (b/d) \in \mathbb{Z}^*$, temos

$$\texttt{mdc}(a',b') = 1 \wedge (a,b) \equiv (a',b')$$

Portanto, podemos restringir as classes de equivalência aos pares coprimos:

$$B = A/\mathcal{R} = \{[(a,b)]_{\mathcal{R}} : (a,b) \in A \wedge \texttt{mdc}(a,b) = 1\}$$

Operações para o conjunto B

Conseguimos construir B assumindo apenas a existência de $\mathbb{Z}$ e vemos que B "se comporta" como $\mathbb{Q}$...

Mas como definir as operações, adição, subtração, multiplicação e divisão em B usando apenas as operações dos inteiros?

- Soma: Definimos $[(a,b)]_{\mathcal{R}} + [(c,d)]_{\mathcal{R}} = [(ad+bc, bd)]_{\mathcal{R}}$
- Produto: Definimos $[(a,b)]_{\mathcal{R}} \cdot [(c,d)]_{\mathcal{R}} = [(ac, bd)]_{\mathcal{R}}$
- Subtração: Definimos $[(a,b)]_{\mathcal{R}} - [(c,d)]_{\mathcal{R}} = [(a,b)]_{\mathcal{R}} + ([(-1,1)]_{\mathcal{R}} \cdot [(c,d)]_{\mathcal{R}})$
- Divisão: Se $c \neq 0$, definimos $[(a,b)]_{\mathcal{R}} / [(c,d)]_{\mathcal{R}} = [(a,b)]_{\mathcal{R}} \cdot [(d,c)]_{\mathcal{R}}$.

Operações para o conjunto B

Conseguimos construir B assumindo apenas a existência de $\mathbb{Z}$ e vemos que B "se comporta" como $\mathbb{Q}$...

Mas como definir as operações, adição, subtração, multiplicação e divisão em B usando apenas as operações dos inteiros?

- Soma: Definimos $[(a,b)]_{\mathcal{R}} + [(c,d)]_{\mathcal{R}} = [(ad+bc, bd)]_{\mathcal{R}}$
- Produto: Definimos $[(a,b)]_{\mathcal{R}} \cdot [(c,d)]_{\mathcal{R}} = [(ac, bd)]_{\mathcal{R}}$
- Subtração: Definimos $[(a,b)]_{\mathcal{R}} - [(c,d)]_{\mathcal{R}} = [(a,b)]_{\mathcal{R}} + ([(-1,1)]_{\mathcal{R}} \cdot [(c,d)]_{\mathcal{R}})$
- Divisão: Se $c \neq 0$, definimos $[(a,b)]_{\mathcal{R}} / [(c,d)]_{\mathcal{R}} = [(a,b)]_{\mathcal{R}} \cdot [(d,c)]_{\mathcal{R}}$.

Vamos mostrar que as operações estão bem definidas...

Operações são independentes da representação

O que queremos dizer por "bem definida"?

- $w, z \in A \Rightarrow w \star z \in A$
- $x = w$ e $y = z$, então $x \star y = w \star z$

Operações são independentes da representação

O que queremos dizer por "bem definida"?

- $w, z \in A \Rightarrow w \star z \in A$
- $x = w$ e $y = z$, então $x \star y = w \star z$

Por exemplo, se definirmos a operação

$$[(a,b)]_{\mathcal{R}} \star [(c,d)]_{\mathcal{R}} = [(a,d)]_{\mathcal{R}}$$

Vemos que ele é mal definida, pois

$$[(1,1)]_{\mathcal{R}} \star [(1,2)]_{\mathcal{R}} = [(1,2)]_{\mathcal{R}}$$

mas

$$[(1,1)]_{\mathcal{R}} \star [(2,4)]_{\mathcal{R}} = [(1,4)]_{\mathcal{R}}$$

no entanto,

$$[(1,2)]_{\mathcal{R}} \neq [(1,4)]_{\mathcal{R}}$$

A multiplicação de classes de equivalência é bem definida

Relembrando a definição:

$$[(a,b)]_{\mathcal{R}} \cdot [(c,d)]_{\mathcal{R}} = [(ac,bd)]_{\mathcal{R}}$$

<u>Primeiro:</u> note que como $b, d \in \mathbb{Z}^*$, temos $bd \neq 0$, logo, $(ac, bd) \in A$ e $[(ac,bd)]_{\mathcal{R}}$ é uma classe de equivalência válida.

A multiplicação de classes de equivalência é bem definida

Relembrando a definição:

$$[(a,b)]_{\mathcal{R}} \cdot [(c,d)]_{\mathcal{R}} = [(ac,bd)]_{\mathcal{R}}$$

<u>Primeiro:</u> note que como $b, d \in \mathbb{Z}^*$, temos $bd \neq 0$, logo, $(ac, bd) \in A$ e $[(ac,bd)]_{\mathcal{R}}$ é uma classe de equivalência válida.

<u>Segundo:</u> se $(a,b) \equiv (x,y)$ e $(c,d) \equiv (w,z)$, então como mostramos o seguinte?

$$(a,b) \cdot (c,d) \equiv (x,y) \cdot (w,z)$$

A multiplicação de classes de equivalência é bem definida

Relembrando a definição:

$$[(a,b)]_{\mathcal{R}} \cdot [(c,d)]_{\mathcal{R}} = [(ac,bd)]_{\mathcal{R}}$$

<u>Primeiro:</u> note que como $b, d \in \mathbb{Z}^*$, temos $bd \neq 0$, logo, $(ac, bd) \in A$ e $[(ac,bd)]_{\mathcal{R}}$ é uma classe de equivalência válida.

<u>Segundo:</u> se $(a,b) \equiv (x,y)$ e $(c,d) \equiv (w,z)$, então como mostramos o seguinte?

$$(a,b) \cdot (c,d) \equiv (x,y) \cdot (w,z)$$

Mostrando que todas as operações são bem definidas, podemos finalmente dizer que

$$\mathbb{Q} = A/\mathcal{R}$$

Perguntas, observações, comentários?