

UNIVERSIDADE DE BRASÍLIA
DEPARTAMENTO DE MATEMÁTICA -IE

ÁLGEBRA I

(Álgebra Abstrata)

Texto de aula

PROFESSOR RUDOLF R. MAIER

Versão atualizada

2005

Índice

CAPÍTULO I

TEORIA ELEMENTAR DOS CONJUNTOS

	pg.
§ I.0 Fundamentos	1
Algumas observações sobre lógica elementar	
Conceitos primitivos e conjuntos	
Igualdade entre conjuntos	
Subconjuntos	
Diferença e complementar	
Reunião e interseção	
Uma propriedade fundamental do conjunto \mathbb{N}	
O conjunto das partes	
O teorema binomial	
O triângulo de PASCAL	
§ I.1 Produtos Cartesianos e Relações	23
Produtos CARTESIANOS	
Relações	
Relação inversa	
Composição de relações	
Relações de equivalência	
§ I.2 Aplicações (funções)	37
Definição e exemplos	
Composição de aplicações	
A caracterização das aplicações entre as relações	
Aplicações injetoras, sobrejetoras e bijetoras	
Conjuntos equipotentes	
A decomposição canónica de uma aplicação	
O axioma da escolha	
As ordens $ \mathbf{Inj}(m, n) $ e $ \mathbf{Sob}(m, n) $	

CAPÍTULO II

ESTRUTURAS ALGÉBRICAS

§	II.1	Definições das mais importantes estruturas algébricas	65
		Composições internas	
		Estruturas algébricas	
		Propriedades especiais de estruturas	
		Centralizador e centro	
		Semigrupos e monóides	
		Elementos regulares, inversíveis e grupos	
§	II.2	Subestruturas, estruturas quocientes e homomorfismos	89
		Subestruturas	
		Subestrutura gerada por um subconjunto	
		Relações de congruência e estruturas quocientes	
		Estruturas quocientes	
		Homomorfismos e Isomorfismos	
		O teorema geral do homomorfismo e estruturas simples	
		Associatividade, comutatividade, identidades e inversos sob homomorfismos	
§	II.3	Grupos	110
		Grupos	
		Os grupos simétricos	
		Subgrupos	
		O grupo dos automorfismos de uma estrutura algébrica	
		As relações de equivalência modulo um subgrupo	
		As relações de congruência de um grupo e subgrupos normais	
		Grupos quocientes e homomorfismos de grupos	
		Imagens homomórficas abelianas de grupos	
		Os grupos cíclicos	
§	II.4	Anéis e Corpos	130
		Anéis e subanéis	
		Homomorfismos e relações de congruência num anel - ideais	
		Anéis quocientes e ideais	
		Propriedades especiais de anéis	
		Ideais principais em anéis comutativos com identidade	
		Anéis simples e Corpos	
		Ideais primos e ideais maximais	
		Elementos idempotentes	

ÁLGEBRA I

(Álgebra Abstrata)

Notas de aula

PROF. RUDOLF R. MAIER

Versão atualizada 2005

CAPÍTULO I

TEORIA ELEMENTAR DOS CONJUNTOS

§ I.0 Fundamentos

ALGUMAS OBSERVAÇÕES SOBRE LÓGICA ELEMENTAR

I.0.1

Símbolos da lógica:

\forall leia-se: "para todo" ou "qualquer que seja"

\exists leia-se: "existe (pelo menos) um"

I.0.2

Implicação - condição necessária - condição suficiente

Suponhamos, \mathfrak{A} e \mathfrak{B} são "asserções" (ou "propriedades") - as quais podem ser verdadeiras ou falsas e cuja veracidade ou falsidade pode ser constatada de forma única. Quando escrevemos

$$\mathfrak{A} \implies \mathfrak{B}$$

queremos dizer que \mathfrak{A} implica em \mathfrak{B} ,

ou seja, sempre quando \mathfrak{A} for verdadeira, também \mathfrak{B} será verdadeira.

Outra maneira de dizer isto é:

(A validade de) \mathfrak{A} é *condição suficiente* para (a validade de) \mathfrak{B} ,
 ou \mathfrak{B} é *condição necessária* para \mathfrak{A} ,
 ou \mathfrak{A} vale *somente se* \mathfrak{B} vale,
 ou \mathfrak{B} vale *se* \mathfrak{A} vale,
 ou ainda *Se* \mathfrak{A} , *então* \mathfrak{B} .

É claro que $\mathfrak{A} \implies \mathfrak{B}$
 $\mathfrak{B} \iff \mathfrak{A}$ ou também \Downarrow ou \Uparrow
 \mathfrak{B} \mathfrak{A}

significam o mesmo quanto $\mathfrak{A} \implies \mathfrak{B}$. Vejamos exemplos:

Seja \mathfrak{A} a asserção: "um certo número natural n é múltiplo de 4"
 (dependendo do n , isto pode ser verdadeiro ou falso),
 \mathfrak{B} a asserção: " n é par".

Claramente temos neste caso

$$\mathfrak{A} \implies \mathfrak{B},$$

pois sempre se n é múltiplo de 4, concluímos que n é par. Assim, podemos dizer:

- " n ser múltiplo de 4" *implica que* " n é par".
- " n ser múltiplo de 4" é *condição suficiente* para " n ser par".
- " n ser par" é *condição necessária* para " n ser múltiplo de 4".
- " n é múltiplo de 4" *somente se* " n é par".
- " n é par", *se* " n é múltiplo de 4".
- "*se* n é múltiplo de 4", *então* " n é par".

Um outro exemplo:

Seja \mathfrak{A} a asserção: "*está chovendo*"
 (também isto pode ser verdadeiro ou falso aqui e agora),
 \mathfrak{B} a asserção: "*a praça está molhada*".

Também neste caso temos

$$\mathfrak{A} \implies \mathfrak{B},$$

pois, se realmente está chovendo, temos certeza que a praça está molhada. Assim,

podemos dizer:

"estar chovendo" *implica que* "a praça está molhada"
"estar chovendo" *é condição suficiente* para termos "uma praça molhada"
"uma praça molhada" *é condição necessária* para "estar chovendo"
"está chovendo" *somente se* "a praça está molhada"
"a praça está molhada" *se* "está chovendo"
se "está chovendo", *então* "a praça está molhada"

Exercício.

Pensando-se num certo quadrângulo Q , façam o mesmo com as asserções

\mathfrak{A} : " Q é um quadrado"
 \mathfrak{B} : " Q é um losângo".

É claro que a seta numa implicação $\mathfrak{A} \implies \mathfrak{B}$ não pode ser simplesmente invertida: \mathfrak{A} é condição suficiente para \mathfrak{B} significa que \mathfrak{B} é condição necessária para \mathfrak{A} , mas não que \mathfrak{B} é condição suficiente para \mathfrak{A} :

O fato de " n ser par" é condição necessária mas não suficiente para " n ser múltiplo de 4". O fato de " n ser múltiplo de 4" é condição suficiente mas não necessária para " n ser par": Também 6 é par sem ser múltiplo de 4.

O fato de termos "uma praça molhada" é condição necessária mas não suficiente para "estar chovendo". O fato de "estar chovendo" é condição suficiente mas não necessária para termos "uma praça molhada": A praça pode estar molhada sem que esteja chovendo (por exemplo devido a uma operação dos bombeiros).

Existem asserções \mathfrak{A} e \mathfrak{B} que ambas implicam na outra, ou seja, as quais satisfazem simultaneamente

$$\mathfrak{A} \implies \mathfrak{B} \quad \text{e} \quad \mathfrak{B} \implies \mathfrak{A}.$$

Nesta situação temos então que \mathfrak{A} é suficiente para \mathfrak{B} e também \mathfrak{A} é necessário para \mathfrak{B} . Dizemos que \mathfrak{A} é (condição) *necessário(a) e suficiente* para \mathfrak{B} , ou também \mathfrak{A} vale *se e somente se* vale \mathfrak{B} .

Este fato indicamos por

$$\mathfrak{A} \iff \mathfrak{B}.$$

Dizemos também que \mathcal{A} e \mathcal{B} são *asserções equivalentes*, ou ainda que \mathcal{A} constitui uma *propriedade característica para* \mathcal{B} (e vice versa).

Por exemplo:

Seja \mathcal{A} a asserção: " n é múltiplo de 6",
 \mathcal{B} a asserção: " n é um número par que é múltiplo de 3".

Cada uma destas duas propriedades, as quais um número n pode ter ou não, é suficiente para a outra. Cada uma é necessária para a outra. Cada uma é necessária e suficiente para a outra. Cada uma vale se e somente se a outra vale.

Exercício.

Pensar sobre as asserções equivalentes, quando Q é um certo quadrângulo:

\mathcal{A} : " Q é um quadrado"

\mathcal{B} : " Q é um losângo que é um retângulo".

Se \mathcal{A} é uma asserção, indicamos por $\bar{\mathcal{A}}$ a asserção "*não*- \mathcal{A} ", a qual é verdadeira se e somente se \mathcal{A} é falsa. Sejam \mathcal{A} e \mathcal{B} duas asserções e suponha

$$\mathcal{A} \implies \mathcal{B}.$$

O que acontece com esta implicação se negarmos as duas asserções? A resposta é que devemos também *inverter a seta da implicação*, ou seja, teremos

$$\bar{\mathcal{A}} \iff \bar{\mathcal{B}}.$$

Em outras palavras: Se \mathcal{A} é suficiente para \mathcal{B} , então $\bar{\mathcal{B}}$ é suficiente para $\bar{\mathcal{A}}$.

Ou também: Se \mathcal{A} é suficiente para \mathcal{B} , então $\bar{\mathcal{A}}$ é necessário para $\bar{\mathcal{B}}$.

Por exemplo, se negarmos a implicação

"ser múltiplo de 4 é suficiente para ser par",

a implicação negada é:

"não ser múltiplo de 4 é necessário para ser ímpar".

Porém, não ser múltiplo de 4 não é suficiente para ser ímpar.

Claro que numa equivalência podemos negar as asserções dos dois lados, ou seja, não importa se escrevemos

$$\mathfrak{A} \iff \mathfrak{B} \quad \text{ou} \quad \bar{\mathfrak{A}} \iff \bar{\mathfrak{B}}.$$

Existem teoremas que afirmam simplesmente *implicações*, do modo que na sua demonstração deve ser verificado que uma certa propriedade \mathfrak{B} é conseqüência de uma propriedade \mathfrak{A} (a hipótese).

outros teoremas matemáticos afirmam *equivalências* de certas propriedades. Eles têm a forma:

Sob certas condições são equivalentes:

- a) Vale a propriedade \mathfrak{A}
- b) Vale a propriedade \mathfrak{B} .

A demonstração de um tal teorema sempre se divide em duas partes:

"a) \Rightarrow b)" : Aqui deve ser mostrado que \mathfrak{A} é suficiente para \mathfrak{B} .

Isto pode ser mostrado diretamente, mostrando-se que \mathfrak{B} é verdade, supondo-se a veracidade de \mathfrak{A} . Ou indiretamente, supondo-se a veracidade de $\bar{\mathfrak{B}}$ e concluindo-se que $\bar{\mathfrak{A}}$ é verdade.

"b) \Rightarrow a)" : Aqui deve ser mostrado que \mathfrak{A} é necessário para \mathfrak{B} (que \mathfrak{B} é suficiente para \mathfrak{A}).

Isto pode ser mostrado, verificando-se que \mathfrak{A} é verdade, supondo-se a veracidade de \mathfrak{B} . Ou indiretamente, supondo-se que \mathfrak{A} é falso e concluindo-se que \mathfrak{B} é falso.

CONCEITOS PRIMITIVOS E CONJUNTOS

I.0.3

Como conceitos primitivos admitiremos: A noção de *elemento*, a relação de *igualdade* " $=$ ", a noção de *conjunto* e a relação da *pertinência* " \in ":

Um conjunto A é uma "coleção" ou "família" de "elementos" ou "objetos".

Dado um conjunto A . Para indicar que um elemento a pertence a A escrevemos $a \in A$ (ou também $A \ni a$). Se isto não é o caso, escreve-se $a \notin A$ (ou também $A \not\ni a$). Admitimos que, para qualquer objeto a ocorra exatamente uma das possibilidades:

$$\text{Ou } "a \in A" \text{ ou } "a \notin A".$$

Além disso, para dois elementos $a, b \in A$ queremos que exatamente uma das possibilidades

$$\text{ou } a = b \text{ ou } a \neq b$$

seja verdade.

Um conjunto pode ser dado pela simples colocação de todos os seus elementos, como por exemplo

$$A = \{\spadesuit, \heartsuit, \clubsuit\} \quad \text{ou} \quad A = \{1, 2, 3, 4, 5\}$$

Ele pode ser dado pela descrição exata das propriedades dos seus elementos, como por exemplo

$$A = \{n \mid n \text{ é um número natural}\} \quad \text{ou} \\ A = \{x \mid x \text{ é um número real tal que } \cos x = 0\} .$$

$A = \{a \mid \dots\}$ é lido: *A é o conjunto de todos os (elementos) a, tais que ...*

IGUALDADE ENTRE CONJUNTOS

I.0.4 Observação.

Dado dois conjuntos A e B , queremos saber se $A = B$ ou $A \neq B$. Isto é decidido assim:

$A = B$ significa: Para todo objeto x temos: $x \in A \iff x \in B$.

Assim, $A = B$



Para todo $a \in A$ vale $a \in B$ e para todo $b \in B$ vale $b \in A$.

Portanto, temos por exemplo

$$\{1, 2, 3, 4\} = \{3, 4, 1, 2\} \quad \text{ou}$$

$$\{n \mid n \text{ é um número natural}\} = \{n \mid n \text{ é um número inteiro positivo}\}$$

I.0.5 Exemplos.

Os seguintes conjuntos têm notação padrão e serão sempre usados:

$$\mathbb{N} = \{1, 2, 3, \dots\} = \textit{o conjunto dos números naturais},$$

$$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, 3, \dots\} = \textit{o conjunto dos números inteiros},$$

$$\mathbb{N}_0 = \{0, 1, 2, 3, \dots\} = \textit{o conjunto dos números inteiros não-negativos}.$$

Como fonte de exemplos admitiremos também sem mais explicações :

$\mathbb{R} =$ o conjunto dos números reais ,

$\mathbb{Q} = \left\{ \frac{m}{n} \mid m \in \mathbb{Z}, n \in \mathbb{N} \right\} =$ o conjunto dos números racionais .

I.0.6 Observação.

Um conjunto A pode conter só uma quantidade finita de elementos distintos. Tal conjunto é denominado um conjunto *finito*.

A *quantidade dos elementos distintos* nele contidos é um número natural (ou 0), indicado por $|A|$, é chamado de *ordem* de A . Temos por exemplo

$$\{\spadesuit, \heartsuit, \clubsuit\}, \quad \{1, 2, 3, 1, 3, 1, 3, \dots, 3, 1, \dots\} \quad \text{e} \quad \{x \in \mathbb{Z} \mid x^2 = 36\}$$

são conjuntos finitos. Suas ordens são

$$\begin{aligned} |\{\spadesuit, \heartsuit, \clubsuit\}| &= 4, & |\{1, 2, 3, 1, 3, 1, 3, \dots, 3, 1, \dots\}| &= |\{1, 2, 3\}| = 3 \quad \text{e} \\ |\{x \in \mathbb{Z} \mid x^2 = 36\}| &= |\{6, -6\}| = 2. \end{aligned}$$

Os conjuntos $A = \{a\}$ que possuem um único elemento (i.e. $|A| = 1$) são denominados os *conjuntos unitários*. Por exemplo, temos

$$A = \{x \in \mathbb{R} \mid x^3 + 5 = 0\} = \{-\sqrt[3]{5}\} \quad \text{é um conjunto unitário.}$$

SUBCONJUNTOS

I.0.7 Definição.

Se A e B são dois conjuntos, dizemos que A é um *subconjunto* (ou uma *parte*) de B (também: B *abrange* A), se todo elemento de A for elemento de B , ou seja, se para todo elemento a , a implicação

$$a \in A \implies a \in B$$

for verdade. Escreve-se este fato como $A \subseteq B$ ou também $B \supseteq A$. Temos

$$A = B \iff A \subseteq B \quad \text{e} \quad B \subseteq A.$$

I.0.8 Observação.

Para quaisquer três conjuntos A, B, C temos as regras

- Sempre* $A \subseteq A$ (lei da reflexividade)
- Se $A \subseteq B$ e $B \subseteq A$, então $A = B$ (lei da anti-simetria)
- Se $A \subseteq B$ e $B \subseteq C$, então $A \subseteq C$ (lei da transitividade)

Se $A \subseteq B$ e $A \neq B$, escreve-se $A \subset B$, ou $B \supset A$. Às vezes também:

$A \subsetneq B$ ou $B \supsetneq A$, lido: A é um subconjunto *próprio* (parte própria) de B .

Também: B *abrange* A *própriamente*.

$A \subset B$ significa então que todo elemento de A também é elemento de B , mas existe pelo menos um $b \in B$ com $b \notin A$.

Observamos que sempre vale a implicação

$$A \subset B \implies A \subseteq B.$$

Temos por exemplo, $\mathbb{N} \subseteq \mathbb{N}_0$, $\mathbb{N}_0 \subseteq \mathbb{Z}$, $\mathbb{Z} \subseteq \mathbb{Q}$ e $\mathbb{Q} \subseteq \mathbb{R}$.

Mais abreviadamente:

$$\mathbb{N} \subseteq \mathbb{N}_0 \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R},$$

Na verdade, podemos até afirmar

$$\mathbb{N} \subset \mathbb{N}_0 \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R},$$

pois $0 \in \mathbb{N}_0 \setminus \mathbb{N}$, $-1 \in \mathbb{Z} \setminus \mathbb{N}_0$, $\frac{1}{2} \in \mathbb{Q} \setminus \mathbb{Z}$ e $\sqrt{2} \in \mathbb{R} \setminus \mathbb{Q}$ (ver I.0.9). ■

Se $A \subseteq B$ não é verdade para dois conjuntos A e B , escreve-se

$$A \not\subseteq B \text{ ou } B \not\supseteq A.$$

Isto é lido: " A não está contido em B " ou também " B não abrange A " e significa que existe pelo menos um $a \in A$ com $a \notin B$.

Por exemplo, se

$$A = \{n \in \mathbb{N} \mid 2 \text{ divide } n\} = \{2, 4, 6, 8, \dots\}$$

é o conjunto dos números naturais pares e

$$B = \{n \in \mathbb{N} \mid 3 \text{ divide } n\} = \{3, 6, 9, 12, \dots\}$$

é o conjunto dos números naturais divisíveis por 3, temos

$$A \not\subseteq B \text{ e também } B \not\subseteq A ,$$

pois $4 \in A$, mas $4 \notin B$ e também $3 \in B$ mas $3 \notin A$.

Devemos advertir também que $A \not\subseteq B$ não necessariamente significa $B \subset A$, como mostra nosso exemplo.

DIFERENÇA E COMPLEMENTAR

I.0.9 Definição.

Dado dois conjuntos A e B , indicamos por

$$A \setminus B = \{a \in A \mid a \notin B\}$$

o conjunto dos elementos em A que não estão em B . Este conjunto

$A \setminus B$ é denominado a *diferença A menos B* .

Mencionamos que $A \setminus B \subseteq A$ e $B \setminus A \subseteq B$.

Por exemplo, se $A = \{2, 4, 6, 8, \dots\}$ e $B = \{3, 6, 9, 12, \dots\}$, temos

$$A \setminus B = \{2, 4, 8, 10, 14, 16, \dots\} \text{ e } B \setminus A = \{3, 9, 15, 21, 27, \dots\} ,$$

i.e. $A \setminus B$ é o conjunto dos números pares que não são múltiplos de 3, enquanto $B \setminus A$ é o conjunto dos múltiplos de 3 que não são pares.

No caso particular quando A e E são dois conjuntos tais que $A \subseteq E$, escrevemos

$$Cpt_E(A) = E \setminus A$$

e chamamos $Cpt_E(A)$ de *conjunto complementar de A relativo a E* .

Por exemplo

$Cpt_{\mathbb{R}}(\mathbb{Q})$ é o conjunto dos números *irracionais*.

Claramente temos

$$Cpt_E(Cpt_E(A)) = A .$$

Se $A = E$, o conjunto complementar $Cpt_E(E)$ é caracterizado por

$$Cpt_E(E) = \{a \in E \mid a \notin E\}$$

e é denominado o *subconjunto vazio* de E , indicado por

$$\emptyset = Cpt_E(E) .$$

I.0.10 Observação.

Se $A \subseteq B \subseteq E$, então

$$Cpt_E(B) \subseteq Cpt_E(A) .$$

Demonstração: Seja $A \subseteq B \subseteq E$ (hipótese) e seja $x \in Cpt_E(B)$ um elemento arbitrário. Segue $x \notin B$ e pela hipótese então $x \notin A$. Isto significa $x \in Cpt_E(A)$. Como $x \in Cpt_E(B)$ foi arbitrário, concluímos $Cpt_E(B) \subseteq Cpt_E(A)$.

■

REUNIÃO E INTERSEÇÃO

I.0.11 Definição.

Dado dois conjuntos, entendemos por

$$A \cup B = \{x \mid x \in A \text{ ou } x \in B\} ,$$

o conjunto dos elementos que pertencem a (pelo menos) um de A ou B e

$$A \cap B = \{x \mid x \in A \text{ e } x \in B\} ,$$

o conjunto dos elementos que pertencem a ambos A e B .

$A \cup B$ chama-se a *reunião*, $A \cap B$ a *interseção* dos conjuntos A e B .

I.0.12 Exemplos.

- a) Quando $A = \{2, 4, 6, 8, \dots\}$ é o conjunto dos números naturais pares e $\{3, 6, 9, 12, \dots\}$ o dos divisíveis por 3, temos

$$A \cup B = \{n \in \mathbb{N} \mid n \text{ é par ou divisível por } 3\} ,$$

$$A \cap B = \{n \in \mathbb{N} \mid n \text{ é divisível por } 6\} .$$

- b) Se $A = \{\heartsuit, \spadesuit, \heartsuit, \clubsuit\}$ e $B = \{\clubsuit, \heartsuit, 2, 3, 4\}$, então

$$A \cup B = \{\heartsuit, \spadesuit, \heartsuit, \clubsuit, 2, 3, 4\} ,$$

$$A \cap B = \{\heartsuit, \clubsuit\} .$$

As seguintes propriedades são facilmente verificadas:

I.0.13 Observação.

Para quaisquer conjuntos A e B temos

- a) $A \subseteq A \cup B$ e $B \subseteq A \cup B$
- b) $A \supseteq A \cap B$ e $B \supseteq A \cap B$
- c) $A \subseteq B \iff A \cap B = A \iff A \cup B = B$.

Se ainda C é um terceiro conjunto, então

- d) Se $A \subseteq C$ e $B \subseteq C$, então $A \cup B \subseteq C$
- e) Se $A \supseteq C$ e $B \supseteq C$, então $A \cap B \supseteq C$.

■

O conceito da \cup e da \cap pode ser generalizado para mais de dois conjuntos:

I.0.14 Definição.

Se A_1, A_2, \dots, A_n são n conjuntos dados, então

$$A_1 \cup A_2 \cup \dots \cup A_n = \bigcup_{k=1}^n A_k$$

é o conjunto dos elementos x que pertencem a *peelo menos um* dos A_1, A_2, \dots, A_n , enquanto

$$A_1 \cap A_2 \cap \dots \cap A_n = \bigcap_{k=1}^n A_k$$

é o conjunto dos elementos x que pertencem a *todos os* A_1, A_2, \dots, A_n .

As regras de "De Morgan" (Augustus DE MORGAN [1806 - 1871]):

I.0.15 Proposição.

Para qualquer conjunto E e os subconjuntos $A_1, A_2, \dots, A_n \subseteq E$ valem

$$Cpt_E \left(\bigcup_{k=1}^n A_k \right) = \bigcap_{k=1}^n Cpt_E(A_k) \text{ e}$$

$$Cpt_E \left(\bigcap_{k=1}^n A_k \right) = \bigcup_{k=1}^n Cpt_E(A_k).$$

Demonstração: Para todo $x \in E$ temos

$$\begin{aligned} x \in \text{Cpt}_E \left(\bigcup_{k=1}^n A_k \right) &\iff x \notin \bigcup_{k=1}^n A_k \iff x \notin A_k \quad \forall k \iff \\ &\iff x \in \text{Cpt}_E(A_k) \quad \forall k \iff x \in \bigcap_{k=1}^n \text{Cpt}_E(A_k). \end{aligned}$$

Da mesma forma

$$\begin{aligned} x \in \text{Cpt}_E \left(\bigcap_{k=1}^n A_k \right) &\iff x \notin \bigcap_{k=1}^n A_k \iff \exists k \text{ com } x \notin A_k \iff \\ &\iff \exists k \text{ com } x \in \text{Cpt}_E(A_k) \iff x \in \bigcup_{k=1}^n \text{Cpt}_E(A_k). \end{aligned}$$

■

Também famílias arbitrárias (possivelmente infinitas) de conjuntos podem ser consideradas: Se E é um conjunto e \mathfrak{F} é uma família de subconjuntos de E colocamos

$$\bigcup_{X \in \mathfrak{F}} X,$$

a reunião de todos os conjuntos $X \in \mathfrak{F}$. Esta é o subconjunto dos elementos de E contidos em pelo menos um dos $X \in \mathfrak{F}$, enquanto

$$\bigcap_{X \in \mathfrak{F}} X,$$

a interseção de todos os conjuntos $X \in \mathfrak{F}$, é o subconjunto dos elementos de E contidos em todos os $X \in \mathfrak{F}$.

Se $\mathfrak{F} = \{A_1, A_2, \dots, A_n\}$ é uma família finita, voltamos ao caso anterior. Dado um conjunto infinito E (por exemplo $E = \mathbb{N}$).

$$\mathfrak{F} = \{X \mid X \text{ é um subconjunto finito de } E\}$$

é um exemplo de uma família infinita.

As regras de DE MORGAN podem ser formuladas agora assim:

$$\text{Cpt}_E \left(\bigcup_{X \in \mathfrak{F}} X \right) = \bigcap_{X \in \mathfrak{F}} \text{Cpt}_E(X)$$

e

$$\text{Cpt}_E \left(\bigcap_{X \in \mathfrak{F}} X \right) = \bigcup_{X \in \mathfrak{F}} \text{Cpt}_E(X).$$

■

UMA PROPRIEDADE FUNDAMENTAL DO CONJUNTO \mathbb{N}

A adição $+$ em \mathbb{N} e também em \mathbb{Z} , a qual queremos admitir sem mais explicações, dá origem a uma *ordem natural* " \leq " em \mathbb{Z} :

$\forall n, m \in \mathbb{Z}$ temos

$$m \leq n \iff \text{a equação } m + x = n \text{ possui uma solução } x \in \mathbb{N}_0 .$$

A seguinte propriedade do conjunto \mathbb{N} é fundamental:

O princípio da indução.

Todo conjunto não vazio de números naturais possui um elemento mínimo. Em símbolos:

$$\forall S, \text{ com } \emptyset \neq S \subseteq \mathbb{N} \exists m \in S \text{ tal que } m \leq n \quad \forall n \in S.$$

Deste princípio segue a importante

I.0.16 Proposição.

Seja T um conjunto de alguns números naturais (i.e. $T \subseteq \mathbb{N}$) satisfazendo às propriedades:

- a) $1 \in T$
- b) *Sempre se $n \in T$, então também $n+1 \in T$.*

Então $T = \mathbb{N}$ é o conjunto de todos os números naturais.

Demonstração: Suponhamos $T \neq \mathbb{N}$. Então vale $S \neq \emptyset$ quando $S = Cpt_{\mathbb{N}}(T) \subseteq \mathbb{N}$ é o conjunto complementar de T em \mathbb{N} . Pelo princípio da indução existe $m \in S$ tal que $m \leq n$ para todos os $n \in S$. Como $1 \in T$ pela propriedade a), temos $1 \notin S$, particularmente $m > 1$. Daí concluímos $n = m-1 \in T$. Pela propriedade b) temos porém $m = n+1 \in T$, de onde sai o absurdo $m \in S \cap T = \emptyset$. Isto mostra que $S \neq \emptyset$ é impossível. Temos que ter $S = \emptyset$ e daí $T = \mathbb{N}$. ■

Esta fundamental proposição I.0.16 aplica-se para verificar a validade geral de fórmulas as quais envolvem números naturais, como mostra o seguinte

I.0.17 Exemplo.

Para todos os números naturais n vale

$$1 + 3 + 5 + \dots + (2n-3) + (2n-1) = n^2 \quad (*) .$$

Em palavras: A soma dos n primeiros números naturais ímpares é o n -ésimo quadrado perfeito.

Demonstração: Seja $T = \left\{ n \in \mathbb{N} \mid \sum_{k=1}^n (2k-1) = n^2 \right\}$ o conjunto dos números naturais para os quais a fórmula (*) é verdadeira (o "conjunto verdade" ou o "conjunto de validade" de (*)). Para mostrar que $T = \mathbb{N}$, só é preciso verificar a) e b) da Proposição I.0.16 para este T :

Para $n = 1$ (*) simplesmente afirma que $1 = 1^2$, o que certamente é verdade, ou seja, $1 \in T$.

Suponhamos $n \in T$ para algum número natural n , isto é,

$$1 + 3 + \dots + (2n-1) = n^2 .$$

Somando-se $2n+1$ a ambos os lados, obtemos

$$1 + 3 + \dots + (2n-1) + (2n+1) = n^2 + 2n + 1 ,$$

de onde segue

$$1 + 3 + \dots + (2n-1) + (2(n+1)-1) = (n+1)^2 .$$

Isto por sua vez significa $n+1 \in T$. Pela proposição concluímos que o conjunto verdade da fórmula (*) é o conjunto $T = \mathbb{N}$ de todos os números naturais. ■

Vejamos mais um

I.0.18 Exemplo.

Para todos os números naturais n e todo real $a \neq 1$ vale

$$1 + a + a^2 + a^3 + \dots + a^{n-1} + a^n = \frac{a^{n+1} - 1}{a - 1} .$$

Particularmente (quando $a = 2$) obtemos

$$1 + 2 + 4 + \dots + 2^{n-1} + 2^n = 2^{n+1} - 1 .$$

Demonstração: Mais uma vez temos que verificar a asserção para $n = 1$ e para $n+1$ sob a hipótese que ela já é válida para algum n :

Para $n = 1$ simplesmente afirma-se que $1+a = \frac{a^2-1}{a-1}$, o que é verdade (porquê?).

Suponhamos, para algum número natural n já provado

$$1 + a + a^2 + a^3 + \dots + a^{n-1} + a^n = \frac{a^{n+1} - 1}{a - 1} .$$

Somando-se a^{n+1} a ambos os lados, obtemos

$$1 + a + a^2 + \dots + a^{n-1} + a^n + a^{n+1} = \frac{a^{n+1} - 1}{a - 1} + a^{n+1} ,$$

de onde segue

$$1 + a + a^2 + \dots + a^n + a^{n+1} = \frac{a^{n+1} - 1 + (a - 1)a^{n+1}}{a - 1} = \frac{a^{(n+1)+1} - 1}{a - 1} .$$

Isto diz que a fórmula continua válida para $n+1$. Concluimos que ela vale para todo $n \in \mathbb{N}$.

■

Mencionamos que às vezes é conveniente trabalhar com a seguinte generalização de I.0.16:

I.0.19 Proposição.

Seja $n_0 \in \mathbb{Z}$ um inteiro fixo e seja T' um conjunto de (alguns) números inteiros maiores ou iguais a n_0 (i.e. $T' \subseteq \{n \mid n_0 \leq n \in \mathbb{Z}\}$), satisfazendo às propriedades:

- a) $n_0 \in T'$
- b) Sempre se $n \in T'$, então também $n+1 \in T'$.

Então $T' = \{n \mid n_0 \leq n \in \mathbb{Z}\}$ é o conjunto de todos os números inteiros maiores ou iguais a n_0 .

Isto é facilmente verificado pela aplicação de I.0.16 ao conjunto

$$T = \{n - n_0 + 1 \mid n \in T'\} .$$

Observamos que para este T temos $T \subseteq \mathbb{N}$ e $n_0 \in T'$ é equivalente a $1 \in T$. (I.0.16 é obtido de volta a partir de I.0.19 fazendo-se $n_0 = 1$).

A título de ilustração mencionamos o seguinte exemplo. A afirmação (correta) que o leitor queira verificar:

$$2^n > n^2 \quad \text{para todos os } n \geq 5$$

podemos substituir pela afirmação equivalente

$$2^{n+4} > (n+4)^2 \text{ para todos os } n \in \mathbb{N}.$$

O CONJUNTO DAS PARTES

I.0.20 Definição.

Para qualquer conjunto A , indicamos por

$$\mathfrak{A} = \mathbf{2}^A = \{X \mid X \subseteq A\}$$

o conjunto de todas as partes de A . Os elementos deste conjunto são portanto os subconjuntos de A . Dizer $X \in \mathbf{2}^A$ significa o mesmo quanto $X \subseteq A$. Particularmente temos $\emptyset \in \mathbf{2}^A$ e $A \in \mathbf{2}^A$.

I.0.21 Exemplos.

- Para $A = \emptyset$ temos $\mathbf{2}^\emptyset = \{\emptyset\}$
- Para $A = \{a\}$ temos $\mathbf{2}^{\{a\}} = \{\emptyset, \{a\}\}$.
- Para $A = \{a, b\}$ temos $\mathbf{2}^{\{a, b\}} = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$.
- Para $A = \mathbb{R}$ temos $\mathbf{2}^{\mathbb{R}} = \{X \mid X \subseteq \mathbb{R}\}$. Por exemplo $\mathcal{Q} \in \mathbf{2}^{\mathbb{R}}$.

A escolha do símbolo $\mathbf{2}^A$ para indicar o conjunto \mathfrak{A} de todas as partes de um conjunto A se justifica, se considerarmos A um conjunto *finito* com n elementos. Pois neste caso $\mathbf{2}^A$ terá exatamente 2^n elementos:

I.0.22 Observação.

Seja A finito. Então

$$|\mathbf{2}^A| = 2^{|A|}.$$

Demonstração: Provaremos a afirmação por indução sobre o número $n = |A|$: Se $n = 0$, temos $A = \emptyset$ e de fato $\mathbf{2}^A = \mathbf{2}^\emptyset = \{\emptyset\}$ é um conjunto contendo exatamente $1 = 2^0 = 2^{|A|}$ elemento.

Também se $A = \{a\}$ é um conjunto unitário, teremos $\mathbf{2}^A = \mathbf{2}^{\{a\}} = \{\emptyset, \{a\}\}$ e

vemos que 2^A é um conjunto com $2 = 2^1 = 2^{|A|}$ elementos.

Vamos supor A é um conjunto de $n+1$ elementos para algum $n \in \mathbb{N}$ e podemos pensar que

$$A = \{1, 2, 3, \dots, n, *\} .$$

Seja $A^* = \{1, 2, 3, \dots, n\} = A \setminus \{*\}$. Podemos supor que já foi provado que

$$|2^{A^*}| = 2^{|A^*|} = 2^n .$$

Os 2^n subconjuntos distintos de A^* podemos escrever (sem especificação) como

$$X_1, X_2, X_3, \dots, X_{2^n-1}, X_{2^n} .$$

Agora, os subconjuntos Y de A se dividem em duas classes: Os Y que não contêm o elemento $*$ e os que contêm $*$. Portanto, os subconjuntos distintos de A são

$$X_1, X_2, X_3, \dots, X_{2^n-1}, X_{2^n} \text{ junto com}$$

$$X_1 \cup \{*\}, X_2 \cup \{*\}, X_3 \cup \{*\}, \dots, X_{2^n-1} \cup \{*\}, X_{2^n} \cup \{*\} .$$

Vemos que A possui um total de 2 vezes 2^n subconjuntos distintos. Mas isto quer dizer que

$$|2^A| = 2 \cdot |2^{A^*}| = 2 \cdot 2^n = 2^{n+1} = 2^{|A|} .$$

■

Dado um conjunto $A = \{1, 2, 3, \dots, n\}$ com n elementos e um inteiro k com $0 \leq k \leq n$, podemos perguntar, quantos subconjuntos de k elementos existem em A ? Isto é, queremos saber o tamanho da família

$$\mathfrak{C}_{n,k} = \{X \mid X \subseteq A; |X| = k\} \subseteq \mathfrak{A} = 2^A .$$

Assim, a questão é

$$|\mathfrak{C}_{n,k}| = ?$$

Vamos abreviar, por enquanto, $c_{n,k} = |\mathfrak{C}_{n,k}| = |\{X \mid X \subseteq A; |X| = k\}|$.

Imediato é:

$$c_{n,0} = c_{n,n} = 1 ,$$

pois A possui um único subconjunto de 0 (o subconjunto vazio) e um único de n elementos (o próprio A). Também

$$c_{n,1} = c_{n,n-1} = n ,$$

pois A possui exatamente n subconjuntos unitários e também n subconjuntos de $n-1$ elementos $A \setminus \{j\}$, obtidos por remoção de um dos n elementos de A . Em geral, podemos dizer que

$$c_{n,k} = c_{n,n-k},$$

pois os subconjuntos de $n-k$ elementos são obtidos por remoção de um subconjunto de k elementos de A .

Queremos pensar agora sobre, se $k < n$, como é obtido $c_{n,k+1}$ a partir de $c_{n,k}$?

Como é obtido $c_{n,2}$ a partir de $c_{n,1}$?

Temos n conjuntos unitários $\{1\}, \{2\}, \dots, \{i\}, \dots, \{n\}$. A cada $\{i\}$ podemos acrescentar de $n-1$ maneiras diferentes um elemento $j \neq i$ e obtemos o conjunto $\{i, j\}$ de 2 elementos. Desta forma surgem $n(n-1)$ subconjuntos de 2 elementos. Mas cada um $\{i, j\}$ é obtido 2 vezes: Uma vez, acrescentando-se j ao i e uma segunda vez, acrescentando-se i ao j . Portanto, temos $\frac{n(n-1)}{2}$ subconjuntos *distintos* de 2 elementos (e também de $n-2$ elementos) em A :

$$c_{n,2} = c_{n,n-2} = \frac{n(n-1)}{2}.$$

Agora, de k para $k+1$: Seja $X \in \mathfrak{C}_{n,k}$ um dos $c_{n,k}$ subconjuntos de k elementos. Podemos acrescentar de $n-k$ maneiras um $(k+1)$ -ésimo ponto $j \in A \setminus X$, obtendo um total de $c_{n,k} \cdot (n-k)$ conjuntos da forma $X \cup \{j\} \in \mathfrak{C}_{n,k+1}$. Mas cada conjunto $Y \in \mathfrak{C}_{n,k+1}$ surge desta maneira exatamente $k+1$ vezes. Logo obtemos um total de $c_{n,k} \cdot \frac{n-k}{k+1}$ subconjuntos *distintos* de $k+1$ elementos. Portanto,

$$c_{n,k+1} = c_{n,k} \cdot \frac{n-k}{k+1}.$$

A partir de $c_{n,0} = 1$ vemos, colocando-se $k = 0, 1, 2, \dots, n-1$ que

$$c_{n,1} = c_{n,0} \cdot \frac{n}{1} = 1 \cdot n = n, \quad c_{n,2} = c_{n,1} \cdot \frac{n-1}{2} = n \cdot \frac{n-1}{2} = \frac{n(n-1)}{2}$$

$$c_{n,3} = c_{n,2} \cdot \frac{n-2}{3} = \frac{n(n-1)}{2} \cdot \frac{n-2}{3} = \frac{n(n-1)(n-2)}{6}$$

.....

$$c_{n,k} = \frac{n(n-1)(n-2)\dots(n-k+1)}{k!}, \quad c_{n,k+1} = c_{n,k} \cdot \frac{n-k}{k+1} = \frac{n(n-1)\dots(n-k+1)(n-k)}{(k+1)!}.$$

Convém lembrar aqui que, se $k \in \mathbb{N}_0$, entende-se por $k!$ o produto

$$k! = \prod_{\ell=1}^k \ell = 1 \cdot 2 \cdot 3 \cdot \dots \cdot k, \quad \text{se } k \in \mathbb{N}$$

e acrescentando

$$0! = 1, \quad \text{se } k = 0 \quad (\text{produto vazio}).$$

$k!$ leia-se: k fatorial.

É imediato que se tem $0! = 1! = 1$, $2! = 2$, $3! = 2! \cdot 3 = 6$, $4! = 3! \cdot 4 = 24$, ..., $k! = (k-1)! \cdot k$, $(k+1)! = k! \cdot (k+1)$,

■

I.0.23 Definição.

Para todo $n \in \mathbb{N}$ e todos os $k \in \mathbb{N}_0$ com $k \leq n$ coloca-se

$$\binom{n}{k} = \frac{n!}{k!(n-k)!},$$

número este que se chama de *coeficiente binomial n sobre k* .

Vemos que os coeficientes binomiais nada mais são do que os nossos números $c_{n,k}$ (ver I.0.25 a)):

$$\binom{n}{k} = c_{n,k} = \frac{n(n-1)\dots(n-k+1)}{k!} = \frac{n!}{k!(n-k)!}$$

e vemos que o conjunto $A = \{1, 2, 3, \dots, n\}$ possui exatamente $\binom{n}{k}$ subconjuntos de k elementos.

Particularmente, isto explica que

Os coeficientes binomiais são números inteiros.

Como $2^A = \mathfrak{C}_{n,0} \cup \mathfrak{C}_{n,1} \cup \mathfrak{C}_{n,2} \cup \dots \cup \mathfrak{C}_{n,n-1} \cup \mathfrak{C}_{n,n}$

e $\mathfrak{C}_{n,i} \cap \mathfrak{C}_{n,j} = \emptyset$, para todos os i, j com $0 \leq i \neq j \leq n$ [porquê?],

concluimos

$$|2^A| = |\mathfrak{C}_{n,0}| + |\mathfrak{C}_{n,1}| + |\mathfrak{C}_{n,2}| + \dots + |\mathfrak{C}_{n,n-1}| + |\mathfrak{C}_{n,n}|.$$

Portanto, vale a

I.0.24 Conseqüência.

Para todo $n \in \mathbb{N}$ temos

$$\sum_{k=0}^n \binom{n}{k} = \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \dots + \binom{n}{n-1} + \binom{n}{n} = 2^n.$$

■

O TEOREMA BINOMIAL

Neste contexto cabe também o chamado *teorema binomial*, ou seja, a fórmula do desenvolvimento de

$$(a + b)^n .$$

Temos as seguintes propriedades dos coeficientes binomiais:

I.0.25 Observação.

Para todo $n \in \mathbb{N}$ e todos os $k \in \mathbb{N}_0$ com $0 \leq k \leq n$ valem

- a) $\binom{n}{k} = \frac{n(n-1)\cdots(n-k+1)}{k!}$.
- b) $\binom{n}{k} = \binom{n}{n-k}$.
- c) $\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k}$ se $k \geq 1$.

Demonstração: a) $\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n(n-1)\cdots(n-k+1)\cdot(n-k)\cdots 2\cdot 1}{k!(n-k)!} = \frac{n(n-1)\cdots(n-k+1)}{k!}$.

b) Observamos primeiro que com $0 \leq k \leq n$ temos também $0 \leq n-k \leq n$. Pela definição temos de imediato

$$\binom{n}{n-k} = \frac{n!}{(n-k)![n-(n-k)]!} = \frac{n!}{(n-k)!k!} = \binom{n}{k}.$$

c) Se $k \geq 1$ calculamos $\binom{n}{k} + \binom{n}{k-1} = \frac{n!}{k!(n-k)!} + \frac{n!}{(k-1)![n-(k-1)]!} =$
 $= \frac{n!(n-k+1) + n!k}{k!(n-k+1)!} = \frac{n!(n+1)}{k!(n-k+1)!} = \frac{(n+1)!}{k![(n+1)-k]!} = \binom{n+1}{k}$.

■

Eis alguns valores específicos de coeficientes binomiais:

$$\binom{n}{0} = \binom{n}{n} = 1, \quad \binom{n}{1} = \binom{n}{n-1} = n, \quad \binom{n}{2} = \binom{n}{n-2} = \frac{n(n-1)}{2} .$$

Podemos enunciar e provar agora o fundamental

teorema do desenvolvimento binomial:

I.0.26 Teorema.

Para todo $n \in \mathbb{N}$ e todos os números reais a, b temos

$$(a + b)^n = \sum_{k=0}^n \binom{n}{k} a^{n-k} b^k .$$

Por extenso:

$$(a + b)^n = a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \dots + \binom{n}{k}a^{n-k}b^k + \dots + \binom{n}{n-1}ab^{n-1} + b^n.$$

Demonstração: Demonstraremos isto por indução sobre o expoente n , isto é, provaremos $1 \in T$ e a implicação " $n \in T \Rightarrow n+1 \in T$ " quando T é o conjunto de validade da fórmula.

Para $n = 1$ afirma-se que $(a + b)^1 = \sum_{k=0}^1 \binom{1}{k}a^{1-k}b^k = \binom{1}{0}a^{1-0}b^0 + \binom{1}{1}a^{1-1}b^1$, sendo igual a $a + b$ de ambos os lados, i.e. $1 \in T$.

Suponhamos então que para algum $n \in \mathbb{N}$ já esteja provado

$$(a + b)^n = \sum_{k=0}^n \binom{n}{k}a^{n-k}b^k \quad (*)$$

e provamos a validade para $n+1$. Para isto multiplicamos os dois lados de $(*)$ por $(a + b)$ e obtemos, usando-se a observação I.0.25 c):

$$\begin{aligned} (a + b)^{n+1} &= \left(\sum_{k=0}^n \binom{n}{k}a^{n-k}b^k \right) (a + b) = \sum_{k=0}^n \binom{n}{k}a^{n-k+1}b^k + \sum_{k=0}^n \binom{n}{k}a^{n-k}b^{k+1} = \\ &= a^{n+1} + \sum_{k=1}^n \binom{n}{k}a^{n-k+1}b^k + \sum_{k=0}^{n-1} \binom{n}{k}a^{n-k}b^{k+1} + b^{n+1} = \\ &= a^{n+1} + b^{n+1} + \sum_{k=1}^n \binom{n}{k}a^{n-k+1}b^k + \sum_{k=1}^n \binom{n}{k-1}a^{n-k+1}b^k = \\ &= a^{n+1} + b^{n+1} + \sum_{k=1}^n \left[\binom{n}{k} + \binom{n}{k-1} \right] a^{n+1-k}b^k = a^{n+1} + b^{n+1} + \sum_{k=1}^n \binom{n+1}{k}a^{n+1-k}b^k = \\ &= \sum_{k=0}^{n+1} \binom{n+1}{k}a^{n+1-k}b^k, \end{aligned}$$

isto é,

$$(a + b)^{n+1} = \sum_{k=0}^{n+1} \binom{n+1}{k}a^{n+1-k}b^k.$$

Isto significa que, a partir da suposta validade da fórmula $(*)$ para algum n , conseguimos provar a sua validade para $n+1$ (i.e. $n \in T \Rightarrow n+1 \in T$). Concluimos que $(*)$ tem validade para todo $n \in \mathbb{N}$. ■

§ I.1 Produtos Cartesianos e Relações

PRODUTOS CARTESIANOS

(René DESCARTES [1596-1650] Filósofo e Matemático francês)

I.1.1 Definição.

Sejam $A_1, A_2, \dots, A_m \neq \emptyset$ conjuntos. O conjunto

$$\begin{aligned} M &= A_1 \times A_2 \times \dots \times A_m = \\ &= \{ (a_1, a_2, \dots, a_m) \mid a_1 \in A_1, a_2 \in A_2, \dots, a_m \in A_m \} \end{aligned}$$

chama-se o *produto* CARTESIANO dos A_1, A_2, \dots, A_m (nesta ordem). Os elementos (a_1, a_2, \dots, a_m) em M chamam-se *m-uplas*. O elemento $a_i \in A_i$ é a *i-ésima coordenada da m-úpla* (a_1, a_2, \dots, a_m) ($1 \leq i \leq m$).

Para dois elementos (a_1, a_2, \dots, a_m) e (b_1, b_2, \dots, b_m) em M temos sua *igualdade* definida por

$$(a_1, a_2, \dots, a_m) = (b_1, b_2, \dots, b_m) \iff a_1 = b_1, a_2 = b_2, \dots, a_m = b_m .$$

No caso particular, quando $m = 2$, $A_1 = A$ e $A_2 = B$, temos

$$M = A \times B = \{ (a, b) \mid a \in A, b \in B \}$$

onde $(a, b) = (c, d) \iff a = c$ e $b = d$.

No caso m arbitrário e $A_1 = A_2 = \dots = A_m = A$, o produto CARTESIANO passa a ser a *potência* CARTESIANA *m-ésima* de A , indicada por

$$M = A^m = \{ (a_1, a_2, \dots, a_m) \mid a_1, a_2, \dots, a_m \in A \} .$$

Particularmente, se $m = 2$ e $A = B$, temos $A^2 = \{ (a, b) \mid a, b \in A \}$.

I.1.2 Observação.

Se $C = \{x_1, x_2, \dots, x_r\}$ e $B = \{y_1, y_2, \dots, y_s\}$ são conjuntos finitos, temos

$$C \times B = \left\{ \begin{array}{l} (x_1, y_1), (x_1, y_2), \dots, (x_1, y_s), \\ (x_2, y_1), (x_2, y_2), \dots, (x_2, y_s), \\ \dots\dots\dots \\ (x_r, y_1), (x_r, y_2), \dots, (x_r, y_s) \end{array} \right\}$$

Portanto, $|C \times B| = rs = |C||B|$.

I.1.3 Conseqüência.

Se A_1, A_2, \dots, A_m são conjuntos finitos, então vale

$$|A_1 \times A_2 \times \dots \times A_m| = |A_1||A_2| \dots |A_m| .$$

Particularmente, se $A_1 = A_2 = \dots = A_m = A$, temos

$$|A^m| = |A|^m .$$

Demonstração: Esta afirmação é clara se $m = 1$. Se já foi provado

$$|A_1 \times A_2 \times \dots \times A_{m-1}| = |A_1||A_2| \dots |A_{m-1}| ,$$

podemos considerar $C = A_1 \times A_2 \times \dots \times A_{m-1}$ e temos

$$A_1 \times A_2 \times \dots \times A_m = C \times A_m .$$

Por I.1.2 vemos $|C \times A_m| = |C||A_m|$ e portanto

$$|A_1 \times A_2 \times \dots \times A_m| = |C \times A_m| = |C||A_m| = |A_1||A_2| \dots |A_{m-1}||A_m| .$$

I.1.4 Exemplos.

Para $A = \{\heartsuit, \spadesuit, \diamondsuit, \clubsuit\}$ e $B = \{1, 2, 3\}$ temos

$$A \times B = \left\{ \begin{array}{l} (\heartsuit, 1), (\spadesuit, 1), (\diamondsuit, 1), (\clubsuit, 1), \\ (\heartsuit, 2), (\spadesuit, 2), (\diamondsuit, 2), (\clubsuit, 2), \\ (\heartsuit, 3), (\spadesuit, 3), (\diamondsuit, 3), (\clubsuit, 3) \end{array} \right\} ,$$

porém

$$B \times A = \left\{ \begin{array}{l} (1, \heartsuit), (2, \heartsuit), (3, \heartsuit), \\ (1, \spadesuit), (2, \spadesuit), (3, \spadesuit), \\ (1, \diamondsuit), (2, \diamondsuit), (3, \diamondsuit), \\ (1, \clubsuit), (2, \clubsuit), (3, \clubsuit) \end{array} \right\} .$$

Vemos $|A \times B| = |B \times A| = 12$. Mas $A \times B \neq B \times A$.

Mais exatamente: $(A \times B) \cap (B \times A) = \emptyset$.

I.1.5 Definição.

Seja $A \neq \emptyset$ um conjunto. O conjunto

$$\delta_A = \{(a, a) \mid a \in A\} \subseteq A^2$$

chama-se a *diagonal* de A (mais correto: a diagonal de A^2).

I.1.6 Exemplos.

a) Para $A = \mathbb{R}$ temos

$\mathbb{R}^2 = \{(x, y) \mid x, y \in \mathbb{R}\}$ é o *plano CARTESIANO* (EUCLIDIANO) real,

$\delta_{\mathbb{R}} = \{(x, x) \mid x \in \mathbb{R}\}$ é a sua diagonal (a primeira mediana).

b) Para $A = \{\spadesuit, \heartsuit, \clubsuit\}$ temos

$$A^2 = \left\{ \begin{array}{l} (\spadesuit, \spadesuit), (\spadesuit, \heartsuit), (\spadesuit, \clubsuit), \\ (\heartsuit, \spadesuit), (\heartsuit, \heartsuit), (\heartsuit, \clubsuit), \\ (\clubsuit, \spadesuit), (\clubsuit, \heartsuit), (\clubsuit, \clubsuit) \end{array} \right\} \text{ e } \delta_A = \{(\spadesuit, \spadesuit), (\heartsuit, \heartsuit), (\clubsuit, \clubsuit)\} .$$

RELAÇÕES

I.1.7 Definição.

Sejam $A, B \neq \emptyset$ dois conjuntos.

Uma *relação* ρ de A em B (uma relação entre certos elementos de A com certos elementos de B) é um subconjunto do produto CARTESIANO $A \times B$:

$$\rho \subseteq A \times B, \quad \text{equivalentemente: } \rho \in \mathbf{2}^{A \times B} .$$

$\mathbf{2}^{A \times B}$ é portanto o *conjunto de todas as relações* de A em B .

Um $a \in A$ chama-se ρ -relacionado com $b \in B$, abreviado por

$$a \rho b, \quad \text{se } (a, b) \in \rho .$$

Caso contrário: Se a não é ρ -relacionado com b , escrevemos $a \not\rho b$, o que significa o mesmo quanto $(a, b) \notin \rho$.

$$\mathbf{D}(\rho) = \{a \in A \mid \exists b \in B \text{ com } a \rho b\} \subseteq A$$

chama-se o *domínio de definição*,

$$\mathbf{I}(\rho) = \{ b \in B \mid \exists a \in A \text{ com } a \rho b \} \subseteq B$$

chama-se a *imagem* da relação ρ .

Se $A = B$, uma $\rho \in \mathbf{2}^{A \times A}$ é denominada *uma relação em A*.

I.1.8 Exemplos.

a) Para quaisquer dois conjuntos $A, B \neq \emptyset$ temos que

$$A \times B \in \mathbf{2}^{A \times B} \quad \text{e} \quad \emptyset \in \mathbf{2}^{A \times B} .$$

Temos $a (A \times B) b \quad \forall a \in A$ e $b \in B$, i.e. todo elemento $a \in A$ é $(A \times B)$ -relacionado com todo $b \in B$. Portanto, $A \times B$ é também denominada a *relação universal entre A e B*.

Temos $a \emptyset b$ nunca, i.e. nenhum elemento $a \in A$ é \emptyset -relacionado com nenhum $b \in B$.

As relações $A \times B$ e \emptyset são as *relações triviais* entre A e B que possuem pouco interesse, mas mostram que *sempre existem relações* entre A e B , quaisquer que sejam os conjuntos A e B .

b) Sejam $A = \{ \spadesuit, \heartsuit, \clubsuit \}$ e $B = 1, 2, 3$. Temos

$$\rho = \{ (\spadesuit, 2), (\clubsuit, 2), (\spadesuit, 3), (\heartsuit, 3) \} \in \mathbf{2}^{A \times B}$$

é uma relação de A em B . Temos $\mathbf{D}(\rho) = \{ \spadesuit, \clubsuit, \heartsuit \}$ e $\mathbf{I}(\rho) = \{ 2, 3 \}$.

$$\sigma = \{ (1, \heartsuit), (1, \clubsuit), (3, \spadesuit) \} \in \mathbf{2}^{B \times A}$$

é uma relação de B em A . Temos $\mathbf{D}(\sigma) = \{ 1, 3 \}$ e $\mathbf{I}(\sigma) = \{ \spadesuit, \heartsuit, \clubsuit \}$.

c) Uma relação importante em qualquer conjunto A é a diagonal $\delta_A \in \mathbf{2}^{A \times A}$ (ver I.1.5). Temos para todos os $a, a' \in A$:

$$a \delta_A a' \iff a = a' .$$

Portanto a diagonal δ_A é também denominada a *relação da igualdade em A*.

Observamos que, se A e B são conjuntos *finitos* de tamanhos $|A| = m$ e $|B| = n$, temos para a *quantidade* das relações entre A e B :

$$|\mathbf{2}^{A \times B}| = |\mathbf{2}^{B \times A}| = 2^{|A||B|} = 2^{mn} .$$

Particularmente, $|\mathbf{2}^{A \times A}| = 2^{m^2}$.

Por exemplo: Entre $A = \{\heartsuit, \spadesuit, \clubsuit, \diamondsuit\}$ e $B = \{1, 2, 3\}$ (e também entre B e A) existem $2^{12} = 4096$ relações distintas.

Em $A = \{a, b, c\}$ existem $2^9 = 512$ relações distintas.

RELAÇÃO INVERSA

I.1.9 Definição.

Sejam $A, B \neq \emptyset$ dois conjuntos e $\rho \in \mathbf{2}^{A \times B}$ uma relação. A relação

$$\rho^{-1} = \{(b, a) \mid (a, b) \in \rho\} \in \mathbf{2}^{B \times A}$$

chama-se a *relação inversa* da ρ . Observamos que

$$\mathbf{D}(\rho^{-1}) = \mathbf{I}(\rho) \quad \text{e} \quad \mathbf{I}(\rho^{-1}) = \mathbf{D}(\rho) .$$

Além do mais,

$$(\rho^{-1})^{-1} = \rho .$$

I.1.10 Exemplo.

a) Para $A = \mathbb{Z}$ e $B = \mathbb{R}$ e considerando-se a relação

$$\rho = \{(a, b) \mid a \in \mathbb{Z}, b \in \mathbb{R}, 4a^2 + 9b^2 = 36\} ,$$

temos

$$\rho = \{(0, \pm 2), (\pm 1, \pm \frac{4\sqrt{2}}{3}), (\pm 2, \pm \frac{2\sqrt{5}}{3}), (\pm 3, 0)\} \in \mathbf{2}^{\mathbb{Z} \times \mathbb{R}}$$

e

$$\rho^{-1} = \{(\pm 2, 0), (\pm \frac{4\sqrt{2}}{3}, \pm 1), (\pm \frac{2\sqrt{5}}{3}, \pm 2), (0, \pm 3)\} \in \mathbf{2}^{\mathbb{R} \times \mathbb{Z}} .$$

$$\mathbf{D}(\rho) = \mathbf{I}(\rho^{-1}) = \{-3, -2, -1, 0, 1, 2, 3\}$$

e

$$\mathbf{D}(\rho^{-1}) = \mathbf{I}(\rho) = \left\{-2, -\frac{4\sqrt{2}}{3}, -\frac{2\sqrt{5}}{3}, 0, \frac{2\sqrt{5}}{3}, \frac{4\sqrt{2}}{3}, 2\right\}.$$

b) Para $A = \{\nabla, \spadesuit, \heartsuit, \clubsuit\}$ e $B = \{1, 2, 3\}$ e considerando-se a relação

$$\rho = \{(\nabla, 3), (\nabla, 1), (\clubsuit, 3)\} \in \mathbf{2}^{A \times B},$$

temos

$$\rho^{-1} = \{(3, \nabla), (1, \nabla), (3, \clubsuit)\} \in \mathbf{2}^{B \times A},$$

$$\mathbf{D}(\rho) = \mathbf{I}(\rho^{-1}) = \{\nabla, \clubsuit\} \quad \text{e} \quad \mathbf{D}(\rho^{-1}) = \mathbf{I}(\rho) = \{1, 3\}.$$

COMPOSIÇÃO DE RELAÇÕES

I.1.11 Definição.

Sejam $A, B, C \neq \emptyset$ conjuntos, $\rho \in \mathbf{2}^{A \times B}$ e $\sigma \in \mathbf{2}^{B \times C}$ relações.

Definamos a relação composta $\sigma \circ \rho \in \mathbf{2}^{A \times C}$ por:

$$\forall a \in A, c \in C : \quad a \sigma \circ \rho c \iff \exists b \in B \text{ tal que } \begin{cases} a \rho b \\ b \sigma c \end{cases}.$$

I.1.12 Exemplos.

a) Sejam $A = B = C = \mathbb{R}$, $\rho, \sigma \in \mathbf{2}^{\mathbb{R} \times \mathbb{R}}$ definidas por

$$\rho = \{(a, b) \mid a^2 + 3b^2 = 5\} \quad \text{e} \quad \sigma = \{(b, c) \mid b = 4c^2\}.$$

Então

$$\sigma \circ \rho = \{(a, c) \mid a^2 + 48c^4 = 5\}.$$

b) Sejam $A = \{\nabla, \spadesuit, \heartsuit, \clubsuit\}$, $B = \{1, 2, 3, 4\}$ e $C = \{a, b, c, d, e\}$.

Sejam $\rho \in \mathbf{2}^{A \times B}$ e $\sigma \in \mathbf{2}^{B \times C}$ definidas por

$$\rho = \{(\heartsuit, 3), (\heartsuit, 4), (\spadesuit, 3), (\nabla, 2)\} \quad \text{e} \quad \sigma = \{(3, c), (1, e), (3, a), (2, d)\}.$$

Então

$$\sigma \circ \rho = \{(\heartsuit, c), (\heartsuit, a), (\spadesuit, c), (\spadesuit, a), (\nabla, d)\} .$$

■

I.1.13 Observação.

Sejam $A, B \neq \emptyset$ conjuntos. Se $\rho \in \mathbf{2}^{A \times B}$, então valem

$$\delta_B \circ \rho = \rho \quad e \quad \rho \circ \delta_A = \rho .$$

Demonstração: Para $a \in A, b \in B$ temos

$$a (\delta_B \circ \rho) b \iff \exists b' \in B \text{ com } \begin{cases} a \rho b' \\ e \\ b' \delta_B b \end{cases} \iff b = b' \text{ e } a \rho b' \\ \iff a \rho b. \text{ Logo } \delta_B \circ \rho = \rho.$$

$$\text{Também: } a (\rho \circ \delta_A) b \iff \exists a' \in A \text{ com } \begin{cases} a \delta_A a' \\ e \\ a' \rho b \end{cases} \iff a = a' \text{ e } a' \rho b \\ \iff a \rho b. \text{ Logo } \rho \circ \delta_A = \rho.$$

■

I.1.14 Proposição.

Sejam $A, B, C, D \neq \emptyset$ conjuntos, $\rho \in \mathbf{2}^{A \times B}$, $\sigma \in \mathbf{2}^{B \times C}$ e $\tau \in \mathbf{2}^{C \times D}$ relações. Então valem:

- $(\tau \circ \sigma) \circ \rho = \tau \circ (\sigma \circ \rho)$, (a lei associativa da composição).
- $(\sigma \circ \rho)^{-1} = \rho^{-1} \circ \sigma^{-1}$ (lei de inversão da composta).

Demonstração: a) Para $a \in A$ e $d \in D$ temos:

$$a ((\tau \circ \sigma) \circ \rho) d \iff \exists b \in B \text{ com } \begin{cases} a \rho b \\ e \\ b (\tau \circ \sigma) d \end{cases} \iff \exists b \in B, \exists c \in C$$

$$\text{com } \begin{cases} a \rho b \\ e \\ b \sigma c \\ e \\ c \tau d \end{cases} \iff \exists c \in C \text{ com } \begin{cases} a (\sigma \circ \rho) c \\ e \\ c \tau d \end{cases} \iff a (\tau \circ (\sigma \circ \rho)) d.$$

b) Para $a \in A$ e $c \in C$ temos

$$c (\sigma \circ \rho)^{-1} a \iff a (\sigma \circ \rho) c \iff \exists b \in B \text{ tal que } \begin{cases} a \rho b \\ e \\ b \sigma c \end{cases} \iff \exists b \in B$$

$$\text{tal que } \begin{cases} c \sigma^{-1} b \\ e \\ b \rho^{-1} a \end{cases} \iff c (\rho^{-1} \circ \sigma^{-1}) a. \text{ Logo, } (\sigma \circ \rho)^{-1} = \rho^{-1} \circ \sigma^{-1}.$$

■

RELAÇÕES DE EQUIVALÊNCIA

I.1.15 Definição.

Seja $A \neq \emptyset$ um conjunto e $\rho \in \mathbf{2}^{A \times A}$ uma relação em A .

Dizemos que ρ é uma relação

- i) *reflexiva*, se $a \rho a$ para todo $a \in A$.
- ii) *simétrica*, se $\forall a, b \in A : a \rho b \iff b \rho a$.
- iii) *antisimétrica*, se $\forall a, b \in A : a \rho b \text{ e } b \rho a \implies a = b$.
- iv) *transitiva*, se $\forall a, b, c \in A : a \rho b \text{ e } b \rho c \implies a \rho c$.

Estas eventuais propriedades de uma relação podem ser assim caracterizadas:

I.1.16 Observação.

Para toda $\rho \in \mathbf{2}^{A \times A}$ temos

- a) ρ é reflexiva $\iff \delta_A \subseteq \rho$
- b) ρ é simétrica $\iff \rho^{-1} = \rho$

c) ρ é antisimétrica $\iff \rho \cap \rho^{-1} \subseteq \delta_A$

d) ρ é transitiva $\iff \rho \circ \rho \subseteq \rho$

Demonstração: a) ρ é reflexiva $\iff a \rho a \ \forall a \in A \iff (a, a) \in \rho$
 $\forall a \in A \iff \delta_A = \{(a, a) \mid a \in A\} \subseteq \rho$.

b) ρ é simétrica $\iff (a \rho b \iff b \rho a) \iff ((a, b) \in \rho \iff (b, a) \in \rho)$
 $\iff ((a, b) \in \rho \iff (a, b) \in \rho^{-1}) \iff \rho = \rho^{-1}$.

c) " \Rightarrow ": Seja ρ antisimétrica (hipótese) e suponha $(a, b) \in \rho \cap \rho^{-1}$. Isto significa que $a \rho b$ e $a \rho^{-1} b$, ou seja, $a \rho b$ e $b \rho a$. Pela anti-simetria concluímos $a = b$ e daí $(a, b) = (a, a) \in \delta_A$. Logo, $\rho \cap \rho^{-1} \subseteq \delta_A$.

" \Leftarrow ": Seja $\rho \cap \rho^{-1} \subseteq \delta_A$ (hipótese) e suponha $a, b \in A$ são tais que $a \rho b$ e $b \rho a$. Isto significa $(a, b) \in \rho \cap \rho^{-1}$. Pela hipótese portanto $(a, b) \in \delta_A$, ou seja, $a = b$. Vemos que ρ é antisimétrica.

d) " \Rightarrow ": Seja ρ transitiva (hipótese) e suponha $a, c \in A$ são tais que

$(a, c) \in \rho \circ \rho$. Existe portanto $b \in A$ tal que $\begin{cases} a \rho b \\ e \\ b \rho c \end{cases}$. Devido à transitividade,

concluímos $a \rho c$, ou seja, $(a, c) \in \rho$. Logo, $\rho \circ \rho \subseteq \rho$.

" \Leftarrow ": Seja $\rho \circ \rho \subseteq \rho$ (hipótese) e suponha $a, b, c \in A$ são tais que $a \rho b$ e $b \rho c$. Isto significa que $(a, c) \in \rho \circ \rho$. Por hipótese então, $(a, c) \in \rho$, ou seja, $a \rho c$. Vemos que ρ é transitiva.

■

I.1.17 Definição.

Uma relação $\varepsilon \in \mathbf{2}^{A \times A}$ chama-se uma *relação de equivalência em A*, se ε é reflexiva, simétrica e transitiva, i.e. se

$$1) \ \delta_A \subseteq \varepsilon, \quad 2) \ \varepsilon^{-1} = \varepsilon \quad \text{e} \quad 3) \ \varepsilon \circ \varepsilon \subseteq \varepsilon.$$

O conjunto de todas as relações de equivalência em A denotamos por $\mathbf{Eq}(A)$. Temos portanto

$$\mathbf{Eq}(A) \subseteq \mathbf{2}^{A \times A}.$$

Se $\varepsilon \in \mathbf{Eq}(A)$ e se $a, b \in A$ com $a \varepsilon b$, dizemos que

a e b são *equivalentes modulo ε* .

I.1.18 Exemplos.

a) Para qualquer conjunto $A \neq \emptyset$, temos

$$\delta_A \in \mathbf{Eq}(A) \quad \text{e também} \quad A \times A \in \mathbf{Eq}(A),$$

i.e. tanto a relação da igualdade, quanto a relação universal em A são relações de equivalência em A . Particularmente, sempre $\mathbf{Eq}(A) \neq \emptyset$.

b) Seja A um conjunto de bolas (de várias cores). Definindo-se $\forall a, b \in A$:

$$a \varepsilon b \iff a \text{ e } b \text{ possuem a mesma cor},$$

temos que $\varepsilon \in \mathbf{Eq}(A)$.

■

I.1.19 Definição.

Se ε é uma relação de equivalência em A , e se $a \in A$, então colocamos

$$\bar{a} = \{x \in A \mid x \varepsilon a\}.$$

O subconjunto \bar{a} de A chama-se

a *classe de equivalência de a mod ε* (lido: a modulo ε).

I.1.20 Exemplo.

Seja A um conjunto de bolas e $\varepsilon \in \mathbf{Eq}(A)$ a relação

$$\forall a, b \in A : \quad a \varepsilon b \iff a \text{ e } b \text{ têm a mesma cor}.$$

Para cada $a \in A$, a classe de equivalência de a mod ε é

$$\bar{a} = \{x \in A \mid x \text{ tem a cor de } a\}.$$

■

I.1.21 Proposição.

Seja $A \neq \emptyset$ um conjunto e $\varepsilon \in \mathbf{Eq}(A)$. Então valem para todos os $a, b \in A$:

a) $a \in \bar{a}$, particularmente, $\bar{a} \neq \emptyset$.

b) $\bar{a} = \bar{b} \iff a \varepsilon b$.

$$c) \quad \bar{a} \neq \bar{b} \implies \bar{a} \cap \bar{b} = \emptyset.$$

$$d) \quad \bigcup_{a \in A} \bar{a} = A.$$

Demonstração: a) Pela reflexividade de ε temos $a \in \bar{a}$ e portanto $\bar{a} \neq \emptyset \quad \forall a \in A$.

b) " \Rightarrow ": De $\bar{a} = \bar{b}$ segue $a \in \bar{b} = \{x \in A \mid x \varepsilon b\}$. Logo $a \varepsilon b$.

" \Leftarrow ": Seja $a \varepsilon b$. Para todo $x \in \bar{a}$ temos $x \varepsilon a \varepsilon b$ e daí $x \in \bar{b}$. Segue $\bar{a} \subseteq \bar{b}$. Da mesma forma: Para todo $x \in \bar{b}$ temos $x \varepsilon b \varepsilon a$ e daí $x \in \bar{a}$. Segue $\bar{b} \subseteq \bar{a}$. Logo $\bar{a} = \bar{b}$.

c) Suponhamos $\bar{a} \cap \bar{b} \neq \emptyset$ e seja $x \in \bar{a} \cap \bar{b}$. Temos $a \varepsilon x \varepsilon b$ e daí por b): $\bar{a} = \bar{x} = \bar{b}$.

d) Claramente, $\bigcup_{a \in A} \bar{a} \subseteq A$. Mas, como $a \in \bar{a}$, temos de fato $\bigcup_{a \in A} \bar{a} = A$.

■

I.1.22 Definição.

Seja $A \neq \emptyset$ um conjunto e $\mathfrak{P} \subseteq 2^A$ uma família de subconjuntos de A . Dizemos que \mathfrak{P} é uma *partição* de A , se

$$a) \quad \emptyset \notin \mathfrak{P}$$

$$b) \quad \text{Para todos os } X, Y \in \mathfrak{P} \text{ temos } X = Y \text{ ou } X \cap Y = \emptyset.$$

$$c) \quad \bigcup_{X \in \mathfrak{P}} X = A.$$

Por I.1.21 temos o

I.1.23 Exemplo.

Seja $\varepsilon \in \mathbf{Eq}(A)$ e

$$\mathfrak{P}_\varepsilon = \{\bar{a} \mid a \in A\} \quad \text{com } \bar{a} = \{x \in A \mid x \varepsilon a\},$$

o conjunto das classes de equivalência de $A \text{ mod } \varepsilon$.

Então \mathfrak{P}_ε é uma partição de A .

\mathfrak{P}_ε chama-se a *partição de A induzida por ε* .

■

Vale também ao contrário que

toda partição é induzida por uma relação de equivalência:

I.1.24 Proposição.

Seja $\mathfrak{P} \subseteq 2^A$ uma partição de A e defina uma relação $\varepsilon_{\mathfrak{P}}$ por $\forall a, b \in A$:

$$a \varepsilon_{\mathfrak{P}} b \iff \exists X \in \mathfrak{P} \text{ com } a, b \in X.$$

Então

a) $\varepsilon_{\mathfrak{P}} \in \mathbf{Eq}(A)$

b) $\mathfrak{P}_{\varepsilon_{\mathfrak{P}}} = \mathfrak{P}.$

Demonstração: a) Como $\bigcup_{X \in \mathfrak{P}} X = A$, vemos que para todo $a \in A$ existe $X \in \mathfrak{P}$ com $a \in X$. Isto mostra $a \varepsilon_{\mathfrak{P}} a \quad \forall a \in A$, i.e. a reflexividade da relação $\varepsilon_{\mathfrak{P}}$.

Se $a, b \in A$ são tais que $a \varepsilon_{\mathfrak{P}} b$, então existe $X \in \mathfrak{P}$ com $a, b \in X$. Segue $b \varepsilon_{\mathfrak{P}} a$ e vemos a simetria de $\varepsilon_{\mathfrak{P}}$.

Sejam $a, b, c \in A$ com $a \varepsilon_{\mathfrak{P}} b$ e $b \varepsilon_{\mathfrak{P}} c$. Assim, existem $X, Y \in \mathfrak{P}$ com $a, b \in X$ e $b, c \in Y$. Como $b \in X \cap Y$, concluímos $X = Y$, ou seja, $a, c \in X = Y \in \mathfrak{P}$. Logo, $a \varepsilon_{\mathfrak{P}} c$ e temos a transitividade de $\varepsilon_{\mathfrak{P}}$.

Assim provamos $\varepsilon_{\mathfrak{P}} \in \mathbf{Eq}(A)$.

b) Como $a \varepsilon_{\mathfrak{P}} b \iff a$ e b pertencem ao mesmo $X \in \mathfrak{P}$, é claro que as classes de equivalência $\text{mod } \varepsilon_{\mathfrak{P}}$ são exatamente os conjuntos de \mathfrak{P} .

■

I.1.25 Definição.

Seja A um conjunto, $\varepsilon \in \mathbf{Eq}(A)$ e $\bar{a} = \{x \in A \mid x \varepsilon a\}$ a classe de equivalência de $a \text{ mod } \varepsilon$ para todo $a \in A$.

A partição $\mathfrak{P}_{\varepsilon}$ escrevemos também como

$$A/\varepsilon = \mathfrak{P}_{\varepsilon} = \{\bar{a} \mid a \in A\}$$

e chamamos A/ε o conjunto quociente de $A \text{ mod } \varepsilon$.

Ao invés de usar letras como ε, η, \dots , etc. para indicar relações de equivalência, os sinais mais comuns empregados na literatura são \equiv, \sim, \approx , etc. Assim, devemos escrever, por exemplo:

Se $\equiv, \sim \in \mathbf{Eq}(A)$, então

$A/\equiv = \{\bar{a} \mid a \in A\}$ é o conjunto quociente de $A \bmod \equiv$,

$A/\sim = \{\hat{a} \mid a \in A\}$ é o conjunto quociente de $A \bmod \sim$,

onde $\bar{a} = \{x \in A \mid x \equiv a\}$ é a classe de $a \bmod \equiv$,

$\hat{a} = \{x \in A \mid x \sim a\}$ é a classe de $a \bmod \sim$.

$$a \equiv b \iff \bar{a} = \bar{b}, \quad a \sim b \iff \hat{a} = \hat{b},$$

etc.

■

I.1.26 Exemplo importante

Seja $A = \mathbb{Z}$ e $n \in \mathbb{N}_0$. Para todos os $a, b \in \mathbb{Z}$ definamos

$$a \equiv_n b \iff a - b \text{ é múltiplo de } n.$$

Leia-se: "a é congruente a b modulo n". Então valem:

- $\equiv_n \in \mathbf{Eq}(\mathbb{Z})$.
- Vale $\equiv_0 = \delta_{\mathbb{Z}}$ e $\equiv_1 = \mathbb{Z} \times \mathbb{Z}$, i.e. \equiv_0 é a relação da igualdade, enquanto \equiv_1 é a relação universal em \mathbb{Z} .
- Para todo $a \in \mathbb{Z}$ temos $\bar{a} = \{a + nk \mid k \in \mathbb{Z}\}$.
- Se $n > 0$, então $\mathbb{Z} = \bar{0} \cup \bar{1} \cup \dots \cup \overline{n-1}$ e $\bar{i} \neq \bar{j}$ para todos os i, j com $0 \leq i \neq j \leq n-1$.
- Se $n > 0$, o conjunto quociente de $\mathbb{Z} \bmod n$ é

$$\mathbb{Z}/\equiv_n = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\} \text{ e vale } |\mathbb{Z}/\equiv_n| = n.$$

É mais comum, escrever-se o conjunto quociente \mathbb{Z}/\equiv_n como $\mathbb{Z}/n\mathbb{Z}$ ou $\mathbb{Z}/(n)$. A partição

$$\mathbb{Z}/(n) = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$$

chama-se o conjunto das *classes de resto* mod n .

Demonstração: a) Para todos os $a \in \mathbb{Z}$ temos $a - a = 0 = 0 \cdot n$. Portanto, $a \equiv_n a$ e vemos que \equiv_n é uma relação reflexiva.

Se $a \equiv_n b$, então $a - b$ é múltiplo de n . Segue que também $b - a = -(a - b)$ é múltiplo de n e daí $b \equiv_n a$, mostrando a simetria da \equiv_n .

Se $a \equiv_n b$ e $b \equiv_n c$, isto significa que $a - b$ e $b - c$ são múltiplos de n . Segue que também $a - c = (a - b) + (b - c)$ é múltiplo de n , ou seja, $a \equiv_n c$. Vemos a transitividade da \equiv_n .

b) $a \equiv_0 b$ significa $a - b = 0$, ou seja $a = b$. Logo $\equiv_0 = \delta_{\mathbb{Z}}$ é a relação da igualdade em \mathbb{Z} .

Como qualquer número em \mathbb{Z} é múltiplo de 1, vemos que $a \equiv_1 b$ vale para todos os $a, b \in \mathbb{Z}$. Portanto, $\equiv_1 = \mathbb{Z} \times \mathbb{Z}$ é a relação universal em \mathbb{Z} .

c) Temos $x \in \bar{a} \iff x \equiv_n a \iff x - a = nk$ é múltiplo de $n \iff x = a + kn$ com $k \in \mathbb{Z}$.

d) Todo $a \in \mathbb{Z}$ pode ser dividido por $n > 0$ com resto entre 0 e $n-1$, ou seja, existem $k, r \in \mathbb{Z}$ com $a = nk + r$ e $0 \leq r \leq n-1$. Logo $a \equiv_n r$, mostrando $\mathbb{Z} = \bar{0} \cup \bar{1} \cup \dots \cup \overline{n-1}$. Se $0 \leq i, j \leq n-1$, então $0 \leq |i-j| \leq n-1$. A única maneira de $i-j$ ser múltiplo de n é portanto $i-j = 0$, ou seja, $i = j$. Logo, as classes $\bar{0}, \bar{1}, \dots, \overline{n-1}$ são distintas e segue $|\mathbb{Z}/\equiv_n| = n$.

e) É consequência de d).

I.1.27 Exemplos.

a) Para $n = 2$ obtemos

$$\mathbb{Z} = \bar{0} \cup \bar{1} \quad \text{e} \quad \mathbb{Z}/\equiv_2 = \{\bar{0}, \bar{1}\}.$$

Esta é a partição de \mathbb{Z} nos números *pares e ímpares*.

b) Para $n = 3$ obtemos

$$\mathbb{Z} = \bar{0} \cup \bar{1} \cup \bar{2} \quad \text{e} \quad \mathbb{Z}/\equiv_3 = \{\bar{0}, \bar{1}, \bar{2}\}.$$

.....

c) Para $n = 9$ obtemos

$$\mathbb{Z} = \bar{0} \cup \bar{1} \cup \bar{2} \cup \bar{3} \cup \bar{4} \cup \bar{5} \cup \bar{6} \cup \bar{7} \cup \bar{8} \quad \text{e} \\ \mathbb{Z}/\equiv_9 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}, \bar{8}\}.$$

d) etc.

§ I.2 Aplicações (funções)

DEFINIÇÃO E EXEMPLOS

I.2.1 Definição.

Sejam $A, B \neq \emptyset$ dois conjuntos.

Uma relação $\varphi \in \mathbf{2}^{A \times B}$ chama-se uma *aplicação (função)* de A em B , se

- i) $\forall a \in A \exists b \in B$ com $a \varphi b$.
 - ii) $\forall a \in A, \forall b, b'$ temos: $a \varphi b$ e $a \varphi b' \implies b = b'$.
- i) diz que $\mathbf{D}(\varphi) = A$, i.e. o domínio de definição de φ é o conjunto A todo.
ii) diz que o elemento $b \in B$ que é φ -relacionado com $a \in A$ é determinado de maneira única por a .

Este único $b \in B$ que é φ -relacionado com $a \in A$ chama-se o *valor* de φ em a e é escrito como

$$b = \varphi(a) .$$

A imagem de φ , i.e. $\mathbf{I}(\varphi) = \{b \in B \mid \exists a \in A \text{ com } a \varphi b\}$ é agora o conjunto de todos os valores de φ . Portanto

$$\mathbf{I}(\varphi) = \{\varphi(a) \mid a \in A\} .$$

Escreve-se portanto também $\mathbf{I}(\varphi) = \varphi(A)$.

O conjunto de todas as aplicações de A em B denotamos por

$$B^A = \{\varphi \in \mathbf{2}^{A \times B} \mid \varphi \text{ é uma aplicação de } A \text{ em } B\} .$$

(ver a explicação desta notação em I.2.9).

Temos portanto

$$B^A \subseteq \mathbf{2}^{A \times B} .$$

Se $\varphi \in B^A$, então podemos escrever

$$\varphi = \{(a, \varphi(a)) \mid a \in A\} .$$

I.2.2 Exemplos.

a₁) Seja $A = B = \mathbb{R}$. A relação $\rho \in \mathbf{2}^{\mathbb{R} \times \mathbb{R}}$ seja definida por

$$\rho = \{ (a, b) \mid 4a^2 + 9b^2 = 36 \} .$$

Temos $\mathbf{D}(\rho) = [-3, 3]$ e $\mathbf{I}(\rho) = [-2, 2]$ e $\rho \notin \mathbb{R}^{\mathbb{R}}$,

i.e. esta ρ não é uma aplicação de \mathbb{R} em \mathbb{R} .

a₂) Seja $A = [-3, 3]$ e $B = \mathbb{R}$. $\varphi \in \mathbf{2}^{[-3,3] \times \mathbb{R}}$ seja definida por

$$\varphi = \{ (a, b) \mid 4a^2 + 9b^2 = 36; b \leq 0 \} .$$

Temos $\mathbf{D}(\varphi) = [-3, 3] = A$ e $\mathbf{I}(\varphi) = [-2, 0]$ e $\varphi \in \mathbb{R}^{[-3,3]}$.

Também podemos escrever

$$\varphi = \left\{ \left(a, -\frac{\sqrt{36-4a^2}}{3} \right) \mid a \in [-3, 3] \right\} .$$

b) Seja $A = \{ \spadesuit, \heartsuit, \clubsuit \}$, $B = \{ a, b, c, d, e \}$.

b₁) Para

$$\varphi = \{ (\spadesuit, b), (\heartsuit, a), (\clubsuit, d) \}$$

temos $\varphi \in B^A$ e vale $\mathbf{I}(\varphi) = \varphi(A) = \{ a, b, d \}$.

b₂) Para

$$\rho = \{ (\spadesuit, b), (\heartsuit, a), (\spadesuit, b), (\clubsuit, d) \}$$

temos $\rho \notin B^A$, pois o "valor de ρ " em \heartsuit não é único.

b₃) Para

$$\rho = \{ (\spadesuit, b), (\heartsuit, a), (\clubsuit, d) \}$$

temos $\rho \notin B^A$, pois $\mathbf{D}(\rho) = \{ \spadesuit, \heartsuit, \clubsuit \} \neq A$.

■

I.2.3 Três Exemplos importantes

a) Seja B um conjunto e consideremos $A = \mathbb{N} = \{ 1, 2, 3, \dots \}$.

Toda aplicação $\varphi \in B^{\mathbb{N}}$ é denominada uma *seqüência* em B .

Se $\varphi(n) = b_n \in B$ é o valor de φ em $n \in \mathbb{N}$, temos que

$$\varphi = \{ (n, \varphi(n)) \mid n \in \mathbb{N} \} = \{ (n, b_n) \mid n = 1, 2, 3, \dots \} .$$

Escreve-se a seqüência φ também como

$$\varphi = (b_1, b_2, b_3, \dots, b_n, \dots) = (b_n)_{n \in \mathbb{N}} .$$

$B^{\mathbb{N}}$ é portanto o conjunto de todas as seqüências em B .

b) Seja $A \neq \emptyset$ um conjunto e $\varepsilon \in \mathbf{Eq}(A)$. Seja

$$A/\varepsilon = \{\bar{a} \mid a \in A\} \text{ o conjunto quociente de } A \text{ mod } \varepsilon.$$

Lembrando: $\forall a \in A : \bar{a} = \{x \in A \mid x \varepsilon a\}$ é a classe de equivalência de $a \text{ mod } \varepsilon$. A aplicação

$$\gamma \in (A/\varepsilon)^A ,$$

definida por $\gamma(a) = \bar{a} \quad \forall a \in A$ chama-se a *aplicação canónica de A sobre A/ε* . Temos portanto

$$\gamma = \{(a, \bar{a}) \mid a \in A\} ,$$

i.e. a aplicação canónica associa a cada elemento $a \in A$ a sua classe de equivalência $\text{mod } \varepsilon$ na qual ele está.

Por exemplo, se $A = \{1, 2, 3, 4, 5\}$ e se

$$\begin{aligned} \varepsilon &= \{(1, 1), (2, 2), (3, 3), (4, 4), (5, 5), (2, 5), (5, 2), (3, 4), (4, 3)\} = \\ &= \delta_A \cup \{(2, 5), (5, 2), (3, 4), (4, 3)\} , \end{aligned}$$

temos assim:

$$A/\varepsilon = \{\{1\}, \{2, 5\}, \{3, 4\}\}$$

e $\gamma = \{(1, \{1\}), (2, \{2, 5\}), (3, \{3, 4\}), (4, \{3, 4\}), (5, \{2, 5\})\}$.

c) Sejam $A_1, A_2, \dots, A_r \neq \emptyset$ conjuntos e

$$M = A_1 \times A_2 \times \dots \times A_r$$

seu produto CARTESIANO. Seja $i \in \{1, 2, \dots, r\}$. A aplicação

$$\pi_i \in A_i^M \subseteq M^M \text{ tal que}$$

$$\pi_i((a_1, a_2, \dots, a_r)) = a_i \quad \forall (a_1, a_2, \dots, a_r) \in M$$

chama-se a *projeção de M sobre A_i*
 (também: a *i -ésima projeção de M*).

Por exemplo, se $M = A \times B = \{(a, b) \mid a \in A, b \in B\}$, as duas projeções de M sobre A e sobre B são dadas por

$$\pi_1((a, b)) = a \quad \text{e} \quad \pi_2((a, b)) = b \quad \forall (a, b) \in M.$$

■

Será que uma relação de equivalência ε pode ser uma aplicação? A resposta é:

I.2.4 Observação.

Se A é um conjunto e $\varepsilon \in \mathbf{Eq}(A)$ é uma relação de equivalência em A , então

$$\varepsilon \in A^A \iff \varepsilon = \delta_A,$$

i.e. uma relação de equivalência é uma aplicação, se e somente se ela é a relação da igualdade.

A diagonal δ_A é portanto também denominada a *função idêntica em A* .

Demonstração: Claro que δ_A é uma aplicação (detalhar!).

Reciprocamente, se $\varepsilon \neq \delta_A$, vai existir um par $(a, b) \in \varepsilon$ com $a \neq b$. Vamos ter $(a, a) \in \varepsilon$ e também $(a, b) \in \varepsilon$, ou seja ε "assume dois valores distintos" em a . Logo, $\varepsilon \notin A^A$.

■

A CARACTERIZAÇÃO DAS APLICAÇÕES ENTRE AS RELAÇÕES

I.2.5 Proposição.

Para qualquer relação $\rho \in \mathbf{2}^{A \times B}$ temos

a) $\delta_A \subseteq \rho^{-1} \circ \rho \iff \mathbf{D}(\rho) = A$

b) $\delta_B \supseteq \rho \circ \rho^{-1} \iff$ para todo $a \in \mathbf{D}(\rho)$ existe um único $b \in B$ com $a \rho b$.

Demonstração: a) " \Rightarrow ": Suponhamos $\delta_A \subseteq \rho^{-1} \circ \rho$ (hipótese) e seja dado qualquer $a \in A$. Temos $(a, a) \in \delta_A$ e pela hipótese, concluímos $(a, a) \in \rho^{-1} \circ \rho$. Isto

significa que existe $b \in B$ com $\begin{cases} a \rho b \\ b \rho^{-1} a \end{cases}$. Particularmente, a é ρ -relacionado com b . Portanto, $\mathbf{D}(\rho) = A$.

" \Leftarrow ": Suponhamos $\mathbf{D}(\rho) = A$ (hipótese) e seja dado um qualquer $(a, a) \in \delta_A$.

Pela hipótese, existe pelo menos um $b \in B$ com $a \rho b$. Temos então $\begin{cases} a \rho b \\ b \rho^{-1} a \end{cases}$.

Isto significa $(a, a) \in \rho^{-1} \circ \rho$. Logo $\delta_A \subseteq \rho^{-1} \circ \rho$.

b) " \Rightarrow ": Suponha, $\delta_B \supseteq \rho \circ \rho^{-1}$ (hipótese) e sejam $a \in A, b, b' \in B$ com

$a \rho b$ e $a \rho b'$. Vale então $\begin{cases} b \rho^{-1} a \\ a \rho b' \end{cases}$. Isto significa $b \rho \circ \rho^{-1} b'$, ou seja,

$(b, b') \in \rho \circ \rho^{-1}$. Por hipótese então, $(b, b') \in \delta_B$. Portanto, $b = b'$.

" \Leftarrow ": Suponha, para todo $a \in \mathbf{D}(\rho)$ exista um *único* $b \in B$ com $a \rho b$ (hipótese) e seja dado qualquer $(b, b') \in \rho \circ \rho^{-1}$. Existe portanto $a \in A$ com

$\begin{cases} b \rho^{-1} a \\ a \rho b' \end{cases}$. Isto significa $\begin{cases} a \rho b \\ a \rho b' \end{cases}$. Pela hipótese, $b = b'$. Logo,

$(b, b') = (b, b) \in \delta_B$ e portanto $\delta_B \supseteq \rho \circ \rho^{-1}$.

■

Portanto: As seguintes propriedades

caracterizam as *aplicações* entre todas as *relações* de A em B :

I.2.6 Conseqüência.

Seja $\varphi \in \mathbf{2}^{A \times B}$. Equivalentes são:

a) $\varphi \in B^A$.

b) $\delta_A \subseteq \varphi^{-1} \circ \varphi$ e $\delta_B \supseteq \varphi \circ \varphi^{-1}$

■

I.2.7 Exemplos.

a) Para $A = B = \mathbb{R}$ e $\varphi = \{(x, x^2) \mid x \in \mathbb{R}\} \in \mathbf{2}^{\mathbb{R} \times \mathbb{R}}$ temos

$$\begin{aligned}\varphi^{-1} \circ \varphi &= \{(x^2, x) \mid x \in \mathbb{R}\} \circ \{(x, x^2) \mid x \in \mathbb{R}\} = \\ &= \{(x, x) \mid x \in \mathbb{R}\} \cup \{(x, -x) \mid x \in \mathbb{R}\} \supseteq \delta_{\mathbb{R}} = \delta_A\end{aligned}$$

e

$$\begin{aligned}\varphi \circ \varphi^{-1} &= \{(x, x^2) \mid x \in \mathbb{R}\} \circ \{(x^2, x) \mid x \in \mathbb{R}\} = \\ &= \{(x^2, x^2) \mid x \in \mathbb{R}\} \subseteq \delta_{\mathbb{R}} = \delta_B.\end{aligned}$$

Portanto φ é uma aplicação de \mathbb{R} em \mathbb{R} .

b) Para $A = B = \mathbb{R}$ e $\rho = \{(x^2, x) \mid x \in \mathbb{R}\} \in \mathbf{2}^{\mathbb{R} \times \mathbb{R}}$ temos

$$\begin{aligned}\rho^{-1} \circ \rho &= \{(x, x^2) \mid x \in \mathbb{R}\} \circ \{(x^2, x) \mid x \in \mathbb{R}\} = \\ &= \{(x^2, x^2) \mid x \in \mathbb{R}\} = \{(y, y) \mid 0 \leq y \in \mathbb{R}\} \not\supseteq \delta_{\mathbb{R}} = \delta_A.\end{aligned}$$

e

$$\begin{aligned}\rho \circ \rho^{-1} &= \{(x^2, x) \mid x \in \mathbb{R}\} \circ \{(x, x^2) \mid x \in \mathbb{R}\} = \\ &= \{(x, x) \mid x \in \mathbb{R}\} \cup \{(x, -x) \mid x \in \mathbb{R}\} \not\subseteq \delta_{\mathbb{R}} = \delta_B.\end{aligned}$$

Portanto, $\mathbf{D}(\rho) \neq A$ e também "os valores da ρ " não são únicos. Particularmente, ρ não é uma aplicação de \mathbb{R} em \mathbb{R} .

Detalhar isto !

■

I.2.8 Proposição.

Sejam $A, B \neq \emptyset$ conjuntos, $\varphi, \psi \in B^A$ duas aplicações de A em B . Então

$$\varphi = \psi \iff \varphi(a) = \psi(a) \quad \forall a \in A.$$

i.e. duas aplicações de A em B coincidem se e somente se elas assumem o mesmo valor para todos os argumentos.

Demonstração: Temos

$$\varphi = \{(a, b) \in A \times B \mid a \varphi b\} = \{(a, \varphi(a)) \mid a \in A\}$$

e
$$\psi = \{(x, y) \in A \times B \mid x \psi y\} = \{(x, \psi(x)) \mid x \in A\}.$$

" \Leftarrow ": $\varphi(a) = \psi(a) \forall a \in A$ significa $(a, \varphi(a)) = (a, \psi(a)) \forall a \in A$.

Portanto, $\varphi = \psi$.

" \Rightarrow ": Se $\varphi = \psi$, então $(a, \varphi(a)) \in \psi \forall a \in A$. Portanto, para todo $a \in A$ existe $x \in A$ com $(a, \varphi(a)) = (x, \psi(x))$. Segue $a = x$ e $\varphi(a) = \psi(x) = \psi(a)$. ■

Vemos que uma aplicação φ de um conjunto finito $A = \{1, 2, \dots, m\}$ em B é essencialmente determinada e pode ser identificada com a m -úpla dos seus valores, i. e. com

$$(\varphi(1), \varphi(2), \dots, \varphi(m)) \in B^m .$$

O conjunto das aplicações de A em B é portanto essencialmente a potência CARTESIANA B^m .

A notação B^A para indicar o conjunto de todas as aplicações de A em B justifica-se agora pela seguinte

I.2.9 Observação.

Se A e B são conjuntos finitos com, digamos $|A| = m$ e $|B| = n$ elementos, então

$$|B^A| = |B|^{|A|} = n^m .$$

Demonstração: Podemos supor $A = \{1, 2, 3, \dots, m\}$. A afirmação fica clara, se lembramos $|B^m| = |B|^m$.

COMPOSIÇÃO DE APLICAÇÕES

I.2.10 Proposição.

Sejam $A, B, C \neq \emptyset$ conjuntos, $\varphi \in B^A$ e $\psi \in C^B$. Então

$$\psi \circ \varphi \in C^A ,$$

i.e. a relação composta (ver I.1.11) de duas aplicações é uma aplicação.

Além disso, o valor único que a composta $\psi \circ \varphi$ assume em todo $a \in A$ é calculado por

$$(\psi \circ \varphi)(a) = \psi(\varphi(a)) .$$

Demonstração: Claro que $\psi \circ \varphi \in \mathbf{2}^{A \times C}$. Por I.2.6 devemos mostrar que

$$\delta_A \subseteq (\psi \circ \varphi)^{-1} \circ (\psi \circ \varphi) \quad \text{e} \quad \delta_C \supseteq (\psi \circ \varphi) \circ (\psi \circ \varphi)^{-1}.$$

Observando-se a hipótese

$$\delta_A \subseteq \varphi^{-1} \circ \varphi, \quad \delta_B \supseteq \varphi \circ \varphi^{-1}, \quad \delta_B \subseteq \psi^{-1} \circ \psi \quad \text{e} \quad \delta_C \supseteq \psi \circ \psi^{-1},$$

obtemos de fato:

$$\begin{aligned} (\psi \circ \varphi)^{-1} \circ (\psi \circ \varphi) &= (\varphi^{-1} \circ \psi^{-1}) \circ (\psi \circ \varphi) = \varphi^{-1} \circ (\psi^{-1} \circ \psi) \circ \varphi \supseteq \\ &\supseteq \varphi^{-1} \circ \delta_B \circ \varphi = \varphi^{-1} \circ \varphi \supseteq \delta_A. \end{aligned}$$

Também

$$\begin{aligned} (\psi \circ \varphi) \circ (\psi \circ \varphi)^{-1} &= (\psi \circ \varphi) \circ (\varphi^{-1} \circ \psi^{-1}) = \psi \circ (\varphi \circ \varphi^{-1}) \circ \psi^{-1} \subseteq \\ &\subseteq \psi \circ \delta_B \circ \psi^{-1} = \psi \circ \psi^{-1} \subseteq \delta_C. \end{aligned}$$

Consequentemente, $\psi \circ \varphi \in C^A$.

Como é calculado o valor $(\psi \circ \varphi)(a) \in C$?

Temos para todo $(a, c) \in A \times C$:

$$\begin{aligned} (a, c) \in \psi \circ \varphi &\iff \exists b \in B \text{ tal que } a \varphi b \text{ e } b \psi c \iff \\ &\iff b = \varphi(a) \text{ e } c = \psi(b) \iff c = \psi(\varphi(a)) \end{aligned}$$

Logo,

$$c = (\psi \circ \varphi)(a) = \psi(\varphi(a)).$$

Portanto, podemos dizer também que

$$\psi \circ \varphi = \left\{ (a, \psi(\varphi(a))) \mid a \in A \right\}.$$

■

I.2.11 Notação.

Se $A = \{1, 2, 3, \dots, m\}$ e B é um conjunto qualquer, uma notação transparente para indicar uma aplicação $\varphi \in B^A$ é escrever-se uma $(2 \times m)$ -matriz que contém na primeira linha os m argumentos $k \in A$, na segunda linha os valores $\varphi(k) \in B$ correspondentes:

$$\varphi = \begin{pmatrix} 1 & 2 & 3 & \dots & m-1 & m \\ \varphi(1) & \varphi(2) & \varphi(3) & \dots & \varphi(m-1) & \varphi(m) \end{pmatrix}.$$

Se $B = \{b_1, b_2, \dots, b_n\}$, podemos escrever

$$\varphi = \begin{pmatrix} 1 & 2 & 3 & \dots & m-1 & m \\ b_{i_1} & b_{i_2} & b_{i_3} & \dots & b_{i_{m-1}} & b_{i_m} \end{pmatrix}$$

onde $\varphi(k) = b_{i_k}$ ($1 \leq k \leq m$) são os valores (talvez com repetições) os quais φ assume:

$$b_{i_1}, b_{i_2}, \dots, b_{i_m} \in B = \{b_1, b_2, \dots, b_n\}.$$

Sejam $A = \{1, 2, \dots, m\}$, $B = \{b_1, b_2, \dots, b_n\}$ dois conjuntos com m e n elementos, respectivamente e seja $C \neq \emptyset$ um conjunto qualquer.

Sejam $\varphi \in B^A$ e $\psi \in C^B$ aplicações, digamos

$$\varphi = \begin{pmatrix} 1 & 2 & 3 & \dots & m-1 & m \\ b_{i_1} & b_{i_2} & b_{i_3} & \dots & b_{i_{m-1}} & b_{i_m} \end{pmatrix}$$

e

$$\psi = \begin{pmatrix} b_1 & b_2 & b_3 & \dots & b_{n-1} & b_n \\ c_1 & c_2 & c_3 & \dots & c_{n-1} & c_n \end{pmatrix}.$$

Então a composta $\psi \circ \varphi \in C^A$ é

$$\psi \circ \varphi = \begin{pmatrix} 1 & 2 & 3 & \dots & m-1 & m \\ c_{i_1} & c_{i_2} & c_{i_3} & \dots & c_{i_{m-1}} & c_{i_m} \end{pmatrix}.$$

Particularmente, se $A = B = C = \{1, 2, \dots, m\}$ e as $\varphi, \psi \in A^A$ são

$$\varphi = \begin{pmatrix} 1 & 2 & 3 & \dots & m-1 & m \\ i_1 & i_2 & i_3 & \dots & i_{m-1} & i_m \end{pmatrix}$$

e

$$\psi = \begin{pmatrix} 1 & 2 & 3 & \dots & m-1 & m \\ j_1 & j_2 & j_3 & \dots & j_{m-1} & j_m \end{pmatrix},$$

temos

$$\psi \circ \varphi = \begin{pmatrix} 1 & 2 & 3 & \dots & m-1 & m \\ j_{i_1} & j_{i_2} & j_{i_3} & \dots & j_{i_{m-1}} & j_{i_m} \end{pmatrix}.$$

APLICAÇÕES INJETORAS, SOBREJETORAS E BIJETORAS

Mencionamos primeiro que a relação inversa de uma aplicação em geral não é uma aplicação:

I.2.12 Exemplos.

i) Para $A = B = \mathbb{R}$ e

$$\varphi = \{(a, a^2) \mid a \in \mathbb{R}\} \in \mathbb{R}^{\mathbb{R}} = B^A,$$

a relação inversa é

$$\varphi^{-1} = \{(a^2, a) \mid a \in \mathbb{R}\} = \{(b, \pm\sqrt{b}) \mid 0 \leq b \in \mathbb{R}\} \notin \mathbb{R}^{\mathbb{R}} = A^B.$$

Isto, pois $\mathbf{D}(\varphi^{-1}) = \mathbf{I}(\varphi) = \{x \in \mathbb{R} \mid x \geq 0\} \neq \mathbb{R} = B$.

Além do mais, $(a^2, a) \in \varphi^{-1}$ e também $(a^2, -a) = ((-a)^2, -a) \in \varphi^{-1}$.

ii) Para $A = \{\spadesuit, \heartsuit, \clubsuit, \diamondsuit\}$ e $B = \{1, 2, 3, 4, 5\}$ e

$$\varphi = \{(\spadesuit, 4), (\heartsuit, 4), (\clubsuit, 2), (\diamondsuit, 5)\} = \begin{pmatrix} \spadesuit & \heartsuit & \clubsuit & \diamondsuit \\ 4 & 4 & 2 & 5 \end{pmatrix} \in B^A,$$

temos

$$\varphi^{-1} = \{(4, \spadesuit), (4, \heartsuit), (2, \clubsuit), (5, \diamondsuit)\} \notin A^B,$$

pois $\mathbf{D}(\varphi^{-1}) = \{2, 4, 5\} \neq B$. Também o "valor de φ^{-1} " em 4 não é único.

I.2.13 Definição.

Sejam $A, B \neq \emptyset$ conjuntos e $\varphi \in B^A$. Dizemos que φ é uma aplicação

a) *injetora* de A em B , se $\forall a, a' \in A: \varphi(a) = \varphi(a') \implies a = a'$.

Equivalentemente: φ é injetora, se $a \neq a' \implies \varphi(a) \neq \varphi(a')$.

b) *sobrejetora* de A sobre B , se $\forall b \in B \exists a \in A$ tal que $\varphi(a) = b$.

Equivalentemente: φ é sobrejetora, se $\varphi(A) = B$.

c) *bijetora* de A sobre B , se φ for injetora e sobrejetora simultaneamente.

I.2.14 Notações.

Se A e B são conjuntos, denotamos por

$$\mathbf{Inj}(A, B), \quad \mathbf{Sob}(A, B) \quad \text{e} \quad \mathbf{Bij}(A, B)$$

os *conjuntos* das aplicações injetoras, sobrejetoras e bijetoras, respectivamente. Temos portanto

$$\mathbf{Bij}(A, B) = \mathbf{Inj}(A, B) \cap \mathbf{Sob}(A, B) \subseteq \mathbf{Inj}(A, B) \cup \mathbf{Sob}(A, B) \subseteq B^A.$$

No caso $A = B$, o conjunto $\mathbf{Bij}(A, A)$ possui um significado importante. Abreviamos escrevendo

$$\mathbf{S}_A = \mathbf{Bij}(A, A).$$

Os elementos em \mathbf{S}_A chamam-se as *permutações* de A , i.e.

\mathbf{S}_A é o conjunto de todas as permutações de A .

Para $A \neq \emptyset$ temos $\delta_A \in \mathbf{S}_A$. Portanto, sempre $\mathbf{S}_A \neq \emptyset$.

Porém:

I.2.15 Advertência.

Para $A \neq B$ é bem possível $\mathbf{Inj}(A, B) = \emptyset$ ou $\mathbf{Sob}(A, B) = \emptyset$:

Por exemplo, se A e B são conjuntos *finitos*, temos

$$\mathbf{Inj}(A, B) \neq \emptyset \iff |B| \geq |A|,$$

$$\mathbf{Sob}(A, B) \neq \emptyset \iff |B| \leq |A|, \quad (\text{porquê? detalhar isto!})$$

$$\mathbf{Bij}(A, B) \neq \emptyset \iff |B| = |A|.$$

I.2.16 Exemplos.

a) Para $A = B = \mathbb{R}$ temos:

a₁) $\varphi = \{(a, 3^a) \mid a \in \mathbb{R}\}$ é uma aplicação injetora de $A = \mathbb{R}$ em $B = \mathbb{R}$. Mas ela não é sobrejetora, pois

$$\varphi(\mathbb{R}) = \{3^a \mid a \in \mathbb{R}\} = \{x \in \mathbb{R} \mid x > 0\} \neq \mathbb{R} = B.$$

Portanto, $\varphi \in \mathbf{Inj}(\mathbb{R}, \mathbb{R}) \setminus \mathbf{Sob}(\mathbb{R}, \mathbb{R})$.

a₂) $\varphi = \{(a, a^3 - a) \mid a \in \mathbb{R}\}$ é uma aplicação sobrejetora de $A = \mathbb{R}$ sobre $B = \mathbb{R}$ (porquê?, demonstração!). Ela não é injetora, pois

$$\varphi(-1) = \varphi(0) = \varphi(1). \text{ Portanto,}$$

$$\varphi \in \mathbf{Sob}(\mathbb{R}, \mathbb{R}) \setminus \mathbf{Inj}(\mathbb{R}, \mathbb{R}).$$

a₃) $\varphi = \{(a, a^3) \mid a \in \mathbb{R}\}$ é uma aplicação bijetora de $A = \mathbb{R}$ sobre $B = \mathbb{R}$, i.e. uma permutação de \mathbb{R} .

$$\text{Portanto } \varphi \in \mathbf{S}_{\mathbb{R}}.$$

b) b₁) Para $A = \{\spadesuit, \heartsuit, \clubsuit\}$ e $B = \{1, 2, 3, 4, 5\}$ temos que

$$\varphi = \{(\spadesuit, 3), (\heartsuit, 4), (\clubsuit, 2), (\spadesuit, 1)\} = \begin{pmatrix} \spadesuit & \heartsuit & \clubsuit \\ 3 & 4 & 2 \\ \spadesuit & & \spadesuit \end{pmatrix} \in \mathbf{Inj}(A, B) \setminus \mathbf{Sob}(A, B).$$

b₂) Para $A = \{\spadesuit, \heartsuit, \clubsuit\}$ e $B = \{1, 2, 3\}$ temos que

$$\varphi = \{(\spadesuit, 3), (\heartsuit, 3), (\clubsuit, 2), (\spadesuit, 1)\} = \begin{pmatrix} \spadesuit & \heartsuit & \clubsuit \\ 3 & 3 & 2 \\ \spadesuit & & \spadesuit \end{pmatrix} \in \mathbf{Sob}(A, B) \setminus \mathbf{Inj}(A, B).$$

b₃) Para $A = \{\spadesuit, \heartsuit, \clubsuit\}$ e $B = \{1, 2, 3, 4\}$ temos que

$$\varphi = \{(\spadesuit, 3), (\heartsuit, 4), (\clubsuit, 2), (\spadesuit, 1)\} = \begin{pmatrix} \spadesuit & \heartsuit & \clubsuit \\ 3 & 4 & 2 \\ \spadesuit & & \spadesuit \end{pmatrix} \in \mathbf{Bij}(A, B).$$

b₄) Para $A = B = \{\spadesuit, \heartsuit, \clubsuit\}$ temos que

$$\varphi = \{(\spadesuit, \heartsuit), (\heartsuit, \spadesuit), (\clubsuit, \clubsuit), (\clubsuit, \heartsuit)\} = \begin{pmatrix} \spadesuit & \heartsuit & \clubsuit \\ \heartsuit & \spadesuit & \clubsuit \\ \spadesuit & & \spadesuit \end{pmatrix} \in \mathbf{S}_A,$$

i.e. φ é uma permutação de A .

■

I.2.17 Proposição.

Sejam $A, B \neq \emptyset$ conjuntos e $\varphi \in B^A$. Então

$$\text{a) } \varphi \text{ é injetora} \iff \delta_A \supseteq \varphi^{-1} \circ \varphi \iff \delta_A = \varphi^{-1} \circ \varphi$$

$$\text{b) } \varphi \text{ é sobrejetora} \iff \delta_B \subseteq \varphi \circ \varphi^{-1} \iff \delta_B = \varphi \circ \varphi^{-1}.$$

$$\text{c) } \varphi \text{ é bijetora} \iff \delta_A = \varphi^{-1} \circ \varphi \text{ e } \delta_B = \varphi \circ \varphi^{-1}.$$

Demonstração: a) Para qualquer aplicação temos $\delta_A \subseteq \varphi^{-1} \circ \varphi$ (I.2.6). Portanto, a segunda equivalência fica clara. Só é preciso provar a primeira:

" \Rightarrow ": Suponha φ injetora e seja dado $(a, a') \in \varphi^{-1} \circ \varphi$. Então existe $b \in B$

tal que $\begin{cases} a \varphi b \\ e \\ b \varphi^{-1} a' \end{cases}$. Isto significa $\begin{cases} a \varphi b \\ e \\ a' \varphi b \end{cases}$, ou seja, $\varphi(a) = b = \varphi(a')$.

Pela injetividade concluímos $a = a'$. Portanto $(a, a') = (a, a) \in \delta_A$, o que mostra $\varphi^{-1} \circ \varphi \subseteq \delta_A$.

" \Leftarrow ": Suponha $\delta_A \supseteq \varphi^{-1} \circ \varphi$ e sejam $a, a' \in A$ com $\varphi(a) = b = \varphi(a')$.

Temos portanto $\begin{cases} a \varphi b \\ e \\ a' \varphi b \end{cases}$. Isto significa $\begin{cases} a \varphi b \\ e \\ b \varphi^{-1} a' \end{cases}$, ou seja, $(a, a') \in \varphi^{-1} \circ \varphi$.

Por hipótese então $(a, a') \in \delta_A$ e segue $a = a'$. Logo φ é injetora.

b) Para qualquer aplicação temos $\delta_B \supseteq \varphi \circ \varphi^{-1}$ (I.2.6). Portanto também agora, a segunda equivalência fica clara. Só é preciso provar a primeira:

" \Rightarrow ": Suponha φ sobrejetora e seja dado $(b, b) \in \delta_B$ onde b é qualquer elemento em B . Por hipótese, existe (pelo menos um) $a \in A$ com $\varphi(a) = b$,

i.e. $\begin{cases} b \varphi^{-1} a \\ e \\ a \varphi b \end{cases}$. Isto significa $(b, b) \in \varphi \circ \varphi^{-1}$. Logo, $\delta_B \subseteq \varphi \circ \varphi^{-1}$.

" \Leftarrow ": Suponha reciprocamente, $\delta_B \subseteq \varphi \circ \varphi^{-1}$ e seja dado $b \in B$. Temos $(b, b) \in \delta_B$ e por hipótese portanto $(b, b) \in \varphi \circ \varphi^{-1}$. Logo existe $a \in A$ com

$\begin{cases} b \varphi^{-1} a \\ e \\ a \varphi b \end{cases}$. Isto significa que descobrimos um $a \in A$ com $b = \varphi(a)$ e vemos que φ é "sobre".

c) é uma consequência de a) e b).

■

I.2.18 Conseqüência.

Sejam $A, B \neq \emptyset$ conjuntos e $\varphi \in B^A$. Então

$$\varphi^{-1} \in A^B \iff \varphi \in \mathbf{Bij}(A, B),$$

i.e. a relação inversa φ^{-1} de uma aplicação $\varphi \in B^A$, é uma aplicação de B em A , se e somente se φ é uma aplicação *bijetora* de A sobre B .

Além do mais: Se φ é uma aplicação bijetora, então a aplicação φ^{-1} também é bijetora, i.e.

$$\varphi^{-1} \in \mathbf{Bij}(B, A) \text{ e vale } (\varphi^{-1})^{-1} = \varphi, \quad \varphi^{-1} \circ \varphi = \delta_A \text{ e } \varphi \circ \varphi^{-1} = \delta_B.$$

■

I.2.19 Exemplos.

a) Para $A = B = \mathbb{R}$, a função $\varphi = \{(x, x^2) \mid x \in \mathbb{R}\} \in \mathbb{R}^{\mathbb{R}}$ não é nem injetora, nem sobrejetora, pois (ver I.2.17)

$$\varphi^{-1} \circ \varphi = \{(x, x) \mid x \in \mathbb{R}\} \cup \{(x, -x) \mid x \in \mathbb{R}\} \neq \delta_{\mathbb{R}} = \delta_A$$

e

$$\varphi \circ \varphi^{-1} = \{(x^2, x^2) \mid x \in \mathbb{R}\} \neq \delta_{\mathbb{R}} = \delta_B.$$

b) Para $A = B = \mathbb{R}$ e $\varphi = \{(x, \arctg x) \mid x \in \mathbb{R}\} \in \mathbb{R}^{\mathbb{R}}$ temos

$$\begin{aligned} \varphi^{-1} \circ \varphi &= \{(\arctg x, x) \mid x \in \mathbb{R}\} \circ \{(x, \arctg x) \mid x \in \mathbb{R}\} = \\ &= \{(x, x) \mid x \in \mathbb{R}\} = \delta_{\mathbb{R}} = \delta_A, \end{aligned}$$

mas

$$\begin{aligned} \varphi \circ \varphi^{-1} &= \{(x, \arctg x) \mid x \in \mathbb{R}\} \circ \{(\arctg x, x) \mid x \in \mathbb{R}\} = \\ &= \{(y, y) \mid -\frac{\pi}{2} < y < \frac{\pi}{2}\} \neq \delta_{\mathbb{R}} = \delta_B. \end{aligned}$$

Portanto φ é uma aplicação *injetora*, mas não *sobrejetora* de \mathbb{R} em \mathbb{R} .

c) Para $A = B = \mathbb{R}$ e $\varphi = \{(x, x^3 - x) \mid x \in \mathbb{R}\} \in \mathbb{R}^{\mathbb{R}}$ temos

$$\begin{aligned} \varphi^{-1} \circ \varphi &= \{(x^3 - x, x) \mid x \in \mathbb{R}\} \circ \{(x, x^3 - x) \mid x \in \mathbb{R}\} = \\ &= \{(x, x) \mid x \in \mathbb{R}\} \cup \left\{ \left(x, \frac{-x + \sqrt{4 - 3x^2}}{2} \right) \mid -\frac{2}{\sqrt{3}} \leq x \leq \frac{2}{\sqrt{3}} \right\} \cup \\ &\quad \cup \left\{ \left(x, \frac{-x - \sqrt{4 - 3x^2}}{2} \right) \mid -\frac{2}{\sqrt{3}} \leq x \leq \frac{2}{\sqrt{3}} \right\} \neq \delta_{\mathbb{R}} = \delta_A. \end{aligned}$$

(provar isto! Sugestão: $x^3 - x = z^3 - z \iff z = ??$)

Mas

$$\begin{aligned}\varphi \circ \varphi^{-1} &= \{(x, x^3 - x) \mid x \in \mathbb{R}\} \circ \{(x^3 - x, x) \mid x \in \mathbb{R}\} = \\ &= \{(y, y) \mid y \in \mathbb{R}\} = \delta_{\mathbb{R}} = \delta_B.\end{aligned}$$

Portanto φ é uma aplicação *sobrejetora*, mas não *injetora* de \mathbb{R} em \mathbb{R} .

d) Para $A = B = \mathbb{R}$ e $\varphi = \{(x, x^3) \mid x \in \mathbb{R}\} \in \mathbb{R}^{\mathbb{R}}$ temos

$$\begin{aligned}\varphi^{-1} \circ \varphi &= \{(x^3, x) \mid x \in \mathbb{R}\} \circ \{(x, x^3) \mid x \in \mathbb{R}\} = \\ &= \{(x, x) \mid x \in \mathbb{R}\} = \delta_{\mathbb{R}} = \delta_A.\end{aligned}$$

Também

$$\begin{aligned}\varphi \circ \varphi^{-1} &= \{(x, x^3) \mid x \in \mathbb{R}\} \circ \{(x^3, x) \mid x \in \mathbb{R}\} = \\ &= \{(x^3, x^3) \mid x \in \mathbb{R}\} = \delta_{\mathbb{R}} = \delta_B.\end{aligned}$$

Portanto φ é uma aplicação *bijetora* de \mathbb{R} em \mathbb{R} .

I.2.20 Proposição.

Sejam $A, B, C \neq \emptyset$ conjuntos, $\varphi \in B^A$ e $\psi \in C^B$. Então valem:

- Se $\varphi \in \mathbf{Inj}(A, B)$ e $\psi \in \mathbf{Inj}(B, C)$, então $\psi \circ \varphi \in \mathbf{Inj}(A, C)$.
- Se $\varphi \in \mathbf{Sob}(A, B)$ e $\psi \in \mathbf{Sob}(B, C)$, então $\psi \circ \varphi \in \mathbf{Sob}(A, C)$.
- Se $\varphi \in \mathbf{Bij}(A, B)$ e $\psi \in \mathbf{Bij}(B, C)$, então $\psi \circ \varphi \in \mathbf{Bij}(A, C)$.

Além disso,

$$(\psi \circ \varphi)^{-1} = \varphi^{-1} \circ \psi^{-1} \in \mathbf{Bij}(C, A).$$

Demonstração: Já sabemos $\psi \circ \varphi \in C^A$.

a) Se $a, a' \in A$ e $(\psi \circ \varphi)(a) = (\psi \circ \varphi)(a')$, então $\psi(\varphi(a)) = \psi(\varphi(a'))$. Como ψ é injetora, concluímos $\varphi(a) = \varphi(a')$. Como φ é injetora, concluímos $a = a'$. Logo $\psi \circ \varphi$ é injetora.

b) Seja dado $c \in C$. Como ψ é sobrejetora, existe $b \in B$ com $c = \psi(b)$. Como φ é sobrejetora, para este b vai existir $a \in A$ com $b = \varphi(a)$. Segue que $(\psi \circ \varphi)(a) = \psi(\varphi(a)) = \psi(b) = c$. Logo $\psi \circ \varphi$ é sobrejetora.

c) Segue por combinação de a) e b).

2ª demonstração: a) A injetividade de φ e ψ significa que

$$\delta_A = \varphi^{-1} \circ \varphi \quad \text{e} \quad \delta_B = \psi^{-1} \circ \psi \quad (\text{I.2.17 a}).$$

Devemos mostrar que

$$\delta_A = (\psi \circ \varphi)^{-1} \circ (\psi \circ \varphi).$$

De fato:

$$(\psi \circ \varphi)^{-1} \circ (\psi \circ \varphi) = \varphi^{-1} \circ (\psi^{-1} \circ \psi) \circ \varphi = \varphi^{-1} \circ \delta_B \circ \varphi = \varphi^{-1} \circ \varphi = \delta_A.$$

b) A sobrejetividade de φ e ψ significa que

$$\delta_B = \varphi \circ \varphi^{-1} \quad \text{e} \quad \delta_C = \psi \circ \psi^{-1} \quad (\text{I.2.17 b}).$$

Devemos mostrar que

$$\delta_C = (\psi \circ \varphi) \circ (\psi \circ \varphi)^{-1}.$$

De fato:

$$(\psi \circ \varphi) \circ (\psi \circ \varphi)^{-1} = \psi \circ (\varphi \circ \varphi^{-1}) \circ \psi^{-1} = \psi \circ \delta_B \circ \psi^{-1} = \psi \circ \psi^{-1} = \delta_C.$$

■

I.2.21 Proposição.

Sejam $A, B \neq \emptyset$ conjuntos e $\varphi \in B^A$. Equivalentes são:

a) $\varphi \in \mathbf{Bij}(A, B)$.

b) Existem $\psi, \omega \in A^B$ tais que

$$\psi \circ \varphi = \delta_A \quad \text{e} \quad \varphi \circ \omega = \delta_B.$$

Demonstração: "a) \Rightarrow b)": Suponha φ é bijetora. Então $\varphi^{-1} \in A^B$ e podemos escolher $\psi = \omega = \varphi^{-1}$ e obtemos com esta escolha: $\psi \circ \varphi = \varphi^{-1} \circ \varphi = \delta_A$ tal como $\varphi \circ \omega = \varphi \circ \varphi^{-1} = \delta_B$.

"b) \Rightarrow a)": Suponha a existência das $\psi, \omega \in A^B$ tais que $\psi \circ \varphi = \delta_A$ e $\varphi \circ \omega = \delta_B$.

i) Seja dado $b \in B$. Escolhamos $a = \omega(b)$ e obtemos com esta escolha

$\varphi(a) = \varphi(\omega(b)) = (\varphi \circ \omega)(b) = \delta_B(b) = b$. Portanto $\varphi \in \mathbf{Sob}(A, B)$.

ii) Sejam $a, a' \in A$ tais que $\varphi(a) = \varphi(a')$. Segue $\psi(\varphi(a)) = \psi(\varphi(a'))$, ou seja, $(\psi \circ \varphi)(a) = (\psi \circ \varphi)(a')$. Mas então $a = \delta_A(a) = \delta_A(a') = a'$. Logo $\varphi \in \mathbf{Inj}(A, B)$.

De i) e ii) segue $\varphi \in \mathbf{Bij}(A, B)$. ■

CONJUNTOS EQUIPOTENTES

I.2.22 Definição.

Dois conjuntos $A, B \neq \emptyset$ chamam-se *equipotentes*, se $\mathbf{Bij}(A, B) \neq \emptyset$.

Para conjuntos equipotentes vamos escrever $A \sim B$. Caso contrário, $A \not\sim B$ significa que A e B não são equipotentes. Temos

I.2.23 Proposição.

Se $A, B, C \neq \emptyset$ são três conjuntos, então valem:

- a) $A \sim A$.
- b) Se $A \sim B$, então $B \sim A$.
- c) Se $A \sim B$ e $B \sim C$, então $A \sim C$.

Estas regras dizem portanto que equipotência entre conjuntos podemos interpretar como *relação de equivalência no universo dos conjuntos*.

Demonstração: a) vale, pois $\delta_A \in \mathbf{Bij}(A, A)$ e portanto $\mathbf{Bij}(A, A) \neq \emptyset$.

b) $A \sim B$ significa $\mathbf{Bij}(A, B) \neq \emptyset$. Se $\varphi \in \mathbf{Bij}(A, B)$, então $\varphi^{-1} \in \mathbf{Bij}(B, A)$ (I.2.18). Logo $\mathbf{Bij}(B, A) \neq \emptyset$ e portanto $B \sim A$.

c) $A \sim B$ e $B \sim C$ significa $\mathbf{Bij}(A, B) \neq \emptyset \neq \mathbf{Bij}(B, C)$.

Se $\varphi \in \mathbf{Bij}(A, B)$ e $\psi \in \mathbf{Bij}(B, C)$, então $\psi \circ \varphi \in \mathbf{Bij}(A, C)$ (I.2.20). Logo $\mathbf{Bij}(A, C) \neq \emptyset$, ou seja, $A \sim C$.

I.2.24 Exemplos.

- i) Se A e B são conjuntos finitos, então $A \sim B \iff |A| = |B|$.
- ii) Seja $\mathbb{N} = \{1, 2, 3, \dots\}$ e $2\mathbb{N} = \{2, 4, 6, \dots\}$. Então $\mathbb{N} \sim 2\mathbb{N}$, sendo que para a aplicação φ definida por

$$\varphi(n) = 2n \quad \forall n \in \mathbb{N} \quad \text{temos} \quad \varphi \in \mathbf{Bij}(\mathbb{N}, 2\mathbb{N}) .$$

- iii) $\mathbb{N} \sim \mathbb{Z}$ podemos verificar, olhando na aplicação $\varphi \in \mathbf{Bij}(\mathbb{N}, \mathbb{Z})$, definida por

$$\varphi(n) = \begin{cases} \frac{n}{2} & \text{se } n \text{ é par} \\ -\frac{n-1}{2} & \text{se } n \text{ é ímpar} \end{cases} .$$

- iv) $\mathbb{R} \sim (0, 1)$, sendo que $\varphi \in \mathbf{Bij}(\mathbb{R}, (0, 1))$, quando se define

$$\varphi(x) = \frac{1}{\pi} \cdot \arctg x + \frac{1}{2} \quad \forall x \in \mathbb{R} .$$

É importante tomarmos conhecimento que

existem conjuntos infinitos que não são equipotentes:

I.2.25 Proposição.

$$\mathbb{N} \not\sim \mathbb{N}^{\mathbb{N}} \quad \text{e também} \quad \mathbb{R} \not\sim \mathbb{R}^{\mathbb{R}} .$$

(Em I.2.33 provaremos $A \not\sim A^A$ para qualquer conjunto com $|A| \geq 2$.)

Demonstração: Provaremos a primeira afirmação. A segunda é análoga.

Afirma-se $\mathbf{Bij}(\mathbb{N}, \mathbb{N}^{\mathbb{N}}) = \emptyset$. Como $\mathbf{Bij}(\mathbb{N}, \mathbb{N}^{\mathbb{N}}) \subseteq \mathbf{Sob}(\mathbb{N}, \mathbb{N}^{\mathbb{N}})$, basta provar que

$$\mathbf{Sob}(\mathbb{N}, \mathbb{N}^{\mathbb{N}}) = \emptyset :$$

Seja dada $\Omega \in (\mathbb{N}^{\mathbb{N}})^{\mathbb{N}}$, i.e. uma qualquer aplicação $\Omega : \mathbb{N} \longrightarrow \mathbb{N}^{\mathbb{N}}$. Afirmamos que Ω *jamais pode ser sobrejetora*: Para todo $n \in \mathbb{N}$ indicamos por $\varphi_n = \Omega(n)$ o valor de Ω em n . Assim temos para a imagem da Ω :

$$\Omega(\mathbb{N}) = \{\varphi_1, \varphi_2, \varphi_3, \dots, \varphi_n, \dots\} .$$

Seja $\psi \in \mathbb{N}^{\mathbb{N}}$ definida por

$$\psi(x) = \varphi_x(x) + 1 \quad \forall x \in \mathbb{N} .$$

Afirmamos que $\psi \notin \Omega(\mathbb{N})$: Se fosse $\psi = \varphi_n$ para algum $n \in \mathbb{N}$, teríamos $\psi(x) = \varphi_n(x) \forall x \in \mathbb{N}$. Particularmente, para $x = n$ obteríamos $\varphi_n(n) + 1 = \psi(n) = \varphi_n(n)$ e daí o absurdo $1 = 0$.

Logo, $\psi \in \mathbb{N}^{\mathbb{N}} \setminus \Omega(\mathbb{N})$, mostrando que Ω não é sobrejetora.

I.2.26 Definição.

Um conjunto A é dito *enumerável*, se $A \sim \mathbb{N}$.

Conjuntos enumeráveis são portanto os conjuntos cujos elementos podem ser escritos em forma de uma seqüência $A = \{a_1, a_2, a_3, \dots\}$.

Temos que $\mathbb{N}^{\mathbb{N}}$ é um conjunto não-enumerável. Pode-se provar facilmente que $\mathbb{R} \sim \mathbb{N}^{\mathbb{N}}$. Portanto também \mathbb{R} não é enumerável.

Mencionamos que \mathbb{Z} e \mathbb{Q} são conjuntos enumeráveis (para \mathbb{Z} ver I.2.24 iii).

I.2.27 Observação.

Para qualquer conjunto A temos

$$A \not\sim 2^A.$$

Demonstração: Vamos colocar $\mathfrak{A} = 2^A$. Afirma-se $\mathbf{Bij}(A, \mathfrak{A}) = \emptyset$ e basta provar $\mathbf{Sob}(A, \mathfrak{A}) = \emptyset$: Seja $\Omega \in \mathfrak{A}^A$ uma qualquer aplicação. Afirmamos que Ω jamais pode ser sobrejetora: Para todo $a \in A$ indicamos por $X_a = \Omega(a) \subseteq A$ o valor de Ω em a . Temos portanto

$$\Omega(A) = \{X_a \mid a \in A\} \subseteq \mathfrak{A}.$$

Seja $Y \in \mathfrak{A}$ definida por

$$Y = \{y \in A \mid y \notin X_y\}.$$

Afirmamos $Y \notin \Omega(A)$: Se fosse $Y = X_a$ para algum $a \in A$, teríamos $a \in X_a \iff a \notin X_a$, um absurdo.

Logo, $Y \in \mathfrak{A} \setminus \Omega(A)$, mostrando que Ω não é sobrejetora.

I.2.28 Proposição.

Para qualquer conjunto A temos

$$\mathbf{2}^A \sim \{0, 1\}^A,$$

ou seja, o conjunto de todas as partes de A é equipotente com o conjunto de todas as funções de A em $\{0, 1\}$.

Demonstração: Mais uma vez colocamos $\mathfrak{A} = \mathbf{2}^A$. É preciso construir uma função $\Omega \in \mathbf{Bij}(\mathfrak{A}, \{0, 1\}^A)$. Para todo $X \in \mathfrak{A}$ definamos $\chi_X \in \{0, 1\}^A$ por

$$\chi_X(a) = \begin{cases} 0 & \text{se } a \notin X \\ 1 & \text{se } a \in X \end{cases}.$$

(χ_X chama-se a *função característica* ou a *função indicadora* do subconjunto $X \subseteq A$). Coloquemos

$$\Omega(X) = \chi_X \quad \forall X \in \mathfrak{A}$$

e afirmamos

$$\Omega \in \mathbf{Bij}(\mathfrak{A}, \{0, 1\}^A).$$

De fato: Claro que Ω está definida para todo $X \in \mathfrak{A}$ e tem valores em $\{0, 1\}^A$.

A injetividade: Sejam $X, X' \in \mathfrak{A}$ com $\Omega(X) = \Omega(X')$, ou seja, $\chi_X = \chi_{X'}$. Para todo $a \in A$ temos:

$$a \in X \iff \chi_X(a) = 1 \iff \chi_{X'}(a) = 1 \iff a \in X'.$$

Logo $X = X'$. Isto significa $\Omega \in \mathbf{Inj}(\mathfrak{A}, \{0, 1\}^A)$.

A sobrejetividade: Seja dado $\varphi \in \{0, 1\}^A$. Definamos um conjunto $X \in \mathfrak{A}$ por

$$a \in X \iff \varphi(a) = 1.$$

Segue com esta escolha: $\Omega(X) = \chi_X = \varphi$, pois

$$a \in X \iff \chi_X(a) = 1.$$

Portanto $\Omega \in \mathbf{Sob}(\mathfrak{A}, \{0, 1\}^A)$.

Logo, como afirmado $\Omega \in \mathbf{Bij}(\mathfrak{A}, \{0, 1\}^A)$.

■

A DECOMPOSIÇÃO CANÔNICA DE UMA APLICAÇÃO

I.2.29 Proposição.

Sejam $A, B \neq \emptyset$ conjuntos e $\varphi \in B^A$. Para todos os $a, a' \in A$ definamos

$$a \varepsilon_{\varphi} a' \iff \varphi(a) = \varphi(a').$$

Então valem:

- $\varepsilon_{\varphi} \in \mathbf{Eq}(A)$ (ε_{φ} chama-se a relação de equivalência associada à φ).
- Seja γ a aplicação canônica de A sobre A/ε_{φ} , i.e.

$$\gamma(a) = \bar{a} = \{x \in A \mid x \varepsilon_{\varphi} a\}.$$

Afirmamos que existe uma única aplicação

$$\psi \in \mathbf{Bij}(A/\varepsilon_{\varphi}, \varphi(A)), \quad \text{tal que } \psi \circ \gamma = \varphi.$$

Particularmente,

$$A/\varepsilon_{\varphi} \sim \varphi(A).$$

Demonstração: a) é visto facilmente (detalhar!).

b) A unicidade de ψ : Sejam ψ, ψ' bijeções de A/ε_{φ} sobre $\varphi(A)$ com

$$\psi \circ \gamma = \varphi = \psi' \circ \gamma.$$

Segue para todo $a \in A$: $(\psi \circ \gamma)(a) = \varphi(a) = (\psi' \circ \gamma)(a)$, ou seja, $\psi(\gamma(a)) = \psi'(\gamma(a))$, ou seja, $\psi(\bar{a}) = \psi'(\bar{a}) \quad \forall \bar{a} \in A/\varepsilon_{\varphi}$. Isto mostra $\psi = \psi'$.

A existência de ψ : Tentemos definir $\psi : A/\varepsilon_{\varphi} \longrightarrow \varphi(A) \subseteq B$ por

$$\psi(\bar{a}) = \varphi(a) \quad \forall \bar{a} \in A/\varepsilon_{\varphi}.$$

Esta tentativa de definição exige um cuidado especial, pois o conjunto de definição da ψ é um conjunto de classes de equivalência. Cada classe \bar{a} em geral é representada "por muitos a ", a saber, por todos os a' que são equivalentes ao a . Como a aplicação ψ tem que ter um valor único em \bar{a} , a tentativa da definição acima só dará certo

se o valor $\psi(\bar{a})$ definido independe do representante escolhido na classe \bar{a} .

Este cuidado especial é conhecido como *o problema da boa definição* da ψ .

No nosso caso temos de fato:

1) ψ é uma aplicação bem definida:

Se $a, a' \in A$ são tais que $\bar{a} = \bar{a}'$, então $a \varepsilon_{\varphi} a'$, i.e. $\varphi(a) = \varphi(a')$. Segue $\psi(\bar{a}) = \varphi(a) = \varphi(a') = \psi(\bar{a}')$. Portanto, o valor $\psi(\bar{a})$ independe da escolha do representante da classe de equivalência \bar{a} . Temos que ψ é de fato uma aplicação de A/ε_{φ} em B .

2) A sobrejetividade da ψ :

Para todo $b \in \varphi(A)$ existe $a \in A$ com $b = \varphi(a) = \psi(\bar{a})$. Logo, $\psi \in \mathbf{Sob}(A/\varepsilon_{\varphi}, \varphi(A))$.

3) A injetividade da ψ :

Suponhamos $a, a' \in A$ são tais que $\psi(\bar{a}) = \psi(\bar{a}')$. Segue $\varphi(a) = \varphi(a')$, ou seja, $\bar{a} = \bar{a}'$. Portanto, $\psi \in \mathbf{Inj}(A/\varepsilon_{\varphi}, \varphi(A))$.

Vemos que $\psi \in \mathbf{Bij}(A/\varepsilon_{\varphi}, \varphi(A))$.

4) Como $(\psi \circ \gamma)(a) = \psi(\gamma(a)) = \psi(\bar{a}) = \varphi(a)$ para todos os $a \in A$, vemos $\psi \circ \gamma = \varphi$.

■

I.2.30 Exemplo.

Sejam $A = B = \mathbb{R}$ e $\varphi \in \mathbb{R}^{\mathbb{R}}$ definida por

$$\varphi(a) = \text{sen } 2\pi a \quad \forall a \in \mathbb{R}.$$

Temos $\varphi(\mathbb{R}) = [-1, 1] \subseteq \mathbb{R}$ e $\forall a, a' \in \mathbb{R}$:

$$\varphi(a) = \varphi(a') \iff a \varepsilon_{\varphi} a' \iff a - a' \in \mathbb{Z} \text{ ou } a + a' \in \frac{1}{2} + \mathbb{Z}.$$

Além disso, para todo $a \in \mathbb{R}$:

$$\bar{a} = \left\{ x \in \mathbb{R} \mid a - x \in \mathbb{Z} \text{ ou } a + x \in \frac{1}{2} + \mathbb{Z} \right\}.$$

A aplicação canônica $\gamma \in (\mathbb{R}/\varepsilon_{\varphi})^{\mathbb{R}}$ é:

$$\gamma(a) = \bar{a} = \left\{ x \in \mathbb{R} \mid a - x \in \mathbb{Z} \text{ ou } a + x \in \frac{1}{2} + \mathbb{Z} \right\} \quad \forall a \in \mathbb{R}.$$

A função $\psi \in \mathbf{Bij}(\mathbb{R}/\varepsilon_{\varphi}, [-1, 1])$ tal que $\varphi = \psi \circ \gamma$ é

$$\psi(\bar{a}) = \text{sen } 2\pi a \quad \forall \bar{a} \in \mathbb{R}/\varepsilon_{\varphi}.$$

Primeiro vamos generalizar o resultado de I.2.21:

I.2.31 Proposição.

Sejam $A, B \neq \emptyset$ conjuntos e $\varphi \in B^A$. Então:

- a) $\varphi \in \mathbf{Inj}(A, B) \iff \exists \psi \in A^B$ com $\psi \circ \varphi = \delta_A$.
 b) $\varphi \in \mathbf{Sob}(A, B) \iff \exists \omega \in A^B$ com $\varphi \circ \omega = \delta_B$.

Demonstração: a) " \Leftarrow ": Suponha a existência de $\psi \in A^B$ com $\psi \circ \varphi = \delta_A$ e sejam $a, a' \in A$ com $\varphi(a) = \varphi(a')$. Segue $\psi(\varphi(a)) = \psi(\varphi(a'))$, ou seja, $a = \delta_A(a) = (\psi \circ \varphi)(a) = (\psi \circ \varphi)(a') = \delta_A(a') = a'$. Logo $\varphi \in \mathbf{Inj}(A, B)$.

" \Rightarrow ": Suponha φ injetora. Escolhamos um $a_0 \in A$ fixo. Para todo $b \in \varphi(A)$ existe um *único* $a \in A$ com $\varphi(a) = b$ devido à injetividade de φ . Definamos $\psi_{a_0} \in A^B$ por

$$\psi_{a_0}(b) = \begin{cases} a & \text{se } \varphi(a) = b \in \varphi(A) \\ a_0 & \text{se } b \notin \varphi(A). \end{cases}$$

Então vale $(\psi_{a_0} \circ \varphi)(a) = \psi_{a_0}(\varphi(a)) = a \quad \forall a \in A$. Portanto $\psi_{a_0} \circ \varphi = \delta_A$.

(Mencionamos que se φ não é sobrejetora, esta função construída ψ_{a_0} não é única, pois ela depende da escolha do $a_0 \in A$).

b) " \Leftarrow ": Suponha a existência de $\omega \in A^B$ com $\varphi \circ \omega = \delta_B$ e seja dado $b \in B$. Escolhendo-se $a = \omega(b)$ obtemos $b = \delta_B(b) = (\varphi \circ \omega)(b) = \varphi(\omega(b)) = \varphi(a)$ e vemos que φ é sobrejetora.

" \Rightarrow ": Suponha φ é sobrejetora. Para todo $b \in B$ consideremos o conjunto

$$X_b = \{a \in A \mid \varphi(a) = b\} \subseteq A.$$

Temos portanto a família

$$\mathfrak{F} = \{X_b \mid b \in B\} \subseteq \mathbf{2}^A,$$

uma certa família de subconjuntos de A . Pela sobrejetividade de φ temos $X_b \neq \emptyset \quad \forall b \in B$, i.e. \mathfrak{F} não contém a parte vazia de A (de fato \mathfrak{F} é uma partição de A ! [porquê?]).

Vamos escolher agora *simultaneamente* em cada um destes conjuntos X_b exatamente um elemento $a \in X_b$ para todo $b \in B$ e vamos chamar este a escolhido

de $a = \omega(b)$. Temos portanto $\omega \in A^B$ e vale para todo $b \in B$:

$$(\varphi \circ \omega)(b) = \varphi(\omega(b)) = \varphi(a) = b = \delta_B(b). \text{ Portanto, } \varphi \circ \omega = \delta_B.$$

■

Olhando-se nesta segunda parte " \Rightarrow " da demonstração de b), vemos que acabamos de usar um argumento estranho: Depois do surgimento de uma partição $\mathfrak{F} = \{X_b \mid b \in B\}$ de A "escolha-se *simultaneamente* para cada $b \in B$ " (i.e. para cada $X_b \in \mathfrak{F}$) um $a \in X_b$ e chame-se este a escolhido de $\omega(b)$.

Porquê esta escolha *simultânea* é possível e é um processo "lógicamente limpo" ?

Em geral não existe nenhuma "hierarquia" dentro do conjunto X_b , i.e. não vamos dispor de nenhuma "regra natural" que possa destacar entre todos os $a \in X_b$ um certo a_0 que seria "melhor" do que todos os outros a (uma espécie de "reizinho" de X_b).

O problema geral podemos ver assim:

Dado é uma família $\mathfrak{F} \subseteq 2^A$ de subconjuntos de um conjunto A com $\emptyset \notin \mathfrak{F}$.

Porquê posso garantir a existência de uma função, digamos α , definida na família \mathfrak{F} com valores em $\bigcup_{X \in \mathfrak{F}} X \subseteq A$ (i.e. $\alpha \in A^{\mathfrak{F}}$), de tal maneira que

$$\alpha(X) \in X \text{ para todo } X \in \mathfrak{F}?$$

Preciso portanto de uma função α que destaque em cada membro X da família \mathfrak{F} um dos seus elementos.

Vejamos exemplos:

1) Enquanto a família \mathfrak{F} é finita ou se $A = \mathbb{N}$ é o conjunto de todos os números naturais, tal procedimento não tem nenhum problema: Se $\mathfrak{F} \subseteq 2^{\mathbb{N}}$, podemos, pelo princípio da indução, escolher em cada $X \in \mathfrak{F}$ por exemplo seu *menor elemento*, ou seja, $\alpha(X) \in X$ é aquele único elemento em X tal que $\alpha(X) \leq n \forall n \in X$. Sabemos desta maneira "quem são os $\alpha(X) \in X$, *simultaneamente* para todo X ". Assim, neste caso é claro, como uma escolha *simultânea* funciona.

2) Seja $A = \mathbb{R}$ e seja, por exemplo

$$\mathfrak{F} = \{(a, b) \mid a, b \in \mathbb{R}; a < b\},$$

a família de todos os intervalos abertos limitados de \mathbb{R} .

Também neste caso existe uma função "natural" $\alpha \in \mathbb{R}^{\mathfrak{F}}$ com $\alpha((a, b)) \in (a, b)$ para todos os $(a, b) \in \mathfrak{F}$: Podemos associar a cada (a, b) seu ponto médio: $\alpha((a, b)) = \frac{a+b}{2}$.

3) Se considerarmos entretanto $\mathfrak{F} = \mathbf{2}^{\mathbb{R}} \setminus \{\emptyset\}$, a família de todas as partes não-vazias de \mathbb{R} , enfrentamos uma certa dificuldade para realizar a mesma tarefa.

De fato, para o caso geral, não é possível provar ou desprovar a existência de uma função que faça uma tal escolha.

Para superar esta dificuldade na situação geral, é comum *exigir axiomáticamente* a existência de uma tal função:

I.2.32 O axioma da escolha.

Seja A um qualquer conjunto e $\mathfrak{F} \subseteq \mathbf{2}^A$ uma qualquer família de subconjuntos de A tal que $\emptyset \notin \mathfrak{F}$. Então existe uma função $\alpha \in A^{\mathfrak{F}}$ de tal maneira que $\alpha(X) \in X$ para todos os $X \in \mathfrak{F}$.

*Cada tal função α chama-se uma **função de escolha** para \mathfrak{F} .*

Também podemos formular o axioma da escolha assim:

Se A é um conjunto e se $\mathfrak{F} \subseteq \mathbf{2}^A$ é tal que $\emptyset \notin \mathfrak{F}$, então

$$\{\alpha \in A^{\mathfrak{F}} \mid \alpha(X) \in X \ \forall X \in \mathfrak{F}\} \neq \emptyset.$$

A demonstração "limpa" de I.2.31 b) " \Rightarrow " deveria ser assim:

" \Rightarrow ": Suponha φ é sobrejetora. Para todo $b \in B$ consideremos o conjunto

$$X_b = \{a \in A \mid \varphi(a) = b\} \subseteq A.$$

Temos portanto a família

$$\mathfrak{F} = \{X_b \mid b \in B\} \subseteq \mathbf{2}^A,$$

uma certa família de subconjuntos de A . Pela sobrejetividade de φ temos $X_b \neq \emptyset \ \forall b \in B$, i.e. \mathfrak{F} não contém a parte vazia de A . Vemos que \mathfrak{F} é uma

partição de A .

Seja agora $\alpha \in A^{\mathfrak{F}}$ uma função de escolha e definamos $\omega \in A^B$ por

$$\omega(b) = \alpha(X_b) \quad \forall b \in B .$$

Vale para todo $b \in B$:

$$(\varphi \circ \omega)(b) = \varphi(\omega(b)) = \varphi(\alpha(X_b)) = b = \delta_B(b),$$

pois $\alpha(X_b) \in X_b = \{a \in A \mid \varphi(a) = b\}$. Portanto, $\varphi \circ \omega = \delta_B$. ■

Para finalizar a digressão sobre esta problemática, vejamos mais uma aplicação do axioma da escolha, provando a seguinte generalização de I.2.25:

I.2.33 Observação.

Para qualquer conjunto A com $|A| \geq 2$ temos

$$A \not\approx A^A .$$

Demonstração: Afirma-se $\mathbf{Bij}(A, A^A) = \emptyset$ e basta provar $\mathbf{Sob}(A, A^A) = \emptyset$: Seja $\Omega \in (A^A)^A$ uma qualquer aplicação. Afirmamos que Ω jamais pode ser sobrejetora: Para todo $a \in A$ indicamos por $\varphi_a = \Omega(a)$ o valor de Ω em a , i.e.

$$\Omega(A) = \{ \varphi_a \mid a \in A \} .$$

Consideremos para cada $a \in A$ o conjunto $Y_a = A \setminus \{\varphi_a(a)\}$. Temos $Y_a \neq \emptyset$, pois $|A| \geq 2$. Considere agora a família

$$\mathfrak{F} = \{ Y_a \mid a \in A \} .$$

Pelo axioma da escolha, existe uma função de escolha $\alpha \in A^{\mathfrak{F}}$. Temos portanto

$$\alpha(Y_a) \in Y_a , \quad \text{particularmente,} \quad \alpha(Y_a) \neq \varphi_a(a) \quad \forall a \in A .$$

Definamos uma função $\psi \in A^A$ por

$$\psi(x) = \alpha(Y_x) \quad \forall x \in A .$$

Afirmamos $\psi \notin \Omega(A)$: Se fosse $\psi = \varphi_a$ para algum $a \in A$, teríamos

$$\psi(x) = \varphi_a(x) \quad \forall x \in A .$$

Particularmente, para $x = a$ obteríamos

$$\varphi_a(a) = \psi(a) = \alpha(Y_a) \neq \varphi_a(a) ,$$

um absurdo. Logo, $\psi \in A^A \setminus \Omega(A)$, mostrando que Ω não é sobrejetora.

AS ORDENS $|\mathbf{Inj}(m, n)|$ E $|\mathbf{Sob}(m, n)|$

Sejam A e B conjuntos finitos com $|A| = m \in \mathbb{N}$ e $|B| = n \in \mathbb{N}$. Para simplificar, vamos supor

$$A = \{1, 2, 3, \dots, m\} \text{ e } B = \{b_1, b_2, b_3, \dots, b_n\} .$$

Sabemos B^A é finito e vale $|B^A| = |B|^{|A|} = n^m$.

Quantas destas n^m aplicações são injetoras e quantas são sobrejetoras? Queremos portanto descobrir $|\mathbf{Inj}(A, B)|$ e $|\mathbf{Sob}(A, B)|$. Abreviamos

$$\mathbf{Inj}(m, n) = \mathbf{Inj}(A, B) \text{ e } \mathbf{Sob}(m, n) = \mathbf{Sob}(A, B)$$

e colocamos

$$i_n(m) = |\mathbf{Inj}(m, n)| \text{ e } s_n(m) = |\mathbf{Sob}(m, n)| .$$

A pergunta é:

$$i_n(m) = ? \text{ e } s_n(m) = ?$$

Claramente vamos ter

$$i_n(m) \leq n^m \text{ e também } s_n(m) \leq n^m .$$

A resposta para $i_n(m)$ é facilmente obtida: Toda $\varphi \in \mathbf{Inj}(m, n)$ é determinada pela m -upla

$$(\varphi(1), \varphi(2), \dots, \varphi(m)) = (b_{i_1}, b_{i_2}, \dots, b_{i_m})$$

dos valores de φ , cujas coordenadas devem ser *distintas* para que φ seja injetora. Assim, existem n possibilidades para a escolha de $b_{i_1} \in B$, depois $n-1$ escolhas para $b_{i_2} \in B$, depois $n-2$ escolhas para b_{i_3} , ... e finalmente $n-m+1$ escolhas para b_{i_m} . Isto dá um total de $n(n-1)\dots(n-m+1)$ m -uplas distintas com coordenadas distintas, ou seja

$$i_n(m) = n(n-1)(n-2)\dots(n-m+1) = \binom{n}{m} \cdot m! .$$

Portanto temos

I.2.34 Proposição.

A quantidade $i_n(m)$ de aplicações injetoras de um conjunto A com m para um conjunto B com n elementos é dada por

$$i_n(m) = n(n-1)(n-2)\dots(n-m+1) = \binom{n}{m} \cdot m! .$$

Observamos que, para $m > n$ obtemos $i_n(m) = 0$, em acordo com o fato que B tem que conter pelo menos $m = |A|$ elementos para que uma aplicação injetora de A para B possa existir.

Para $m = n$ vemos que $i_n(n) = n!$.

Neste caso temos

$$\mathbf{Inj}(n, n) = \mathbf{Sob}(n, n) = \mathbf{Bij}(n, n),$$

devido à finitude dos conjuntos. Particularmente, o conjunto das permutações \mathbf{S}_A de um conjunto $A = \{1, 2, \dots, n\}$ contém exatamente

$$|\mathbf{S}_A| = i_n(n) = n! \quad \text{elementos.}$$

A determinação de $s_n(m)$ é mais complicada e mencionamos somente o resultado:

I.2.35 Proposição.

A quantidade $s_n(m)$ das aplicações sobrejetoras de um conjunto A de m para um conjunto B de n elementos é dada por

$$s_n(m) = n^m - \binom{n}{n-1}(n-1)^m + \binom{n}{n-2}(n-2)^m \mp \dots + (-1)^k \binom{n}{n-k}(n-k)^m \pm \dots \\ + (-1)^{n-k} \binom{n}{k} k^m \pm \dots + (-1)^{n-1} \binom{n}{1} 1^m ,$$

ou seja,

$$s_n(m) = \sum_{k=1}^n (-1)^{n+k} k^m \cdot \binom{n}{k} .$$

CAPÍTULO II

ESTRUTURAS ALGÉBRICAS

§ II.1 Definições das mais importantes estruturas algébricas

COMPOSIÇÕES INTERNAS

II.1.1 Definição.

Seja $M \neq \emptyset$ um conjunto. Uma (lei de) *composição interna* em M é um elemento

$$\top \in M^{M \times M},$$

i.e. \top (lido: "top") é uma função definida em $M \times M$ com valores em M . \top associa portanto - de forma única - a cada par (a, b) de elementos em M um terceiro elemento

$$\top((a, b)) \in M.$$

\top é uma função de duas variáveis de M com valores em M .

II.1.2 Exemplos.

a) Seja $M = \mathbb{N}$ e

a₁) $\top_1 \in \mathbb{N}^{\mathbb{N} \times \mathbb{N}}$ definida por $\top_1((a, b)) = a + b \quad \forall a, b \in \mathbb{N}$.

a₂) $\top_2 \in \mathbb{N}^{\mathbb{N} \times \mathbb{N}}$ definida por $\top_2((a, b)) = a \cdot b \quad \forall a, b \in \mathbb{N}$.

a₃) $\top_3 \in \mathbb{N}^{\mathbb{N} \times \mathbb{N}}$ definida por $\top_3((a, b)) = a^b \quad \forall a, b \in \mathbb{N}$.

\top_1, \top_2 e \top_3 são 3 exemplos de composições internas de \mathbb{N} .

b) Seja $M = \mathbb{Z}$ e

b₁) $\top_1 \in \mathbb{Z}^{\mathbb{Z} \times \mathbb{Z}}$ definida por $\top_1((a, b)) = a + b \quad \forall a, b \in \mathbb{Z}$.

b₂) $\top_2 \in \mathbb{Z}^{\mathbb{Z} \times \mathbb{Z}}$ definida por $\top_2((a, b)) = a \cdot b \quad \forall a, b \in \mathbb{Z}$.

b₃) $\top_3 \in \mathbb{Z}^{\mathbb{Z} \times \mathbb{Z}}$ definida por $\top_3((a, b)) = a - b \quad \forall a, b \in \mathbb{Z}$.

b₄) $\tau_4 \in \mathbb{Z}^{\mathbb{Z} \times \mathbb{Z}}$ definida por $\tau_4((a, b)) = a^4b - b^5a \quad \forall a, b \in \mathbb{Z}$.

τ_1, τ_2, τ_3 e τ_4 são 4 exemplos de composições internas de \mathbb{Z} .

c) Seja $M = \mathbb{R}$ e

c₁) $\tau_1 \in \mathbb{R}^{\mathbb{R} \times \mathbb{R}}$ definida por $\tau_1((a, b)) = a + b \quad \forall a, b \in \mathbb{R}$.

c₂) $\tau_2 \in \mathbb{R}^{\mathbb{R} \times \mathbb{R}}$ definida por $\tau_2((a, b)) = a \cdot b \quad \forall a, b \in \mathbb{R}$.

c₃) $\tau_3 \in \mathbb{R}^{\mathbb{R} \times \mathbb{R}}$ definida por $\tau_3((a, b)) = a - b \quad \forall a, b \in \mathbb{R}$.

c₄) $\tau_4 \in \mathbb{R}^{\mathbb{R} \times \mathbb{R}}$ definida por

$$\tau_4((a, b)) = \sqrt{a^2 + b^2} - \cos(e^a + ba^2) \quad \forall a, b \in \mathbb{R}.$$

τ_1, τ_2, τ_3 e τ_4 são 4 exemplos de composições internas em \mathbb{R} .

Devemos mencionar que a τ_4 de c₄) não define uma composição interna em \mathbb{Z} ou em \mathbb{N} . Também a $\tau_3 b = a - b$ não é uma composição interna de \mathbb{N} .

d) Seja E um conjunto, $\mathfrak{M} = 2^E$ e

d₁) $\tau_1 \in \mathfrak{M}^{\mathfrak{M} \times \mathfrak{M}}$ definida por $\tau_1((X, Y)) = X \cap Y \quad \forall X, Y \in \mathfrak{M}$.

d₂) $\tau_2 \in \mathfrak{M}^{\mathfrak{M} \times \mathfrak{M}}$ definida por $\tau_2((X, Y)) = X \cup Y \quad \forall X, Y \in \mathfrak{M}$.

d₃) $+$ $\in \mathfrak{M}^{\mathfrak{M} \times \mathfrak{M}}$ definida por

$$+((X, Y)) = (X \cup Y) \setminus (X \cap Y) \quad \forall X, Y \in \mathfrak{M}.$$

τ_1, τ_2 e $+$ (i.e. \cap, \cup e $+$) são 3 exemplos de composições internas de $\mathfrak{M} = 2^E$.

e) Seja $M = \{\spadesuit, \heartsuit, \clubsuit\}$.

A seguinte tabela define uma composição interna de M :

τ	\spadesuit	\heartsuit	\clubsuit
\spadesuit	\spadesuit	\heartsuit	\clubsuit
\heartsuit	\heartsuit	\spadesuit	\heartsuit
\clubsuit	\heartsuit	\spadesuit	\clubsuit

Por exemplo temos $\tau((\clubsuit, \heartsuit)) = \spadesuit$ e $\tau((\spadesuit, \heartsuit)) = \heartsuit$.

■

As composições internas "naturais" em \mathbb{N} , \mathbb{Z} e \mathbb{R} ,

a adição " + " e a multiplicação " · ",

tornam-se nesta interpretação

" funções de duas variáveis com valores no próprio conjunto."

Assim, deveríamos escrever por exemplo

$$+ \in \mathbb{R}^{\mathbb{R} \times \mathbb{R}} \quad \text{e} \quad \cdot \in \mathbb{N}^{\mathbb{N} \times \mathbb{N}} \quad \text{etc. .}$$

Como ninguém escreve $+(a, b)$ para indicar a soma $a + b$, introduzimos também em geral:

Se M é um conjunto e $\top \in M^{M \times M}$ uma composição interna de M , o valor $\top((a, b))$ desta função em (a, b) é indicado por

$$\top((a, b)) = a \top b .$$

$a \top b$ pode ser chamado por exemplo de

" o resultado da \top -composição de a com b ".

O resultado da \top_4 -composição do exemplo c_4) é portanto

$$a \top_4 b = \sqrt{a^2 + b^2} - \cos(e^a + ba^2) \quad \forall a, b \in \mathbb{R} .$$

No exemplo e) temos

$$\clubsuit \top \heartsuit = \nabla \quad \text{e} \quad \spadesuit \top \nabla = \heartsuit .$$

Em geral, o cruzamento da linha do a com a coluna do b é o resultado $a \top b$, para todos os $a, b \in \{ \nabla, \spadesuit, \heartsuit, \clubsuit \}$.

Vemos que uma composição interna \top num conjunto finito $M = \{ a_1, a_2, \dots, a_m \}$ de m elementos é dada e pode ser identificada por um quadro de m^2 entradas:

\top	a_1	a_2	\dots	a_k	\dots	a_m
a_1	$a_1 \top a_1$	$a_1 \top a_2$	\dots	$a_1 \top a_k$	\dots	$a_1 \top a_m$
a_2	$a_2 \top a_1$	$a_2 \top a_2$	\dots	$a_2 \top a_k$	\dots	$a_2 \top a_m$
\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\vdots
a_i	$a_i \top a_1$	$a_i \top a_2$	\dots	$a_i \top a_k$	\dots	$a_i \top a_m$
\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\vdots
a_m	$a_m \top a_1$	$a_m \top a_2$	\dots	$a_m \top a_k$	\dots	$a_m \top a_m$

O resultado $a_i \top a_k \in M$ da \top -composição encontramos no ponto de cruzamento da i -ésima linha com a k -ésima coluna. Como $M^{M \times M}$ é o conjunto de todas as composições internas de M , vemos que existem num conjunto M de m elementos exatamente

$$|M^{M \times M}| = m^{m^2}$$

composições internas (i.e. possibilidades de preencher um quadro de $m \times m$ entradas arbitrariamente com os m elementos de M).

Para que tenhamos uma idéia: Por exemplo no conjunto $\{\heartsuit, \spadesuit, \clubsuit, \diamondsuit\}$ existem

$$4^{16} = 65536^2 \approx 4,29 \cdot 10^9$$

(em palavras: 4,29 bilhões de) composições internas distintas. ■

ESTRUTURAS ALGÉBRICAS

II.1.3 Definição.

Seja $M \neq \emptyset$ um conjunto e $\top \in M^{M \times M}$ uma composição interna de M .

O par

$$(M; \top)$$

chama-se uma *estrutura algébrica com uma composição interna*.

II.1.4 Exemplos.

a) $(\mathbb{N}; \top_1)$, $(\mathbb{N}; \top_2)$, $(\mathbb{N}; \top_3)$, onde $\forall a, b \in \mathbb{N}$:

$$a \top_1 b = a + b, \quad a \top_2 b = a \cdot b, \quad a \top_3 b = a^b$$

são 3 estruturas algébricas com uma composição interna cada.

b) $(\mathbb{Z}; \top_1)$, $(\mathbb{Z}; \top_2)$, $(\mathbb{Z}; \top_3)$, onde $\forall a, b \in \mathbb{Z}$:

$$a \top_1 b = a + b, \quad a \top_2 b = a \cdot b, \quad a \top_3 b = a - b$$

são 3 estruturas algébricas com uma composição interna cada.

c) $(\mathbb{R}; \top_1)$, $(\mathbb{R}; \top_2)$, $(\mathbb{R}; \top_3)$, $(\mathbb{R}; \top_4)$, onde $\forall a, b \in \mathbb{R}$:

$$a \top_1 b = a + b, \quad a \top_2 b = a \cdot b, \quad a \top_3 b = a - b$$

$$a \top_4 b = \sqrt{a^2 + b^2} - \cos(e^a + ba^2),$$

são 4 estruturas algébricas com uma composição interna cada.

d) Para todo conjunto E e $\mathfrak{M} = 2^E$, os pares

$$(\mathfrak{M}; \cap), (\mathfrak{M}; \cup) \text{ e } (\mathfrak{M}; +),$$

(onde $X + Y = (X \cup Y) \setminus (X \cap Y) \quad \forall X, Y \in \mathfrak{M}$)

são três estruturas algébricas com uma composição interna cada.

e) O par

$$(\{\nabla, \spadesuit, \heartsuit, \clubsuit\}; \top),$$

onde a composição

$$\top \in \{\nabla, \spadesuit, \heartsuit, \clubsuit\}^{\{\nabla, \spadesuit, \heartsuit, \clubsuit\}} \times \{\nabla, \spadesuit, \heartsuit, \clubsuit\}^{\{\nabla, \spadesuit, \heartsuit, \clubsuit\}}$$

é definida pela tabela

\top	∇	\spadesuit	\heartsuit	\clubsuit
∇	∇	\spadesuit	∇	\heartsuit
\spadesuit	\heartsuit	∇	\spadesuit	\clubsuit
\heartsuit	\spadesuit	\heartsuit	\clubsuit	\clubsuit
\clubsuit	\spadesuit	\clubsuit	∇	\heartsuit

é uma estrutura algébrica com uma composição interna (entre mais de 4 bilhões possíveis outras no mesmo conjunto!)

■

Às vezes convém considerar no mesmo conjunto várias composições internas simultaneamente:

II.1.5 Definição.

Se $M \neq \emptyset$ é um conjunto e $\top_1, \top_2, \dots, \top_r \in M^{M \times M}$ são r composições internas de M , então o "objeto"

$$(M; \top_1, \top_2, \dots, \top_r)$$

chama-se uma *estrutura algébrica com r composições internas*.

II.1.6 Exemplos.

a) $(\mathbb{R}; +, \cdot)$ é uma estrutura com duas composições internas.

b) Seja E um conjunto, $\mathfrak{M} = 2^E$,

$$(\mathfrak{M}; \cap, \cup, +)$$

é uma estrutura com três composições internas (ver II.1.4 d)).

c) Seja $M = \{\spadesuit, \heartsuit, \clubsuit, \diamondsuit\}$ e $\tau_1, \tau_2 \in M^{M \times M}$ definidas por

τ_1		◇	♠	♥	♣	e	τ_2		◇	♠	♥	♣	
		◇	♠	◇	♥				◇	♣	◇	♠	
		♠	♥	◇	♠				♠	♠	♥	♣	◇
		♥	♠	♥	♣				♥	♥	◇	♠	♣
		♣	♠	♣	◇				♣	♠	◇	♣	♥

Então

$$(\{\spadesuit, \heartsuit, \clubsuit, \diamondsuit\}; \tau_1, \tau_2)$$

é uma estrutura algébrica com 2 composições internas.

d) $(\mathbb{N}; +, \cdot, \top)$ onde $a \top b = a^b \forall a, b \in \mathbb{N}$, é uma estrutura algébrica com 3 composições internas.

Como toda estrutura $(M; \tau_1, \tau_2, \dots, \tau_r)$ com r composições dá origem a r estruturas com uma composição

$$(M; \tau_i) \quad (i = 1, 2, \dots, r),$$

o mais importante é o estudo das estruturas com uma composição interna. ■

É importante que uma composição interna em M induz uma composição interna no conjunto M^A de todas as funções de A em M , para qualquer conjunto A , como mostra a seguinte

II.1.7 Observação.

Seja $(M; \tau_1, \tau_2, \dots, \tau_r)$ uma estrutura algébrica com r composições internas $\tau_1, \tau_2, \dots, \tau_r \in M^{M \times M}$.

Seja $A \neq \emptyset$ um conjunto. Então M^A , o conjunto de todas as aplicações de A em M , torna-se uma estrutura algébrica

$$(M^A; \tau_1^*, \tau_2^*, \dots, \tau_r^*)$$

com r composições internas $\top_1^*, \top_2^*, \dots, \top_r^* \in (M^A)^{M^A \times M^A}$, definindo-se para todos os $i = 1, 2, \dots, r$ e todas as $\varphi, \psi \in M^A$, a função $\varphi \top_i^* \psi \in M^A$ por:

$$(\varphi \top_i^* \psi)(a) = \varphi(a) \top_i \psi(a) \quad \forall a \in A.$$

II.1.8 Exemplos.

- a) Para $A = \{\heartsuit, \spadesuit, \clubsuit, \diamondsuit\}$ e $(M; \top) = (\mathbb{Z}; +)$, a composição $+^*$ em \mathbb{Z}^A é dada por

$$(\varphi +^* \psi)(a) = \varphi(a) + \psi(a) \quad \forall a \in \{\heartsuit, \spadesuit, \clubsuit, \diamondsuit\}.$$

- b) Para $A = \{1, 2, 3, \dots, n\}$ e $(M; \top) = (\mathbb{R}; +)$, os elementos de $M^A = \mathbb{R}^n$ são os vetores n -dimensionais reais.

Se $\varphi = (x_1, x_2, x_3, \dots, x_n)$ e $\psi = (y_1, y_2, y_3, \dots, y_n)$ são dois vetores, sua composição $\varphi +^* \psi$, definida por

$$\begin{aligned} (\varphi +^* \psi)(a) &= \varphi(a) + \psi(a) \quad \forall a \in A \text{ agora é} \\ \varphi +^* \psi &= (x_1, x_2, x_3, \dots, x_n) +^* (y_1, y_2, y_3, \dots, y_n) = \\ &= (x_1 + y_1, x_2 + y_2, x_3 + y_3, \dots, x_n + y_n). \end{aligned}$$

Isto é simplesmente a *adição dos vetores* coordenada a coordenada. ■

PROPRIEDADES ESPECIAIS DE ESTRUTURAS

II.1.9 Definição.

Uma estrutura algébrica $(M; \top)$ é dita *comutativa*, se

$$a \top b = b \top a \quad \forall a, b \in M.$$

II.1.10 Exemplos.

- a) $(\mathbb{N}; +)$ e $(\mathbb{N}; \cdot)$ são duas *estruturas comutativas*.
- b) $(\mathbb{N}; \top)$ com $a \top b = a^b \quad \forall a, b \in \mathbb{N}$ é uma *estrutura não comutativa*.
- c) $(\mathbb{Z}; \top)$ com $a \top b = a - b \quad \forall a, b \in \mathbb{Z}$ é uma *estrutura não comutativa*.

d) Seja $M = \{a_1, a_2, a_3, \dots, a_m\}$ e a estrutura algébrica $(M; \top)$ definida pela tábua

\top	a_1	a_2	\dots	a_i	\dots	a_k	\dots	a_m
a_1	$a_1 \top a_1$	$a_1 \top a_2$	\dots	$a_1 \top a_i$	\dots	$a_1 \top a_k$	\dots	$a_1 \top a_m$
a_2	$a_2 \top a_1$	$a_2 \top a_2$	\dots	$a_2 \top a_i$	\dots	$a_2 \top a_k$	\dots	$a_2 \top a_m$
\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\vdots
a_i	$a_i \top a_1$	$a_i \top a_2$	\dots	$a_i \top a_i$	\dots	$a_i \top a_k$	\dots	$a_i \top a_m$
\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\vdots
a_k	$a_k \top a_1$	$a_k \top a_2$	\dots	$a_k \top a_i$	\dots	$a_k \top a_k$	\dots	$a_k \top a_m$
\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\vdots
a_m	$a_m \top a_1$	$a_m \top a_2$	\dots	$a_m \top a_i$	\dots	$a_m \top a_k$	\dots	$a_m \top a_m$

Temos que $(M; \top)$ é comutativa, se e somente se, a tábua é simétrica com relação a sua diagonal principal.

Demonstração: a) é claro.

b) Por exemplo: $2 \top 3 = 2^3 = 8 \neq 9 = 3^2 = 3 \top 2$

c) Por exemplo: $3 \top -5 = 3 - (-5) = 8 \neq -8 = -5 - 3 = -5 \top 3$

d) A simetria da tábua diz: $a_i \top a_k = a_k \top a_i$ para todos os $i, k = 1, 2, \dots, m$.

■

II.1.11 Observação.

Num conjunto finito de m elementos $M = \{a_1, a_2, \dots, a_m\}$, existem exatamente

$$m^{\frac{m(m+1)}{2}}$$

composições internas comutativas distintas.

Por exemplo, das 4^{16} composições existentes em $M = \{\nabla, \spadesuit, \heartsuit, \clubsuit\}$

4^{10} são comutativas .

Demonstração: Uma composição interna comutativa é determinada, preenchendo-se livremente as posições na diagonal e superior à diagonal. A quantidade destas posições é $1 + 2 + 3 + \dots + m = \frac{m(m+1)}{2}$.

■

CENTRALIZADOR E CENTRO

Em geral, uma estrutura algébrica $(M; \top)$ não é comutativa. Isto não impede que certos elementos nela sejam comutáveis.

II.1.12 Definição.

Seja $(M; \top)$ uma estrutura algébrica e $\emptyset \neq X \subseteq M$. O conjunto

$$\mathbf{C}_M(X) = \{c \in M \mid c \top x = x \top c \ \forall x \in X\}$$

chama-se o *centralizador de X em M*.

$\mathbf{C}_M(X)$ é portanto o conjunto dos elementos em M que comutam com cada elemento de X .

Casos particulares:

1) Para $X = \{x\}$ um conjunto unitário, temos

$$\mathbf{C}_M(x) = \mathbf{C}_M(\{x\}) = \{c \in M \mid c \top x = x \top c\},$$

o *centralizador de x em M*.

2) Para $X = M$ obtemos o *centro de M*:

$$\mathbf{Z}(M) = \mathbf{C}_M(M) = \{c \in M \mid c \top x = x \top c \ \forall x \in M\}$$

Este é o conjunto dos elementos de M que comutam com todo elemento de M .

Claro que $(M; \top)$ é comutativa $\iff \mathbf{Z}(M) = M$.

■

II.1.13 Proposição.

Seja $(M; \top)$ uma estrutura algébrica e $\emptyset \neq X \subseteq Y \subseteq M$ e $x \in M$. Então

- $x \in \mathbf{C}_M(x)$, particularmente, $\mathbf{C}_M(x) \neq \emptyset$.
- $\mathbf{C}_M(Y) \subseteq \mathbf{C}_M(X)$.
- $\mathbf{Z}(M) = \bigcap_{X \subseteq M} \mathbf{C}_M(X) = \bigcap_{x \in M} \mathbf{C}_M(x)$.
- Observamos que $\mathbf{C}_M(X) = \emptyset$ é possível, se $|X| \geq 2$.

Demonstração: a) é claro, pois x comuta com si mesmo.

b) Para $c \in \mathbf{C}_M(Y)$ temos $c \top x = x \top c \quad \forall x \in Y$. Particularmente, como $X \subseteq Y$, temos $c \top x = x \top c \quad \forall x \in X$. Segue $c \in \mathbf{C}_M(X)$ e portanto $\mathbf{C}_M(Y) \subseteq \mathbf{C}_M(X)$.

c) Usando b), a afirmação segue, refletindo-se sobre as seguintes contenções:

$$\mathbf{Z}(M) \subseteq \bigcap_{X \subseteq M} \mathbf{C}_M(X) \subseteq \bigcap_{\{x\} \subseteq M} \mathbf{C}_M(\{x\}) = \bigcap_{x \in M} \mathbf{C}_M(x) \subseteq \mathbf{Z}(M).$$

Para a estrutura $(M; \top)$ com $M = \{a, b\}$ e \top definida por:

\top	a	b
a	b	b
b	a	a

temos por exemplo $\mathbf{Z}(M) = \emptyset$.

Também para $(\mathbb{N}; \top)$, se $a \top b = a^b \quad \forall a, b \in \mathbb{N}$, temos $\mathbf{Z}(\mathbb{N}) = \emptyset$.

■

II.1.14 Definição.

Seja $(M; \top)$ uma estrutura algébrica. Um elemento $e \in M$ é chamado um

a) *elemento neutro (ou identidade) à esquerda*, se

$$e \top x = x \quad \forall x \in M.$$

b) *elemento neutro (ou identidade) à direita*, se

$$x \top e = x \quad \forall x \in M.$$

c) *elemento neutro (ou identidade) bilateral*, se

$$e \top x = x \top e = x \quad \forall x \in M.$$

Claro que, quando $(M; \top)$ é uma estrutura *comutativa*, as noções de identidade (neutro) "à esquerda", "à direita" e "bilateral" são as mesmas.

II.1.15 Exemplos.

- a) a₁) O número 1 é a identidade de $(\mathbb{N}; \cdot)$.
 a₂) A estrutura $(\mathbb{N}; +)$ não possui elemento neutro ($0 \notin \mathbb{N}!$)
 a₃) 1 é a única identidade à direita de $(\mathbb{N}; \top)$ se $a \top b = a^b \forall a, b \in \mathbb{N}$.
 $(\mathbb{N}; \top)$ não possui identidade bilateral.
 a₄) 0 é a única identidade à direita de $(\mathbb{Z}; \top)$ se $a \top b = a - b \forall a, b \in \mathbb{Z}$.
 $(\mathbb{Z}; \top)$ não possui identidade bilateral.
 a₅) 2 e -3 são as identidades à esquerda de $(\mathbb{Z}; \top)$, quando

$$a \top b = a^2b + ab - 5b \quad \forall a, b \in \mathbb{Z} :$$

Temos $e \top b = b \quad \forall b \in \mathbb{Z} \iff e^2b + eb - 5b = b \quad \forall b \in \mathbb{Z} \iff (e - 2)(e + 3)b = 0 \quad \forall b \in \mathbb{Z}$. Para $b \neq 0$, a afirmação segue.

- b) Seja $M = \{\nabla, \spadesuit, \heartsuit, \clubsuit\}$.

- b₁) Se a composição \top em M é dada pela tabela

\top	∇	\spadesuit	\heartsuit	\clubsuit
∇	∇	\spadesuit	\heartsuit	\clubsuit
\spadesuit	\clubsuit	\clubsuit	∇	\spadesuit
\heartsuit	∇	\spadesuit	\heartsuit	\clubsuit
\clubsuit	\clubsuit	\heartsuit	∇	\spadesuit

temos que ∇ e \heartsuit são *dois elementos neutros à esquerda* de $(M; \top)$.

- b₂) Se a composição \top em M é dada pela tabela

\top	∇	\spadesuit	\heartsuit	\clubsuit
∇	\heartsuit	∇	∇	\clubsuit
\spadesuit	\clubsuit	\spadesuit	\spadesuit	\heartsuit
\heartsuit	∇	\heartsuit	\heartsuit	\clubsuit
\clubsuit	∇	\clubsuit	\clubsuit	\spadesuit

temos que \spadesuit e \heartsuit são *dois elementos neutros à direita* de $(M; \top)$.

- b₃) Se a composição \top em M é dada pela tabela

\top	∇	\spadesuit	\heartsuit	\clubsuit
∇	\heartsuit	∇	∇	\clubsuit
\spadesuit	∇	\spadesuit	\heartsuit	\clubsuit
\heartsuit	∇	\heartsuit	\heartsuit	\clubsuit
\clubsuit	∇	\clubsuit	\clubsuit	\spadesuit

temos que \spadesuit é a *identidade bilateral* de $(M; \top)$.

■

II.1.16 Observação.

Seja $(M; \top)$ uma estrutura algébrica, $e' \in M$ uma identidade à esquerda, $e'' \in M$ uma identidade à direita de $(M; \top)$. Então

$$e' = e'' \text{ é a identidade bilateral de } (M; \top) .$$

Particularmente, se $(M; \top)$ possuir mais de uma identidade à esquerda (à direita), então não pode existir nenhuma à direita (à esquerda) e nenhuma bilateral. Além disso, a identidade *bilateral* de $(M; \top)$ (eventualmente existente), é *única*.

Demonstração: Temos $e' \top x = x \quad \forall x \in M$. Particularmente, para $x = e''$ segue $e' \top e'' = e''$. Também $x \top e'' = x \quad \forall x \in M$. Particularmente, para $x = e'$ segue $e' \top e'' = e'$. Logo,

$$e'' = e' \top e'' = e' .$$

■

II.1.17 Observação.

Seja $(M; \top)$ uma estrutura algébrica com identidade bilateral e , digamos.

$$\text{Então } e \in \mathbf{Z}(M) .$$

Particularmente, $\mathbf{C}_M(X) \neq \emptyset$ para todo $\emptyset \neq X \subseteq M$.

Demonstração: Observe que $e \top x = x \top e \quad \forall x \in M$ e $\mathbf{Z}(M) \subseteq \mathbf{C}_M(X)$.

■

II.1.18 Definição.

- a) Uma estrutura algébrica com uma composição interna $(M; \top)$ é denominada um *semigrupo* se a composição interna obedecer à lei associativa, i. e. se temos

$$a \top (b \top c) = (a \top b) \top c$$

para todos os elementos $a, b, c \in M$.

- b) O semigrupo $(M; \top)$ é dito um *monóide*, se possuir uma identidade bilateral.

II.1.19 Exemplos.

- a) $(\mathbb{N}; +)$ e $(\mathbb{N}; \cdot)$ são os semigrupos dos *números naturais aditivo* e dos *números naturais multiplicativo*.

Ambos estes semigrupos são comutativos. $(\mathbb{N}; \cdot)$ é um monóide.

$(\mathbb{N}; +)$ não possui identidade (lembrar: $0 \notin \mathbb{N}$).

- b) Seja $M = (0, 5]$ o intervalo real semi-fechado à direita entre 0 a 5, $\top \in M^{M \times M}$ a composição

$$a \top b = \frac{ab}{5} \quad \forall a, b \in M.$$

Então $(M; \top)$ é um monóide comutativo. Sua identidade é $e = 5$.

Se substituirmos $M = (0, 5]$ pelo intervalo aberto $M' = (0, 5)$,

$(M'; \top)$ será um semigrupo comutativo sem identidade.

- c) A estrutura algébrica $(\mathbb{N}; \top)$ com

$$a \top b = a^b \quad \forall a, b \in \mathbb{N}$$

não é um semigrupo.

- d) A estrutura algébrica $(\mathbb{Z}; \top)$ com

$$a \top b = a - b \quad \forall a, b \in \mathbb{Z}$$

não é um semigrupo.

Demonstração: a) é claro.

b) Para todos os $a, b \in M = (0, 5]$ temos também $a \top b = b \top a = \frac{ab}{5} \in M$. Portanto de fato $\top \in M^{M \times M}$. Além disso, para todos os $a, b, c \in M$ temos

$$a \top (b \top c) = \frac{a \cdot \frac{bc}{5}}{5} = \frac{abc}{25} = \frac{\frac{ab}{5} \cdot c}{5} = (a \top b) \top c.$$

$e \top b = \frac{eb}{5} = b \quad \forall b \in M$ significa $e = 5$. Isto mostra que o semigrupo $(M; \top)$ é um monóide. Além disso, $(M'; \top)$ não possui identidade, pois $5 \notin M'$.

c) Temos $2 \top (3 \top 4) = 2 \top 3^4 = 2^{81}$. Mas $(2 \top 3) \top 4 = 2^3 \top 4 = 8^4 \neq 2^{81}$.

d) Temos $2 \top (3 \top 4) = 2 \top (3 - 4) = 2 - (-1) = 3$.

Mas $(2 \top 3) \top 4 = (2 - 3) \top 4 = (-1) - 4 = -5 \neq 3$.

■

II.1.20 Exemplo importante

Seja $A \neq \emptyset$ um qualquer conjunto e consideremos

$M = A^A$, o conjunto de todas as aplicações de A em si mesmo.

Considerando-se para todas as $\psi, \varphi \in M$ a aplicação composta

$$\psi \circ \varphi,$$

definida por $(\psi \circ \varphi)(a) = \psi(\varphi(a)) \quad \forall a \in A$, vemos que " \circ " define uma composição interna de A^A , i. e.

$$\circ \in M^{M \times M} = (A^A)^{(A^A \times A^A)},$$

e portanto,

$(A^A; \circ)$ é uma estrutura algébrica com uma composição interna.

Sabemos que $\omega \circ (\psi \circ \varphi) = (\omega \circ \psi) \circ \varphi$ para todas as $\omega, \psi, \varphi \in A^A$ (a lei associativa válida e provada em I.1.14 para a composição de relações vale particularmente quando as relações são aplicações!). Portanto, a estrutura algébrica

$$(A^A; \circ)$$

é um *semigrupo*. Além disso, $\delta_A \circ \varphi = \varphi \circ \delta_A = \varphi \quad \forall \varphi \in A^A$.

Logo, $(A^A; \circ)$ possui a identidade δ_A e é portanto um monóide.

$(A^A; \circ)$ chama-se o *monóide de todas as aplicações de A em A*.

II.1.21 Observação.

Para $|A| \geq 2$, o monóide

$(A^A; \circ)$ não é comutativo .

Demonstração: Seja, digamos, A decomposto como $A = \{a, b\} \cup X$ com $X = A \setminus \{a, b\}$, onde $a, b \in A$ são quaisquer dois elementos escolhidos com $a \neq b$ (observe $|A| \geq 2$). Sejam $\varphi, \psi \in M = A^A$ definidas por

$$\varphi(x) = \begin{cases} a & \text{se } x = a \\ a & \text{se } x = b \\ x & \text{se } x \in X \end{cases} \quad \text{e} \quad \psi(x) = \begin{cases} b & \text{se } x = a \\ a & \text{se } x = b \\ x & \text{se } x \in X \end{cases} .$$

Temos $(\psi \circ \varphi)(a) = \psi(\varphi(a)) = \psi(a) = b$, porém

$$(\varphi \circ \psi)(a) = \varphi(\psi(a)) = \varphi(b) = a .$$

Portanto, $(\psi \circ \varphi)(a) \neq (\varphi \circ \psi)(a)$ e segue $\psi \circ \varphi \neq \varphi \circ \psi$.

■

II.1.22 Exemplo.

Para os elementos φ, ψ do monóide $(\mathbb{R}^{\mathbb{R}}; \circ)$ definidos por

$$\varphi(t) = \text{sen } t \quad \text{e} \quad \psi(t) = t^2 \quad \forall t \in \mathbb{R}$$

temos

$$(\psi \circ \varphi)(t) = \psi(\varphi(t)) = (\text{sen } t)^2 = \text{sen }^2 t , \quad \text{porém}$$

$$(\varphi \circ \psi)(t) = \varphi(\psi(t)) = \text{sen}(t^2) .$$

De fato vale para o centro do monóide $(A^A; \circ)$:

II.1.23 Proposição.

Para qualquer conjunto $A \neq \emptyset$ temos

$$\mathbf{Z}(A^A; \circ) = \{\delta_A\} ,$$

i.e. a identidade δ_A é o **único** elemento em A^A que comuta com todos os elementos de A^A .

Demonstração: Esta afirmação certamente está correta se $|A| = |A^A| = 1$. Seja $|A| \geq 2$. Se $\delta_A \neq \varphi \in A^A$, vai existir $x_0 \in A$ tal que $\varphi(x_0) \neq x_0$. Considerando-se a função constante $\psi \in A^A$ definida por $\psi(x) = x_0 \quad \forall x \in A$, vemos

$$(\varphi \circ \psi)(x_0) = \varphi(\psi(x_0)) = \varphi(x_0) \neq x_0 \quad \text{porém} \quad (\psi \circ \varphi)(x_0) = \psi(\varphi(x_0)) = x_0.$$

Logo, $(\varphi \circ \psi)(x_0) \neq (\psi \circ \varphi)(x_0)$ e daí $\varphi \circ \psi \neq \psi \circ \varphi$. Portanto, $\varphi \notin \mathbf{Z}(A^A)$. ■

II.1.24 Proposição.

Seja $(M; \top)$ um semigrupo e $\emptyset \neq X \subseteq M$. Então $\mathbf{C}_M(X)$ é \top -fechado, *i.e.*

$$c_1, c_2 \in \mathbf{C}_M(X) \quad \implies \quad c_1 \top c_2 \in \mathbf{C}_M(X).$$

Demonstração: Temos $c_1 \top x = x \top c_1$ e também $c_2 \top x = x \top c_2$ para todo $x \in X$. Segue

$$\begin{aligned} (c_1 \top c_2) \top x &= c_1 \top (c_2 \top x) = c_1 \top (x \top c_2) = \\ &= (c_1 \top x) \top c_2 = (x \top c_1) \top c_2 = x \top (c_1 \top c_2) \end{aligned}$$

para todos os $x \in X$. Logo $c_1 \top c_2 \in \mathbf{C}_M(X)$.

Se além disso, $(M; \top)$ é um monóide e e é a identidade dele, temos $e \in \mathbf{C}_M(X) \neq \emptyset$. ■

ELEMENTOS REGULARES, INVERSÍVEIS E GRUPOS

II.1.25 Exemplo.

Considerando-se as $\varphi, \psi, \omega \in \mathbb{R}^{\mathbb{R}}$, definidas por

$$\varphi(t) = t^2, \quad \psi(t) = |t^3| \quad \text{e} \quad \omega(t) = t^3 \quad \forall t \in \mathbb{R},$$

temos

$$\varphi \circ \psi = \varphi \circ \omega, \quad \text{e também} \quad \psi \circ \varphi = \omega \circ \varphi,$$

porém

$$\psi \neq \omega .$$

Isto significa que, no monóide $(\mathbb{R}^{\mathbb{R}}; \circ)$ não podemos simplesmente cancelar o "fator" φ de uma equação

$$\varphi \circ \psi = \varphi \circ \omega \quad \text{ou de} \quad \psi \circ \varphi = \omega \circ \varphi :$$

Portanto: *Num monóide não dispomos de nenhuma lei (geral) de cancelamento.*

II.1.26 Definição.

Seja $(M; \top)$ uma estrutura algébrica com uma composição interna. Um $r \in M$ chama-se um elemento

a) *regular à esquerda*, se $\forall x, x' \in M$:

$$r \top x = r \top x' \quad \text{implica que} \quad x = x' .$$

b) *regular à direita*, se $\forall x, x' \in M$:

$$x \top r = x' \top r \quad \text{implica que} \quad x = x' .$$

c) *regular bilateral*, se é regular à esquerda e à direita.

Por $\mathbf{R}'(M)$ indicamos o conjunto dos elementos regulares à esquerda, por $\mathbf{R}''(M)$ o conjunto dos elementos regulares à direita e por $\mathbf{R}(M) = \mathbf{R}'(M) \cap \mathbf{R}''(M)$ o conjunto dos elementos regulares bilaterais de M .

II.1.27 Definição.

Se $(M; \top)$ é uma estrutura algébrica, a todo elemento $a \in M$ podemos associar duas aplicações $\lambda_a, \xi_a \in M^M$, definidas por

$$\lambda_a(x) = a \top x \quad \text{e} \quad \xi_a(x) = x \top a \quad \forall x \in M .$$

λ_a chama-se a *translação à esquerda*, ξ_a a *translação à direita* de M pelo elemento a .

A regularidade de um elemento podemos caracterizar assim:

II.1.28 Observação.

Para todo $r \in (M; \top)$ valem:

a) r é regular à esquerda $\iff \lambda_r \in \mathbf{Inj}(M, M)$.

c) r é regular à direita $\iff \xi_r \in \mathbf{Inj}(M, M)$.

c) r é regular bilateral \iff ambas $\lambda_r, \xi_r \in \mathbf{Inj}(M, M)$.

Demonstração: a) $(\forall x, x' \in M : r \top x = r \top x' \implies x = x') \iff$
 $\iff (\forall x, x' \in M : \lambda_r(x) = \lambda_r(x') \implies x = x')$

A demonstração de b) é análoga. c) é combinação de a) e b).

Se M é finito e se \top é dada através de uma tábua, a regularidade à esquerda (à direita) de um elemento $a \in M$ significa que na linha (coluna) do a não existem repetições

■

II.1.29 Exemplo.

Seja $M = \{\nabla, \spadesuit, \heartsuit, \clubsuit\}$ e $\top \in M^M$ definida por

\top	∇	\spadesuit	\heartsuit	\clubsuit
∇	∇	\spadesuit	\heartsuit	\heartsuit
\spadesuit	\heartsuit	∇	\spadesuit	\clubsuit
\heartsuit	\spadesuit	\heartsuit	\clubsuit	\clubsuit
\clubsuit	\spadesuit	\clubsuit	∇	\heartsuit

Temos que

- \clubsuit é um regular à esquerda, porém não à direita,
- \heartsuit é um regular à direita, porém não à esquerda,
- \spadesuit é regular bilateral.

II.1.30 Exemplo.

Em $(\mathbb{N}; \top)$ com $a \top b = a^b$ temos:

- 1) Todo elemento é regular à direita.
- 2) Todo elemento $a \neq 1$ é regular à esquerda.

II.1.31 Observação.

Seja $(M; \top)$ um semigrupo. Então os conjuntos

$$\mathbf{R}'(M), \quad \mathbf{R}''(M) \quad e \quad \mathbf{R}(M)$$

são fechados com respeito à composição \top .

Demonstração: Sejam $r_1, r_2 \in \mathbf{R}'(M)$ e suponhamos $(r_1 \top r_2) \top x = (r_1 \top r_2) \top x'$ para dois elementos $x, x' \in M$. Segue $r_1 \top (r_2 \top x) = r_1 \top (r_2 \top x')$. Devido à regularidade à esquerda do r_1 concluímos $r_2 \top x = r_2 \top x'$. Pela mesma razão $x = x'$. Logo $r_1 \top r_2 \in \mathbf{R}'(M)$.

O fechamento de $\mathbf{R}''(M)$ é análogo (fazer a demonstração !).

■

II.1.32 Definição.

Seja $(M; \top)$ uma estrutura algébrica com identidade bilateral e . Um elemento $u \in M$ chama-se um elemento

- i) *inversível à esquerda*, se existe $y \in M$ com $y \top u = e$.
- ii) *inversível à direita*, se existe $z \in M$ com $u \top z = e$.
- iii) *bilateralmente inversível*, se é inversível à esquerda e à direita.

Às vezes usa-se a denominação " *unidade* " (à esquerda, à direita, bilateral) para esta espécie de elementos.

Por $\mathbf{U}'(M)$ indicamos o conjunto das unidades à esquerda,

por $\mathbf{U}''(M)$ o conjunto das unidades à direita,

por $\mathbf{U}(M)$ o conjunto das unidades bilaterais de M .

$$\text{Claramente, } e \in \mathbf{U}(M) = \mathbf{U}'(M) \cap \mathbf{U}''(M)$$

Todo elemento $y \in M$ com $y \top u = e$, chama-se
um inverso à esquerda de u .

Todo elemento $z \in M$ com $u \top z = e$, chama-se
um inverso à direita de u .

Claro que para todo inverso à esquerda y de um $u \in \mathbf{U}'(M)$, temos $y \in \mathbf{U}''(M)$ e para todo inverso à direita z de um $u \in \mathbf{U}''(M)$, temos $z \in \mathbf{U}'(M)$.

II.1.33 Observação.

Seja $(M; \top)$ um monóide. Então valem:

a) Toda unidade à esquerda é regular à esquerda, ou seja

$$\mathbf{U}'(M) \subseteq \mathbf{R}'(M) .$$

b) Toda unidade à direita é regular à direita, ou seja

$$\mathbf{U}''(M) \subseteq \mathbf{R}''(M) .$$

c) Toda unidade bilateral é bilateralmente regular, ou seja

$$\mathbf{U}(M) \subseteq \mathbf{R}(M) .$$

Demonstração: Seja $u \in \mathbf{U}'(M)$. Assim, existe $y \in M$ com $y \top u = e$. Suponhamos, $x, x' \in M$ são tais que $u \top x = u \top x'$. Segue $y \top (u \top x) = y \top (u \top x')$ e daí pela lei associativa, $(y \top u) \top x = (y \top u) \top x'$. Logo, $e \top x = e \top x'$, i.e. $x = x'$. Portanto, $u \in \mathbf{R}'(M)$. Logo, $\mathbf{U}'(M) \subseteq \mathbf{R}'(M)$.

Da mesma forma mostra-se b).

c) é consequência de a) e b).

■

II.1.34 Observação.

Seja $(M; \top)$ um monóide, e sua identidade. Seja $u \in \mathbf{U}(M)$. Então, para todos os $y, z \in M$ com $y \top u = e = u \top z$ temos

$$y = z .$$

Demonstração: $y = y \top e = y \top (u \top z) = (y \top u) \top z = e \top z = z$.

Isto significa que, para um elemento bilateralmente inversível, todo inverso à esquerda é igual a todo inverso à direita. Particularmente, existe somente um inverso à esquerda e somente um inverso à direita para $u \in \mathbf{U}(M)$. Este único $\hat{u} \in M$ com

$$\hat{u} \top u = u \top \hat{u} = e$$

chama-se o inverso de u . Vale também $\hat{u} \in \mathbf{U}(M)$ e $\hat{\hat{u}} = u$. ■

II.1.35 Proposição.

Seja $(M; \top)$ um monóide, e sua identidade e seja $u \in M$. Sejam $\lambda_u, \xi_u \in M^M$ as translações à esquerda e à direita de M por u , respectivamente.

Então valem:

- a) $u \in \mathbf{U}'(M) \iff \xi_u \in \mathbf{Sob}(M, M)$, i.e. u é inversível à esquerda, se e somente se a translação à direita por u , é sobrejetora.
- b) $u \in \mathbf{U}''(M) \iff \lambda_u \in \mathbf{Sob}(M, M)$, i.e. u é inversível à direita, se e somente se a translação à esquerda por u , é sobrejetora.
- c) $u \in \mathbf{U}(M) \iff$ ambas, $\lambda_u, \xi_u \in \mathbf{Sob}(M, M)$.

Demonstração: a) " \implies ": Seja $u \in \mathbf{U}'(M)$. Assim, existe $y \in M$ com $y \top u = e$. Se $w \in M$ é um elemento qualquer, temos

$$\xi_u(w \top y) = (w \top y) \top u = w \top (y \top u) = w \top e = w .$$

Consequentemente, $a = w \top y$ é uma ξ_u -préimagem de w e vemos que $\xi_u \in \mathbf{Sob}(M, M)$.

" \impliedby ": Supnhamos $\xi_u \in \mathbf{Sob}(M, M)$. Particularmente, para $w = e \in M$, existe $y \in M$ com $\xi_u(y) = e$. Isto significa, $y \top u = e$, ou seja, $u \in \mathbf{U}'(M)$.

b) é análogo. c) é conseqüência de a) e b) (fazer estas demonstrações !). ■

II.1.36 Exemplo.

No monóide (comutativo) $(\mathbb{Z}; \cdot)$ temos

$$\mathbf{R}(\mathbb{Z}) = \mathbb{Z} \setminus \{0\} \quad \text{enquanto} \quad \mathbf{U}(\mathbb{Z}) = \{1, -1\} .$$

II.1.37 Proposição.

Seja $A \neq \emptyset$ um conjunto. No monóide $(A^A; \circ)$ de todas as aplicações de A em A temos

$$\mathbf{U}'(A^A) = \mathbf{Inj}(A, A) ,$$

$$\mathbf{U}''(A^A) = \mathbf{Sob}(A, A) ,$$

$$\mathbf{U}(A^A) = \mathbf{Bij}(A, A) = \mathbf{S}_A .$$

Demonstração: Ver I.2.31. ■

II.1.38 Observação.

Seja $(M; \top)$ um monóide, e sua identidade. Então os conjuntos

$$\mathbf{U}'(M), \quad \mathbf{U}''(M) \quad \text{e} \quad \mathbf{U}(M)$$

são fechados com respeito à composição \top . Mais exatamente:

- a) Se $u_1, u_2 \in \mathbf{U}'(M)$, se y_1 é um inverso à esquerda de u_1 e y_2 é um inverso à esquerda de u_2 , então

$$y_2 \top y_1 \quad \text{é um inverso á esquerda de } u_1 \top u_2 .$$

- b) Se $u_1, u_2 \in \mathbf{U}''(M)$, se z_1 é um inverso à direita de u_1 e z_2 é um inverso à direita de u_2 , então

$$z_2 \top z_1 \quad \text{é um inverso á direita de } u_1 \top u_2 .$$

- c) Se $u_1, u_2 \in \mathbf{U}(M)$, então o inverso bilateral (único) de $u_1 \top u_2$ é calculado por

$$u_1 \widehat{\top} u_2 = \hat{u}_2 \top \hat{u}_1 .$$

Demonstração: a) Sejam $u_1, u_2 \in \mathbf{U}'(M)$ e sejam $y_1, y_2 \in M$ tais que $y_1 \top u_1 = e = y_2 \top u_2$. Segue

$$\begin{aligned} (y_2 \top y_1) \top (u_1 \top u_2) &= y_2 \top (y_1 \top u_1) \top u_2 = \\ &= (y_2 \top e) \top u_2 = y_2 \top u_2 = e . \end{aligned}$$

Isto mostra, $u_1 \top u_2 \in \mathbf{U}'(M)$ e que $y_2 \top y_1$ é um dos inversos à esquerda de $u_1 \top u_2$.

b) O fechamento de $\mathbf{U}''(M)$ é análogo (fazer isto!).

c) é consequência de a) e b). ■

II.1.39 Definição.

Um monóide $(M; \top)$ é denominado um *grupo*, se

$$\mathbf{U}(M) = M,$$

i.e. se todo elemento em M é inversível.

II.1.40 Observação.

Para todo monóide $(M; \top)$ temos que

$$(\mathbf{U}(M); \top) \text{ é um grupo.}$$

II.1.41 Exemplos.

a) Para todo conjunto $A \neq \emptyset$, temos que

$$(\mathbf{U}(A^A); \circ) = (\mathbf{S}_A; \circ) \text{ é um grupo.}$$

b) Para o monóide $(\mathbb{Z}; \cdot)$, temos que

$$(\mathbf{U}(\mathbb{Z}); \cdot) = (\{1, -1\}; \cdot) \text{ é um grupo.}$$

II.1.42 Definição.

Se $A \neq \emptyset$ é um conjunto, o grupo

$$(\mathbf{S}_A; \circ)$$

consistindo de todas as permutações de A , é chamado

o grupo de todas as permutações de A ou o grupo simétrico sobre A .

Observamos que estes grupos simétricos são as estruturas algébricas mais fundamentais para toda a Álgebra.

Às vezes vale também a lei comutativa num grupo:

II.1.43 Definição.

Um grupo $(M; \top)$ é dito *comutativo* ou *abeliano* se

$$a \top b = b \top a \quad \forall a, b \in M$$

(Niels Henrik ABEL [1802- 1829]. Matemático norueguês).

II.1.44 Exemplos.

a) $(\mathbb{Z}; +)$, $(\mathbb{R}; +)$, $(\mathbb{Q}; +)$ são grupos abelianos.

b) Seja $\mathbf{P} = \{x \in \mathbb{R} \mid x > 0\}$ o conjunto dos números reais positivos.

$(\mathbf{P}; \cdot)$ é um grupo abeliano .

c) Se $i = \sqrt{-1}$ indica uma solução (formal) da equação $x^2 + 1 = 0$, temos que

$(\{1, -1, i, -i\}; \cdot)$ é um grupo abeliano,

Sua tabela de multiplicação é:

\cdot	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

§ II.2 Subestruturas, estruturas quocientes e homomorfismos

SUBESTRUTURAS

II.2.1 Definição.

Seja $(M; \tau_1, \tau_2, \dots, \tau_r)$ uma estrutura algébrica com r composições internas $\tau_1, \tau_2, \dots, \tau_r \in M^{M \times M}$. Um subconjunto $S \subseteq M$ chama-se

uma *subestrutura* de $(M; \tau_1, \tau_2, \dots, \tau_r)$, se

- i) $S \neq \emptyset$
- ii) Para todos os $a, b \in S$ temos

$$a \tau_1 b \in S, \quad a \tau_2 b \in S, \quad \dots, \quad a \tau_r b \in S.$$

Abreviado:

$$a \tau_i b \in S \quad \forall a, b \in S \quad \forall i = 1, 2, \dots, r$$

Isto significa portanto que S é fechado com respeito às composições internas definidas em M .

Indicamos isto por

$$(S; \tau_1, \tau_2, \dots, \tau_r) \leq (M; \tau_1, \tau_2, \dots, \tau_r),$$

ou simplesmente por $S \leq M$, se não houver dúvidas sobre as composições consideradas.

O próprio $S = M$ sempre é um exemplo de uma subestrutura de M .

Se temos uma única composição τ em M :

$$(S; \tau) \leq (M; \tau) \iff a \tau b \in S \quad \forall a, b \in S.$$

Se $(M; \tau)$ é um semigrupo, uma subestrutura $(S; \tau) \leq (M; \tau)$ chama-se também um *sub-semigrupo* de M .

II.2.2 Exemplos.

- a) Para $(\mathbb{Z}; +, \cdot)$ temos que

$$a_1) \quad (\mathbb{N}; +, \cdot) \leq (\mathbb{Z}; +, \cdot)$$

- a₂) Para $S = \{-10, -11, -12, -13, \dots\}$ temos $(S; +) \leq (\mathbb{Z}; +)$
- a₃) $S = \{\dots, -5, -3, -1, 1, 3, 5, \dots\}$, o subconjunto dos números ímpares de \mathbb{Z} ; é uma subestrutura de $(\mathbb{Z}; \cdot)$, porém, não é uma subestrutura de $(\mathbb{Z}; +)$.
- b) O conjunto $\mathbb{P} = \{2, 3, 5, 7, 11, \dots\}$, dos números primos, não é uma subestrutura, nem de $(\mathbb{N}; +)$ nem de $(\mathbb{N}; \cdot)$.
- c) Se a estrutura $(M; \top)$ possuir um elemento neutro bilateral, digamos e , então
- $$(\{e\}; \top) \text{ é uma subestrutura de } (M; \top).$$

■

II.2.3 Proposição.

Seja $(M; \top)$ um monóide.

- a) Os conjuntos $\mathbf{R}'(M)$, $\mathbf{R}''(M)$ e $\mathbf{R}(M) = \mathbf{R}'(M) \cap \mathbf{R}''(M)$, dos elementos regulares à esquerda, à direita e bilaterais, respectivamente, são subestruturas de $(M; \top)$:

$$\begin{aligned} (\mathbf{R}'(M); \top) &\leq (M; \top), & (\mathbf{R}''(M); \top) &\leq (M; \top), \\ (\mathbf{R}(M); \top) &\leq (M; \top). \end{aligned}$$

- b) Os conjuntos $\mathbf{U}'(M)$, $\mathbf{U}''(M)$ e $\mathbf{U}(M) = \mathbf{U}'(M) \cap \mathbf{U}''(M)$, dos elementos inversíveis à esquerda, à direita e bilaterais, respectivamente, são subestruturas de $(M; \top)$ com

$$\mathbf{U}'(M) \subseteq \mathbf{R}'(M), \quad \mathbf{U}''(M) \subseteq \mathbf{R}''(M), \quad \mathbf{U}(M) \subseteq \mathbf{R}(M),$$

i.e.

$$\begin{aligned} (\mathbf{U}'(M); \top) &\leq (\mathbf{R}'(M); \top) \leq (M; \top), \\ (\mathbf{U}''(M); \top) &\leq (\mathbf{R}''(M); \top) \leq (M; \top), \\ (\mathbf{U}(M); \top) &\leq (\mathbf{R}(M); \top) \leq (M; \top). \end{aligned}$$

- c) Para qualquer conjunto $\emptyset \neq X \subseteq M$ temos que os centralizadores

$$\mathbf{C}_M(X) \text{ são subestruturas de } M, \text{ i.e. } (\mathbf{C}_M(X); \top) \leq (M; \top)$$

Demonstração: Ver II.1.31, II.1.33 e II.1.38

■

II.2.4 Observação.

Seja $(M; \tau_1, \tau_2, \dots, \tau_r)$ uma estrutura algébrica com r composições internas. Seja $\mathfrak{S} \subseteq 2^M$ uma família de subestruturas de M tal que $\bigcap_{S \in \mathfrak{S}} S \neq \emptyset$. Então

$\bigcap_{S \in \mathfrak{S}} S$ é uma subestrutura de M .

$\bigcap_{S \in \mathfrak{S}} S$ é a **maior** subestrutura de M , contida em todas as $S \in \mathfrak{S}$.

Demonstração: Por hipótese temos $\bigcap_{S \in \mathfrak{S}} S \neq \emptyset$. Sejam $a, b \in \bigcap_{S \in \mathfrak{S}} S$. Isto significa $a, b \in S \quad \forall S \in \mathfrak{S}$. Segue $a \tau_i b \in S \quad \forall S \in \mathfrak{S}$ e todos os $i = 1, 2, \dots, r$. Mas então $a \tau_i b \in \bigcap_{S \in \mathfrak{S}} S \quad \forall i = 1, 2, \dots, r$. Logo,

$$\bigcap_{S \in \mathfrak{S}} S \leq M.$$

■

II.2.5 Definição.

Seja $(M; \tau_1, \tau_2, \dots, \tau_r)$ uma estrutura algébrica com r composições internas. Seja $\emptyset \neq X \subseteq M$ um subconjunto não-vazio de M . Chamamos

$$\langle X \rangle = \bigcap_{\substack{S \leq M \\ X \subseteq S}} S$$

a subestrutura de $(M; \tau_1, \tau_2, \dots, \tau_r)$ **gerada** pelo subconjunto X de M .

$\langle X \rangle$ é portanto a interseção de todas as subestruturas de M que contêm o subconjunto X .

$\langle X \rangle$, como interseção não-vazia de subestruturas de M , é de fato uma subestrutura de M devido a II.2.4. Obviamente,

$\langle X \rangle$ é a **menor** subestrutura de M contendo X .

Se $\langle X \rangle = M$, dizemos que a estrutura $(M; \tau_1, \tau_2, \dots, \tau_r)$ é gerada pelo conjunto $X \subseteq M$.

Isto significa que a única subestrutura de M que contém X é a própria M . Neste caso o conjunto X é denominado um *sistema de geradores para* $(M; \tau_1, \tau_2, \dots, \tau_r)$.

II.2.6 Exemplo.

a) A subestrutura de $(\mathbb{N}; +)$ gerada pelo conjunto $X = \{6, 15\}$ é

$$\langle X \rangle = \{6, 12, 15, 18, 21, 24, 27, 30, \dots\} = \{6k + 15\ell > 0 \mid k, \ell \in \mathbb{N}_0\}.$$

b) $\langle \mathbb{P} \rangle = (\mathbb{N}; \cdot)$, i.e. o conjunto dos números primos $X = \mathbb{P}$ é um sistema de geradores para o monóide multiplicativo \mathbb{N} dos números naturais.

Demonstração: a) Ponhamos $E = \{6k + 15\ell > 0 \mid k, \ell \in \mathbb{N}_0\}$. Temos $\{6, 15\} \subseteq E$ e é claro que toda subestrutura S que contiver $\{6, 15\}$, tem que conter todas as somas $6k + 15\ell \neq 0$ com $k, \ell \in \mathbb{N}_0$. Portanto $E \subseteq S$.

Para todos os $a = 6k_1 + 15\ell_1$ e $b = 6k_2 + 15\ell_2$ em E temos

$$a + b = 6k_1 + 15\ell_1 + 6k_2 + 15\ell_2 = 6(k_1 + k_2) + 15(\ell_1 + \ell_2) \in E.$$

Portanto, E é uma das subestruturas que contêm X . Logo, $E = \langle X \rangle$.

b) Isto deve se ao fato que todo número natural é produto de primos. ■

RELAÇÕES DE CONGRUÊNCIA E ESTRUTURAS QUOCIENTES

II.2.7 Definição.

Seja $(M; \tau_1, \tau_2, \dots, \tau_r)$ uma estrutura algébrica. Uma relação de equivalência $\kappa \in \mathbf{Eq}(M)$ chama-se uma

relação de congruência da estrutura $(M; \tau_1, \tau_2, \dots, \tau_r)$,

se para todos os $a, a', b, b' \in M$ tivermos as seguintes compatibilidades de κ com as composições $\tau_1, \tau_2, \dots, \tau_r$:

$$\text{Se } \begin{cases} a \kappa a' \\ b \kappa b' \end{cases} \quad \text{então } \begin{cases} a \tau_1 b \kappa a' \tau_1 b', \\ a \tau_2 b \kappa a' \tau_2 b', \\ \vdots \\ a \tau_r b \kappa a' \tau_r b'. \end{cases}$$

Mais abreviadamente:

$$\begin{cases} a \kappa a' \\ b \kappa b' \end{cases} \implies a \tau_i b \kappa a' \tau_i b' \quad \forall i = 1, 2, \dots, r.$$

Por

$$\mathbf{Cg}(M; \tau_1, \dots, \tau_r)$$

indicamos o *conjunto de todas as relações de congruência* da estrutura algébrica $(M; \tau_1, \dots, \tau_r)$. Assim temos

$$\mathbf{Cg}(M; \tau_1, \dots, \tau_r) \subseteq \mathbf{Eq}(M).$$

Para uma relação de congruência κ temos portanto:

$$\begin{array}{l} \text{Se} \\ \text{e} \end{array} \quad \begin{array}{l} a \kappa a' \\ b \kappa b' \end{array}$$

$$\text{então} \quad a \tau_i b \kappa a' \tau_i b' \quad \forall i = 1, 2, \dots, r.$$

Isto significa que duas congruências modulo κ podemos τ_i -compor verticalmente, sem destruir a κ -equivalência do resultado - como se as congruências fossem duas igualdades.

Claro que temos

$$\mathbf{Cg}(M; \tau_1, \tau_2, \dots, \tau_r) = \bigcap_{i=1}^r \mathbf{Cg}(M; \tau_i).$$

II.2.8 Exemplo.

Para toda estrutura algébrica $(M; \tau_1, \tau_2, \dots, \tau_r)$ temos

$$\delta_M \in \mathbf{Cg}(M; \tau_1, \tau_2, \dots, \tau_r) \quad \text{e} \quad M \times M \in \mathbf{Cg}(M; \tau_1, \tau_2, \dots, \tau_r),$$

i.e. tanto a relação da igualdade como a relação universal em M são exemplos de relações de congruência. Particularmente,

$$\mathbf{Cg}(M; \tau_1, \tau_2, \dots, \tau_r) \neq \emptyset.$$

II.2.9 Exemplos.

Seja $(M; \tau_1, \tau_2) = (\mathbb{Z}; +, \cdot)$.

a) Para as relações de equivalência \equiv_n (ver I.1.26) vale de fato

$$\equiv_n \in \mathbf{Cg}(\mathbb{Z}; +, \cdot) = \mathbf{Cg}(\mathbb{Z}; +) \cap \mathbf{Cg}(\mathbb{Z}; \cdot) .$$

b) Seja $\varepsilon \in \mathbf{Eq}(\mathbb{Z})$ definida pela partição

$$\mathfrak{P}_\varepsilon = \{ \{x \in \mathbb{Z} \mid x \geq 0\} , \{x \in \mathbb{Z} \mid x < 0\} \} .$$

Então $\varepsilon \notin \mathbf{Cg}(\mathbb{Z}; +)$.

Demonstração: a) Sejam $a, a', b, b' \in \mathbb{Z}$ tais que $\begin{cases} a \equiv_n a' \\ b \equiv_n b' \end{cases}$. Temos que $a - a'$ e $b - b'$ são múltiplos de n . Segue que também $(a + b) - (a' + b') = (a - a') + (b - b')$ é múltiplo de n . Mas isto significa $a + b \equiv_n a' + b'$.

Portanto, $\equiv_n \in \mathbf{Cg}(\mathbb{Z}; +)$.

Também $ab - a'b' = ab - a'b + a'b - a'b' = (a - a')b + a'(b - b')$ é múltiplo de n . Isto significa $ab \equiv_n a'b'$.

Portanto, $\equiv_n \in \mathbf{Cg}(\mathbb{Z}; \cdot)$.

Assim, $\equiv_n \in \mathbf{Cg}(\mathbb{Z}; +) \cap \mathbf{Cg}(\mathbb{Z}; \cdot) = \mathbf{Cg}(\mathbb{Z}; +, \cdot)$.

b) Temos por exemplo $\begin{cases} -8 \varepsilon -2 \\ 6 \varepsilon 3 \end{cases}$. Porém $-2 = -8 + 6 \notin -2 + 3 = 1$.

Logo, esta $\varepsilon \in \mathbf{Eq}(\mathbb{Z})$ não é compatível com a adição em \mathbb{Z} .

■

As relações de congruência da estrutura algébrica $(\mathbb{Z}; +)$ podem ser completamente descritas. De fato, não existem outras além das \equiv_n :

II.2.10 Teorema.

$$\mathbf{Cg}(\mathbb{Z}; +) = \{ \equiv_n \mid n = 0, 1, 2, 3, \dots \} ,$$

i.e. as relações de congruência de $(\mathbb{Z}; +)$ são exatamente as congruências mod n .

(O mesmo vale a fortiori para $\mathbf{Cg}(\mathbb{Z}; +, \cdot)$)

Demonstração: Sabemos $\{ \equiv_n \mid n = 0, 1, 2, 3, \dots \} \subseteq \mathbf{Cg}(\mathbb{Z}; +)$, devido

a II.2.9 a).

Seja dado uma qualquer $\kappa \in \text{Cg}(\mathbb{Z}; +)$. Devemos provar que $\kappa = \equiv_n$ para algum n . Como podemos construir este n a partir da κ ?

1) Sejam $a, b \in \mathbb{Z}$. Somando-se as congruências $\begin{cases} a \kappa b \\ -b \kappa -b \end{cases}$, segue $a - b \kappa 0$.

Somando-se as $\begin{cases} a - b \kappa 0 \\ b \kappa b \end{cases}$, segue $a \kappa b$. Portanto temos

$$a \kappa b \iff a - b \kappa 0.$$

Vemos que é importante considerarmos

$$\bar{0} = \{x \in \mathbb{Z} \mid x \kappa 0\},$$

a classe de $0 \pmod{\kappa}$:

2) Para todo $x \in \bar{0}$ temos também $-x \in \bar{0}$: De fato: De $\begin{cases} x \kappa 0 \\ -x \kappa -x \end{cases}$ concluímos

$x + (-x) \kappa 0 + (-x)$, ou seja, $0 \kappa -x$. Isto significa que, se $\bar{0} \neq \{0\}$, então $\bar{0}$ contém algum número natural: $\bar{0} \cap \mathbb{N} \neq \emptyset$.

Caso I: Se $\bar{0} = \{0\}$, vamos ter $\kappa = \delta_{\mathbb{Z}} = \equiv_0$.

Caso II: Neste caso, $\bar{0} \cap \mathbb{N} \neq \emptyset$. Pelo princípio da indução, existe um número natural *mínimo* $n \in \bar{0}$. Afirmamos que

$$\bar{0} = \{kn \mid k \in \mathbb{Z}\},$$

i.e. a classe de 0 consiste dos múltiplos deste n . De fato:

i) De $\pm n \kappa 0$ segue para todo $k \in \mathbb{Z}$ que

$$kn = \pm n \pm n \pm \dots \pm n \kappa 0 + 0 + \dots + 0 = 0. \text{ Logo,}$$

$$\bar{0} \supseteq \{kn \mid k \in \mathbb{Z}\}.$$

ii) Todo $x \in \bar{0}$ podemos dividir por n com resto r entre 0 e $n-1$: Existe $k \in \mathbb{Z}$

com $x = kn + r$. Temos $\begin{cases} x \kappa 0 \\ -kn \kappa 0 \end{cases}$ e segue $r = x - kn \kappa 0 + 0 = 0$. Logo,

$r \in \bar{0}$ com $0 \leq r < n$. Como n foi escolhido como número natural *mínimo* em $\bar{0}$, concluímos $r = 0$ e daí $x = nk$. Segue

$$\bar{0} \subseteq \{kn \mid k \in \mathbb{Z}\}.$$

De i) e ii) vemos que $\bar{0} = \{ kn \mid k \in \mathbb{Z} \}$. Agora,

$$a \kappa b \iff a - b \kappa 0 \iff a - b = kn \text{ com } k \in \mathbb{Z} \iff a \equiv_n b$$

Portanto, $\kappa = \equiv_n$.

■

ESTRUTURAS QUOCIENTES

II.2.11 Observação.

Seja $(M; \tau_1, \tau_2, \dots, \tau_r)$ uma estrutura algébrica com r composições internas. Seja $\kappa \in \mathbf{Cg}(M; \tau_1, \dots, \tau_r)$ e considere o conjunto quociente M/κ . Definindo-se para todos os $\bar{a}, \bar{b} \in M/\kappa$ e todos os $i = 1, 2, \dots, r$:

$$\bar{a} \bar{\tau}_i \bar{b} = \overline{a \tau_i b},$$

temos que $\bar{\tau}_1, \bar{\tau}_2, \dots, \bar{\tau}_r$ são composições internas bem definidas no conjunto quociente M/κ .

A estrutura algébrica

$$(M/\kappa; \bar{\tau}_1, \bar{\tau}_2, \dots, \bar{\tau}_r)$$

chama-se a *estrutura quociente* $M \pmod{\kappa}$.

Demonstração: Seja $\bar{a} = \bar{a}'$ e $\bar{b} = \bar{b}'$. Isto significa $a \kappa a'$ e $b \kappa b'$. Como κ é uma relação de congruência, concluímos $a \tau_i b \kappa a' \tau_i b'$. Segue

$$\bar{a}' \bar{\tau}_i \bar{b}' = \overline{a' \tau_i b'} = \overline{a \tau_i b} = \bar{a} \bar{\tau}_i \bar{b}.$$

Portanto, a definição de $\bar{\tau}_i$ independe da escolha do representante das classes de equivalência. Assim, $\bar{\tau}_i \in (M/\kappa)^{M/\kappa \times M/\kappa}$ são composições internas bem definidas de M/κ .

■

II.2.12 Exemplo.

Para a estrutura $(\mathbb{Z}; +, \cdot)$ e qualquer uma das $\equiv_n \in \mathbf{Cg}(\mathbb{Z}; +, \cdot)$ temos a estrutura quociente

$$(\mathbb{Z}/\equiv_n; \bar{+}, \bar{\cdot}) = (\{\bar{a} \mid a \in \mathbb{Z}\}; \bar{+}, \bar{\cdot}),$$

onde duas classes $\bar{a}, \bar{b} \in \mathbb{Z}/\equiv_n$ são somadas e multiplicadas por

$$\bar{a} \bar{+} \bar{b} = \overline{a + b} \quad \text{e} \quad \bar{a} \bar{\cdot} \bar{b} = \overline{a \cdot b}.$$

Tendo em vista que a classe \bar{a} é o conjunto $\bar{a} = \{a + nk \mid k \in \mathbb{Z}\}$, temos mais detalhadamente

$$\{a + nk \mid k \in \mathbb{Z}\} + \{b + nk \mid k \in \mathbb{Z}\} = \{(a+b) + nk \mid k \in \mathbb{Z}\},$$

$$\{a + nk \mid k \in \mathbb{Z}\} \cdot \{b + nk \mid k \in \mathbb{Z}\} = \{ab + nk \mid k \in \mathbb{Z}\}.$$

Para $n = 6$ temos por exemplo que

$$\mathbb{Z}/\equiv_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}.$$

A adição e a multiplicação em \mathbb{Z}/\equiv_6 podem ser descritas pelas tábuas

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$

.	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$						
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{2}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

HOMOMORFISMOS E ISOMORFISMOS

II.2.13 Definição.

Sejam $(M; \tau_1, \tau_2, \dots, \tau_r)$ e $(N; \perp_1, \perp_2, \dots, \perp_r)$ duas estruturas algébricas com r composições internas, cada:

$$\tau_1, \tau_2, \dots, \tau_r \in M^{M \times M} \quad \text{e} \quad \perp_1, \perp_2, \dots, \perp_r \in N^{N \times N}$$

(a composição interna \perp é lida: "bot"). Uma aplicação $\varphi \in N^M$ é denominada

um *homomorfismo* de $(M; \tau_1, \tau_2, \dots, \tau_r)$ em $(N; \perp_1, \perp_2, \dots, \perp_r)$,

se para todos os $a, b \in M$ tivermos

$$\begin{aligned} \varphi(a \tau_1 b) &= \varphi(a) \perp_1 \varphi(b), \\ \varphi(a \tau_2 b) &= \varphi(a) \perp_2 \varphi(b), \\ &\dots\dots\dots \\ \varphi(a \tau_r b) &= \varphi(a) \perp_r \varphi(b). \end{aligned}$$

Mais conciso:

$$\varphi(a \top_i b) = \varphi(a) \perp_i \varphi(b), \quad \forall i = 1, 2, \dots, r, \quad \forall a, b \in M.$$

II.2.14 Exemplos.

a) Para $(M; \top) = (\mathbb{N}; +)$ e $(N; \perp) = (\mathbb{N}; \cdot)$ temos:

A aplicação $\varphi \in \mathbb{N}^{\mathbb{N}}$ com $\varphi(a) = 2^a \quad \forall a \in \mathbb{N}$ é um homomorfismo.

b) Para $(M; \top) = (\mathbb{Z}; +)$ e $(N; \perp) = (\{1, -1\}; \cdot)$ temos: A aplicação

$\varphi \in \{1, -1\}^{\mathbb{Z}}$ com $\varphi(a) = (-1)^a \quad \forall a \in \mathbb{Z}$ é um homomorfismo.

II.2.15 Definição.

Um homomorfismo φ da estrutura algébrica $(M; \top_1, \top_2, \dots, \top_r)$ na estrutura algébrica $(N; \perp_1, \perp_2, \dots, \perp_r)$ chama-se

- i) um *monomorfismo*, se $\varphi \in \mathbf{Inj}(M, N)$,
- ii) um *epimorfismo*, se $\varphi \in \mathbf{Sob}(M, N)$,
- iii) um *isomorfismo*, se $\varphi \in \mathbf{Bij}(M, N)$,
- iv) um *endomorfismo* de $(M; \top_1, \top_2, \dots, \top_r)$, se $M = N$ e $\top_1 = \perp_1, \top_2 = \perp_2, \dots, \top_r = \perp_r$.
- v) um *automorfismo* de $(M; \top_1, \top_2, \dots, \top_r)$, se φ é um endomorfismo bijetor (= um isomorfismo de $(M; \top_1, \top_2, \dots, \top_r)$ sobre si mesmo).

II.2.16 Exemplos.

a) Sejam $(M; \top) = (\mathbb{N}; \cdot)$ e $(N; \perp) = (\mathbb{R}; +)$. A aplicação $\varphi \in \mathbb{R}^{\mathbb{N}}$ definida por

$$\varphi(x) = \lg x \quad \forall x \in \mathbb{N},$$

é um monomorfismo que não é epimorfismo.

b) Sejam $(M; \top) = (\mathbb{Z}; \cdot)$ e $(N; \perp) = (\mathbb{N}_0; \cdot)$. A aplicação $\varphi \in \mathbb{N}_0^{\mathbb{Z}}$ definida por

$$\varphi(x) = |x| \quad \forall x \in \mathbb{Z},$$

é um epimorfismo mas não é monomorfismo.

- c) Sejam $(M; \top) = (\mathbb{R}; +)$ e $(N; \perp) = (\mathbf{P}; \cdot)$ onde
 $\mathbf{P} = \{x \in \mathbb{R} \mid x > 0\}$.

A aplicação $\varphi \in \mathbf{P}^{\mathbb{R}}$ definida por

$$\varphi(x) = 10^x \quad \forall x \in \mathbb{R},$$

é um isomorfismo.

- d) A aplicação $\varphi \in \mathbb{Z}^{\mathbb{Z}}$ definida por

$$\varphi(x) = 2x \quad \forall x \in \mathbb{Z},$$

é um endomorfismo injetor de $(\mathbb{Z}; +)$, mas não é um automorfismo.

- e) A aplicação $\varphi \in \mathbb{Z}^{\mathbb{Z}}$ definida por

$$\varphi(x) = -x \quad \forall x \in \mathbb{Z},$$

é um automorfismo de $(\mathbb{Z}; +)$.

- f) Seja $(M; \top) = (\mathbb{R}; \cdot)$. A aplicação $\varphi \in \mathbb{R}^{\mathbb{R}}$, definida por

$$\varphi(x) = x^3 \quad \forall x \in \mathbb{R},$$

é um automorfismo de $(M; \top)$.

- g) Seja o intervalo real $M = (0, 4]$ com a composição interna definida por
 $a \top b = \frac{ab}{4} \quad \forall a, b \in M$. A aplicação $\varphi \in \mathbf{S}_M$, definida por

$$\varphi(x) = \frac{x^2}{4} \quad \forall x \in M,$$

é um automorfismo de $(M; \top)$, pois $\forall a, b \in M$:

$$\begin{aligned} \varphi(a \top b) &= \frac{(a \top b)^2}{4} = \frac{\left(\frac{ab}{4}\right)^2}{4} = \frac{(ab)^2}{64} = \\ &= \frac{\frac{a^2}{4} \cdot \frac{b^2}{4}}{4} = \frac{\varphi(a) \cdot \varphi(b)}{4} = \varphi(a) \top \varphi(b). \end{aligned}$$

■

II.2.17 Observação.

Sejam $(M; \top_1, \top_2, \dots, \top_r)$, $(N; \perp_1, \perp_2, \dots, \perp_r)$ e $(P; *_1, *_2, \dots, *_r)$ três estruturas algébricas com r composições internas, cada. Sejam $\varphi \in N^M$ e $\psi \in P^N$ homomorfismos. Então a aplicação composta

$\psi \circ \varphi$ é um homomorfismo de M em P .

Demonstração: Temos para todos os $a, b \in M$ e todos os $i = 1, 2, \dots, r$:

$$\begin{aligned} (\psi \circ \varphi)(a \top_i b) &= \psi(\varphi(a \top_i b)) = \psi(\varphi(a) \perp_i \varphi(b)) = \\ &= \psi(\varphi(a)) *_i \psi(\varphi(b)) = (\psi \circ \varphi)(a) *_i (\psi \circ \varphi)(b). \end{aligned}$$

■

II.2.18 Observação.

Sejam $(M; \top_1, \top_2, \dots, \top_r)$ e $(N; \perp_1, \perp_2, \dots, \perp_r)$ duas estruturas algébricas com r composições internas, cada.

Se $\varphi : M \longrightarrow N$ é um isomorfismo de $(M; \top_1, \top_2, \dots, \top_r)$ sobre $(N; \perp_1, \perp_2, \dots, \perp_r)$, então $\varphi^{-1} : N \longrightarrow M$ é um isomorfismo de $(N; \perp_1, \perp_2, \dots, \perp_r)$ sobre $(M; \top_1, \top_2, \dots, \top_r)$.

Demonstração: Já sabemos que a aplicação inversa de uma aplicação bijetora é bijetora. Só falta provar que φ^{-1} é um homomorfismo: Dados $c, c' \in N$, existem (únicos) $a, a' \in M$ com $c = \varphi(a)$ e $c' = \varphi(a')$.

Segue para todo $i = 1, 2, \dots, r$:

$$\begin{aligned} \varphi^{-1}(c \perp_i c') &= \varphi^{-1}(\varphi(a) \perp_i \varphi(a')) = \varphi^{-1}(\varphi(a \top_i a')) = \\ &= a \top_i a' = \varphi^{-1}(c) \top_i \varphi^{-1}(c'). \end{aligned}$$

■

II.2.19 Definição.

Dois estruturas $(M; \top_1, \top_2, \dots, \top_r)$ e $(N; \perp_1, \perp_2, \dots, \perp_r)$ chamam-se *isomorfas*, denotado por

$$(M; \top_1, \top_2, \dots, \top_r) \cong (N; \perp_1, \perp_2, \dots, \perp_r),$$

se existe um isomorfismo de $(M; \top_1, \top_2, \dots, \top_r)$ sobre $(N; \perp_1, \perp_2, \dots, \perp_r)$.

II.2.20 Exemplos.

a) Seja $\mathbf{P} = \{x \in \mathbb{R} \mid x > 0\}$. Temos

$$(\mathbb{R}; +) \cong (\mathbf{P}; \cdot).$$

Para $0 < a \in \mathbb{R}$, $a \neq 1$, as aplicações $\varphi_a \in \mathbf{P}^{\mathbb{R}}$ com

$$\varphi_a(x) = a^x \quad \forall x \in \mathbb{R}$$

são isomorfismos de $(\mathbb{R}; +)$ sobre $(\mathbf{P}; \cdot)$.

Suas inversas $\varphi_a^{-1} \in \mathbb{R}^{\mathbf{P}}$ são

$$\varphi_a^{-1}(y) = \log_a y \quad \forall y \in \mathbf{P}.$$

b) Sejam os intervalos reais $M = (0, 5]$ e $N = (0, 7]$. As estruturas

$$(M; \top) \quad \text{e} \quad (N; \perp),$$

definidas pelas composições internas

$$a \top b = \frac{ab}{5} \quad \forall a, b \in M \quad \text{e} \quad a \perp b = \frac{ab}{7} \quad \forall a, b \in N$$

são dois monóides. A aplicação

$$\varphi \in N^M \quad \text{definida por} \quad \varphi(x) = \frac{7}{5}x \quad \forall x \in M$$

é um isomorfismo de $(M; \top)$ sobre $(N; \perp)$. Portanto

$$(M; \top) \cong (N; \perp).$$

A inversa de φ é a $\varphi^{-1} \in M^N$ com $\varphi^{-1}(y) = \frac{5}{7}y \quad \forall y \in N$.

■

II.2.21 Proposição.

Sejam $(M; \top_1, \top_2, \dots, \top_r)$, $(N; \perp_1, \perp_2, \dots, \perp_r)$ e $(P; *_1, *_2, \dots, *_r)$ três estruturas algébricas com r composições internas, cada.

a) Sempre $(M; \top_1, \top_2, \dots, \top_r) \cong (M; \top_1, \top_2, \dots, \top_r)$.

- b) Se $(M; \top_1, \top_2, \dots, \top_r) \cong (N; \perp_1, \perp_2, \dots, \perp_r)$,
então $(N; \perp_1, \perp_2, \dots, \perp_r) \cong (M; \top_1, \top_2, \dots, \top_r)$.
- c) Se $(M; \top_1, \top_2, \dots, \top_r) \cong (N; \perp_1, \perp_2, \dots, \perp_r)$ e
 $(N; \perp_1, \perp_2, \dots, \perp_r) \cong (P; *_{1}, *_{2}, \dots, *_{r})$,
então $(M; \top_1, \top_2, \dots, \top_r) \cong (P; *_{1}, *_{2}, \dots, *_{r})$.

Demonstração: a) segue, pois a aplicação identica δ_M é um isomorfismo de $(M; \top_1, \top_2, \dots, \top_r)$ sobre si mesma.

b) Se φ é um isomorfismo de $(M; \top_1, \top_2, \dots, \top_r)$ sobre $(N; \perp_1, \perp_2, \dots, \perp_r)$, então φ^{-1} é um isomorfismo de $(N; \perp_1, \perp_2, \dots, \perp_r)$ sobre $(M; \top_1, \top_2, \dots, \top_r)$

c) Se $\varphi : M \longrightarrow N$ e $\psi : N \longrightarrow P$ são isomorfismos, então a composta $\psi \circ \varphi : M \longrightarrow P$ é um isomorfismo.

■

Estas regras dizem que

isomorfa entre estruturas algébricas é um conceito de equivalência no universo das estruturas algébricas

(da mesma forma que *equipotência entre conjuntos* é um conceito de equivalência no universo dos conjuntos).

Se $(M; \top_1, \top_2, \dots, \top_r) \cong (N; \perp_1, \perp_2, \dots, \perp_r)$ são duas estruturas isomorfas, então, particularmente os conjuntos $M \sim N$ são equipotentes.

Também podemos pensar ao contrário:

Numa estrutura algébrica $(M; \top_1, \top_2, \dots, \top_r)$ podemos substituir o conjunto M por qualquer conjunto equipotente, como mostra

II.2.22 Proposição.

Seja $(M; \top_1, \top_2, \dots, \top_r)$ uma estrutura algébrica, $N \sim M$ um conjunto equipotente com M e seja $\varphi \in \mathbf{Bij}(M, N)$.

Definindo-se composições internas $\perp_1, \perp_2, \dots, \perp_r \in N^{N \times N}$ por

$$c \perp_i d = \varphi \left(\varphi^{-1}(c) \top_i \varphi^{-1}(d) \right) \quad \forall c, d \in N,$$

temos que

$$(N; \perp_1, \perp_2, \dots, \perp_r)$$

é uma estrutura algébrica que é isomorfa com

$$(M; \top_1, \top_2, \dots, \top_r),$$

sendo que a bijeção φ dada torna-se um isomorfismo de $(M; \top_1, \top_2, \dots, \top_r)$ sobre $(N; \perp_1, \perp_2, \dots, \perp_r)$.

Demonstração: Para todos os $a, b \in M$ e todos os $i = 1, 2, \dots, r$ temos com esta definição das $\perp_1, \perp_2, \dots, \perp_r$ de fato:

$$\varphi(a \top_i b) = \varphi\left(\varphi^{-1}(\varphi(a)) \top_i \varphi^{-1}(\varphi(b))\right) = \varphi(a) \perp_i \varphi(b).$$

■

II.2.23 Exemplos.

- a) Queremos definir uma composição interna \perp no intervalo real $N = \left(-\frac{\pi}{2}, \frac{\pi}{2}\right)$ tal que

$$(N; \perp) \cong (\mathbb{R}; +).$$

Tendo em vista que $\varphi \in N^{\mathbb{R}}$ com $\varphi(x) = \arctg x \quad \forall x \in \mathbb{R}$, é uma bijeção de \mathbb{R} sobre N , definamos para todos os $c, d \in N$:

$$c \perp d = \arctg(\operatorname{tg}(c) + \operatorname{tg}(d)).$$

Temos $\forall a, b \in \mathbb{R}$:

$$\begin{aligned} \varphi(a + b) &= \arctg(a + b) = \arctg\left(\operatorname{tg}(\arctg(a)) + \operatorname{tg}(\arctg(b))\right) = \\ &= \arctg(a) \perp \arctg(b) = \varphi(a) \perp \varphi(b). \end{aligned}$$

- b) Seja o intervalo real $M = (0, 3]$ munido da composição interna

$$a \top b = \frac{ab}{3} \quad \forall a, b \in M.$$

Temos que $(M; \top)$ é um monóide e seu neutro é $e_M = 3$ (comparar II.2.20 b)).

Queremos "transplantar" esta composição para o intervalo $N = [-8, 4)$ e definir uma composição $\perp \in N^{N \times N}$, tal que $(N; \perp)$ seja um monóide isomorfo com $(M; \top)$ e tal que $e_N = -8$ seja o elemento neutro de $(N; \perp)$.

Temos que $\varphi \in N^M$ com $\varphi(x) = -4x + 4 \quad \forall x \in M$ é uma possível bijeção de

M sobre N com $\varphi(3) = -8$.

Para $\varphi^{-1} \in M^N$ vale $\varphi^{-1}(y) = -\frac{y}{4} + 1 \quad \forall y \in N$ e vemos que para $c, d \in N$:

$$\begin{aligned} \varphi(\varphi^{-1}(c) \top \varphi^{-1}(d)) &= \varphi\left(\left(-\frac{c}{4} + 1\right) \top \left(-\frac{d}{4} + 1\right)\right) = \\ &= -4 \cdot \frac{\left(-\frac{c}{4} + 1\right)\left(-\frac{d}{4} + 1\right)}{3} + 4 = -\frac{cd}{12} + \frac{c}{3} + \frac{d}{3} + \frac{8}{3}. \end{aligned}$$

Portanto, uma possível composição \perp em $N = [-8, 4)$, tal que

$$(M; \top) \cong (N; \perp) \text{ com identidade } e_N = -8$$

é dada por

$$c \perp d = -\frac{cd}{12} + \frac{c}{3} + \frac{d}{3} + \frac{8}{3} \quad \forall c, d \in N.$$

O TEOREMA GERAL DO HOMOMORFISMO E ESTRUTURAS SIMPLES

II.2.24 Teorema.

Seja $(M; \top_1, \top_2, \dots, \top_r)$ uma estrutura algébrica, $\kappa \in \mathbf{Cg}(M; \top_1, \top_2, \dots, \top_r)$ e $(M/\kappa; \bar{\top}_1, \bar{\top}_2, \dots, \bar{\top}_r)$ a estrutura quociente $M \text{ mod } \kappa$.

Então a aplicação canónica $\gamma \in (M/\kappa)^M$, i.e.

$$\gamma(a) = \bar{a} \quad \forall a \in M \quad (\text{onde } \bar{a} = \{x \in M \mid x \kappa a\})$$

é um epimorfismo de M sobre M/κ , chamado o

epimorfismo canónico de

$$(M; \top_1, \top_2, \dots, \top_r) \text{ sobre } (M/\kappa; \bar{\top}_1, \bar{\top}_2, \dots, \bar{\top}_r).$$

Demonstração: É só preciso mostrar que γ é um homomorfismo. Isto segue, pois $\forall a, b \in M$ e todos os $i = 1, 2, \dots, r$:

$$\gamma(a \top_i b) = \overline{a \top_i b} = \bar{a} \bar{\top}_i \bar{b} = \gamma(a) \bar{\top}_i \gamma(b).$$

■

Particularmente: A estrutura quociente de uma estrutura algébrica mod uma qualquer de suas relações de congruência, é uma imagem homomórfica da estrutura

original.

Reciprocamente temos:

II.2.25 Teorema.

Sejam $(M; \top_1, \top_2, \dots, \top_r)$ e $(N; \perp_1, \perp_2, \dots, \perp_r)$ duas estruturas algébricas com r composições internas, cada.

Seja φ um homomorfismo de $(M; \top_1, \top_2, \dots, \top_r)$ em $(N; \perp_1, \perp_2, \dots, \perp_r)$.

Seja κ_φ a relação de equivalência associada ao $\varphi : \forall a, a' \in M :$

$$a \kappa_\varphi a' \iff \varphi(a) = \varphi(a') .$$

Então valem:

- $\varphi(M)$ é uma subestrutura de $(N; \perp_1, \perp_2, \dots, \perp_r)$.
- $\kappa_\varphi \in \mathbf{Cg}(M; \top_1, \top_2, \dots, \top_r)$
- Existe um único isomorfismo ψ da estrutura quociente $(M/\kappa_\varphi; \bar{\top}_1, \bar{\top}_2, \dots, \bar{\top}_r)$ sobre a imagem $(\varphi(M); \perp_1, \perp_2, \dots, \perp_r)$, tal que $\varphi = \psi \circ \gamma$.

Particularmente,

$$(M/\kappa_\varphi; \bar{\top}_1, \bar{\top}_2, \dots, \bar{\top}_r) \cong (\varphi(M); \perp_1, \perp_2, \dots, \perp_r) .$$

Esta fundamental observação, conhecida como *teorema geral do homomorfismo*, diz portanto:

A imagem homomórfica de uma estrutura algébrica por um homomorfismo φ é uma estrutura algébrica, a qual pode ser reencontrada isomórficamente em forma de uma estrutura quociente, olhando a estrutura original mod a relação de congruência κ_φ associada ao homomorfismo φ .

Demonstração: a) Claro que $\emptyset \neq \varphi(M) \subseteq N$. Sejam $b, b' \in \varphi(M)$, digamos $b = \varphi(a)$ e $b' = \varphi(a')$ com $a, a' \in M$. Segue $\forall i = 1, 2, \dots, r :$

$$b \perp_i b' = \varphi(a) \perp_i \varphi(a') = \varphi(a \top_i a') \in \varphi(M) .$$

Logo $\varphi(M)$ é uma subestrutura de $(N; \perp_1, \perp_2, \dots, \perp_r)$.

b) Já sabemos que $\kappa_\varphi \in \mathbf{Eq}(M)$. Se $a, a', c, c' \in M$ são tais que $\begin{cases} a \kappa_\varphi a' \\ c \kappa_\varphi c' \end{cases}$, temos $\varphi(a) = \varphi(a')$ e $\varphi(c) = \varphi(c')$. Segue para todo $i = 1, 2, \dots, r :$

$$\varphi(a \top_i c) = \varphi(a) \perp_i \varphi(c) = \varphi(a') \perp_i \varphi(c') = \varphi(a' \top_i c')$$

e portanto $a \tau_i c \kappa_\varphi a' \tau_i c'$. Isto significa $\kappa_\varphi \in \mathbf{Cg}(M; \tau_1, \dots, \tau_r)$.

c) Por I.2.29, existe uma única bijeção $\psi: M/\kappa_\varphi \rightarrow \varphi(M)$ com $\varphi = \psi \circ \gamma$, a saber a bijeção definida por

$$\psi(\bar{a}) = \varphi(a) \quad \forall \bar{a} \in M/\kappa_\varphi.$$

Só falta provar que ψ é um homomorfismo. De fato temos para todos os $\bar{a}, \bar{a}' \in M/\kappa_\varphi$ e todos os $i = 1, 2, \dots, r$:

$$\psi(\bar{a} \bar{\tau}_i \bar{a}') = \psi(\overline{a \tau_i a'}) = \varphi(a \tau_i a') = \varphi(a) \perp_i \varphi(a') = \psi(\bar{a}) \perp_i \psi(\bar{a}').$$

■

Pelo teorema geral do homomorfismo,

as imagens homomórficas de uma estrutura $(M; \tau_1, \tau_2, \dots, \tau_r)$ são essencialmente determinadas *pelo conhecimento de suas relações de congruência*, i.e. pelo conjunto $\mathbf{Cg}(M; \tau_1, \tau_2, \dots, \tau_r)$.

Toda estrutura sempre possui as congruências *triviais*, a relação da igualdade e a relação universal, i.e. $\{\delta_M, M \times M\} \subseteq \mathbf{Cg}(M; \tau_1, \tau_2, \dots, \tau_r)$.

As estruturas quocientes (i.e. as imagens homomórficas) modulo estas duas congruências triviais são

$$(M/\delta_M; \bar{\tau}_1, \bar{\tau}_2, \dots, \bar{\tau}_r) \cong (M; \tau_1, \tau_2, \dots, \tau_r)$$

e

$$(M/M \times M; \bar{\tau}_1, \bar{\tau}_2, \dots, \bar{\tau}_r) \cong (\{e\}; \perp_1, \perp_2, \dots, \perp_r),$$

onde $(\{e\}; \perp_1, \perp_2, \dots, \perp_r)$ é uma estrutura algébrica trivial, definida num conjunto unitário $\{e\}$ com as r composições $\perp_1 = \perp_2 = \dots = \perp_r$ coincidentes com a única possível: $e \perp_i e = e$.

Destaque merece o caso quando as congruências triviais são as *únicas* relações de congruência de uma estrutura $(M; \tau_1, \tau_2, \dots, \tau_r)$:

II.2.26 Definição.

Uma estrutura algébrica

$(M; \tau_1, \tau_2, \dots, \tau_r)$ é dita *simples*,

se $|M| \geq 2$ e se

$$\mathbf{Cg}(M; \tau_1, \dots, \tau_r) = \{\delta_M, M \times M\},$$

i.e. se as únicas relações de congruência dela forem a relação da igualdade e a relação universal.

II.2.27 Exemplos.

- Se $|M| = 2$, certamente, $(M; \tau_1, \tau_2, \dots, \tau_r)$ será uma estrutura simples, pois $|\mathbf{Eq}(M)| = 2$ neste caso.
- $(\mathbb{Z}; +, \cdot)$ não é uma estrutura simples, pois ela tem as infinitas relações de congruência distintas \equiv_n com $n = 0, 1, 2, 3, \dots$ (ver II.2.9 a))

II.2.28 Exemplo.

$(\mathbb{R}; +, \cdot)$ é uma estrutura simples.

Demonstração: Devemos mostrar $\mathbf{Cg}(\mathbb{R}; +, \cdot) = \{\delta_{\mathbb{R}}, \mathbb{R} \times \mathbb{R}\}$: Seja dada $\delta_{\mathbb{R}} \neq \kappa \in \mathbf{Cg}(\mathbb{R}; +, \cdot)$ e é preciso mostrar $\kappa = \mathbb{R} \times \mathbb{R}$:

Como $\kappa \neq \delta_{\mathbb{R}}$, existem $a, b \in \mathbb{R}$ com $a \kappa b$ mas $a \neq b$.

De $\begin{cases} a \kappa b \\ -b \kappa -b \end{cases}$ segue $a - b \kappa 0$, mas $a - b \neq 0$. Coloquemos $c = \frac{1}{a-b}$. De

$\begin{cases} a-b \kappa 0 \\ c \kappa c \end{cases}$ segue por multiplicação $1 = c \cdot (a - b) \kappa c \cdot 0 = 0$, i.e.

$$1 \kappa 0.$$

Para todos os $x, y \in \mathbb{R}$ segue agora

$$x = x \cdot 1 \kappa x \cdot 0 = 0 = y \cdot 0 \kappa y \cdot 1 = y,$$

i.e. $x \kappa y$. Mas isto significa que $\kappa = \mathbb{R} \times \mathbb{R}$. Logo, $\mathbf{Cg}(\mathbb{R}; +, \cdot) = \{\delta_{\mathbb{R}}, \mathbb{R} \times \mathbb{R}\}$ e vemos que $(\mathbb{R}; +, \cdot)$ é uma estrutura simples.

Entretanto temos

II.2.29 Exemplo.

A estrutura $(\mathbb{R}; +)$ não é simples.

Demonstração: Basta dar um exemplo de uma relação $\kappa \in \mathbf{Cg}(\mathbb{R}; +)$ com $\delta_{\mathbb{R}} \neq \kappa \neq \mathbb{R} \times \mathbb{R}$: Definamos para todos os $a, b \in \mathbb{R}$

$$a \kappa b \iff a - b \in \mathbb{Z} .$$

É fácil mostrar que $\kappa \in \mathbf{Cg}(\mathbb{R}; +)$.

Temos $\frac{1}{2} \not\kappa \frac{1}{3} \kappa \frac{4}{3}$. Portanto, $\delta_{\mathbb{R}} \neq \kappa \neq \mathbb{R} \times \mathbb{R}$.

■

ASSOCIATIVIDADE, COMUTATIVIDADE, IDENTIDADES E INVERSOS
SOB HOMOMORFISMOS

II.2.30 Proposição.

Sejam $(M; \top)$ e $(N; \perp)$ duas estruturas algébricas e $\varphi \in N^M$ um homomorfismo.

- Suponha $(M; \top)$ é comutativa. Então a subestrutura imagem $\varphi(M)$ de $(N; \perp)$ é comutativa também.*
- Se $(M; \top)$ é um semigrupo, então a subestrutura imagem $\varphi(M)$ de $(N; \perp)$ é um semigrupo também.*

Demonstração: a) Para todos os $b, c \in \varphi(M)$ existem $x, y \in M$ com $b = \varphi(x)$ e $c = \varphi(y)$. Segue

$$b \perp c = \varphi(x) \perp \varphi(y) = \varphi(x \top y) = \varphi(y \top x) = \varphi(y) \perp \varphi(x) = c \perp b .$$

Portanto, $(\varphi(M); \perp)$ é uma estrutura comutativa também.

b) Suponha $b, c, d \in \varphi(M)$ são três quaisquer elementos. Existem $x, y, z \in M$ com $b = \varphi(x)$, $c = \varphi(y)$, $d = \varphi(z)$. Segue

$$b \perp (c \perp d) = \varphi(x) \perp (\varphi(y) \perp \varphi(z)) = \varphi(x) \perp \varphi(y \top z) =$$

$$\begin{aligned}
&= \varphi(x \top (y \top z)) = \varphi((x \top y) \top z) = \varphi(x \top y) \perp \varphi(z) = \\
&= (\varphi(x) \perp \varphi(y)) \perp \varphi(z) = (b \perp c) \perp d
\end{aligned}$$

Logo, $(\varphi(M); \perp)$ é semigrupo também. ■

II.2.31 Proposição.

Sejam $(M; \top)$ e $(N; \perp)$ duas estruturas algébricas e $\varphi \in N^M$ um homomorfismo.

- a) Se $e \in M$ é uma identidade à esquerda [à direita, bilateral], então $\varphi(e)$ é uma identidade à esquerda [à direita, bilateral] da subestrutura imagem $(\varphi(M); \perp)$.
- b) Suponha $(M; \top)$ possua uma identidade bilateral, digamos e . Se $u \in \mathbf{U}'(M)$ [$u \in \mathbf{U}''(M)$, $u \in \mathbf{U}(M)$] é um elemento inversível à esquerda [à direita, bilateral], então
- $$\varphi(u) \in \mathbf{U}'(\varphi(M)) \quad [\varphi(u) \in \mathbf{U}''(\varphi(M)), \varphi(u) \in \mathbf{U}(\varphi(M))].$$

Demonstração: a) Para todo $b \in \varphi(M)$ existe $a \in M$ com $b = \varphi(a)$. Segue

$$\varphi(e) \perp b = \varphi(e) \perp \varphi(a) = \varphi(e \top a) = \varphi(a) = b.$$

Portanto, $\varphi(e) \perp b = b \quad \forall b \in \varphi(M)$. Isto significa que $\varphi(e)$ é uma identidade à esquerda de $\varphi(M)$.

("à direita" e "bilateral" é tratado da mesma forma).

b) Suponha e é identidade bilateral de M e seja $u \in \mathbf{U}'(M)$. Seja $y \in M$ com $y \top u = e$ um qualquer inverso à esquerda de u . Segue

$$\varphi(y) \perp \varphi(u) = \varphi(y \top u) = \varphi(e).$$

Como $\varphi(e)$ é a identidade bilateral de $\varphi(M)$, vemos que $\varphi(u) \in \mathbf{U}'(\varphi(M))$.

("à direita" e "bilateral" é tratado da mesma forma).

Particularmente, um *epi* morfismo $\varphi : M \longrightarrow N$ leva identidades e inversos de $(M; \top)$ a identidades e inversos correspondentes de $(N; \perp)$. ■

§ II.3 Grupos

GRUPOS

O conceito mais básico em toda álgebra é o de um *grupo*.

Em II.1.39 já vimos uma possível definição desta categoria de estruturas algébricas: Entende-se por um grupo

$$\text{um monóide } (M; \tau) \text{ no qual } \mathbf{U}(M) = M,$$

i.e. uma estrutura associativa com identidade na qual todo elemento possui um inverso bilateral.

O mais comum para se escrever a composição interna de um grupo é a notação multiplicativa " \cdot " ou a aditiva "+". Para grupos de aplicações bijetoras (permutações) usa-se às vezes o círculo da composição " \circ ". A notação aditiva usa-se preferencialmente no caso de grupos comutativos (abelianos).

O elemento neutro é usualmente escrito como " 1 " em notação multiplicativa, como " 0 " em notação aditiva.

O inverso \hat{a} de um a é denotado por a^{-1} em notação multiplicativa, por $-a$ em notação aditiva.

Em notação múltiplicativa (o ponto \cdot da multiplicação é muitas vezes desprezado), a definição de grupo pode ser repetida assim:

II.3.1 Definição.

Uma estrutura algébrica com uma composição interna $(G; \cdot)$ é denominada um *grupo*, se

- i) $a(bc) = (ab)c$ para todos os $a, b, c \in G$
- ii) Existe $1 \in G$ com $a \cdot 1 = 1 \cdot a = a$ para todos os $a \in G$.
- iii) Para todo $a \in G$ existe $a^{-1} \in G$ com $aa^{-1} = a^{-1}a = 1$.

Lembramos que o neutro 1 e para cada $a \in G$ o inverso bilateral a^{-1} são únicos. Além disso, $(a^{-1})^{-1} = a$ e $(ab)^{-1} = b^{-1}a^{-1}$ para todos os $a, b \in G$.

II.3.2 Exemplos.

a) Para qualquer conjunto $A \neq \emptyset$, temos

$$(\mathbf{S}_A; \circ), \quad \text{o grupo simétrico sobre } A.$$

Este é o grupo das unidades do monóide $(A^A; \circ)$ de todas as aplicações do conjunto A em si mesmo.

b) $(\mathbb{Z}; +)$, o grupo aditivo dos inteiros.

c) $(\mathbf{P}; \cdot)$, o grupo multiplicativo dos números reais positivos.

d) O grupo multiplicativo $(\{1, -1\}; \cdot)$

e) Para qualquer monóide $(M; \top)$: O grupo

$$(\mathbf{U}(M); \top), \quad \text{consistindo dos elementos inversíveis de } (M; \top)$$

■

OS GRUPOS SIMÉTRICOS

No monóide $(A^A; \circ)$ existem aplicações não comutáveis se $|A| \geq 2$ (ver II.1.21).

Entretanto, se $A = \{1, 2\}$, os dois elementos do grupo simétrico

$$\mathbf{S}_A = \left\{ \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\}$$

comutam. Mas vale a

I.3.3 Observação.

Para A um conjunto com $|A| \geq 3$, o grupo simétrico \mathbf{S}_A não é comutativo.

Demonstração: Sejam $a, b, c \in A$ três elementos distintos. Para as permutações $\pi, \sigma \in \mathbf{S}_A$ definidas por

$$\pi(x) = \begin{cases} b & \text{se } x = a \\ a & \text{se } x = b \\ x & \text{se } x \neq a, b \end{cases} \quad \text{e} \quad \sigma(x) = \begin{cases} c & \text{se } x = a \\ a & \text{se } x = c \\ x & \text{se } x \neq a, c \end{cases}$$

temos

$$(\pi \circ \sigma)(a) = \pi(\sigma(a)) = \pi(c) = c,$$

enquanto

$$(\sigma \circ \pi)(a) = \sigma(\pi(a)) = \sigma(b) = b .$$

Portanto, $\sigma \circ \pi \neq \pi \circ \sigma$.

■

II.3.4 Proposição.

Sejam A e B conjuntos equipotentes. Então

$$(\mathbf{S}_A; \circ) \cong (\mathbf{S}_B; \circ) ,$$

i.e. os grupos simétricos sobre conjuntos equipotentes são isomorfos.

Demonstração: Seja $\varphi : A \longrightarrow B$ uma bijeção.

Consideremos a aplicação

$$\Omega : \mathbf{S}_A \longrightarrow \mathbf{S}_B ,$$

definida por

$$\Omega(\pi) = \varphi \circ \pi \circ \varphi^{-1} \quad \forall \pi \in \mathbf{S}_A .$$

Para toda $\pi \in \mathbf{S}_A$, a aplicação $\Omega(\pi)$ é uma permutação de B , pois ela é a composta de três bijeções

$$B \xrightarrow{\varphi^{-1}} A \xrightarrow{\pi} A \xrightarrow{\varphi} B .$$

Portanto, de fato $\Omega(\pi) \in \mathbf{S}_B$, i.e. $\Omega \in (\mathbf{S}_B)^{\mathbf{S}_A}$. Além disso:

1) Para todas as $\pi_1, \pi_2 \in \mathbf{S}_A$ temos

$$\begin{aligned} \Omega(\pi_1 \circ \pi_2) &= \varphi \circ (\pi_1 \circ \pi_2) \circ \varphi^{-1} = \varphi \circ \pi_1 \circ (\varphi^{-1} \circ \varphi) \circ \pi_2 \circ \varphi^{-1} = \\ &= (\varphi \circ \pi_1 \circ \varphi^{-1}) \circ (\varphi \circ \pi_2 \circ \varphi^{-1}) = \Omega(\pi_1) \circ \Omega(\pi_2) . \end{aligned}$$

Portanto, Ω é um homomorfismo do grupo simétrico $(\mathbf{S}_A; \circ)$ em $(\mathbf{S}_B; \circ)$.

2) Para toda $\tau \in \mathbf{S}_B$ temos $\pi = \varphi^{-1} \circ \tau \circ \varphi \in \mathbf{S}_A$ e vale para este π :

$\Omega(\pi) = \varphi \circ (\varphi^{-1} \circ \tau \circ \varphi) \circ \varphi^{-1} = (\varphi \circ \varphi^{-1}) \circ \tau \circ (\varphi \circ \varphi^{-1}) = \tau$, mostrando a sobrejetividade de Ω .

3) Se temos $\Omega(\pi_1) = \Omega(\pi_2)$ para $\pi_1, \pi_2 \in \mathbf{S}_A$, concluímos

$$\varphi \circ \pi_1 \circ \varphi^{-1} = \varphi \circ \pi_2 \circ \varphi^{-1} .$$

Daí por multiplicação por φ à direita e por φ^{-1} à esquerda,

segue $\varphi \circ \pi_1 = \varphi \circ \pi_2$ e finalmente $\pi_1 = \pi_2$.

Isto mostra a injetividade de Ω .

Portanto, Ω é um isomorfismo de $(\mathbf{S}_A; \circ)$ sobre $(\mathbf{S}_B; \circ)$.

■

Por exemplo

$$(\mathbf{S}_{\{1,2,3,4\}}; \circ) \cong (\mathbf{S}_{\{\heartsuit, \spadesuit, \diamondsuit, \clubsuit\}}; \circ).$$

Portanto, não importa se substituimos no grupo simétrico \mathbf{S}_A o conjunto permutado A por qualquer outro conjunto equipotente B .

Particularmente, se o conjunto A é finito com n elementos, podemos supor $A = \{1, 2, 3, \dots, n\}$ e escrevemos

$$\mathbf{S}_{\{1,2,3,\dots,n\}} = \mathbf{S}_n.$$

O grupo

$$(\mathbf{S}_n; \circ)$$

chama-se o grupo simétrico de grau n . Por I.2.34 temos

$$|\mathbf{S}_n| = n!.$$

Os $n!$ elementos π, σ, \dots de \mathbf{S}_n podemos escrever (ver I.2.11) como

$$\pi = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ i_1 & i_2 & i_3 & \cdots & i_n \end{pmatrix}, \quad \sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ j_1 & j_2 & j_3 & \cdots & j_n \end{pmatrix}$$

(onde $\pi(k) = i_k$, $\sigma(k) = j_k \forall k = 1, 2, 3, \dots, n$),

com a regra de multiplicação

$$\begin{aligned} \sigma \circ \pi &= \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ j_1 & j_2 & j_3 & \cdots & j_n \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ i_1 & i_2 & i_3 & \cdots & i_n \end{pmatrix} = \\ &= \begin{pmatrix} i_1 & i_2 & i_3 & \cdots & i_n \\ j_{i_1} & j_{i_2} & j_{i_3} & \cdots & j_{i_n} \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ i_1 & i_2 & i_3 & \cdots & i_n \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ j_{i_1} & j_{i_2} & j_{i_3} & \cdots & j_{i_n} \end{pmatrix}. \end{aligned}$$

II.3.5 Exemplo.

O grupo simétrico de grau 3 indicamos em seguida por

$$G = \mathbf{S}_3 = \{\mathbf{1}, \tau_1, \tau_2, \tau_3, \sigma, \rho\}$$

onde

$$\mathbf{1} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \tau_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad \tau_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},$$

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \quad \text{e} \quad \rho = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

com a composição

$$\begin{pmatrix} 1 & 2 & 3 \\ j_1 & j_2 & j_3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ i_1 & i_2 & i_3 \end{pmatrix} = \begin{pmatrix} i_1 & i_2 & i_3 \\ j_{i_1} & j_{i_2} & j_{i_3} \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ i_1 & i_2 & i_3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ j_{i_1} & j_{i_2} & j_{i_3} \end{pmatrix}.$$

A tábua de composição de $(\mathbf{S}_3; \circ)$ é:

\circ	$\mathbf{1}$	τ_1	τ_2	τ_3	σ	ρ
$\mathbf{1}$	$\mathbf{1} \circ \mathbf{1}$	$\mathbf{1} \circ \tau_1$	$\mathbf{1} \circ \tau_2$	$\mathbf{1} \circ \tau_3$	$\mathbf{1} \circ \sigma$	$\mathbf{1} \circ \rho$
τ_1	$\tau_1 \circ \mathbf{1}$	$\tau_1 \circ \tau_1$	$\tau_1 \circ \tau_2$	$\tau_1 \circ \tau_3$	$\tau_1 \circ \sigma$	$\tau_1 \circ \rho$
τ_2	$\tau_2 \circ \mathbf{1}$	$\tau_2 \circ \tau_1$	$\tau_2 \circ \tau_2$	$\tau_2 \circ \tau_3$	$\tau_2 \circ \sigma$	$\tau_2 \circ \rho$
τ_3	$\tau_3 \circ \mathbf{1}$	$\tau_3 \circ \tau_1$	$\tau_3 \circ \tau_2$	$\tau_3 \circ \tau_3$	$\tau_3 \circ \sigma$	$\tau_3 \circ \rho$
σ	$\sigma \circ \mathbf{1}$	$\sigma \circ \tau_1$	$\sigma \circ \tau_2$	$\sigma \circ \tau_3$	$\sigma \circ \sigma$	$\sigma \circ \rho$
ρ	$\rho \circ \mathbf{1}$	$\rho \circ \tau_1$	$\rho \circ \tau_2$	$\rho \circ \tau_3$	$\rho \circ \sigma$	$\rho \circ \rho$

Já calculada temos

\circ	$\mathbf{1}$	τ_1	τ_2	τ_3	σ	ρ
$\mathbf{1}$	$\mathbf{1}$	τ_1	τ_2	τ_3	σ	ρ
τ_1	τ_1	$\mathbf{1}$	ρ	σ	τ_3	τ_2
τ_2	τ_2	σ	$\mathbf{1}$	ρ	τ_1	τ_3
τ_3	τ_3	ρ	σ	$\mathbf{1}$	τ_2	τ_1
σ	σ	τ_2	τ_3	τ_1	ρ	$\mathbf{1}$
ρ	ρ	τ_3	τ_1	τ_2	$\mathbf{1}$	σ

■

SUBGRUPOS

II.3.6 Definição.

Um subconjunto H de um grupo $(G; \cdot)$ é um *subgrupo de G* , (abreviado: $H \leq G$) se

- i) $H \neq \emptyset$.
- ii) $xy \in H$ para todos os $x, y \in H$.
- iii) $x^{-1} \in H$ para todo $x \in H$.

Isto significa portanto que os subgrupos H são as subestruturas de $(G; \cdot)$ que ainda são fechadas a inversos.

II.3.7 Exemplos.

- a) Sempre existem os subgrupos triviais $\{1\}$ e G em cada grupo G .
- b) $\mathbb{Z} \leq (\mathbb{R}; +)$.
- c) Para todo $n \in \mathbb{N}_0$, o conjunto $U_n = \{nk \mid k \in \mathbb{Z}\}$ dos múltiplos de n , é um subgrupo de $(\mathbb{Z}; +)$.
- e) A subestrutura $(\mathbb{N}; +)$ de $(\mathbb{Z}; +)$ não é um subgrupo.

■

II.3.8 Observação.

Para um subconjunto H de um grupo G são equivalentes

- a) $H \leq G$, i.e. H possui as propriedades i) - iii) da Def. II.3.6
- b) $1 \in H$ e $ab^{-1} \in H$ para todos os $a, b \in H$.

Demonstração: "b) \Rightarrow a)": Se b) é verdade, então $1 \in H$, particularmente $H \neq \emptyset$. Logo 3.6 i) vale.

Se $x \in H$ e já sabendo que $1 \in H$, vemos por b) que também $x^{-1} = 1 \cdot x^{-1} \in H$. Logo 3.6 iii) vale.

Se $x, y \in H$, então $x, y^{-1} \in H$ e finalmente $xy = x(y^{-1})^{-1} \in H$. Isto é 3.6 ii). Logo $H \leq G$.

"a) \Rightarrow b)": Suponha, $H \leq G$. Então H possui as 3 propriedades i) - iii) da

definição II.3.6. Sabemos então $H \neq \emptyset$. Pegando qualquer $b \in H$, vemos também $b^{-1} \in H$ e daí $1 = bb^{-1} \in H$.

Para $a, b \in H$ vemos $a, b^{-1} \in H$ e daí $ab^{-1} \in H$.

Logo H possui a propriedade estabelecida em b). ■

O conjunto de todos os subgrupos de um grupo G é às vezes escrito como

$$\mathfrak{S}(G) = \{H \mid H \text{ é subgrupo de } G\} .$$

Escrever $H \leq G$ ou $H \in \mathfrak{S}(G)$ significa portanto o mesmo. Sempre temos

$$G, \{1\} \in \mathfrak{S}(G) .$$

II.3.9 Exemplo.

O conjunto de todos os subgrupos de $(\mathbf{S}_3; \circ)$ é

$$\mathfrak{S}(\mathbf{S}_3) = \{\{1\}, \mathbf{S}_3, \{1, \tau_1\}, \{1, \tau_2\}, \{1, \tau_3\}, \{1, \sigma, \rho\}\} .$$
■

O GRUPO DOS AUTOMORFISMOS DE UMA ESTRUTURA ALGÉBRICA

II.3.10 Proposição.

Seja $(M; \tau_1, \tau_2, \dots, \tau_r)$ uma estrutura algébrica com r composições internas. Seja $(\mathbf{S}_M; \circ)$ o grupo simétrico sobre o conjunto M . O conjunto

$$\mathbf{A} = \left\{ \alpha \in \mathbf{S}_M \mid \alpha(a \tau_i b) = \alpha(a) \tau_i \alpha(b) \quad \forall a, b \in M \quad \forall i = 1, 2, \dots, r \right\} ,$$

forma um subgrupo de \mathbf{S}_M , i.e.

$$(\mathbf{A}; \circ) \leq (\mathbf{S}_M; \circ) .$$

Demonstração: 1) Para a permutação identica $\mathbf{1} = \delta_M \in \mathbf{S}_M$ temos certamente $\mathbf{1} \in \mathbf{A}$, pois $\mathbf{1}(a \tau_i b) = a \tau_i b = \mathbf{1}(a) \tau_i \mathbf{1}(b) \quad \forall a, b \in M \quad \forall i = 1, 2, \dots, r$.

2) Se $\alpha, \beta \in \mathbf{A}$. Então $\alpha \circ \beta^{-1} \in \mathbf{A}$. Isto é uma consequência de II.2.17/18. ■

II.3.11 Definição.

Seja $(M; \tau_1, \tau_2, \dots, \tau_r)$ uma estrutura algébrica com r composições internas. O subgrupo

$$(\mathbf{A}; \circ) \text{ do grupo simétrico } (\mathbf{S}_M; \circ)$$

chama-se

$$\textit{o grupo dos automorfismos de } (M; \tau_1, \tau_2, \dots, \tau_r) .$$

Mais detalhado, escreve-se também

$$(\mathbf{A}; \circ) = (\mathbf{aut}(M; \tau_1, \tau_2, \dots, \tau_r); \circ)$$

ou simplesmente

$$\mathbf{A} = \mathbf{aut}(M; \tau_1, \tau_2, \dots, \tau_r) .$$

O grupo \mathbf{A} dos automorfismos da estrutura $(M; \tau_1, \tau_2, \dots, \tau_r)$ consiste portanto das *permutações de M que são compatíveis* com todas as composições internas $\tau_1, \tau_2, \dots, \tau_r$ definidas em M .

II.3.12 Proposição.

Sejam

$$(M; \tau_1, \tau_2, \dots, \tau_r) \cong (N; \perp_1, \perp_2, \dots, \perp_r)$$

duas estruturas algébricas isomorfas. Então seus grupos de automorfismos

$$(\mathbf{aut}(M; \tau_1, \tau_2, \dots, \tau_r); \circ) \text{ e } (\mathbf{aut}(N; \perp_1, \perp_2, \dots, \perp_r); \circ) .$$

são isomorfos.

Demonstração: Seja $\varphi : M \longrightarrow N$ um isomorfismo de $(M; \tau_1, \tau_2, \dots, \tau_r)$ sobre $(N; \perp_1, \perp_2, \dots, \perp_r)$ e defina

$$\Omega : \mathbf{aut}(M; \tau_1, \tau_2, \dots, \tau_r) \longrightarrow \mathbf{aut}(N; \perp_1, \perp_2, \dots, \perp_r)$$

por

$$\Omega(\alpha) = \varphi \circ \alpha \circ \varphi^{-1} \quad \forall \alpha \in \mathbf{aut}(M; \tau_1, \tau_2, \dots, \tau_r) .$$

Afirmamos que Ω é um isomorfismo procurado entre os grupos

$$(\mathbf{aut}(M; \tau_1, \tau_2, \dots, \tau_r); \circ) \text{ e } (\mathbf{aut}(N; \perp_1, \perp_2, \dots, \perp_r); \circ) .$$

De fato temos $\Omega(\alpha) \in \mathbf{aut}(N; \perp_1, \perp_2, \dots, \perp_r) \quad \forall \alpha \in \mathbf{aut}(M; \top_1, \top_2, \dots, \top_r)$, pois $\Omega(\alpha)$ é composta dos isomorfismos

$$N \xrightarrow{\varphi^{-1}} M \xrightarrow{\alpha} M \xrightarrow{\varphi} N .$$

Isto significa

$$\Omega \in \mathbf{aut}(N; \perp_1, \perp_2, \dots, \perp_r)^{\mathbf{aut}(M; \top_1, \top_2, \dots, \top_r)} .$$

O fato que Ω é um isomorfismo entre os dois grupos de automorfismos, segue como em II.3.4

■

AS RELAÇÕES DE EQUIVALÊNCIA MODULO UM SUBGRUPO

II.3.13 Observação.

Seja G um grupo e H um subgrupo de G . Definindo-se para todos os $a, b \in G$ as relações ε_H e η_H por

$$a \varepsilon_H b \iff ab^{-1} \in H \quad e \quad a \eta_H b \iff a^{-1}b \in H ,$$

temos

a) $\varepsilon_H, \eta_H \in \mathbf{Eq}(G)$.

b₁) Para todo $g \in G$, a classe de equivalência de $g \pmod{\varepsilon_H}$ é o conjunto $Hg = \{xg \mid x \in H\} \subseteq G$ e o conjunto quociente de $G \pmod{\varepsilon_H}$ é

$$G/\varepsilon_H = \{Hg \mid g \in G\} .$$

b₂) Para todo $g \in G$, a classe de equivalência de $g \pmod{\eta_H}$ é o conjunto $gH = \{gx \mid x \in H\} \subseteq G$ e o conjunto quociente de $G \pmod{\eta_H}$ é

$$G/\eta_H = \{gH \mid g \in G\} .$$

Observamos que as classes de equivalência Hg de $G \pmod{\varepsilon_H}$ chamam-se as *classes laterais à direita* de $G \pmod{H}$, enquanto as gH de $G \pmod{\eta_H}$ chamam-se as *classes laterais à esquerda* de $G \pmod{H}$.

Demonstração: a) i) $a \varepsilon_H a \quad \forall a \in G$ segue pois $aa^{-1} = 1 \in H$.

ii) $a \varepsilon_H b$ significa $ab^{-1} \in H$. Segue $ba^{-1} = (ab^{-1})^{-1} \in H$ e daí $b \varepsilon_H a$.

iii) $a \varepsilon_H b$ e $b \varepsilon_H c$ significam $ab^{-1} \in H$ e $bc^{-1} \in H$.

Segue $ac^{-1} = (ab^{-1})(bc^{-1}) \in H$ e daí $a \varepsilon_H c$.

Logo $\varepsilon_H \in \mathbf{Eq}(G)$.

A demonstração para $\eta_H \in \mathbf{Eq}(G)$ é análoga.

b₁) Seja \bar{g} a classe de equivalência de $g \pmod{\varepsilon_H}$. A afirmação b₁) segue, pois

$$y \in \bar{g} \iff y \varepsilon_H g \iff yg^{-1} = x \in H \iff y = xg \in Hg.$$

A demonstração de b₂) é análoga. ■

Observamos que, em geral, estas duas relações de equivalência ε_H e η_H são distintas e não são relações de congruência.

II.3.14 Exemplo.

Seja $G = \mathbf{S}_3$ com $H = \{1, \tau_1\}$. Temos (ver a tabela de multiplicação em II.3.5)

$$\begin{aligned} G/\varepsilon_H &= \{Hg \mid g \in G\} = \{\{1, \tau_1\}, \{1, \tau_1\} \circ \tau_2, \{1, \tau_1\} \circ \tau_3\} = \\ &= \{\{1, \tau_1\}, \{\tau_2, \tau_1 \circ \tau_2\}, \{\tau_3, \tau_1 \circ \tau_3\}\} = \{\{1, \tau_1\}, \{\tau_2, \rho\}, \{\tau_3, \sigma\}\}, \end{aligned}$$

enquanto

$$\begin{aligned} G/\eta_H &= \{gH \mid g \in G\} = \{\{1, \tau_1\}, \tau_2 \circ \{1, \tau_1\}, \tau_3 \circ \{1, \tau_1\}\} = \\ &= \{\{1, \tau_1\}, \{\tau_2, \tau_2 \circ \tau_1\}, \{\tau_3, \tau_3 \circ \tau_1\}\} = \{\{1, \tau_1\}, \{\tau_2, \sigma\}, \{\tau_3, \rho\}\} \end{aligned}$$

Consequentemente

$$G/\varepsilon_H \neq G/\eta_H, \quad \text{i.e.} \quad \varepsilon_H \neq \eta_H.$$

Multiplicando-se por exemplo as duas ε_H -equivalências

$$\begin{cases} \rho & \varepsilon_H & \rho \\ \mathbf{1} & \varepsilon_H & \tau_1 \end{cases} \quad \text{obtemos} \quad \rho \circ \mathbf{1} = \rho \not\equiv_H \tau_3 = \rho \circ \tau_1.$$

Portanto, $\varepsilon_H \notin \mathbf{Cg}(\mathbf{S}_3; \circ)$.

Multiplicando-se as η_H -equivalências

$$\begin{cases} \mathbf{1} & \eta_H & \tau_1 \\ \rho & \eta_H & \rho \end{cases} \quad \text{obtemos} \quad \mathbf{1} \circ \rho = \rho \not\equiv_H \tau_2 = \tau_1 \circ \rho.$$

Portanto, também $\eta_H \notin \mathbf{Cg}(\mathbf{S}_3; \circ)$.

■

Vale a seguinte importante

II.3.15 Proposição.

Seja G um grupo, H um subgrupo, ε_H , e η_H as relações de equivalência introduzidas em II.3.13. Equivalentes são

a) $\varepsilon_H = \eta_H$

b) $Hg = gH \quad \forall g \in G$

Demonstração: "b) \implies a)": Se $Hg = gH \quad \forall g \in G$ temos também $G/\varepsilon_H = \{Hg \mid g \in G\} = \{gH \mid g \in G\} = G/\eta_H$ e daí $\varepsilon_H = \eta_H$.

"a) \implies b)": Suponhamos $\varepsilon_H = \eta_H$, i.e.

$$G/\varepsilon_H = \{Hg \mid g \in G\} = \{yH \mid y \in G\} = G/\eta_H.$$

Para todo $g \in G$ existe portanto $y \in G$ com $Hg = yH$.

De $g \in gH \cap Hg = gH \cap yH$ concluímos $yH = gH$ e daí $Hg = gH$.

■

AS RELAÇÕES DE CONGRUÊNCIA DE UM GRUPO E SUBGRUPOS NORMAIS

Para classificar (a menos de isomorfismo) as imagens homomórficas de um grupo $(G; \cdot)$, é preciso determinar ou descrever o conjunto $\mathbf{Cg}(G; \cdot)$ de suas relações de congruência.

Uma relação de congruência $\kappa \in \mathbf{Cg}(G; \cdot)$ do grupo G é um elemento

$$\kappa \in \mathbf{Eq}(G) \subseteq \mathbf{2}^{G \times G},$$

tal que $\forall a, a', b, b' \in G$:

$$\begin{cases} a \kappa a' \\ b \kappa b' \end{cases} \implies a \cdot b = a' \cdot b'.$$

Como podemos conseguir uma descrição de $\mathbf{Cg}(G; \cdot)$?

II.3.16 Definição.

Um subgrupo N de um grupo G é dito *normal em G* , indicado por $N \trianglelefteq G$, se

$$gN = Ng \quad \forall g \in G.$$

Por II.3.15, os subgrupos normais são portanto exatamente aqueles, para os quais

$$\varepsilon_N = \eta_N.$$

O conjunto dos subgrupos normais de um grupo G indicamos por $\mathfrak{N}(G)$. Escrever $N \in \mathfrak{N}(G)$ significa portanto o mesmo quanto $N \trianglelefteq G$.

Observamos que

$$\{1\}, G \in \mathfrak{N}(G) \subseteq \mathfrak{S}(G)$$

e portanto $\mathfrak{N}(G) \neq \emptyset$. Os subgrupos $\{1\}$ e G chamam-se os *subgrupos normais triviais* de G .

II.3.17 Observação.

Para um subgrupo H de um grupo G são equivalentes:

- a) $H \trianglelefteq G$.
- b) $g^{-1}Hg = H \quad \forall g \in G$, onde $g^{-1}Hg = \{g^{-1}xg \mid x \in H\}$.
- c) $g^{-1}xg \in H \quad \forall x \in H, \quad \forall g \in G$.

Demonstração: "a) \Rightarrow b)": $H \trianglelefteq G$ significa $Hg = gH \quad \forall g \in G$. Multiplicando-se pela esquerda por g^{-1} segue $g^{-1}Hg = g^{-1}gH = H$.

"b) \Rightarrow c)": $\forall x \in H, \quad g \in G$ temos $g^{-1}xg \in g^{-1}Hg$. Mas $g^{-1}Hg = H$ pela hipótese b). Logo, $g^{-1}xg \in H$.

"c) \Rightarrow a)": Suponha $g^{-1}xg \in H \quad \forall x \in H, \quad g \in G$.

i) Para todo $y \in Hg$ temos $y = xg$ com $x \in H$. Logo, $g^{-1}y = g^{-1}xg \in H$ e daí $y \in gH$. Portanto $Hg \subseteq gH$.

ii) Como a hipótese $g^{-1}xg \in H$ vale para todo $g \in G$, o mesmo vale também para g^{-1} ao invés de g . Vale portanto também

$$gxg^{-1} = (g^{-1})^{-1}xg^{-1} \in H \quad \forall x \in H, \quad g \in G.$$

Se agora $y \in gH$, temos $y = gx$ com $x \in H$. Segue $yg^{-1} = gxg^{-1} \in H$ e daí $y \in Hg$. Logo $gH \subseteq Hg$.

De i) e ii) concluímos $Hg = gH \quad \forall g \in G$, i.e. $H \trianglelefteq G$.

■

Os subgrupos normais de G dão origem a relações de congruência, como mostra a seguinte

II.3.18 Proposição.

Seja G um grupo, $N \trianglelefteq G$ e definamos para todos os $a, b \in G$:

$$a \kappa_N b \iff ab^{-1} \in N.$$

Então

- a) $\kappa_N \in \mathbf{Cg}(G; \cdot)$.
- b) Se $N_1, N_2 \trianglelefteq G$ com $N_1 \neq N_2$, então $\kappa_{N_1} \neq \kappa_{N_2}$.

Demonstração: Certamente $\kappa_N = \varepsilon_N = \eta_N \in \mathbf{Eq}(G)$.

Suponhamos $a, a', b, b' \in G$ são tais que $\begin{cases} a \kappa_N a' \\ b \kappa_N b' \end{cases}$. Isto significa

$aa'^{-1} \in N$ e $bb'^{-1} \in N$. Como N é subgrupo normal de G , concluímos $ay \in aN = Na$ e daí $aya^{-1} \in N$. Segue

$$(ab)(a'b')^{-1} = abb'^{-1}a'^{-1} = aya'^{-1} = ay(a^{-1}a)a'^{-1} = \underbrace{(aya^{-1})}_{\in N} \underbrace{(aa'^{-1})}_{\in N} \in N.$$

Portanto, $ab \kappa_N a'b'$ e vemos que $\kappa_N \in \mathbf{Cg}(G; \cdot)$.

Se $N_1 \neq N_2$, digamos $N_1 \not\subseteq N_2$, vamos ter algum $x \in N_1 \setminus N_2$. Para este x temos $x \kappa_{N_1} 1 \not\kappa_{N_2} x$. Portanto $\kappa_{N_1} \neq \kappa_{N_2}$.

■

Para todo grupo G temos então

$$\{\kappa_N \mid N \in \mathfrak{N}(G)\} \subseteq \mathbf{Cg}(G; \cdot).$$

Mas também ao contrário vale: Toda relação de congruência de $(G; \cdot)$ é induzida por um subgrupo normal de G da forma descrita em II.3.18:

II.3.19 Proposição.

Seja G um grupo, $\kappa \in \mathbf{Cg}(G; \cdot)$ uma relação de congruência. Então

- a) $N_\kappa = \{x \in G \mid x \kappa 1\}$ é um subgrupo normal de G .
 b) Para todos os $a, b \in G$ temos

$$a \kappa b \iff ab^{-1} \in N_\kappa.$$

Demonstração: a) Certamente $1 \kappa 1$ e portanto $1 \in N_\kappa$.

Se $x, y \in N_\kappa$, temos $\begin{cases} x \kappa 1 \\ y \kappa 1 \end{cases}$ e daí $xy \kappa 1 \cdot 1 = 1$. Logo, $xy \in N_\kappa$.

Também de $\begin{cases} x \kappa 1 \\ x^{-1} \kappa x^{-1} \end{cases}$ segue $1 = xx^{-1} \kappa 1 \cdot x^{-1} = x^{-1}$. Logo $x^{-1} \in N_\kappa$.

Portanto, N_κ é um subgrupo de G .

Para todo $x \in N_\kappa$ e $g \in G$ temos $\begin{cases} g^{-1} \kappa g^{-1} \\ x \kappa 1 \\ g \kappa g \end{cases}$ e daí $g^{-1}xg \kappa g^{-1} \cdot 1 \cdot g =$

$(g^{-1}g) \cdot 1 = 1$. Logo $g^{-1}xg \in N_\kappa$. Por II.3.17 isto significa $N_\kappa \trianglelefteq G$.

Além disso, $\forall a, b \in G$:

$$a \kappa b \iff ab^{-1} \kappa 1 \iff ab^{-1} \in N_\kappa.$$

■

Portanto, vale de fato

$$\{\kappa_N \mid N \in \mathfrak{N}(G)\} = \mathbf{Cg}(G; \cdot) \quad \text{e temos a}$$

II.3.20 Conseqüência.

Seja G um grupo. Entre o conjunto $\mathfrak{N}(G)$ dos subgrupos normais de G e o conjunto $\mathbf{Cg}(G; \cdot)$ das suas relações de congruência, existe uma correspondência biunívoca, estabelecida por

$$N \longrightarrow \kappa_N \quad \forall N \in \mathfrak{N}(G),$$

cuja inversa é

$$\kappa \longrightarrow N_\kappa \quad \forall \kappa \in \mathbf{Cg}(G; \cdot).$$

Particularmente, $\mathfrak{N}(G)$ e $\mathbf{Cg}(G; \cdot)$ são conjuntos equipotentes.

Além disso,

$$\{1\} \longrightarrow \kappa_{\{1\}} = \delta_G \quad \text{e} \quad G \longrightarrow \kappa_G = G \times G ,$$

i.e. nesta correspondência, o subgrupo normal $N = \{1\}$ corresponde à relação da igualdade, o subgrupo normal $N = G$ corresponde à relação universal em G .

■

II.3.21 Conseqüência.

Um grupo $(G; \cdot)$ é simples, se e somente se

$$G \neq \{1\} \quad \text{e} \quad \mathfrak{N}(G) = \{\{1\}, G\} .$$

■

GRUPOS QUOCIENTES E HOMOMORFISMOS DE GRUPOS

Se $N \trianglelefteq G$ e κ_N é a congruência associada ao N , é comum escrever o conjunto quociente $G/\kappa_N = \{Ng \mid g \in G\}$ como

$$G/N = G/\kappa_N .$$

$(G/N; \cdot)$ é a estrutura quociente com a multiplicação induzida (ver II.2.11).

II.3.22 Observação.

Seja $(G; \cdot)$ um grupo, $N \trianglelefteq G$ e

$$G/N = \{Ng \mid g \in G\}$$

o conjunto quociente de G mod N . Então

a) A multiplicação induzida em G/N é dada por

$$(Na)(Nb) = Nab \quad \forall Na, Nb \in G/N .$$

b) O epimorfismo canônico $\gamma \in (G/N)^G$ é a aplicação dada por

$$\gamma(g) = Ng \quad \forall g \in G .$$

c) A estrutura quociente $(G/N; \cdot)$ é de fato um grupo.

N , a classe de 1, é o elemento identidade de G/N .

Para todo $Na \in G/N$, seu inverso é $(Na)^{-1} = Na^{-1}$.

A estrutura $(G/N; \cdot)$ chama-se portanto o grupo quociente de $G \bmod N$.

Demonstração: Abreviamos $\bar{g} = Ng$,

a) Se $a, b \in G$, esta multiplicação indicada é

$$\bar{a} \cdot \bar{b} = (Na)(Nb) = N(ab) = \overline{ab}$$

i.e. é de fato a multiplicação (bem definida) das classes através da multiplicação dos representantes.

b) Lembrar que $\gamma(g) = \bar{g} = Ng \quad \forall g \in G$.

A associatividade da estrutura $G/N = \gamma(G)$ segue de II.2.30.

Como $\gamma(1) = N$, vemos por II.2.31 que N é a identidade de G/N .

Para todo $a \in G$ temos $(Na)^{-1} = (\gamma(a))^{-1} = \gamma(a^{-1}) = Na^{-1}$. Isto mostra que Na^{-1} é o inverso bilateral de Na .

■

II.3.23 Observação.

Sejam $(G; \cdot)$ e $(L; *)$ grupos e $\varphi \in L^G$ um homomorfismo.

Seja κ_φ a relação de congruência associada ao φ , i.e.

$$a \kappa_\varphi b \iff \varphi(a) = \varphi(b).$$

Então valem:

$$a) \quad N_{\kappa_\varphi} = \{x \in G \mid x \kappa_\varphi 1_G\} = \{x \in G \mid \varphi(x) = 1_L\} \trianglelefteq G.$$

$$b) \quad \forall a, b \in G: \quad a \kappa_\varphi b \iff \varphi(ab^{-1}) = 1_L \iff ab^{-1} \in N_{\kappa_\varphi}.$$

Este subgrupo normal N_{κ_φ} de G é usualmente indicado por

$$\text{Nuc } \varphi = \{x \in G \mid \varphi(x) = 1_L\}$$

e se chama o núcleo do homomorfismo φ .

Demonstração: a) Temos $\varphi(1_G) = 1_L$. Logo, $N_{\kappa_\varphi} = \{x \in G \mid x \kappa_\varphi 1_G\} = \{x \in G \mid \varphi(x) = \varphi(1_G)\} = \{x \in G \mid \varphi(x) = 1_L\}$.

$$b) \quad a \kappa_\varphi b \iff \varphi(a) = \varphi(b) \iff \varphi(a)\varphi(b^{-1}) = \varphi(b)\varphi(b^{-1}) \iff \\ \iff \varphi(ab^{-1}) = \varphi(bb^{-1}) = \varphi(1_G) = 1_L \iff ab^{-1} \in N_{\kappa_\varphi}.$$

■

II.3.24 Observação.

Se $(G; \cdot)$ e $(L; *)$ são grupos e $\varphi \in L^G$ um homomorfismo, então

- a) $\varphi(G)$ é um subgrupo de $(L; *)$.
- b) $\text{Nuc } \varphi \trianglelefteq G$.
- a) $\kappa_\varphi = \kappa_{\text{Nuc } \varphi}$

Demonstração: a) Certamente, $\varphi(G)$ é uma subestrutura de $(L; *)$. Mas para todo $\varphi(x) \in \varphi(G)$ temos $\varphi(x)^{-1} = \varphi(x^{-1}) \in \varphi(G)$. Logo $\varphi(G)$ é de fato um subgrupo de L .

b) e c) seguem de II.3.23.

O teorema geral do homomorfismo (ver II.2.24), reformulado para grupos, é agora assim:

II.3.25 Teorema. (teorema do homomorfismo para grupos)

Sejam $(G; \cdot)$ e $(L; *)$ dois grupos. Seja $\varphi \in L^G$ um homomorfismo de $(G; \cdot)$ em $(L; *)$. Seja $\text{Nuc } \varphi = \{x \in G \mid \varphi(x) = 1_L\}$ o núcleo do φ . Então valem:

- a) $\varphi(G) = \{\varphi(x) \mid x \in G\}$ é um subgrupo de $(L; *)$.
- b) $\text{Nuc } \varphi$ é um subgrupo normal de G .
- c) Existe um único isomorfismo ψ do grupo quociente $(G/\text{Nuc } \varphi; \cdot)$ sobre o subgrupo imagem $(\varphi(G); *)$, de tal maneira que $\varphi = \psi \circ \gamma$.

Particularmente,

$$(G/\text{Nuc } \varphi; \cdot) \cong (\varphi(G); *) .$$

O teorema do homomorfismo para grupos diz portanto:

O grupo quociente de um grupo mod um qualquer subgrupo normal, é uma imagem homomórfica do grupo original.

E reciprocamente vale: A imagem homomórfica de um grupo por um homomorfismo φ é um grupo, o qual pode ser reencontrado isomórficamente em forma de um grupo quociente, olhando o grupo original mod o subgrupo normal $\text{Nuc } \varphi$ associado ao homomorfismo

φ .

IMAGENS HOMOMÓRFICAS ABELIANAS DE GRUPOS

Um grupo G em geral não é comutativo. Queremos agora descobrir como deve ser o núcleo N de um homomorfismo φ , para que a imagem $\varphi(G) \cong G/N$ seja um grupo abeliano.

II.3.26 Observação.

Seja G um grupo e $N \trianglelefteq G$. As seguintes afirmações são equivalentes:

- O grupo quociente G/N é abeliano.
- Para todos os $a, b \in G$ temos $a^{-1}b^{-1}ab \in N$.

Demonstração: Temos G/N é abeliano $\iff (aN)(bN) = (bN)(aN)$
 $\forall aN, bN \in G/N \iff abN = baN \quad \forall a, b \in G \iff$
 $\iff a^{-1}b^{-1}abN = N \quad \forall a, b \in G \iff a^{-1}b^{-1}ab \in N \quad \forall a, b \in G.$

O elemento $a^{-1}b^{-1}ab$ chama-se o *comutador dos elementos* $a, b \in G$. ■

II.3.27 Definição.

Seja G um grupo. O subgrupo normal

$$G' = \bigcap_{\substack{N \trianglelefteq G \\ G/N \text{ abel}}} N,$$

a interseção de todos os (i.e. o menor dos) subgrupos normais de G com quociente abeliano chama-se o *derivada* de G .

Vemos por II.3.26 que a derivada G' é ao mesmo tempo o *menor subgrupo normal de G que contém todos os comutadores de G* .

Portanto, a caracterização das imagens homomórficas comutativas de grupos é:

Um grupo quociente G/N é abeliano, se e somente se $G' \leq N$.

OS GRUPOS CÍCLICOS

Uma aplicação importante do teorema do homomorfismo na teoria dos grupos é a classificação dos chamados *grupos cíclicos*.

II.3.28 Observação.

Seja $(G; \cdot)$ um grupo e $x \in G$ um elemento fixo. Então:

a) A aplicação $\varphi_x \in G^{\mathbb{Z}}$ definida por

$$\varphi_x(m) = x^m \quad \forall m \in \mathbb{Z},$$

é um homomorfismo do grupo $(\mathbb{Z}; +)$ em $(G; \cdot)$

b) A imagem de φ_x , indicada por

$$\langle x \rangle = \varphi_x(\mathbb{Z}) = \{x^m \mid m \in \mathbb{Z}\},$$

consistindo de todas as potências (positivas e negativas) deste x , é chamado o subgrupo cíclico de G gerado por x

c) Existe um único $n \in \mathbb{N}_0$, tal que o núcleo de φ_x é o subgrupo

$$\text{Nuc } \varphi_x = U_n = \{nk \mid k \in \mathbb{Z}\} = \{m \in \mathbb{Z} \mid x^m = 1\} \leq \mathbb{Z}$$

e vale o isomorfismo

$$\mathbb{Z}/U_n = \mathbb{Z}/\text{Nuc } \varphi_x \cong \varphi_x(\mathbb{Z}) = \langle x \rangle.$$

Particularmente, $|\langle x \rangle| = n$ se $n > 0$ e $|\langle x \rangle| = \infty$ se $n = 0$.

Demonstração: a) Para todos os $m_1, m_2 \in \mathbb{Z}$ temos

$$\varphi_x(m_1 + m_2) = x^{m_1+m_2} = x^{m_1}x^{m_2} = \varphi_x(m_1)\varphi_x(m_2).$$

b) é claro.

c) Temos $n = 0$ ou n é o menor dos números naturais m com $x^m = 1$ (comparar II.2.10).

■

II.3.29 Definição.

Seja $(G; \cdot)$ um grupo e $x \in G$ um dos seus elementos. Seja $n \in \mathbb{N}_0$ o único número tal que U_n é o núcleo do homomorfismo φ_x de II.3.28. Colocamos

$$\mathbf{o}(x) = \begin{cases} n & \text{se } n > 0 \\ \infty & \text{se } n = 0 \end{cases}$$

e chamamos $o(x)$ a *ordem* do elemento x .

II.3.30 Definição.

Um grupo G é chamado um grupo *cíclico*, se existe um elemento $x \in G$ tal que $G = \langle x \rangle$.

Se $G = \langle x \rangle$ é cíclico, isto significa então que o homomorfismo $\varphi_x : \mathbb{Z} \longrightarrow G$ de II.3.28 é um epimorfismo para este x , ou seja, G é uma imagem homomórfica de $(\mathbb{Z}; +)$. Portanto temos:

A menos de isomorfismo, *os grupos cíclicos são exatamente o grupo $(\mathbb{Z}; +)$ e suas imagens homomórficas.*

Também: *Quaisquer dois grupos cíclicos da mesma ordem n são isomorfos $(1 \leq n \leq \infty)$.*

II.3.31 Exemplo.

Seja $n \in \mathbb{N}$ e consideremos a matriz

$$x = \begin{pmatrix} \cos \frac{2\pi}{n} & \text{sen} \frac{2\pi}{n} \\ -\text{sen} \frac{2\pi}{n} & \cos \frac{2\pi}{n} \end{pmatrix}.$$

A matriz x descreve no plano Euclidiano uma rotação pelo ângulo $\frac{2\pi}{n}$. As fórmulas da trigonometria elementar mostram (realizar estas contas!) que temos para todos os $m \in \mathbb{Z}$:

$$\varphi_x(m) = x^m = \begin{pmatrix} \cos \frac{2\pi}{n} & \text{sen} \frac{2\pi}{n} \\ -\text{sen} \frac{2\pi}{n} & \cos \frac{2\pi}{n} \end{pmatrix}^m = \begin{pmatrix} \cos \frac{2\pi m}{n} & \text{sen} \frac{2\pi m}{n} \\ -\text{sen} \frac{2\pi m}{n} & \cos \frac{2\pi m}{n} \end{pmatrix}$$

e

$$\text{Nuc } \varphi_x = \left\{ m \in \mathbb{Z} \mid x^m = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\} = n\mathbb{Z}.$$

Portanto,

$$\left\langle \left(\begin{pmatrix} \cos \frac{2\pi}{n} & \text{sen} \frac{2\pi}{n} \\ -\text{sen} \frac{2\pi}{n} & \cos \frac{2\pi}{n} \end{pmatrix} \right) \right\rangle$$

é um grupo cíclico de ordem n . ■

§ II.4 Anéis e Corpos

ANÉIS E SUBANÉIS

As mais importantes estruturas algébricas com *duas composições* internas, são os chamados *anéis*:

II.4.1 Definição.

Uma estrutura algébrica com duas composições internas $(A; +, \cdot)$ é denominada um *anel*, se

- i) $(A; +)$ é um grupo comutativo.
- ii) $(A; \cdot)$ é um semigrupo.
- iii) Valem as leis distributivas

$$a(b + c) = ab + ac \quad \text{e} \quad (b + c)a = ba + ca \quad \forall a, b, c \in A.$$

II.4.2 Exemplos.

- a) $(\mathbb{Z}; +, \cdot)$ é um anel, o *anel dos números inteiros*.
- b) $(\mathbb{R}; +, \cdot)$ é o *anel dos números reais*.
- c) Seja $(A; +)$ um grupo comutativo aditivo.

Definindo-se uma *multiplicação trivial* em A por $ab = 0 \quad \forall a, b \in A$, temos que $(A; +, \cdot)$ é um anel.

Particularmente, se $(\{0\}; +)$ é um grupo com um só elemento, $(\{0\}; +, \cdot)$ é o *anel unitário com um só elemento*.

- d) Seja

$$A = \mathbf{M}_2(\mathbb{R}) = \left\{ \left(\begin{array}{cc} a_{11} & a_{12} \\ a_{21} & a_{22} \end{array} \right) \mid a_{11}, a_{12}, a_{21}, a_{22} \in \mathbb{R} \right\},$$

o conjunto das (2×2) -matrizes com entradas reais.

Definindo-se para todas as

$$\left(\begin{array}{cc} a_{11} & a_{12} \\ a_{21} & a_{22} \end{array} \right), \left(\begin{array}{cc} b_{11} & b_{12} \\ b_{21} & b_{22} \end{array} \right) \in A$$

a soma e o produto por

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} + \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11} + b_{11} & a_{12} + b_{12} \\ a_{21} + b_{21} & a_{22} + b_{22} \end{pmatrix},$$

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \cdot \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11}b_{11} + a_{12}b_{21} & a_{11}b_{12} + a_{12}b_{22} \\ a_{21}b_{11} + a_{22}b_{21} & a_{21}b_{12} + a_{22}b_{22} \end{pmatrix},$$

temos que $(\mathbf{M}_2(\mathbb{R}); +, \cdot)$ é um anel, o *anel das (2×2) -matrizes reais*.

e) Seja E um conjunto e considere $\mathfrak{A} = \mathbf{2}^E$, o conjunto de todas as partes de E . Definindo-se para todas as $X, Y \in \mathfrak{A}$:

$$X + Y = (X \cup Y) \setminus (X \cap Y) \quad \text{e} \quad X \cdot Y = X \cap Y,$$

temos que $(\mathfrak{A}; +, \cdot)$ é um anel, chamado o *anel de BOOLE sobre o conjunto E* .

(Provar estas asserções !)

■

Uma conseqüência das leis distributivas em anéis é:

II.4.3 Observação.

Seja $(A; +, \cdot)$ um anel. Então

$$0 \cdot x = x \cdot 0 = 0 \quad \text{para qualquer elemento } x \in A.$$

Demonstração: Temos $0 + 0 = 0$. Segue $x(0 + 0) = x \cdot 0$ e daí pela lei distributiva: $x \cdot 0 + x \cdot 0 = x \cdot 0$. Somando-se $-(x \cdot 0)$ a ambos os lados, obtemos $(x \cdot 0 + x \cdot 0) + (-(x \cdot 0)) = x \cdot 0 + (-(x \cdot 0))$. Portanto também $x \cdot 0 + (x \cdot 0 + (-(x \cdot 0))) = x \cdot 0 + (-(x \cdot 0))$. Mas $x \cdot 0 + (-(x \cdot 0)) = 0$, o que mostra $x \cdot 0 = x \cdot 0 + 0 = 0$.

$0 \cdot x = 0$ é mostrado da mesma forma, empregando-se a outra lei distributiva.

II.4.4 Definição.

Um subconjunto S de um anel $(A; +, \cdot)$ é dito um *subanel de A* , se

- i) S é um subgrupo de $(A; +)$.
- ii) S é um subsemigrupo de $(A; \cdot)$.

Isto significa portanto que $S \neq \emptyset$ e vale $a - b \in S$ e $ab \in S$ para todos os $a, b \in S$.

II.4.5 Exemplos.

- a) Para todos os $n \in \mathbb{N}_0$, os subgrupos $U_n = \{nk \mid k \in \mathbb{Z}\}$ de $(\mathbb{Z}; +)$ são de fato subanéis de $(\mathbb{Z}; +, \cdot)$.
- b) \mathbb{Z} é um subanel de $(\mathbb{R}; +, \cdot)$.
- c) O subgrupo $\frac{1}{2}\mathbb{Z} = \{\frac{1}{2}k \mid k \in \mathbb{Z}\} = \{0, \pm\frac{1}{2}, \pm 1, \pm\frac{3}{2}, \pm 2, \dots\}$ de $(\mathbb{R}; +)$ não é um subanel de $(\mathbb{R}; +, \cdot)$.
- d) Para qualquer anel $(A; +, \cdot)$ temos os *subanéis triviais* $\{0\}$ e A .

(Detalhar !)

■

HOMOMORFISMOS E RELAÇÕES DE CONGRUÊNCIA NUM ANEL - IDEAIS

Um homomorfismo φ de um anel $(A; +, \cdot)$ para uma estrutura algébrica $(L; +, \cdot)$ é uma aplicação $\varphi \in L^A$ tal que, para todos os $a, b \in A$:

$$\varphi(a + b) = \varphi(a) + \varphi(b) \quad \text{e} \quad \varphi(ab) = \varphi(a)\varphi(b).$$

II.4.6 Observação.

Seja φ um homomorfismo do anel $(A; +, \cdot)$ para a estrutura algébrica $(L; +, \cdot)$.
Então

a subestrutura $(\varphi(A); +, \cdot)$ de $(L; +, \cdot)$ é um anel.

(Não estamos supondo que $(L; +, \cdot)$ é um anel !)

Demonstração: Certamente, $\varphi(A)$ é uma subestrutura de $(L; +, \cdot)$. Mas $\varphi(A)$ é de fato um *subgrupo comutativo* de $(L; +)$ e um *sub-semigrupo* de $(L; \cdot)$ (ver II.2.30/31).

Também valem as leis ditributivas em $\varphi(A)$: Para todos os $x, y, z \in \varphi(A)$, existem $a, b, c \in A$ com $\varphi(a) = x$, $\varphi(b) = y$, $\varphi(c) = z$. Segue

$$\begin{aligned} x(y+z) &= \varphi(a) (\varphi(b) + \varphi(c)) = \varphi(a)\varphi(b+c) = \varphi(a(b+c)) = \\ &= \varphi(ab+ac) = \varphi(ab) + \varphi(ac) = \varphi(a)\varphi(b) + \varphi(a)\varphi(c) = xy + xz. \end{aligned}$$

A lei $(y+z)x = yx + zx$ é análoga. Logo a subestrutura $\varphi(A)$ de L é de fato um *anel*. ■

Uma relação de congruência do anel A , i.e. uma $\kappa \in \mathbf{Cg}(A; +, \cdot)$, é um elemento

$$\kappa \in \mathbf{Eq}(A) \subseteq \mathbf{2}^{A \times A},$$

tal que $\forall a, a', b, b' \in A$:

$$\begin{cases} a \kappa a' \\ b \kappa b' \end{cases} \implies a+b \kappa a'+b' \quad \text{e} \quad a \cdot b \kappa a' \cdot b'.$$

Se κ é uma relação de congruência do anel $(A; +, \cdot)$ e γ é o epimorfismo canónico de A sobre A/κ , vemos por II.4.6 que a estrutura quociente $(A/\kappa; +, \cdot)$ é de fato um anel.

$(A/\kappa; +, \cdot)$ chama-se o *anel quociente de A mod κ* .

Para classificar (a menos de isomorfismos) os anéis que são as imagens homomórficas de um anel $(A; +, \cdot)$, é preciso determinar ou descrever o conjunto $\mathbf{Cg}(A; +, \cdot)$ de suas relações de congruência (ver II.2.24/25).

Se $(A; +, \cdot)$ é um anel e S é um subanel de A , podemos claramente considerar a relação de equivalência κ_S definida por $a \kappa_S b \iff a - b \in S$. Esta relação é compatível com a adição, pois todo subgrupo S do grupo comutativo $(A; +)$ é normal nele (ver II.3.18). Logo

$$\kappa_S \in \mathbf{Cg}(A; +).$$

Além disso, sabemos que toda relação de congruência de $(A; +)$ é assim obtida. Problemas vamos ter em geral quanto à compatibilidade de κ_S com a multiplicação:

Considerando-se em $(\mathbb{R}; +, \cdot)$ o subanel \mathbb{Z} dos números inteiros e a relação

$$a \kappa_{\mathbb{Z}} b \iff a - b \in \mathbb{Z} \quad (a, b \in \mathbb{R}),$$

temos

$$\left\{ \begin{array}{l} \frac{1}{2} \kappa_{\mathbb{Z}} \frac{3}{2} \\ \frac{1}{4} \kappa_{\mathbb{Z}} \frac{5}{4} \end{array} \right., \quad \text{mas } \frac{1}{8} = \frac{1}{2} \cdot \frac{1}{4} \notin_{\mathbb{Z}} \frac{3}{2} \cdot \frac{5}{4} = \frac{15}{8}.$$

Qual a propriedade adicional que um subanel S deve ter para que a relação κ_S seja também *multiplicativamente compatível*?

II.4.7 Definição.

Um subconjunto I de um anel A é denominado um *ideal de A* , indicado por $I \trianglelefteq A$ (i.e. usamos a mesma notação usada para indicar subgrupos normais em grupos), se

- 1) I é um subgrupo do grupo aditivo $(A; +)$, i.e. $I \neq \emptyset$ e $x - y \in I$ para todos os $x, y \in I$.
- 2) $ax \in I$ e $xa \in I \quad \forall x \in I; \quad \forall a \in A$,
i.e. I não é apenas multiplicativamente fechado: I contém um produto ax ou xa sempre se (pelo menos) um fator está em I .

Por $\mathfrak{I}(A)$ indicamos *o conjunto de todos os ideais de A* .

Escrever $I \in \mathfrak{I}(A)$ significa o mesmo quanto $I \trianglelefteq A$.

Os *ideais* de um anel são portanto uma categoria especial de subanéis - da mesma forma que os *subgrupos normais* de um grupo são uma categoria especial de subgrupos.

II.4.8 Exemplos.

- a) Para qualquer anel A temos $\{0\}$, $A \in \mathfrak{I}(A)$, i. e. os subgrupos aditivos triviais $\{0\}$ e A são ideais de A , os chamados *ideais triviais*.
- b) Seja $(A; +, \cdot) = (\mathbb{Z}; +, \cdot)$ e $n \in \mathbb{N}_0$.
Para os subanéis $U_n = \{nk \mid k \in \mathbb{Z}\}$ de $(\mathbb{Z}; +, \cdot)$ temos de fato

$$U_n \in \mathfrak{I}(\mathbb{Z}).$$

c) O subanel \mathbb{Z} de $(\mathbb{R}; +, \cdot)$ não é um ideal de \mathbb{R} .

(Confirmar estas asserções !)

■

Parecido aos subgrupos normais em grupos, os ideais são responsáveis pelas relações de congruência de um anel:

II.4.9 Proposição.

Seja $(A; +, \cdot)$ um anel e $I \trianglelefteq A$. Definindo-se para todos os $a, b \in A$:

$$a \kappa_I b \iff a - b \in I, \text{ temos}$$

a) $\kappa_I \in \mathbf{Cg}(A; +, \cdot)$.

b) Se $I_1, I_2 \trianglelefteq A$ com $I_1 \neq I_2$, então $\kappa_{I_1} \neq \kappa_{I_2}$.

Demonstração: Já sabemos $\kappa_I \in \mathbf{Cg}(A; +)$. Também sabemos que $\kappa_{I_1} \neq \kappa_{I_2}$ se $I_1 \neq I_2$. (ver II.3.18)

Suponhamos $a, a', b, b' \in A$ são tais que $\begin{cases} a \kappa_I a' \\ b \kappa_I b' \end{cases}$. Isto significa

$$a - a' \in I \quad \text{e} \quad b - b' \in I.$$

Como I é um ideal de A , temos

$$a(b - b') \in I \quad \text{e} \quad (a - a')b' \in I.$$

Segue

$$ab - a'b' = a(b - b') + (a - a')b' \in I \quad \text{e portanto} \quad ab \kappa_I a'b'.$$

Vemos que $\kappa_I \in \mathbf{Cg}(A; +, \cdot)$.

■

Também ao contrário vale: Toda relação de congruência de A é induzida por um ideal de A :

II.4.10 Proposição.

Seja $(A; +, \cdot)$ um anel, $\kappa \in \mathbf{Cg}(A; +, \cdot)$ uma relação de congruência. Então

a) $I_\kappa = \{x \in A \mid x \kappa 0\}$ é um ideal de A .

b) Para todos os $a, b \in A$ temos

$$a \kappa b \iff a - b \in I_\kappa .$$

Demonstração: a) Sabemos que I_κ é um subgrupo do grupo aditivo $(A; +)$.

Se $x \in I_\kappa$ e $a \in A$, temos $\begin{cases} x \kappa 0 \\ a \kappa a \end{cases}$ e segue $xa \kappa 0 \cdot a = 0 = a \cdot 0 \kappa ax$. Logo,

$xa, ax \in I_\kappa$. Isto significa $I_\kappa \trianglelefteq A$.

Além disso, $\forall a, b \in A$:

$$a \kappa b \iff a - b \kappa 0 \iff a - b \in I_\kappa .$$

■

Portanto temos a

II.4.11 Conseqüência.

Seja A um anel. Entre o conjunto $\mathfrak{I}(A)$ dos ideais de A e o conjunto $\mathbf{Cg}(A; +, \cdot)$ das suas relações de congruência, existe uma correspondência biunívoca, estabelecida por

$$I \longrightarrow \kappa_I \quad \forall I \in \mathfrak{I}(A) ,$$

cujas inversa é

$$\kappa \longrightarrow I_\kappa \quad \forall \kappa \in \mathbf{Cg}(A; +, \cdot) .$$

Particularmente, $\mathfrak{I}(A)$ e $\mathbf{Cg}(A; +, \cdot)$ são conjuntos equipotentes.

Além disso,

$$\{0\} \longrightarrow \kappa_{\{0\}} = \delta_A \quad \text{e} \quad A \longrightarrow \kappa_A = A \times A ,$$

i.e. nesta correspondência, o ideal $I = \{0\}$ corresponde à relação da igualdade, o ideal $I = A$ corresponde à relação universal em A .

II.4.12 Conseqüência.

Um anel $(A; +, \cdot)$ é simples, se e somente se

$$A \neq \{0\} \quad \text{e} \quad \mathfrak{I}(A) = \{\{0\}, A\} .$$

■

II.4.13 Observação.

Seja $(A; +, \cdot)$ um anel, $I \trianglelefteq A$ e κ_I é a congruência associada ao I .

a) A classe de equivalência \bar{a} do elemento $a \in A \pmod{\kappa_I}$ é

$$\bar{a} = a + I = \{a + x \mid x \in I\} .$$

b) O anel quociente A/κ_I é

$$A/\kappa_I = \{a+I \mid a \in A\} .$$

Escreve-se também $A/I = A/\kappa_I$.

Demonstração: a) $x \in \bar{a} \iff x \kappa_I a \iff x - a \in I \iff x \in a + I$.

b) também é claro. ■

II.4.14 Observação.

Seja $(A; +, \cdot)$ um anel, $I \trianglelefteq A$ e

$$A/I = \{a+I \mid a \in A\}$$

o anel quociente de $A \pmod{I}$. Então

a) A adição e multiplicação induzidas em A/I são dadas por

$$\begin{aligned} (a+I) + (b+I) &= (a+b) + I \\ (a+I) \cdot (b+I) &= ab + I \end{aligned} \quad \forall a+I, b+I \in A/I .$$

I , a classe de 0 , é o elemento nulo de A/I .

Para todo $a+I \in A/I$ seu negativo é $-(a+I) = (-a)+I$.

b) O epimorfismo canónico $\gamma \in (A/I)^A$ é a aplicação dada por

$$\gamma(a) = a+I \quad \forall a \in A .$$

Demonstração: Abreviamos $\bar{a} = a+I$,

a) Se $a, b \in A$, a adição e multiplicação indicadas são

$$\bar{a} + \bar{b} = (a+I) + (b+I) = (a+b) + I = \overline{a+b} ,$$

$$\bar{a} \cdot \bar{b} = (a+I) \cdot (b+I) = ab + I = \overline{ab}$$

i.e. são de fato as composições das classes através das composições dos representantes.

As demais afirmações também são imediatas.

b) Lembrar que $\gamma(a) = \bar{a} = a+I \quad \forall a \in A$.

■

II.4.15 Observação.

Sejam $(A; +, \cdot)$ e $(L; +, \cdot)$ anéis e $\varphi \in L^A$ um homomorfismo. Seja κ_φ a relação de congruência associada ao φ , i.e.

$$a \kappa_\varphi b \iff \varphi(a) = \varphi(b).$$

Então valem:

a) O ideal I_{κ_φ} é

$$I_{\kappa_\varphi} = \{x \in A \mid x \kappa_\varphi 0_A\} = \{x \in A \mid \varphi(x) = 0_L\}.$$

b) $\forall a, b \in A$:

$$a \kappa_\varphi b \iff \varphi(a - b) = 0_L \iff a - b \in I_{\kappa_\varphi}.$$

Este ideal I_{κ_φ} de A é usualmente indicado por

$$\text{Nuc } \varphi = \{x \in A \mid \varphi(x) = 0_L\}$$

e se chama o *núcleo do homomorfismo* φ

Demonstração: a) Temos $\varphi(0_A) = 0_L$. Logo, $I_{\kappa_\varphi} = \{x \in A \mid x \kappa_\varphi 0_A\} = \{x \in A \mid \varphi(x) = \varphi(0_A)\} = \{x \in A \mid \varphi(x) = 0_L\}$.

b) $a \kappa_\varphi b \iff \varphi(a) = \varphi(b) \iff \varphi(a) + \varphi(-b) = \varphi(b) + \varphi(-b) \iff \iff \varphi(a - b) = \varphi(b - b) = \varphi(0_A) = 0_L \iff a - b \in I_{\kappa_\varphi}$.

■

II.4.16 Conseqüência.

Se $(A; +, \cdot)$ e $(L; +, \cdot)$ são anéis e $\varphi \in L^A$ um homomorfismo, então

- a) $\varphi(A)$ é um subanel de $(L; +, \cdot)$.
- b) $\text{Nuc } \varphi \trianglelefteq A$.
- c) $\kappa_\varphi = \kappa_{\text{Nuc } \varphi}$

Demonstração: a) Ver II.4.6.

b) e c) seguem de II.4.15. ■

O teorema geral do homomorfismo (ver II.2.24), reformulado para anéis é agora assim:

II.4.17 Teorema. (teorema do homomorfismo para anéis)

Sejam $(A; +, \cdot)$ e $(L; +, \cdot)$ dois anéis. Seja $\varphi \in L^A$ um homomorfismo de $(A; +, \cdot)$ em $(L; +, \cdot)$. Então valem:

- a) A imagem $\varphi(A) = \{\varphi(x) \mid x \in A\}$ é um subanel de $(L; +, \cdot)$.
- b) O núcleo $\text{Nuc } \varphi = \{x \in A \mid \varphi(x) = 0_L\}$ é um ideal de A .
- c) Existe um único isomorfismo ψ do anel quociente $(A/\text{Nuc } \varphi; +, \cdot)$ sobre o subanel imagem $(\varphi(A); +, \cdot)$, de tal maneira que $\varphi = \psi \circ \gamma$.
Particularmente,

$$(A/\text{Nuc } \varphi; +, \cdot) \cong (\varphi(A); +, \cdot).$$

O teorema do homomorfismo para anéis diz então:

O anel quociente de um anel mod um qualquer ideal, é uma imagem homomórfica do anel original.

Reciprocamente vale: A imagem homomórfica de um anel por um homomorfismo φ é um anel, o qual pode ser reencontrado isomórficamente em forma de um anel quociente, olhando o anel original mod o ideal $\text{Nuc } \varphi$ associado ao homomorfismo φ .

II.4.18 Definição.

Um anel $(A; +, \cdot)$ chama-se

- a) um *anel com identidade* se existe um elemento $1 \in A$ tal que

$$1 \cdot a = a \cdot 1 = a \text{ para todo } a \in A.$$

Isto significa portanto que o semigrupo $(A; \cdot)$ é um monóide.

- b) *anel comutativo*, se $ab = ba$ para todos os $a, b \in A$. Isto significa que o semigrupo $(A; \cdot)$ é comutativo.
- c) *anel comutativo com identidade* se A tem as propriedades de a) e b) simultaneamente. Isto significa portanto que $(A; \cdot)$ é um monóide comutativo.
- d) um *domínio de integridade*, se A é um anel comutativo com identidade, tal que $\mathbf{R}(A; \cdot) = A \setminus \{0\}$. Isto significa que, se $0 \neq a \in A$ e $x, x' \in A$ então temos a lei do cancelamento

$$ax = ax' \implies x = x'.$$

- e) um *corpo*, se A é um anel comutativo com identidade $1 \neq 0$, tal que $\mathbf{U}(A; \cdot) = A \setminus \{0\}$. Isto significa portanto que se $0 \neq a \in A$,

$$\text{então existe } x \in A \text{ com } ax = 1.$$

II.4.19 Exemplos.

- a) $(\mathbb{Z}; +, \cdot)$, o anel dos números inteiros é um domínio de integridade porém não é um corpo.
- b) $(\mathbb{R}; +, \cdot)$, o anel dos números reais, é um corpo.
- c) O anel $(2\mathbb{Z}; +, \cdot)$ dos números inteiros pares é um anel comutativo sem elemento identidade.
- d) Seja $(A; +)$ um grupo comutativo aditivo.

O anel $(A; +, \cdot)$ com a multiplicação trivial ($ab = 0 \quad \forall a, b \in A$), é um anel comutativo. Ele não possui uma identidade se $|A| \geq 2$.

O anel trivial $A = \{0\}$, cujo único elemento é tanto o elemento nulo quanto a sua identidade, no nosso entendimento é um domínio de integridade.

e) O anel

$$A = \mathbf{M}_2(\mathbb{R})$$

das (2×2) -matrizes com entradas reais, é um anel não-comutativo com o elemento identidade $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

f) O anel de BOOLE $(\mathfrak{A}; +, \cdot)$ sobre o conjunto E ($\mathfrak{A} = 2^E$ é o conjunto de todas as partes de E), é um anel comutativo cuja identidade é a parte $E \in \mathfrak{A}$ (a parte vazia $\emptyset \in \mathfrak{A}$ é o elemento nulo!). Ele não é um domínio de integridade se $|E| \geq 2$ (i.e. se $|\mathfrak{A}| \geq 4$ [ver II.4.22 b])). Para $E = \emptyset$ temos que $\mathfrak{A} = \{\emptyset\}$ é um anel trivial com um só elemento. Para $E = \{b\}$ um conjunto unitário, temos que $\mathfrak{A} = \{\emptyset, E\}$ é um corpo com 2 elementos.

(Provar estas asserções !)

■

Pelos nossos conhecimentos podemos afirmar:

II.4.20 Observação.

- Todo corpo $(C; +, \cdot)$ é um domínio de integridade*
- Todo domínio de integridade $(A; +, \cdot)$ é um anel comutativo com identidade*
- Um anel comutativo com identidade A é um domínio de integridade, se e somente se $\forall a, b \in A$:*

$$ab = 0 \implies a = 0 \text{ ou } b = 0.$$

Demonstração: a) Observe $\mathbf{U}(C; \cdot) \subseteq \mathbf{R}(C; \cdot)$.

b) Vale por definição.

c) Se $\mathbf{R}(A; \cdot) = A \setminus \{0\}$ e tendo em vista que $\mathbf{R}(A)$ é multiplicativamente fechado, concluímos $ab \neq 0$ sempre se $a \neq 0 \neq b$.

Reciprocamente, se $\mathbf{R}(A) \subsetneq A \setminus \{0\}$, vai existir $0 \neq a \in A$ que não é regular. Portanto existem $x, x' \in A$ com $x \neq x'$ mas $ax = ax'$. Considerando-se $b = x - x' \neq 0$, obtemos $ab = a(x - x') = ax - ax' = 0$.

■

Um produto de dois elementos num anel é 0, sempre se um dos fatores é 0 (ver II.4.3).

Vemos que esta conclusão, porém, nem sempre é reversível, i.e.

um produto ab num anel *pode* ser 0 com ambos os fatores $a, b \neq 0$.

Isto justifica a

II.4.21 Definição.

Um elemento a de um anel comutativo $A \neq \{0\}$ chama-se um *divisor de zero*, se existe um $0 \neq b \in A$ tal que $ab = 0$.

Observamos que $a = 0$ sempre é um divisor de zero (trivial) (por II.4.3).

Por II.4.20 c), os domínios de integridade $A \neq \{0\}$ portanto, não possuem divisores de zero não-triviais.

II.4.22 Exemplos.

a) No anel quociente $A = \mathbb{Z}/(6) = (\{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}; +, \cdot)$ temos

$$\bar{2} \cdot \bar{3} = \bar{0} \quad \text{e} \quad \bar{2} \neq \bar{0} \neq \bar{3}.$$

Portanto, $\bar{2}$ e $\bar{3}$ são dois divisores de zero não-triviais.

b) Seja E um conjunto com $|E| \geq 2$ e $\mathfrak{A} = \mathbf{2}^E$. Seja $A \subseteq E$ com $\emptyset \neq A \neq E$ e $B = \text{Cpt}_E(A)$. Temos

$$\emptyset \neq A, B \in \mathfrak{A} \text{ com } AB = A \cap B = \emptyset.$$

Portanto, A e B são dois divisores de zero não-triviais do anel de BOOLE $(\mathfrak{A}; +, \cap)$ (observe que \emptyset é o elemento nulo de \mathfrak{A} !).

■

IDEAIS PRINCIPAIS EM ANÉIS COMUTATIVOS COM IDENTIDADE

II.4.23 Observação.

Seja $(A; +, \cdot)$ um anel comutativo com elemento identidade 1 e seja $a \in A$ um qualquer elemento. Então

$$aA = \{ax \mid x \in A\}$$

i.e. o conjunto de todos os múltiplos de a , forma um ideal de A . Vale $a \in aA$ e aA é o menor ideal de A que contém a .

Este ideal aA , às vezes também denotado por I_a ou (a) , é denominado
o ideal principal de A gerado por a .

Demonstração: Certamente, $a = a \cdot 1 \in aA \neq \emptyset$. Se $x, y \in aA$ são dois quaisquer elementos, existem $x_1, y_1 \in A$ com $x = ax_1$ e $y = ay_1$. Segue $x - y = ax_1 - ay_1 = a(x_1 - y_1) \in aA$, mostrando que aA é um subgrupo aditivo de A . Se ainda $c \in A$, segue $xc = cx = (ax_1)c = a(x_1c) \in aA$. Portanto, aA de fato é um ideal de A .

Como qualquer ideal de A que contém a também deve conter todos os múltiplos ax , vemos que aA é de fato o menor ideal de A contendo a .

II.4.24 Exemplos.

a) Seja $(A; +, \cdot) = (\mathbb{Z}; +, \cdot)$

$$(6) = I_6 = 6\mathbb{Z} = \{6x \mid x \in \mathbb{Z}\}$$

é o ideal principal de \mathbb{Z} gerado por 6. Observamos

$$(6) = (-6).$$

b) Seja E um conjunto, $\mathfrak{A} = 2^E$ e seja $(\mathfrak{A}; +, \cdot)$ o anel de BOOLE sobre E , as composições de \mathfrak{A} sendo

$$X + Y = (X \cup Y) \setminus (X \cap Y), \quad X \cdot Y = X \cap Y \quad \forall X, Y \in \mathfrak{A}.$$

O ideal principal de \mathfrak{A} gerado por $A \in \mathfrak{A}$, é

$$\begin{aligned} A\mathfrak{A} = (A) &= \{AX \mid X \in \mathfrak{A}\} = \{A \cap X \mid X \in \mathfrak{A}\} = \\ &= \{Y \mid Y \subseteq A\} = 2^A \trianglelefteq 2^E. \end{aligned}$$

■

Em qualquer anel (comutativo com elemento identidade) temos

$$\{(a) \mid a \in A\} \subseteq \mathfrak{I}(A),$$

isto significa que *os ideais principais formam uma subfamília do conjunto de todos os ideais de A* . Observamos que, além dos ideais principais *podem* existir outros ideais num anel A :

II.4.25 Exemplo.

No anel de BOOLE

$$\mathfrak{A} = 2^{\mathbb{N}}$$

sobre os números naturais (ou sobre qualquer conjunto infinito) temos que

$$\mathfrak{F} = \{ X \mid |X| < \infty \},$$

a família dos subconjuntos finitos de \mathbb{N} , forma um ideal (demonstração?).

\mathfrak{F} não pode ser um ideal principal de $(2^{\mathbb{N}}; +, \cdot)$:

Para qualquer $F \in \mathfrak{F}$ e $X \in \mathfrak{A}$ temos $|FX| = |F \cap X| \leq |F|$.

Como \mathfrak{F} contém subconjuntos de tamanho finito arbitrário, isto significa que $(F) = F\mathfrak{A} = 2^F \subsetneq \mathfrak{F}$, qualquer que seja o elemento $F \in \mathfrak{F}$ e não podemos ter $\mathfrak{F} = (F)$. Por exemplo: $F \cup \{j\} \in \mathfrak{F} \setminus (F)$ se $j \in \mathbb{N} \setminus F$.

■

Portanto: Só excepcionalmente vamos ter

$$\{(a) \mid a \in A\} = \mathfrak{I}(A).$$

A seguinte definição destaca entre os domínios de integridade aqueles nos quais os ideais principais exaurem o conjunto de todos os ideais.

II.4.26 Definição.

Um anel $(A; +, \cdot)$ é chamado um *domínio de ideais principais*, se

- i) A é um domínio de integridade.
- ii) Todo ideal de A é um ideal principal.

II.4.27 Exemplo.

O anel $(\mathbb{Z}; +, \cdot)$ dos números inteiros é um domínio de ideais principais.

Demonstração: Seja dado um ideal J de \mathbb{Z} . Por II.2.10 sabemos: A relação de congruência κ_J de \mathbb{Z} definida pelo J , é da forma $\kappa_J = \equiv_n$ onde

$$\begin{cases} n = 0 & \text{se } J = \{0\} \\ n = \text{o menor número natural contido em } J & \text{se } J \neq \{0\}. \end{cases}$$

Portanto, $J = (n)$ é um ideal principal e vemos

$$\{(a) \mid a \in \mathbb{Z}\} = \mathfrak{I}(\mathbb{Z}).$$

■

ANÉIS SIMPLES E CORPOS

A propriedade da simplicidade (i.e. $A \neq \{0\}$ e $\mathfrak{I}(A) = \{\{0\}, A\}$) tem uma caracterização transparente, se A é um anel comutativo com elemento identidade. Esta queremos mencionar:

II.4.28 Proposição.

Seja $(A; +, \cdot)$ um anel comutativo com elemento identidade 1.

Equivalentes são:

- $(A; +, \cdot)$ é simples
- $(A; +, \cdot)$ é um corpo

Demonstração: "a) \Rightarrow b)": Seja $(A; +, \cdot)$ simples. Isto significa $\mathfrak{I}(A) = \{\{0\}, A\}$ com $A \neq \{0\}$. Seja dado $0 \neq a \in A$ e considere o ideal principal

$$(a) = aA = \{ax \mid x \in A\}.$$

Temos $\{0\} \neq aA \in \mathfrak{I}(A)$. Portanto, $aA = A$, devido à simplicidade de A . Particularmente, $1 \in aA$, i.e. existe $x_0 \in A$ com $ax_0 = 1$. Mas isto significa que $a \in \mathbf{U}(A; \cdot)$. Logo $\mathbf{U}(A; \cdot) = A \setminus \{0\}$ e vemos que A é um corpo.

"b) \Rightarrow a)": Seja $(A; +, \cdot)$ um corpo e seja dado um ideal $\{0\} \neq I \in \mathfrak{I}(A)$. É preciso mostrar que $I = A$. Para isto peguemos um $0 \neq a \in I$. Como A é um corpo, temos $a \in \mathbf{U}(A; \cdot)$. Logo, existe $x_0 \in A$ com $1 = ax_0 \in I$. Para todo $y \in A$ concluímos agora $y = y \cdot 1 \in I$. Isto significa $I = A$ e daí $\mathfrak{I}(A) = \{\{0\}, A\}$. Vemos a simplicidade de A .

■

IDEAIS PRIMOS E IDEAIS MAXIMAIS

Ideais com propriedades específicas conduzem a anéis quocientes específicos. Vejamos alguns exemplos no caso de anéis comutativos com elemento identidade.

Lembremos que qualquer ideal contém um produto ab de elementos de A desde que *ele contenha pelo menos um dos fatores a ou b* . Esta conclusão nem sempre é reversível: O produto de dois elementos ab *pode* estar num ideal com ambos os fatores fora do ideal. A seguinte definição trata dos ideais para os quais isto *não* ocorre:

II.4.29 Definição.

Seja A um anel comutativo com identidade. Um ideal P é denominado *um ideal primo*,

se para todos os $a, b \in A$ pudermos concluir:

$$ab \in P \implies a \in P \text{ ou } b \in P,$$

i.e. P contém um produto ab *somente se* ele contém um dos fatores.

II.4.30 Exemplos.

- Seja p um número primo. Então o ideal principal $P = (p)$ de $(\mathbb{Z}; +, \cdot)$ é um ideal primo.
- O ideal $I = (6)$ de \mathbb{Z} não é um ideal primo.
- Em qualquer anel comutativo com identidade temos que o ideal trivial

$$P = A \text{ é um ideal primo.}$$

O ideal trivial $I = \{0\}$ é primo, se e somente se A é um domínio de integridade.

Demonstração: a) Se $a, b \in \mathbb{Z}$ são tais que $ab \in P$, isto significa que ab é múltiplo de p . Como um primo não pode ser multiplicativamente distribuído para dois fatores, concluímos que p tem que dividir um dos fatores a ou b (ou ambos). Mas então $a \in (p) = P$ ou $b \in (p) = P$. Vemos que (p) é um ideal primo.

b) Pois temos $2 \cdot 3 = 6 \in I$, porém $2 \notin I$ e também $3 \notin I$. Logo (6) não é um

ideal primo.

c) A primeira afirmação é evidente.

De $ab \in \{0\}$ podemos concluir $a \in \{0\}$ ou $b \in \{0\}$, se e somente se $ab = 0$ implica em $a = 0$ ou $b = 0$. Mas isto caracteriza os domínios de integridade entre os anéis comutativos com identidade.

■

Os ideais primos podem ser assim caracterizados:

II.4.31 Proposição.

Seja $(A; +, \cdot)$ um anel comutativo com identidade e $J \in \mathfrak{I}(A)$.

Equivalentes são:

- a) J é um ideal primo.
- b) O anel quociente A/J é um domínio de integridade.
- c) O conjunto complementar $A \setminus J$ é multiplicativamente fechado.

Demonstração: "a) \iff c)": J é um ideal primo \iff

$$\iff (\forall a, b \in A : ab \in J \Rightarrow a \in J \text{ ou } b \in J)$$

$$\iff (\forall a, b \in A : a \notin J \text{ e } b \notin J \Rightarrow ab \notin J)$$

$$\iff (\forall a, b \in A : a, b \in A \setminus J \Rightarrow ab \in A \setminus J).$$

"a) \Rightarrow b)": Seja J é um ideal primo de A e sejam

$$a+J, b+J \in A/J \text{ tais que } (a+J)(b+J) = J$$

(lembrar que J é o elemento nulo de A/J !). Isto significa $ab+J = J$, ou seja, $ab \in J$. Por J ser ideal primo, concluímos $a \in J$ ou $b \in J$. Mas isto quer dizer $a+J = J$ ou $b+J = J$.

Logo o único divisor de zero de A/J é J , o elemento nulo de A/J .

"b) \Rightarrow a)": Suponhamos A/J é um domínio de integridade e sejam $a, b \in A$ com $ab \in J$. Temos portanto $(a+J)(b+J) = ab+J = J$. Por A/J ser domínio de integridade, concluímos $a+J = J$ ou $b+J = J$. Mas então $a \in J$ ou $b \in J$. Vemos que J é um ideal primo de A .

■

Já que os ideais primos são exatamente aqueles cujos anéis quocientes são domínios de integridade, uma pergunta justificada é:

Como são os ideais cujos quocientes são corpos?

Como todo corpo é um domínio de integridade, estes ideais deverão ser *ideais primos específicos*.

II.4.32 Definição.

Seja $(A; +, \cdot)$ um anel comutativo com elemento identidade. Um ideal $M \trianglelefteq A$ é denominado um *ideal maximal de A*, se

- i) $M \neq A$.
- ii) Se $X \trianglelefteq A$ com $M \leq X \neq A$, então $X = M$,
i.e. que entre M e A não existe propriamente nenhum ideal de A .
(Equivalentemente: Se $M < X \trianglelefteq A$, então $X = A$.)

II.4.33 Proposição.

Seja $(A; +, \cdot)$ um anel comutativo com identidade e $J \trianglelefteq A$. Então são equivalentes:

- a) $(A/J; +, \cdot)$ é um corpo.
- b) J é um ideal maximal de A .

Demonstração: Certamente,

A/J é um anel comutativo cujo elemento identidade é $1+J$

(a classe $0+J = J$ é seu elemento nulo).

Por II.4.28, a afirmação da proposição pode ser substituída por:

A/J é um anel simples, se e somente se J é um ideal maximal em A .

"a) \Rightarrow b)": Seja A/J um anel simples. Particularmente temos $|A/J| \geq 2$ e portanto, $J \subsetneq A$.

Suponha, $J \leq X \trianglelefteq A$ e $X \neq A$. Segue que

$$X/J = \{x+J \mid x \in X\}$$

é um ideal de A/J com $\{J\} = J/J \leq X/J \neq A/J$ (detalhar!). Pela simplicidade de A/J concluímos portanto $X/J = \{J\}$ e daí $X = J$. Isto mostra que J é um ideal maximal de A .

"b) \Rightarrow a)": Suponha J é um ideal maximal em A . Isto significa $J \neq A$ e para todo ideal Y com $J \leq Y \trianglelefteq A$ temos $Y = J$ ou $Y = A$. Devemos mostrar que A/J é um corpo:

Certamente, temos $|A/J| \geq 2$. Seja dado um $J \neq a+J \in A/J$. Devemos mostrar que $a+J$ é multiplicativamente inversível, ou seja, devemos encontrar $x_0+J \in A/J$ com

$$(a+J)(x_0+J) = 1+J.$$

Consideremos $Y = J + (a) = \{j + ax \mid j \in J, x \in A\}$ e provemos que $J < Y \trianglelefteq A$: Fazendo $x = 0$, vemos $J \subseteq Y$. Para $x = 1$ e $j = 0$ vemos $a \in Y \setminus J$. Logo, $J \subsetneq Y$. Provemos agora que Y é um ideal de A :

Temos $Y \neq \emptyset$. Sejam $y_1, y_2 \in Y$. Existem $j_1, j_2 \in J, x_1, x_2 \in A$ com $y_1 = j_1 + ax_1$ e $y_2 = j_2 + ax_2$. Segue $y_1 - y_2 = (j_1 - j_2) + a(x_1 - x_2) \in Y$. Se ainda $b \in A$, temos $by_1 = y_1b = j_1b + a(x_1b) \in J + (a) = Y$. Portanto, Y é um ideal de A e vemos $J < Y \trianglelefteq A$.

Pela maximalidade de J concluímos $Y = A$. Segue $1 \in Y$ e vão existir $j_0 \in J, x_0 \in A$ com $1 = j_0 + ax_0$. Segue $1 + J = j_0 + ax_0 + J = ax_0 + J = (a + J)(x_0 + J)$. Logo, $a + J$ é inversível e vemos que A/J é um corpo.

■

II.4.34 Conseqüência.

Todo ideal maximal de um anel comutativo com identidade, é um ideal primo.

II.4.35 Conseqüência.

Seja $(\mathbb{Z}; +, \cdot)$ o anel dos números inteiros e $n \in \mathbb{N}_0$. Então são equivalentes:

- $(\mathbb{Z}/(n); +, \cdot)$ é um corpo.
- $n=p$ é um número primo.

Demonstração: "a) \Rightarrow b)": Seja $\mathbb{Z}/(n)$ um corpo. Por II.4.33 sabemos que (n) tem que ser um ideal maximal de \mathbb{Z} . Como \mathbb{Z} não é um corpo, vemos que $\{0\} \neq (n) \neq \mathbb{Z}$, i.e. $n \geq 2$. Seja n é decomposto como $n = rs$ com $1 \leq r, s \leq n$. Temos $(n) \subseteq (r) \trianglelefteq \mathbb{Z}$ e vemos que devemos ter $(r) = (n)$ ou

$(r) = \mathbb{Z}$. Isto significa $r = n$ ou $r = 1$. Logo, não existe decomposição própria para n : $n=p$ tem que ser primo.

"b) \Rightarrow a)": Suponha $n=p$ é primo. Então $(p) \subsetneq \mathbb{Z}$. Suponha $(p) \leq X \triangleleft \mathbb{Z}$ com $X \neq \mathbb{Z}$. Sabemos que todo ideal de \mathbb{Z} é um ideal principal (ver II.4.27). Portanto existe $\pm 1 \neq a \in \mathbb{Z}$ com $X = a\mathbb{Z} = (a)$. Como $(a) = (-a)$, temos $X = (|a|)$. Como $(p) \subseteq X$, vemos que p é múltiplo de $|a| > 1$. Segue $|a| = p$ e daí $X = (p)$, mostrando a maximalidade do ideal (p) . Por II.4.33 concluímos que $\mathbb{Z}/(p)$ é um corpo. ■

II.4.36 Exemplos.

a) No anel quociente $\mathbb{Z}/(10)$ temos

$$\mathbf{U}(\mathbb{Z}/(10)) = \{\bar{1}, \bar{3}, \bar{7}, \bar{9}\},$$

sendo que $\bar{1} \cdot \bar{1} = \bar{9} \cdot \bar{9} = \bar{7} \cdot \bar{3} = \bar{1}$. Entretanto, as equações

$$\bar{2}\bar{x} = \bar{1}, \quad \bar{4}\bar{x} = \bar{1}, \quad \bar{6}\bar{x} = \bar{1}, \quad \bar{8}\bar{x} = \bar{1}, \quad \bar{5}\bar{x} = \bar{1}$$

não possuem soluções $\bar{x} \in \mathbb{Z}/(10)$.

b) Para o corpo $\mathbb{Z}/(11)$, as 10 equações $\bar{a}\bar{x} = \bar{1}$ com $\bar{0} \neq \bar{a} \in \mathbb{Z}/(11)$, com suas soluções são

$$\begin{array}{ll} \bar{1}\bar{x} = \bar{1} & \longleftarrow \bar{x} = \bar{1} \\ \bar{2}\bar{x} = \bar{1} & \longleftarrow \bar{x} = \bar{6} \\ \bar{3}\bar{x} = \bar{1} & \longleftarrow \bar{x} = \bar{4} \\ \bar{4}\bar{x} = \bar{1} & \longleftarrow \bar{x} = \bar{3} \\ \bar{5}\bar{x} = \bar{1} & \longleftarrow \bar{x} = \bar{9} \\ \bar{6}\bar{x} = \bar{1} & \longleftarrow \bar{x} = \bar{2} \\ \bar{7}\bar{x} = \bar{1} & \longleftarrow \bar{x} = \bar{8} \\ \bar{8}\bar{x} = \bar{1} & \longleftarrow \bar{x} = \bar{7} \\ \bar{9}\bar{x} = \bar{1} & \longleftarrow \bar{x} = \bar{5} \\ \bar{10}\bar{x} = \bar{1} & \longleftarrow \bar{x} = \bar{10} \end{array}$$

ELEMENTOS IDEMPOTENTES

Num domínio de integridade, se um elemento x satisfaz $x^2 = x$, podemos concluir $x(x-1) = 0$ e então $x = 0$ ou $x = 1$. Se existem divisores de zero, tal conclusão não é possível. Num anel de BOOLE $(\mathbf{2}^E; +, \cap)$ por exemplo (E é um conjunto), temos $X^2 = X \cap X = X$ para qualquer $X \in \mathbf{2}^E$. Elementos $x \neq 1$ com $x^2 = x$ são divisores de zero especiais e merecem destaque:

II.4.37 Definição.

Um elemento e de um anel $(A; +, \cdot)$ chama-se um *idempotente de A* , se

$$e^2 = e.$$

Elementos idempotentes *triviais* em qualquer anel são 0 e o elemento identidade 1 (se tiver). Como já explicado, num domínio de integridade, não existem outros além destes.

II.4.38 Exemplo.

- Os elementos idempotentes de $\mathbb{Z}/6\mathbb{Z}$ são $\{\bar{0}, \bar{1}, \bar{3}, \bar{4}\}$.
- Num anel de BOOLE, todo elemento é idempotente.
- O anel $\mathbb{Z}/8\mathbb{Z}$, apesar de possuir os divisores de zero não-triviais, $\bar{2}$, $\bar{4}$ e $\bar{6}$, não possui elementos idempotentes além dos $\{\bar{0}, \bar{1}\}$.

Elementos idempotentes sempre aparecem em pares:

II.4.39 Observação.

Seja $(A; +, \cdot)$ um anel comutativo com elemento identidade 1 e seja $e \in A$ um elemento idempotente. Então:

- Também $1-e$ é idempotente, vale $e(1-e) = 0$ e $1-(1-e) = e$.
- Se $e \in A \setminus \{1, 0\}$, então e e $1-e$ são dois divisores de zero não-triviais.

Observação: Um par de elementos $\{e, 1-e\}$ onde e é idempotente, chama-se um par de *idempotentes ortogonais*.

Demonstração: a) $(1-e)^2 = 1 - 2e + e^2 = 1 - 2e + e = 1 - e$.

Temos $e(1-e) = e - e^2 = e - e = 0$. $1 - (1-e) = e$ é claro.

b) Segue, pois $e(1-e) = 0$ e $e \neq 0, 1$.

II.4.40 Exemplos.

- Os pares de elementos idempotentes do anel $A = (\mathbb{Z}/(10); +, \cdot)$ são

$$\{\bar{0}, \bar{1}\} \quad \text{e} \quad \{\bar{5}, \bar{1}-\bar{5}\} = \{\bar{5}, \bar{6}\}.$$

b) Os pares de elementos idempotentes do anel $A = (\mathbb{Z}/(100); +, \cdot)$ são

$$\{\bar{0}, \bar{1}\} \quad \text{e} \quad \{\bar{25}, \bar{1}-\bar{25}\} = \{\bar{25}, \bar{76}\} .$$

c) Os pares de elementos idempotentes do anel $A = (\mathbb{Z}/(105); +, \cdot)$ são

$$\{\bar{0}, \bar{1}\}, \quad \{\bar{70}, \bar{1}-\bar{70}\} = \{\bar{70}, \bar{36}\} , \\ \{\bar{21}, \bar{1}-\bar{21}\} = \{\bar{21}, \bar{85}\} \quad \text{e} \quad \{\bar{15}, \bar{1}-\bar{15}\} = \{\bar{15}, \bar{91}\} .$$

■

II.4.41 Proposição.

Seja $(A; +, \cdot)$ um anel comutativo com identidade 1 e I um ideal de A .
Equivalentes são:

- O anel I possui uma identidade e .
- Existe um ideal J de A tal que

$$A = I + J \quad \text{e} \quad I \cap J = \{0\} .$$

Demonstração: "a) \Rightarrow b)": Suponhamos, e é uma identidade de I . Consideremos o ideal principal $J = (1-e)A$. Para $x \in I \cap J$ temos

$$x = (1-e)a \quad \text{para algum } a \in A \quad \text{e daí } x = ex = e(1-e)a = 0 \cdot a = 0 .$$

Logo, $I \cap J = \{0\}$.

Temos $1 = e + (1-e)$ e para todo $y \in A$:

$$y = 1 \cdot y = ey + (1-e)y \quad \text{com } ey \in I; \quad (1-e)y \in J .$$

Portanto, $A = I + J$.

"b) \Rightarrow a)": Suponhamos a existência de $J \trianglelefteq A$ com $I + J = A$ e $I \cap J = \{0\}$. Existem $e \in I$ e $f \in J$ com $1 = e + f$. Para todo $x \in A$ temos

$$x = 1 \cdot x = ex + fx .$$

Para todo $x \in I$ temos $fx \in I \cap J = \{0\}$. Portanto $fx = 0$ e $ex = x$. Vemos que e é a identidade de I .

■

II.4.42 Exemplo.

Seja E um conjunto, $\mathfrak{A} = 2^E$ e considere o anel de BOOLE $(\mathfrak{A}; +, \cdot)$. Seja $A \in \mathfrak{A}$ e considere o ideal principal

$$\mathfrak{I} = A\mathfrak{A} = 2^A \trianglelefteq \mathfrak{A}.$$

O elemento identidade de \mathfrak{I} é A , o de \mathfrak{A} é E . Temos

$$E - A = E + A = (E \cup A) \setminus (E \cap A) = E \setminus A.$$

Portanto, para $\mathfrak{J} = (E \setminus A)\mathfrak{A} = 2^{E \setminus A} \trianglelefteq \mathfrak{A}$ temos

$$\mathfrak{I} + \mathfrak{J} = \mathfrak{A} \text{ e } \mathfrak{I} \cap \mathfrak{J} = \{\emptyset\}.$$

■

Com isto queremos encerrar nosso curso de

Álgebra I

Tomara que tenham gostado e que esta apostila sirva para algo além do necessário.