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

CAPÍTULO II

Estruturas Algébricas

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

$$\mathfrak{A} \Longrightarrow \mathfrak{B}$$

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

ou seja, sempre quando $\mathfrak{A}$ fôr 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

$$\mathfrak{B} \Longleftarrow \mathfrak{A} \quad \text{ou também} \quad \begin{array}{c}\mathfrak{A}\\ \Downarrow \\ \mathfrak{B}\end{array} \quad \text{ou} \quad \begin{array}{c}\mathfrak{B}\\ \Uparrow \\ \mathfrak{A}\end{array}$$

significam o mesmo quanto $\mathfrak{A} \Longrightarrow \mathfrak{B}$. 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

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

pois sempre se n é múltiplo de 4, concluimos 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

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

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

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

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 simultâneamente

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

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

Por exemplo:

Seja $\mathfrak{A}$ a asserção: "*n é múltiplo de 6*",
$\mathfrak{B}$ 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:

$\mathfrak{A}$: "*Q é um quadrado*"
$\mathfrak{B}$: "*Q é um losângo que é um retângulo*".

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

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

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

$$\bar{\mathfrak{A}} \Longleftarrow \bar{\mathfrak{B}}.$$

Em outras palavras: Se $\mathfrak{A}$ é suficiente para $\mathfrak{B}$, então $\bar{\mathfrak{B}}$ é suficiente para $\bar{\mathfrak{A}}$.
Ou também: Se $\mathfrak{A}$ é suficiente para $\mathfrak{B}$, então $\bar{\mathfrak{A}}$ é necessário para $\bar{\mathfrak{B}}$.
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 condicões 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:

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

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

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

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

$$A = \{\, n \mid n \text{ é um número natural} \,\} \quad \text{ou}$$

$$A = \{\, x \mid x \text{ é um número real tal que } \cos x = 0 \,\} \ .$$

$A = \{\, a \mid \ldots \}$ 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:

$$A = B \ \text{ significa: } \ \text{Para todo objeto } x \text{ temos: } \quad x \in A \iff x \in B\ .$$

$$\text{Assim,} \qquad A = B$$

$$\Updownarrow$$

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

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:

$$I\!\!N = \{1, 2, 3, \ldots\} = \textit{ o conjunto dos números naturais},$$

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

$$I\!\!N_0 = \{0, 1, 2, 3, \ldots\} = \textit{ o conjunto dos números inteiros não-negativos}.$$

Como fonte de exemplos admitiremos também sem mais explicações :

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

$$\mathbb{Q} = \left\{ \tfrac{m}{n} \;\middle|\; m \in \mathbb{Z},\ n \in \mathbb{N} \right\} = \textit{ o conjunto dos números racionais }.$$

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

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

são conjuntos finitos. Suas ordens são

$$\big|\{\nabla, \spadesuit, \heartsuit, \clubsuit\}\big| = 4, \quad \big|\{1,2,3,1,3,1,3\,,\ldots,\ 3,1,\ldots\}\big| = \big|\{1,2,3\}\big| = 3 \text{ e}$$
$$\big|\{x \in \mathbb{Z} \mid x^2 = 36\}\big| = \big|\{6,-6\}\big| = 2\,.$$

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

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

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 fôr elemento de B, ou seja, se para todo elemento a, a implicação

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

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

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

I.0.8 Observação.

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

a) *Sempre* $A \subseteq A$ (lei da reflexividade)

b) *Se* $A \subseteq B$ *e* $B \subseteq A$, *então* $A = B$ (lei da anti-simetria)

c) *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: $A \underset{\neq}{\subseteq} B$ ou $B \underset{\neq}{\supseteq} A$, 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

$$A = \left\{ n \in \mathbb{N} \;\middle|\; 2 \text{ divide } n \right\} = \left\{ 2, 4, 6, 8, \ldots \right\}$$

é o conjunto dos números naturais pares e

$$B = \left\{ n \in \mathbb{N} \;\middle|\; 3 \text{ divide } n \right\} = \left\{ 3, 6, 9, 12, \ldots \right\}$$

é o conjunto dos números naturais divisíveis por 3, temos

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

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 necessáriamente significa* $B \subset A$, como mostra nosso exemplo.

Diferença e complementar

I.0.9 Definição.

Dado dois conjuntos A e B, indicamos por

$$A \setminus B = \{\, a \in A \;\big|\; a \notin B \,\}$$

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

$$A \setminus B \ \text{ é denominado a } \textit{diferença } A \textit{ menos } B.$$

Mencionamos que $A \setminus B \subseteq A$ e $B \setminus A \subseteq B$.
Por exemplo, se $A = \{2, 4, 6, 8, \ldots\}$ e $B = \{3, 6, 9, 12, \ldots\}$, temos

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

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

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

Claramente temos

$$Cpt_E\big(Cpt_E(A)\big) = A\,.$$

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

$$Cpt_E(E) = \{\, a \in E \;\big|\; a \notin E \,\}$$

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

∎

REUNIÃO E INTERSEÇÃO

I.0.11 Definição.

Dado dois conjuntos, entendemos por

$$A \cup B = \left\{ x \;\middle|\; x \in A \quad \text{ou} \quad x \in B \right\}\ ,$$

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

$$A \cap B = \left\{ x \;\middle|\; x \in A \quad \text{e} \quad x \in B \right\}\ ,$$

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

$$A \cup B = \left\{ n \in I\!N \;\middle|\; n \text{ é par ou divisível por } 3 \right\}\ ,$$

$$A \cap B = \left\{ n \in I\!N \;\middle|\; n \text{ é divisível por } 6 \right\}\ .$$

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

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

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

As seguintes propriedades são fácilmente 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 $A_1, A_2, \ldots, A_n$ são n conjuntos dados, então

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

é o conjunto dos elementos x que pertencem a *pelo menos um* dos $A_1, A_2, \ldots, A_n$, enquanto

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

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

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

I.0.15 Proposição.

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

$$Cpt_E\Big(\bigcup_{k=1}^{n} A_k\Big) = \bigcap_{k=1}^{n} Cpt_E(A_k) \;\; e$$

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

Demonstração: Para todo $x \in E$ temos

$$x \in Cpt_E\left(\bigcup_{k=1}^{n} A_k\right) \iff x \notin \bigcup_{k=1}^{n} A_k \iff x \notin A_k \quad \forall\, k \iff$$

$$\iff x \in Cpt_E(A_k) \quad \forall\, k \iff x \in \bigcap_{k=1}^{n} Cpt_E(A_k)\ .$$

Da mesma forma

$$x \in Cpt_E\left(\bigcap_{k=1}^{n} A_k\right) \iff x \notin \bigcap_{k=1}^{n} A_k \iff \exists\, k \text{ com } x \notin A_k \iff$$

$$\exists\, k \text{ com } x \in Cpt_E(A_k) \iff x \in \bigcup_{k=1}^{n} Cpt_E(A_k)\ .$$

∎

Também famílias arbitrárias (possívelmente infintas) 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 $\mathfrak{F} = \{A_1, A_2\ , \ldots ,\ A_n\}$ é uma família finita, voltamos ao caso anterior.
Dado um conjunto infinito E (por exemplo $E = I\!N$).

$$\mathfrak{F} = \left\{ X \;\middle|\; X \text{ é um subconjunto finito de } E \right\}$$

é um *exemplo de uma família infinita.*

As regras de DE MORGAN podem ser formuladas agora assim:

$$Cpt_E\left(\bigcup_{X\in\mathfrak{F}} X\right) = \bigcap_{X\in\mathfrak{F}} Cpt_E(X)$$

e

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

∎

A *adição* $+$ em $I\!N$ e também em $Z\!\!\!Z$, a qual queremos admitir sem mais explicações, dá origem a uma *ordem natural* " $\le$ " em $Z\!\!\!Z$:
$\forall\, n, m \in Z\!\!\!Z$ temos

$$m \le n \quad \Longleftrightarrow \quad \text{a equação } \; m + x = n \; \text{ possui uma solução } \; x \in I\!N_0 \; .$$

A seguinte propriedade do conjunto $I\!N$ é fundamental:

O princípio da indução.

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

$$\forall\, S, \;\text{ com }\; \emptyset \neq S \subseteq I\!N \quad \exists\, m \in S \;\text{ tal que }\; m \le n \quad \forall\, n \in S.$$

Deste princípio segue a importante

I.0.16 Proposição.

Seja T um conjunto de alguns *números naturais* $($*i.e.* $T \subseteq I\!N)$ *satisfazendo às propriedades*:

a) $1 \in T$

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

Então $T = I\!N$ *é o conjunto de* todos *os números naturais.*

Demonstração: Suponhamos $T \neq I\!N$. Então vale $S \neq \emptyset$ quando $S = Cpt_{I\!N}(T) \subseteq I\!N$ é o conjunto complementar de T em $I\!N$. Pelo princípio da indução existe $m \in S$ tal que $m \le n$ para todos os $n \in S$. Como $1 \in T$ pela propriedade a), temos $1 \notin S$, particularmente $m > 1$. Daí concluimos $n = m{-}1 \in T$. 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 $T = I\!N$.

$\blacksquare$

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*

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

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

Demonstração: Seja $T=\left\{n\in I\!N \;\middle|\; \sum\limits_{k=1}^{n}(2k-1)=n^2\right\}$ o conjunto dos números naturais para os quais a fórmula $(*)$ é verdadeira (o "conjunto verdade" ou o "conjunto de validade" de $(*)$). Para mostrar que $T=I\!N$, 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,

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

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

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

de onde segue

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

Isto por sua vez significa $n+1\in T$. Pela proposição concluimos que o conjunto verdade da fórmula $(*)$ é o conjunto $T=I\!N$ 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*

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

Particularmente (quando $a=2$) obtemos

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

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

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

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

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

de onde segue

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

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

■

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

I.0.19 Proposição.

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

a) $n_0 \in T'$

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

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

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

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

Observamos que para este T temos $T \subseteq I\!N$ 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

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

O conjunto das partes

I.0.20 Definição.

Para qualquer conjunto A, indicamos por

$$\mathfrak{A} \;= \mathbf{2}^A = \left\{ X \;\middle|\; X \subseteq A \right\}$$

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.

a) Para $A = \emptyset$ temos $\mathbf{2}^{\emptyset} = \left\{ \emptyset \right\}$

b) Para $A = \left\{ a \right\}$ temos $\mathbf{2}^{\{a\}} = \left\{ \emptyset, \{a\} \right\}$.

c) Para $A = \left\{ a, b \right\}$ temos $\mathbf{2}^{\{a,b\}} = \left\{ \emptyset, \{a\}, \{b\}, \{a,b\} \right\}$.

d) Para $A = I\!R$ temos $\mathbf{2}^{I\!R} = \left\{ X \;\middle|\; X \subseteq I\!R \right\}$. Por exemplo $\mathbb{Q} \in \mathbf{2}^{I\!R}$.

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

$$\left| \mathbf{2}^A \right| = 2^{|A|} \,.$$

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

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

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

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

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

$$\left|\mathbf{2}^{A^*}\right| = 2^{|A^*|} = 2^n .$$

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

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

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

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

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

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

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

■

Dado um conjunto $A = \{1, 2, 3, \ldots, n\}$ 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

$$\mathfrak{C}_{n,k} = \left\{ X \;\middle|\; X \subseteq A;\ |X| = k \right\} \subseteq \mathfrak{A} = \mathbf{2}^A .$$

Assim, a questão é

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

Vamos abreviar, por enquanto, $c_{n,k} = \left|\mathfrak{C}_{n,k}\right| = \left|\left\{ X \;\middle|\; X \subseteq A;\ |X| = k \right\}\right|$.
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 $\{1\}, \{2\}\ , \ldots, \ \{i\}, \ldots \{n\}$. 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, acrescendo-se j ao i e uma segunda vez, acrescendo-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 $k = 0, 1, 2\ , \ldots, \ n-1$ que

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

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

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

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

Convém lembrar aqui que, se $k \in I\!N_0$, entende-se por $k!$ o produto

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

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 $n \in I\!N$ e todos os $k \in I\!N_0$ 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)):

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

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

Particularmente, isto explica que

Os coeficientes binomiais são números inteiros.

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

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

concluimos

$$\left|\mathbf{2}^A\right| = \left|\mathfrak{C}_{n,0}\right| + \left|\mathfrak{C}_{n,1}\right| + \left|\mathfrak{C}_{n,2}\right| + \ldots + \left|\mathfrak{C}_{n,n-1}\right| + \left|\mathfrak{C}_{n,n}\right| \ .$$

Portanto, vale a

I.0.24 Conseqüência.

Para todo $n \in I\!N$ temos

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

∎

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 $n \in I\!N$ *e todos os* $k \in I\!N_0$ *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:
$$\binom{n}{0} = \binom{n}{n} = 1, \ \ \binom{n}{1} = \binom{n}{n-1} = n, \ \ \binom{n}{2} = \binom{n}{n-2} = \frac{n(n-1)}{2} \ .$$

Podemos enunciar e provar agora o fundamental

teorema do desenvolvimento binomial:

I.0.26 Teorema.
Para todo $n \in I\!N$ *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:

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

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 $(a+b)^1 = \sum\limits_{k=0}^{1} \binom{1}{k}a^{1-k}b^k = \binom{1}{0}a^{1-0}b^0 + \binom{1}{1}a^{1-1}b^1$, sendo igual a $a+b$ de ambos os lados, i.e. $1 \in T$.

Suponhamos então que para algum $n \in I\!N$ já esteja provado

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

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):

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

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

$$= a^{n+1} + b^{n+1} + \sum_{k=1}^{n} \binom{n}{k}a^{n-k+1}b^k + \sum_{k=1}^{n} \binom{n}{k-1}a^{n-k+1}b^k =$$

$$= a^{n+1} + b^{n+1} + \sum_{k=1}^{n} \left[\binom{n}{k} + \binom{n}{k-1}\right] a^{n+1-k}b^k = a^{n+1} + b^{n+1} + \sum_{k=1}^{n} \binom{n+1}{k}a^{n-k+1}b^k =$$

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

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 $n \in I\!N$.

∎

O triângulo de **Pascal**

(Blaise Pascal [1623-1662], Filósofo e Matemático francês).

É usual, escrever-se os coeficientes binomiais $\binom{n}{k}$ (acrescentando-se ainda $\binom{0}{0} = 1$), ordenados no chamado *Triângulo de* Pascal, cuja n-ésima linha fornece então os coeficientes no desenvolvimento de $(a+b)^n$ para $n = 0, 1, 2, 3, \ldots$.

$$
\begin{array}{c}
\binom{0}{0} \\[4pt]
\binom{1}{0} \quad \binom{1}{1} \\[4pt]
\binom{2}{0} \quad \binom{2}{1} \quad \binom{2}{2} \\[4pt]
\binom{3}{0} \quad \binom{3}{1} \quad \binom{3}{2} \quad \binom{3}{3} \\[4pt]
\ldots\ldots\ldots\ldots\ldots \\[4pt]
\binom{n}{0} \; \binom{n}{1} \; \ldots \; \binom{n}{k-1} \; \binom{n}{k} \; \ldots \; \binom{n}{n-1} \; \binom{n}{n} \\[4pt]
\binom{n+1}{0} \; \binom{n+1}{1} \quad \ldots \quad \binom{n+1}{k} \quad \ldots \quad \binom{n+1}{n} \; \binom{n+1}{n+1} \\[4pt]
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots
\end{array}
$$

Vemos ainda a visualização da fórmula I.0.25 c), a qual nos diz como o termo $\binom{n+1}{k}$ da $(n+1)$-ésima linha no triângulo de Pascal é obtido como soma dos termos vizinhos $\binom{n}{k-1}$ e $\binom{n}{k}$ da linha anterior.

§ 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

$$M = A_1 \times A_2 \times \dots \times A_m =$$
$$= \left\{ (a_1, a_2, \dots, a_m) \;\middle|\; a_1 \in A_1,\ a_2 \in A_2, \dots, a_m \in A_m \right\}$$

chama-se o *produto* CARTES*iano* 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 $(a_1, a_2, \dots, a_m)$ $(1 \le i \le m)$.

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

$$M = A \times B = \left\{ (a, b) \;\middle|\; a \in A,\ b \in B \right\}$$

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* CARTES*iana* m-*ésima* de A, indicada por

$$M = A^m = \left\{ (a_1, a_2, \dots, a_m) \;\middle|\; a_1, a_2, \dots, a_m \in A \right\} .$$

Particularmente, se $m = 2$ e $A = B$, temos $A^2 = \left\{ (a, b) \;\middle|\; a, b \in A \right\}$.

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*

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

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

I.1.3 Conseqüência.

Se $A_1, A_2, \ldots, A_m$ *são conjuntos finitos, então vale*

$$\left|A_1 \times A_2 \times \ldots \times A_m\right| = \left|A_1\right|\left|A_2\right| \ldots \left|A_m\right| \ .$$

Particularmente, se $A_1 = A_2 = \ldots = A_m = A$, *temos*

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

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

$$\left|A_1 \times A_2 \times \ldots \times A_{m-1}\right| = \left|A_1\right|\left|A_2\right| \ldots \left|A_{m-1}\right| \ ,$$

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

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

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

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

I.1.4 Exemplos.

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

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

porém

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

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

$$\delta_{_A} = \left\{ (a,a) \;\middle|\; a \in A \right\} \subseteq A^2$$

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

I.1.6 Exemplos.

a) Para $A = I\!R$ temos

$$I\!R^2 = \left\{ (x,y) \;\middle|\; x,y \in I\!R \right\} \text{ é o } \textit{plano } \text{CARTES}\textit{iano} \text{ (EUCLIDiano) real,}$$

$$\delta_{I\!R} = \left\{ (x,x) \;\middle|\; x \in I\!R \right\} \text{ é a sua diagonal (a primeira mediana).}$$

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

$$A^2 = \left\{ \begin{array}{l} (\nabla,\nabla),\ (\nabla,\heartsuit),\ (\nabla,\clubsuit), \\ (\heartsuit,\nabla),\ (\heartsuit,\heartsuit),\ (\heartsuit,\clubsuit), \\ (\clubsuit,\nabla),\ (\clubsuit,\heartsuit),\ (\clubsuit,\clubsuit) \end{array} \right\} \quad \text{e} \quad \delta_{_A} = \left\{ (\nabla,\nabla),\ (\heartsuit,\heartsuit),\ (\clubsuit,\clubsuit) \right\} .$$

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 $A \times B$:

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

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

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 $(a,b) \notin \rho$.

$$\mathbf{D}(\rho) = \left\{ a \in A \;\middle|\; \exists\, b \in B \text{ com } a \,\rho\, b \right\} \subseteq A$$

chama-se o *domínio de definição*,

$$\mathbf{I}(\rho) = \left\{ b \in B \;\middle|\; \exists\, a \in A \text{ com } a\ \rho\ b \right\} \subseteq B$$

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 $A = \left\{ \nabla, \spadesuit, \heartsuit, \clubsuit \right\}$ e $B = 1, 2, 3$. Temos

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

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

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

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

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:

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

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

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

Em $A = \left\{a, b, c\right\}$ 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

$$\rho^{-1} = \left\{ (b, a) \;\middle|\; (a, b) \in \rho\right\} \in \mathbf{2}^{B\times A}$$

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

$$\rho = \left\{ (a, b) \;\middle|\; a \in \mathbb{Z},\ b \in \mathbb{R},\ 4a^2 + 9b^2 = 36\right\} \ ,$$

temos

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

e

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

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

e

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

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

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

temos

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

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

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:

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

I.1.12 Exemplos.

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

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

Então

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

b) Sejam $A = \big\{ \nabla, \spadesuit, \heartsuit, \clubsuit \big\}$, $B = \big\{ 1, 2, 3, 4 \big\}$ e $C = \big\{ a, b, c, d, e \big\}$.
Sejam $\rho \in \mathbf{2}^{A \times B}$ e $\sigma \in \mathbf{2}^{B \times C}$ definidas por

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

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

∎

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

a) $(\tau \circ \sigma) \circ \rho = \tau \circ (\sigma \circ \rho)$, (a lei associativa da composição).

b) $(\sigma \circ \rho)^{-1} = \rho^{-1} \circ \sigma^{-1}$ (lei de inversão da composta).

Demonstração: a) Para $a \in A$ e $d \in D$ temos:
$$a\ \big((\tau \circ \sigma) \circ \rho\big)\ d \iff \exists\, b \in B \ \text{ com} \begin{cases} a\ \rho\ b \\ \text{e} \\ b\ (\tau \circ \sigma)\ d \end{cases} \iff \exists\, b \in B,\ \exists\, c \in C$$

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

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

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

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

∎

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 $\forall\, a, b \in A: \quad a\,\rho\, b \iff b\,\rho\, a$.

iii) *antisimétrica*, se $\forall\, a, b \in A: \quad a\,\rho\, b$ e $b\,\rho\, a \implies a = b$.

iv) *transitiva*, se $\forall\, a, b, c \in A: \quad a\,\rho\, b$ 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 $\iff a\ \rho\ a\ \ \forall\, a \in A \iff (a,a) \in \rho$ $\forall\, a \in A \iff \delta_A = \left\{ (a,a) \;\middle|\; a \in A \right\} \subseteq \rho$.

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

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 concluimos $a = b$ 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, concluimos $a\ \rho\ c$, 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) $\delta_A \subseteq \varepsilon$, 2) $\varepsilon^{-1} = \varepsilon$ e 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

$$\bar{a} = \left\{ x \in A \;\middle|\; x \,\varepsilon\, a \right\} \ .$$

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

a *classe de equivalência de* $a \mod \varepsilon$ (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 $a \mod \varepsilon$ é

$$\bar{a} = \left\{ x \in A \;\middle|\; x \ \text{tem a cor de} \ a \right\} \ .$$

■

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) $\quad \bar a \neq \bar b \quad \Longrightarrow \quad \bar a \cap \bar b = \emptyset.$

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

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

b) " $\Rightarrow$ ": De $\bar a = \bar b$ segue $a \in \bar b = \left\{ x \in A \,\middle|\, x \,\varepsilon\, b \right\}$. 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, $\bigcup\limits_{a\in A} \bar a \subseteq A$. Mas, como $a \in \bar a$, temos de fato $\bigcup\limits_{a\in A} \bar a = A$.

■

I.1.22 Definição.

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

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

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

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

Por I.1.21 temos o

I.1.23 Exemplo.

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

$$\mathfrak{P}_\varepsilon = \left\{ \bar a \,\middle|\, a \in A \right\} \quad \text{com} \quad \bar a = \left\{ x \in A \,\middle|\, x \,\varepsilon\, a \right\},$$

o *conjunto das classes de equivalência* de $A \mod \varepsilon$.

Então $\mathfrak{P}_\varepsilon$ é uma partição de A.

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

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

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

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

Demonstração: a) Como $\bigcup\limits_{X \in \mathfrak{P}} X = A$, 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 $b \in X \cap Y$, concluimos $X = Y$, 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 $\bmod\ \varepsilon_{\mathfrak{P}}$ 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 $a \bmod \varepsilon$ 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 $A \bmod \varepsilon$.

Ao invés de usar letras como ε, η , . . . , 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

$$A/\!\equiv \;=\; \{\bar{a} \mid a \in A\} \text{ é o conjunto quociente de } A \mod \equiv ,$$

$$A/\!\sim \;=\; \{\hat{a} \mid a \in A\} \text{ é o conjunto quociente de } A \mod \sim ,$$

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

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

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

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:*

a) $\equiv_n \in \mathbf{Eq}(\mathbb{Z})$.

b) *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* $\mathbb{Z}$.

c) *Para todo* $a \in \mathbb{Z}$ *temos* $\bar{a} = \{a + nk \mid k \in \mathbb{Z}\}$.

d) *Se* $n > 0$, *então* $\mathbb{Z} = \bar{0} \cup \bar{1} \cup \ldots \cup \overline{n-1}$ *e*

$$\bar{i} \neq \bar{j} \quad \text{para todos os } i, j \text{ com } 0 \leq i \neq j \leq n-1$$

e) *Se* $n > 0$, *o conjunto quociente de* $\mathbb{Z}$ $\mod n$ *é*

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

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

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

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 $\mathbb{Z} = \bar{0} \cup \bar{1} \cup \ldots \cup \overline{n-1}$. 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 $\bar{0}, \bar{1}, \ldots, \overline{n-1}$ são distintas e segue $|\mathbb{Z}/\equiv_n| = n$.

e) É conseqüência de d).

I.1.27 Exemplos.

a) Para $n = 2$ obtemos

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

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

b) Para $n = 3$ obtemos

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

......

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 relacão $\varphi \in \mathbf{2}^{A\times B}$ 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. $\mathbf{I}(\varphi) = \left\{ b \in B \,\middle|\, \exists\, a \in A \text{ com } a\,\varphi\, b \right\}$ é agora o conjunto de todos os valores de φ. Portanto

$$\mathbf{I}(\varphi) = \left\{ \varphi(a) \,\middle|\, a \in A \right\}\ .$$

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

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

$$B^A = \left\{ \varphi \in \mathbf{2}^{A\times B} \,\middle|\, \varphi \text{ é uma aplicação de } A \text{ em } B \right\}\ .$$

(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

$$\varphi = \left\{ \big(a, \varphi(a)\big) \,\middle|\, a \in A \right\}\ .$$

I.2.2 Exemplos.

a$_1$) Seja $A=B=I\!R$. A relação $\rho\in\mathbf{2}^{I\!R\times I\!R}$ seja definida por

$$\rho=\left\{\,(a,b)\;\middle|\;4a^2+9b^2=36\right\}\ .$$

Temos $\mathbf{D}(\rho)=[-3,3]$ e $\mathbf{I}(\rho)=[-2,2]$ e $\rho\notin I\!R^{I\!R}$,
i.e. esta ρ *não é uma aplicação de* $I\!R$ *em* $I\!R$.

a$_2$) Seja $A=[-3,3]$ e $B=I\!R$. $\varphi\in\mathbf{2}^{[-3,3]\times I\!R}$ seja definida por

$$\varphi=\left\{\,(a,b)\;\middle|\;4a^2+9b^2=36;\;\;b\le 0\right\}\ .$$

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

$$\varphi=\left\{\left(a,-\tfrac{\sqrt{36-4a^2}}{3}\right)\;\middle|\;a\in[-3,3]\right\}\ .$$

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

b$_1$) Para

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

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

b$_2$) Para

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

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

b$_3$) Para

$$\rho=\left\{(\nabla,b),(\spadesuit,a),(\clubsuit,d)\right\}$$

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

∎

I.2.3 Três Exemplos importantes

a) Seja B um conjunto e consideremos $A=I\!N=\left\{1,2,3,\ldots\right\}$.
Toda aplicação $\varphi\in B^{I\!N}$ é denominada uma *seqüência* em B.
Se $\varphi(n)=b_n\in B$ é o valor de φ em $n\in I\!N$, temos que

$$\varphi=\left\{\,\big(n,\varphi(n)\big)\;\middle|\;n\in I\!N\right\}=\left\{\,(n,b_n)\;\middle|\;n=1,2,3,\ldots\right\}\ .$$

Escreve-se a seqüência φ também como

$$\varphi = \big(b_1, b_2, b_3, \ldots, b_n, \ldots\big) = (b_n)_{n \in I\!N} \ .$$

$B^{I\!N}$ é portanto *o conjunto de todas as sequências em* B.

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

$$A/\varepsilon = \big\{\, \bar{a} \;\big|\; a \in A \big\} \text{ o conjunto quociente de } A \mod \varepsilon.$$

Lembrando: $\forall\, a \in A :\ \ \bar{a} = \big\{\, x \in A \;\big|\; x \;\varepsilon\; a \big\}$ é a classe de equivalência de $a \mod \varepsilon$. 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

$$\gamma = \big\{\, (a, \bar{a}) \;\big|\; a \in A \big\} \ ,$$

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

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

$$\varepsilon = \big\{(1,1), (2,2), (3,3), (4,4), (5,5), (2,5), (5,2), (3,4), (4,3)\big\} =$$

$$= \delta_A \cup \big\{(2,5), (5,2), (3,4), (4,3)\big\} \ ,$$

temos assim:

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

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

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

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

seu produto CARTESiano. Seja $i \in \big\{1, 2, \ldots, r\big\}$. A aplicação

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

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

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

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

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

■

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 *funcão 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, concluimos $(a,a) \in \rho^{-1} \circ \rho$. Isto significa que existe $b \in B$ com $\begin{cases} a\ \rho\ b \\ \text{e} \\ b\ \rho^{-1}\ a \end{cases}$. 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 $\begin{cases} a\ \rho\ b \\ \text{e} \\ b\ \rho^{-1}\ a \end{cases}$. 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 $\begin{cases} b\ \rho^{-1}\ a \\ \text{e} \\ a\ \rho\ b' \end{cases}$. 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 $\begin{cases} b\ \rho^{-1}\ a \\ \text{e} \\ a\ \rho\ b' \end{cases}$. Isto significa $\begin{cases} a\ \rho\ b \\ \text{e} \\ a\ \rho\ b' \end{cases}$. Pela hipótese, $b = b'$. Logo, $(b,b') = (b,b) \in \delta_B$ e portanto $\delta_B \supseteq \rho \circ \rho^{-1}$.

$\blacksquare$

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* $\delta_B \supseteq \varphi \circ \varphi^{-1}$

$\blacksquare$

I.2.7 Exemplos.

a) Para $A = B = I\!R$ e $\varphi = \big\{ \big(x, x^2\big) \;\big|\; x \in I\!R \big\} \in \mathbf{2}^{I\!R \times I\!R}$ temos

$$\varphi^{-1} \circ \varphi = \big\{ \big(x^2, x\big) \;\big|\; x \in I\!R \big\} \circ \big\{ \big(x, x^2\big) \;\big|\; x \in I\!R \big\} =$$

$$= \big\{ (x, x) \;\big|\; x \in I\!R \big\} \cup \big\{ (x, -x) \;\big|\; x \in I\!R \big\} \supseteq \delta_{I\!R} = \delta_A$$

e

$$\varphi \circ \varphi^{-1} = \big\{ \big(x, x^2\big) \;\big|\; x \in I\!R \big\} \circ \big\{ \big(x^2, x\big) \;\big|\; x \in I\!R \big\} =$$

$$= \big\{ \big(x^2, x^2\big) \;\big|\; x \in I\!R \big\} \subseteq \delta_{I\!R} = \delta_B \; .$$

Portanto φ *é uma aplicação* de $I\!R$ em $I\!R$.

b) Para $A = B = I\!R$ e $\rho = \big\{ \big(x^2, x\big) \;\big|\; x \in I\!R \big\} \in \mathbf{2}^{I\!R \times I\!R}$ temos

$$\rho^{-1} \circ \rho = \big\{ \big(x, x^2\big) \;\big|\; x \in I\!R \big\} \circ \big\{ \big(x^2, x\big) \;\big|\; x \in I\!R \big\} =$$

$$= \big\{ \big(x^2, x^2\big) \;\big|\; x \in I\!R \big\} = \big\{ (y, y) \;\big|\; 0 \leq y \in I\!R \big\} \not\supseteq \delta_{I\!R} = \delta_A \; .$$

e

$$\rho \circ \rho^{-1} = \big\{ \big(x^2, x\big) \;\big|\; x \in I\!R \big\} \circ \big\{ \big(x, x^2\big) \;\big|\; x \in I\!R \big\} =$$

$$= \big\{ (x, x) \;\big|\; x \in I\!R \big\} \cup \big\{ (x, -x) \;\big|\; x \in I\!R \big\} \not\subseteq \delta_{I\!R} = \delta_B \; .$$

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

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

$$\varphi = \big\{ (a, b) \in A \times B \;\big|\; a \,\varphi\, b \big\} = \big\{ \big(a, \varphi(a)\big) \;\big|\; a \in A \big\}$$

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

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

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

∎

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

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

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

$$\left|B^A\right| = |B|^{|A|} = n^m .$$

Demonstração: Podemos supor $A = \{1, 2, 3, \ldots, m\}$. 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

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

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

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

obtemos de fato:

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

Também

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

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

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

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

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

Logo,

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

Portanto, podemos dizer também que

$$\psi\circ\varphi = \Big\{ \Big(a, \psi\big(\varphi(a)\big)\Big) \ \Big|\ a\in A\Big\}\ .$$

■

I.2.11 Notação.

Se $A=\{1,2,3,\ldots,m\}$ 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:

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

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

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

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

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

Sejam $A = \{1, 2, \ldots, m\}$, $B = \{b_1, b_2, \ldots, b_n\}$ 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

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

e

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

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

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

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

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

e

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

temos

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

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 $A = B = I\!R$ e

$$\varphi = \left\{ \left(a, a^2\right) \;\middle|\; a \in I\!R \right\} \in I\!R^{I\!R} = B^A ,$$

a relação inversa é

$$\varphi^{-1} = \left\{ \left(a^2, a\right) \;\middle|\; a \in I\!R \right\} = \left\{ \left(b, \pm\sqrt{b}\right) \;\middle|\; 0 \le b \in I\!R \right\} \notin I\!R^{I\!R} = A^B .$$

Isto, pois $\mathbf{D}(\varphi^{-1}) = \mathbf{I}(\varphi) = \left\{ x \in I\!R \;\middle|\; x \ge 0 \right\} \ne I\!R = B$.
Além do mais, $\left(a^2, a\right) \in \varphi^{-1}$ e também $\left(a^2, -a\right) = \left((-a)^2, -a\right) \in \varphi^{-1}$.

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

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

temos

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

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

I.2.13 Definição.

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

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

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

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 fôr injetora e sobrejetora simultâneamente.

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.

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

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

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

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

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

I.2.16 Exemplos.

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

a$_1$) $\varphi = \left\{ (a, 3^a) \;\middle|\; a \in \mathbb{R} \right\}$ é uma aplicação injetora de $A = \mathbb{R}$ em $B = \mathbb{R}$. Mas ela não é sobrejetora, pois

$$\varphi(\mathbb{R}) = \left\{ 3^a \;\middle|\; a \in \mathbb{R} \right\} = \left\{ x \in \mathbb{R} \;\middle|\; x > 0 \right\} \neq \mathbb{R} = B\,.$$

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

a$_2$) $\varphi = \left\{ \left(a, a^3 - a\right) \;\middle|\; a \in I\!R \right\}$ é uma aplicação sobrejetora de $A = I\!R$ sobre $B = I\!R$ (porquê ?, demonstração !). Ela não é injetora, pois

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

$$\varphi \in \mathbf{Sob}(I\!R, I\!R) \;\setminus\; \mathbf{Inj}(I\!R, I\!R)\ .$$

a$_3$) $\varphi = \left\{ \left(a, a^3\right) \;\middle|\; a \in I\!R \right\}$ é uma aplicação bijetora de $A = I\!R$ sobre $B = I\!R$, i.e. uma permutação de $I\!R$.

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

b) b$_1$) Para $A = \left\{ \nabla, \spadesuit, \heartsuit, \clubsuit \right\}$ e $B = \left\{1, 2, 3, 4, 5\right\}$ temos que

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

b$_2$) Para $A = \left\{ \nabla, \spadesuit, \heartsuit, \clubsuit \right\}$ e $B = \left\{1, 2, 3\right\}$ temos que

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

b$_3$) Para $A = \left\{ \nabla, \spadesuit, \heartsuit, \clubsuit \right\}$ e $B = \left\{1, 2, 3, 4\right\}$ temos que

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

b$_4$) Para $A = B = \left\{ \nabla, \spadesuit, \heartsuit, \clubsuit \right\}$ temos que

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

i.e. φ é uma permutação de A.

∎

I.2.17 Proposição.

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

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

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

c) φ *é bijetora* $\iff \delta_A = \varphi^{-1} \circ \varphi$ *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 $\begin{cases} a\,\varphi\,b \\ \text{e} \\ b\,\varphi^{-1}\,a' \end{cases}$. Isto significa $\begin{cases} a\,\varphi\,b \\ \text{e} \\ a'\,\varphi\,b \end{cases}$, ou seja, $\varphi(a) = b = \varphi(a')$.

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

c) é uma conseqüência de a) e b).

■

I.2.18 Conseqüência.

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

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

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.

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

∎

I.2.19 Exemplos.

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

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

e

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

b) Para $A = B = I\!R$ e $\varphi = \left\{ (x, \operatorname{arctg} x) \mid x \in I\!R \right\} \in I\!R^{I\!R}$ temos

$$\varphi^{-1} \circ \varphi = \left\{ (\operatorname{arctg} x, x) \mid x \in I\!R \right\} \circ \left\{ (x, \operatorname{arctg} x) \mid x \in I\!R \right\} =$$

$$= \left\{ (x,x) \mid x \in I\!R \right\} = \delta_{I\!R} = \delta_A\ ,$$

mas

$$\varphi \circ \varphi^{-1} = \left\{ (x, \operatorname{arctg} x) \mid x \in I\!R \right\} \circ \left\{ (\operatorname{arctg} x, x) \mid x \in I\!R \right\} =$$

$$= \left\{ (y,y) \mid -\tfrac{\pi}{2} < y < \tfrac{\pi}{2} \right\} \neq \delta_{I\!R} = \delta_B\ .$$

Portanto φ é uma aplicação *injetora, mas não sobrejetora* de $I\!R$ em $I\!R$.

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

$$\varphi^{-1} \circ \varphi = \left\{ \left(x^3 - x, x\right) \mid x \in I\!R \right\} \circ \left\{ \left(x, x^3 - x\right) \mid x \in I\!R \right\} =$$

$$= \left\{ (x,x) \mid x \in I\!R \right\} \cup \left\{ \left(x, \tfrac{-x+\sqrt{4-3x^2}}{2}\right) \mid -\tfrac{2}{\sqrt{3}} \leq x \leq \tfrac{2}{\sqrt{3}} \right\} \cup$$

$$\cup \left\{ \left(x, \tfrac{-x-\sqrt{4-3x^2}}{2}\right) \mid -\tfrac{2}{\sqrt{3}} \leq x \leq \tfrac{2}{\sqrt{3}} \right\} \neq \delta_{I\!R} = \delta_A\ .$$

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

Mas

$$\varphi \circ \varphi^{-1} = \left\{ \left(x, x^3 - x\right) \;\middle|\; x \in I\!R \right\} \circ \left\{ \left(x^3 - x, x\right) \;\middle|\; x \in I\!R \right\} =$$

$$= \left\{ (y, y) \;\middle|\; y \in I\!R \right\} = \delta_{I\!R} = \delta_B \ .$$

Portanto φ é uma aplicação *sobrejetora, mas não injetora* de $I\!R$ em $I\!R$.

d) Para $A = B = I\!R$ e $\varphi = \left\{ \left(x, x^3\right) \;\middle|\; x \in I\!R \right\} \in I\!R^{I\!R}$ temos

$$\varphi^{-1} \circ \varphi = \left\{ \left(x^3, x\right) \;\middle|\; x \in I\!R \right\} \circ \left\{ \left(x, x^3\right) \;\middle|\; x \in I\!R \right\} =$$

$$= \left\{ (x, x) \;\middle|\; x \in I\!R \right\} = \delta_{I\!R} = \delta_A \ .$$

Também

$$\varphi \circ \varphi^{-1} = \left\{ \left(x, x^3\right) \;\middle|\; x \in I\!R \right\} \circ \left\{ \left(x^3, x\right) \;\middle|\; x \in I\!R \right\} =$$

$$= \left\{ \left(x^3, x^3\right) \;\middle|\; x \in I\!R \right\} = \delta_{I\!R} = \delta_B \ .$$

Portanto φ é uma aplicação *bijetora* de $I\!R$ em $I\!R$.

I.2.20 Proposição.

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

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

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

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 $\psi\left(\varphi(a)\right) = \psi\left(\varphi(a')\right)$. Como ψ é injetora, concluimos $\varphi(a) = \varphi(a')$. Como φ é injetora, concluimos $a = a'$. 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 $(\psi \circ \varphi)(a) = \psi\left(\varphi(a)\right) = \psi(b) = c$. 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

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

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

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

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*

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

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

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

ii) Sejam $a, a' \in A$ tais que $\varphi(a) = \varphi(a')$. Segue $\psi\big(\varphi(a)\big) = \psi\big(\varphi(a')\big)$, 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 $I\!N = \{1, 2, 3, \ldots\}$ e $2I\!N = \{2, 4, 6, \ldots\}$. Então $I\!N \sim 2I\!N$, sendo que para a aplicação φ definida por

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

iii) $I\!N \sim \mathbb{Z}$ podemos verificar, olhando na aplicação $\varphi \in \mathbf{Bij}\,(I\!N, \mathbb{Z})$, 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) $I\!R \sim (0, 1)$, sendo que $\varphi \in \mathbf{Bij}\,(I\!R\,,\ (0, 1))$, quando se define

$$\varphi(x) = \tfrac{1}{\pi} \cdot \operatorname{arctg} x + \tfrac{1}{2} \quad \forall\, x \in I\!R.$$

É importante tomarmos conhecimento que

existem conjuntos infinitos que não são equipotentes:

I.2.25 Proposição.

$$I\!N \not\sim I\!N^{I\!N} \quad \textit{e também} \quad I\!R \not\sim I\!R^{I\!R} \; .$$

(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 $\mathbf{Bij}\,(I\!N, I\!N^{I\!N}) = \emptyset$. Como $\mathbf{Bij}\,(I\!N, I\!N^{I\!N}) \subseteq \mathbf{Sob}\,(I\!N, I\!N^{I\!N})$, basta provar que

$$\mathbf{Sob}\,(I\!N, I\!N^{I\!N}) = \emptyset \;\; :$$

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

$$\Omega(I\!N) = \{\varphi_1, \varphi_2, \varphi_3, \ldots, \varphi_n, \ldots\} \; .$$

Seja $\psi \in I\!N^{I\!N}$ definida por

$$\psi(x) = \varphi_x(x) + 1 \quad \forall\, x \in I\!N \; .$$

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 $A = \{a_1, a_2, a_3, \ldots\}$.

Temos que $\mathbb{N}^{\mathbb{N}}$ é um conjunto não-enumerável. Pode-se provar fácilmente 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

$$A \not\sim \mathbf{2}^A\ .$$

Demonstração: Vamos colocar $\mathfrak{A} = \mathbf{2}^A$. 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

$$\Omega(A) = \left\{ X_a \;\middle|\; a \in A \right\} \subseteq \mathfrak{A}\ .$$

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

$$Y = \left\{ y \in A \;\middle|\; y \notin X_y \right\}\ .$$

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*

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

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 $\Omega \in \mathbf{Bij}\left(\mathfrak{A}\,,\{0,1\}^A\right)$. Para todo $X \in \mathfrak{A}$ definamos $\chi_{_X} \in \{0,1\}^A$ por

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

($\chi_{_X}$ 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

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

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

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

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

∎

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:

a) $\varepsilon_\varphi \in \mathbf{Eq}(A)$ (ε_φ chama-se a relação de equivalência associada à φ).

b) *Seja* γ *a aplicação canónica de* A *sobre* A/ε_φ, *i.e.*

$$\gamma(a) = \bar{a} = \left\{ x \in A \;\middle|\; x\,\varepsilon_\varphi\, a \right\}\ .$$

Afirmamos que existe uma única aplicação

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

Particularmente,

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

Demonstração: a) é visto fácilmente (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, $\psi\left(\gamma(a)\right) = \psi'\left(\gamma(a)\right)$, 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, $\psi \in \mathbf{Sob}\big(A/\varepsilon_\varphi \ , \ \varphi(A)\big)$.

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, $\psi \in \mathbf{Inj}\big(A/\varepsilon_\varphi \ , \ \varphi(A)\big)$.

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

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

■

I.2.30 Exemplo.

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

$$\varphi(a) = \operatorname{sen} 2\pi a \quad \forall\, a \in I\!R\,.$$

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

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

Além disso, para todo $a \in I\!R$:

$$\bar{a} = \Big\{ x \in I\!R \ \Big| \ a - x \in Z\!\!\!Z \text{ ou } a + x \in \tfrac{1}{2} + Z\!\!\!Z \Big\}\ .$$

A aplicação canónica $\gamma \in (I\!R/\varepsilon_\varphi)^{I\!R}$ é:

$$\gamma(a) = \bar{a} = \Big\{ x \in I\!R \ \Big| \ a - x \in Z\!\!\!Z \text{ ou } a + x \in \tfrac{1}{2} + Z\!\!\!Z \Big\} \quad \forall\, a \in I\!R\,.$$

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

$$\psi(\bar{a}) = \operatorname{sen} 2\pi a \quad \forall\, \bar{a} \in I\!R/\varepsilon_\varphi\ .$$

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 $\psi\big(\varphi(a)\big) = \psi\big(\varphi(a')\big)$, 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 $(\psi_{a_0}\circ\varphi)(a) = \psi_{a_0}\big(\varphi(a)\big) = a \quad \forall\, a \in A$. Portanto $\psi_{a_0}\circ\varphi = \delta_A$. (Mencionamos que se φ não é sobrejetora, esta função construida 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 $b = \delta_B(b) = (\varphi\circ\omega)(b) = \varphi\big(\omega(b)\big) = \varphi(a)$ e vemos que φ é sobrejetora.

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

$$X_b = \big\{\, a \in A \;\big|\; \varphi(a) = b \big\} \subseteq A\ .$$

Temos portanto a família

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

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 *simultâneamente* 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 $b \in B$:

$$(\varphi \circ \omega)(b) = \varphi\big(\omega(b)\big) = \varphi(a) = b = \delta_B(b)\ . \quad \text{Portanto,}\ \ \varphi \circ \omega = \delta_B .$$

∎

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 *simultâneamente* 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 $\mathfrak{F} \subseteq \mathbf{2}^A$ 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 $\bigcup\limits_{X \in \mathfrak{F}} X \subseteq A$ (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 $A = I\!N$ é o conjunto de todos os números naturais, tal procedimento não tem nenhum problema: Se $\mathfrak{F} \subseteq \mathbf{2}^{I\!N}$, 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 $\alpha(X) \in X$, *simultâneamente* para todo X". Assim, neste caso é claro, como uma escolha *simultânea* funciona.

2) Seja $A = I\!R$ 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 $\alpha\big((a,b)\big) \in (a,b)$ para todos os $(a,b) \in \mathfrak{F}$: Podemos associar a cada (a,b) seu ponto médio: $\alpha\big((a,b)\big) = \frac{a+b}{2}$.

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 $X_b \neq \emptyset \quad \forall\, b \in B$, 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 $b \in B$:

$$(\varphi \circ \omega)(b) = \varphi\big(\omega(b)\big) = \varphi\big(\alpha(X_b)\big) = b = \delta_B(b),$$

pois $\alpha(X_b) \in X_b = \big\{\, a \in A \;\big|\; \varphi(a) = b \,\big\}$. 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

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

Demonstração: Afirma-se $\mathbf{Bij}\big(A, A^A\big) = \emptyset$ e basta provar $\mathbf{Sob}\big(A, A^A\big) = \emptyset$: 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.

$$\Omega(A) = \big\{\ \varphi_a \;\big|\; a \in A \big\}\ .$$

Consideremos para cada $a \in A$ o conjunto $Y_a = A \setminus \big\{\varphi_a(a)\big\}$. Temos $Y_a \neq \emptyset$, pois $|A| \geq 2$. Considere agora a família

$$\mathfrak{F} = \big\{\, Y_a \;\big|\; a \in A \big\}\ .$$

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 $|A| = m \in I\!N$ e $|B| = n \in I\!N$. Para simplificar, vamos supor

$$A = \big\{1, 2, 3, \ldots, m\big\} \ \text{ e } \ B = \big\{b_1, b_2, b_3, \ldots, b_n\big\} \ .$$

Sabemos B^A é finito e vale $\left|B^A\right| = |B|^{|A|} = n^m$.

Quantas destas n^m aplicações são injetoras e quantas são sobrejetoras? Queremos portanto descobrir $|\mathbf{Inj}\,(A,B)|$ e $|\mathbf{Sob}\,(A,B)|$. Abreviamos

$$\mathbf{Inj}\,(m,n) = \mathbf{Inj}\,(A,B) \quad \text{e} \ \ \mathbf{Sob}\,(m,n) = \mathbf{Sob}\,(A,B)$$

e colocamos

$$i_n(m) = |\mathbf{Inj}\,(m,n)| \quad \text{e} \ \ s_n(m) = |\mathbf{Sob}\,(m,n)| \ .$$

A pergunta é:

$$i_n(m) = \,? \quad \text{e} \quad s_n(m) = \,?$$

Claramente vamos ter

$$i_n(m) \leq n^m \quad \text{e também} \ \ s_n(m) \leq n^m \ .$$

A resposta para $i_n(m)$ é fácilmente obtida: Toda $\varphi \in \mathbf{Inj}\,(m,n)$ é determinada pela m-upla

$$\big(\varphi(1), \varphi(2), \ldots, \varphi(m)\big) = (b_{i_1}, b_{i_2}, \ldots, b_{i_m})$$

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}, $\ldots$ e finalmente $n-m+1$ escolhas para b_{i_m}. Isto dá um total de $n(n-1)\ldots(n-m+1)$ m-uplas distintas com coordenadas distintas, ou seja

$$i_n(m) = n(n-1)(n-2)\ldots(n-m+1) = \binom{n}{m} \cdot m! \ .$$

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*

$$i_n(m) = n(n-1)(n-2)\ldots(n-m+1) = \binom{n}{m} \cdot m!\ .$$

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 $\qquad i_n(n) = n!\ .$
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 $A = \{1, 2, \ldots, n\}$ 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*

$$s_n(m) = n^m - \tbinom{n}{n-1}(n-1)^m + \tbinom{n}{n-2}(n-2)^m \mp \ldots + (-1)^k\tbinom{n}{n-k}(n-k)^m \pm \ldots$$
$$+(-1)^{n-k}\tbinom{n}{k}k^m \pm \ldots + (-1)^{n-1}\tbinom{n}{1}1^m\ ,$$

ou seja,

$$s_n(m) = \sum_{k=1}^{n} (-1)^{n+k} k^m \cdot \tbinom{n}{k}\ .$$

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

$$\top\big((a, b)\big) \in M.$$

$\top$ é uma função de duas variáveis de M com valores em M.

II.1.2 Exemplos.

a) Seja $M = I\!N$ e

a$_1$) $\top_1 \in I\!N^{I\!N \times I\!N}$ definida por $\top_1\big((a, b)\big) = a + b \quad \forall\, a, b \in I\!N$.

a$_2$) $\top_2 \in I\!N^{I\!N \times I\!N}$ definida por $\top_2\big((a, b)\big) = a \cdot b \quad \forall\, a, b \in I\!N$.

a$_3$) $\top_3 \in I\!N^{I\!N \times I\!N}$ definida por $\top_3\big((a, b)\big) = a^b \quad \forall\, a, b \in I\!N$.

$\top_1$, $\top_2$ e $\top_3$ são 3 *exemplos de composições internas de* $I\!N$.

b) Seja $M = \mathbb{Z}$ e

b$_1$) $\top_1 \in \mathbb{Z}^{\mathbb{Z} \times \mathbb{Z}}$ definida por $\top_1\big((a, b)\big) = a + b \quad \forall\, a, b \in \mathbb{Z}$.

b$_2$) $\top_2 \in \mathbb{Z}^{\mathbb{Z} \times \mathbb{Z}}$ definida por $\top_2\big((a, b)\big) = a \cdot b \quad \forall\, a, b \in \mathbb{Z}$.

b$_3$) $\top_3 \in \mathbb{Z}^{\mathbb{Z} \times \mathbb{Z}}$ definida por $\top_3\big((a, b)\big) = a - b \quad \forall\, a, b \in \mathbb{Z}$.

$b_4)$ $\top_4 \in \mathbb{Z}^{\mathbb{Z}\times\mathbb{Z}}$ definida por $\top_4\big((a,b)\big) = a^4b - b^5a \quad \forall\, a,b \in \mathbb{Z}$.

$\top_1$, $\top_2$, $\top_3$ e $\top_4$ são 4 *exemplos de composições internas de* $\mathbb{Z}$*.*

c) Seja $M = \mathbb{R}$ e

$c_1)$ $\top_1 \in \mathbb{R}^{\mathbb{R}\times\mathbb{R}}$ definida por $\top_1\big((a,b)\big) = a + b \quad \forall\, a,b \in \mathbb{R}$.
$c_2)$ $\top_2 \in \mathbb{R}^{\mathbb{R}\times\mathbb{R}}$ definida por $\top_2\big((a,b)\big) = a \cdot b \quad \forall\, a,b \in \mathbb{R}$.
$c_3)$ $\top_3 \in \mathbb{R}^{\mathbb{R}\times\mathbb{R}}$ definida por $\top_3\big((a,b)\big) = a - b \quad \forall\, a,b \in \mathbb{R}$.
$c_4)$ $\top_4 \in \mathbb{R}^{\mathbb{R}\times\mathbb{R}}$ definida por

$$\top_4\big((a,b)\big) = \sqrt{a^2+b^2} - \cos(e^a + ba^2) \quad \forall\, a,b \in \mathbb{R}\ .$$

$\top_1$, $\top_2$, $\top_3$ e $\top_4$ são 4 *exemplos de composições internas em* $\mathbb{R}$*.*

Devemos mencionar que a $\top_4$ de $c_4)$ não define uma composição interna em $\mathbb{Z}$ ou em $\mathbb{N}$. Também $a \top_3 b = a - b$ não é uma composição interna de $\mathbb{N}$.

d) Seja E um conjunto, $\mathfrak{M} = \mathbf{2}^E$ e

$d_1)$ $\top_1 \in \mathfrak{M}^{\mathfrak{M}\times\mathfrak{M}}$ definida por $\top_1\big((X,Y)\big) = X \cap Y \quad \forall\, X,Y \in \mathfrak{M}$.
$d_2)$ $\top_2 \in \mathfrak{M}^{\mathfrak{M}\times\mathfrak{M}}$ definida por $\top_2\big((X,Y)\big) = X \cup Y \quad \forall\, X,Y \in \mathfrak{M}$.
$d_3)$ $+ \in \mathfrak{M}^{\mathfrak{M}\times\mathfrak{M}}$ definida por

$$+\big((X,Y)\big) = (X\cup Y)\backslash(X\cap Y) \quad \forall\, X,Y \in \mathfrak{M}\ .$$

$\top_1$, $\top_2$ e $+$ (i.e. $\cap$, $\cup$ e $+$) são 3 *exemplos de composições internas de* $\mathfrak{M} = \mathbf{2}^E$.

e) Seja $M = \{\nabla, \spadesuit, \heartsuit, \clubsuit\}$.
A seguinte tabela define uma composição interna de M:

$\top$	∇	$\spadesuit$	$\heartsuit$	$\clubsuit$
∇	∇	$\spadesuit$	∇	$\heartsuit$
$\spadesuit$	$\heartsuit$	∇	$\spadesuit$	$\clubsuit$
$\heartsuit$	$\spadesuit$	$\heartsuit$	$\clubsuit$	$\clubsuit$
$\clubsuit$	$\spadesuit$	$\clubsuit$	∇	$\heartsuit$

Por exemplo temos $\top\big((\clubsuit,\heartsuit)\big) = \nabla$ e $\top\big((\spadesuit,\nabla)\big) = \heartsuit$.

∎

As composições internas "naturais" em $I\!N$, $Z\!\!Z$ e $I\!R$,

a adição " $+$ " e a multiplicação " $\cdot$ ",

tornam-se nesta interpretação

" *funções de duas variáveis com valores no próprio conjunto.*"

Assim, deveriamos escrever por exemplo

$$+ \in I\!R^{I\!R\times I\!R} \quad \text{e} \quad \cdot \in I\!N^{I\!N\times I\!N} \text{ etc. .}$$

Como ninguem escreve $+\big((a,b)\big)$ 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 $\top\big((a,b)\big)$ desta função em (a,b) é indicado por

$$\top\big((a,b)\big) = a \top b \ .$$

$a \top b$ 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

$$a \top_4 b = \sqrt{a^2+b^2} - \cos(e^a + ba^2) \quad \forall\, a,b \in I\!R\ .$$

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 $M = \{a_1, a_2, \ldots, a_m\}$ de m elementos é dada e pode ser identificada por um quadro de m^2 entradas:

$\top$	a_1	a_2	$\ldots$	a_k	$\ldots$	a_m
a_1	$a_1\top a_1$	$a_1\top a_2$	$\ldots$	$a_1\top a_k$	$\ldots$	$a_1\top a_m$
a_2	$a_2\top a_2$	$a_2\top a_2$	$\ldots$	$a_2\top a_k$	$\ldots$	$a_2\top a_m$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
a_i	$a_i\top a_1$	$a_i\top a_2$	$\ldots$	$a_i\top a_k$	$\ldots$	$a_i\top a_m$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
a_m	$a_m\top a_1$	$a_m\top a_2$	$\ldots$	$a_m\top a_k$	$\ldots$	$a_m\top a_m$

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

$$\left|M^{M\times M}\right| = m^{m^2}$$

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 $\{\nabla, \spadesuit, \heartsuit, \clubsuit\}$ existem

$$4^{16} = 65\,536^2 \approx 4,29 \cdot 10^9$$

(em palavras: $4,29$ bilhões de) composições internas distintas.

$\blacksquare$

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) $(I\!N\,;\,\top_1)$, $(I\!N\,;\,\top_2)$, $(I\!N\,;\,\top_3)$, onde $\forall\, a,b \in I\!N$:

$$a \top_1 b = a + b, \quad a \top_2 b = a \cdot b, \quad a \top_3 b = a^b$$

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) $(I\!R;\,\top_1)$, $(I\!R;\,\top_2)$, $(I\!R;\,\top_3)$, $(I\!R;\,\top_4)$, onde $\forall\, a,b \in I\!R$:

$$a \top_1 b = a + b, \quad a \top_2 b = a \cdot b, \quad a \top_3 b = a - b$$

$$a \top_4 b = \sqrt{a^2+b^2} - \cos(e^a + ba^2)\ ,$$

são 4 *estruturas algébricas com uma composição interna cada.*

d) Para todo conjunto E e $\mathfrak{M} = \mathbf{2}^E$, os pares

$$\big(\,\mathfrak{M};\cap\,\big)\,,\quad \big(\,\mathfrak{M};\cup\,\big)\quad \text{e}\quad \big(\,\mathfrak{M};+\,\big)\,,$$

(onde $X+Y=(X\cup Y)\backslash(X\cap Y)\quad \forall\, X,Y\in\mathfrak{M}$)
são três estruturas algébricas com uma composição interna cada.

e) O par

$$\big(\,\{\,\nabla,\spadesuit,\heartsuit,\clubsuit\,\};\,\top\,\big)\ ,$$

onde a composição

$$\top\in\{\,\nabla,\spadesuit,\heartsuit,\clubsuit\,\}^{\{\,\nabla,\spadesuit,\heartsuit,\clubsuit\,\}\times\{\,\nabla,\spadesuit,\heartsuit,\clubsuit\,\}}$$

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 simultâneamente:

II.1.5 Definição.

Se $M\neq\emptyset$ é um conjunto e $\top_1,\top_2\ ,\ldots,\ \top_r\in M^{M\times M}$ são r composições internas de M, então o "objeto"

$$\big(\,M\,;\,\top_1,\top_2\ ,\ldots,\ \top_r\,\big)$$

chama-se uma *estrutura algébrica com r composições internas.*

II.1.6 Exemplos.

a) $\big(\,I\!\!R;+\ ,\ \cdot\,\big)$ é uma estrutura com duas composições internas.

b) Seja E um conjunto, $\mathfrak{M} = \mathbf{2}^E$,

$$\big(\mathfrak{M}; \cap\,,\, \cup\,,\, +\big)$$

é uma estrutura com três composições internas (ver II.1.4 d)).

c) Seja $M = \{\nabla, \spadesuit, \heartsuit, \clubsuit\}$ e $\top_1, \top_2 \in M^{M\times M}$ definidas por

$\top_1$	∇	$\spadesuit$	$\heartsuit$	$\clubsuit$
∇	∇	$\spadesuit$	∇	$\heartsuit$
$\spadesuit$	$\heartsuit$	∇	$\spadesuit$	$\clubsuit$
$\heartsuit$	$\spadesuit$	$\heartsuit$	$\clubsuit$	$\clubsuit$
$\clubsuit$	$\spadesuit$	$\clubsuit$	∇	$\heartsuit$

e

$\top_2$	∇	$\spadesuit$	$\heartsuit$	$\clubsuit$
∇	∇	$\clubsuit$	∇	$\spadesuit$
$\spadesuit$	$\spadesuit$	$\heartsuit$	$\clubsuit$	∇
$\heartsuit$	$\heartsuit$	∇	$\spadesuit$	$\clubsuit$
$\clubsuit$	$\spadesuit$	∇	$\clubsuit$	$\heartsuit$

.

Então

$$\big(\{\nabla, \spadesuit, \heartsuit, \clubsuit\}; \top_1, \top_2\big)$$

é uma estrutura algébrica com 2 composições internas.

d) $\big(I\!N; +\,,\, \cdot\,, \top\big)$ onde $a \top b = a^b \ \ \forall\, a, b \in I\!N$, é uma estrutura algébrica com 3 composições internas.

Como toda estrutura $\big(M; \top_1, \top_2\ , \ldots,\ \top_r\big)$ com r composições dá origem a r estruturas com uma composição

$$\big(M; \top_i\big) \qquad (i = 1, 2\,, \ldots,\ r)\ ,$$

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 $\big(M; \top_1, \top_2\ , \ldots,\ \top_r\big)$ *uma estrutura algébrica com* r *composições internas* $\top_1, \top_2\ , \ldots,\ \top_r \in M^{M\times M}$.

Seja $A \neq \emptyset$ *um conjunto. Então* M^A, *o conjunto de todas as aplicações de* A *em* M, *torna-se uma estrutura algébrica*

$$\big(M^A; \top_1^*, \top_2^*\ , \ldots,\ \top_r^*\big)$$

com r composições internas $\top_1^*, \top_2^*, \ldots, \top_r^* \in (M^A)^{M^A \times M^A}$, definindo-se para todos os $i = 1, 2, \ldots, r$ e todas as $\varphi, \psi \in M^A$, a função $\varphi \top_i^* \psi \in M^A$ por:

$$\left(\varphi \top_i^* \psi\right)(a) = \varphi(a) \top_i \psi(a) \quad \forall\, a \in A\,.$$

II.1.8 Exemplos.

a) Para $A = \{\nabla, \spadesuit, \heartsuit, \clubsuit\}$ e $(M; \top) = (\mathbb{Z}; +)$, a composição $+^*$ em $\mathbb{Z}^A$ é dada por

$$\left(\varphi +^* \psi\right)(a) = \varphi(a) + \psi(a) \quad \forall\, a \in \{\nabla, \spadesuit, \heartsuit, \clubsuit\}\,.$$

b) Para $A = \{1, 2, 3, \ldots, n\}$ e $(M; \top) = (\mathbb{R}; +)$, os elementos de $M^A = \mathbb{R}^n$ são os vetores n-dimensionais reais.
Se $\varphi = (x_1, x_2, x_3, \ldots, x_n)$ e $\psi = (y_1, y_2, y_3, \ldots, y_n)$ são dois vetores, sua composição $\varphi +^* \psi$, definida por

$$\left(\varphi +^* \psi\right)(a) = \varphi(a) + \psi(a) \quad \forall\, a \in A \quad \text{agora é}$$

$$\varphi +^* \psi = (x_1, x_2, x_3, \ldots, x_n) +^* (y_1, y_2, y_3, \ldots, y_n) =$$
$$= (x_1 + y_1,\ x_2 + y_2, x_3 + y_3, \ldots, x_n + y_n)\,.$$

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 $M = \{a_1, a_2, a_3, \ldots, a_m\}$ e a estrutura algébrica $(M; \top)$ definida pela tábua

$\top$	a_1	a_2	$\ldots$	a_i	$\ldots$	a_k	$\ldots$	a_m
a_1	$a_1 \top a_1$	$a_1 \top a_2$	$\ldots$	$a_1 \top a_i$	$\ldots$	$a_1 \top a_k$	$\ldots$	$a_1 \top a_m$
a_2	$a_2 \top a_2$	$a_2 \top a_2$	$\ldots$	$a_2 \top a_i$	$\ldots$	$a_2 \top a_k$	$\ldots$	$a_2 \top a_m$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
a_i	$a_i \top a_1$	$a_i \top a_2$	$\ldots$	$a_i \top a_i$	$\ldots$	$a_i \top a_k$	$\ldots$	$a_i \top a_m$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
a_k	$a_k \top a_1$	$a_k \top a_2$	$\ldots$	$a_k \top a_i$	$\ldots$	$a_k \top a_k$	$\ldots$	$a_k \top a_m$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
a_m	$a_m \top a_1$	$a_m \top a_2$	$\ldots$	$a_m \top a_i$	$\ldots$	$a_m \top a_k$	$\ldots$	$a_m \top a_m$

.

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 $i, k = 1, 2, \ldots, m$.

∎

II.1.11 Observação.

Num conjunto finito de m elementos $M = \{a_1, a_2, \ldots, a_m\}$, 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 $1 + 2 + 3 + \ldots + m = \frac{m(m+1)}{2}$.

∎

Centralizador e centro

Em geral, uma estrutura algébrica $\big(M ; \top \big)$ não é comutativa. Isto não impede que certos elementos nela sejam comutáveis.

II.1.12 Definição.

Seja $\big(M ; \top \big)$ uma estrutura algébrica e $\emptyset \neq X \subseteq M$. O conjunto

$$\mathbf{C}_M(X) = \big\{ c \in M \;\big|\; c \top x = x \top c \;\; \forall\, x \in X \big\}$$

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 $X = \big\{ x \big\}$ um conjunto unitário, temos

$$\mathbf{C}_M(x) = \mathbf{C}_M(\{x\}) = \big\{ c \in M \;\big|\; c \top x = x \top c \;\big\} \;,$$

o *centralizador de* x *em* M.

2) Para $X = M$ obtemos o *centro de* M :

$$\mathbf{Z}(M) = \mathbf{C}_M(M) = \big\{ c \in M \;\big|\; c \top x = x \top c \;\; \forall\, x \in M \big\}$$

Este é o conjunto dos elementos de M que comutam com todo elemento de M. Claro que $\big(M ; \top \big)$ é comutativa $\iff \mathbf{Z}(M) = M$.

$\blacksquare$

II.1.13 Proposição.

Seja $\big(M ; \top \big)$ *uma estrutura algébrica e* $\emptyset \neq X \subseteq Y \subseteq M$ *e* $x \in M$. *Então*

a) $x \in \mathbf{C}_M(x)$, *particularmente,* $\mathbf{C}_M(x) \neq \emptyset$.

b) $\mathbf{C}_M(Y) \subseteq \mathbf{C}_M(X)$.

c) $\mathbf{Z}(M) = \bigcap\limits_{X \subseteq M} \mathbf{C}_M(X) = \bigcap\limits_{x \in M} \mathbf{C}_M(x)$.

d) *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 contenências:

$$\mathbf{Z}(M) \subseteq \bigcap_{X\subseteq M} \mathbf{C}_M(X) \subseteq \bigcap_{\{x\}\subseteq M} \mathbf{C}_M(\{x\}) = \bigcap_{x\in M} \mathbf{C}_M(x) \subseteq \mathbf{Z}(M) \ .$$

Para a estrutura $\big(M\,;\top\big)$ com $M = \big\{a, b\big\}$ e $\top$ definida por:

$\top$	a	b
a	b	b
b	a	a

temos por exemplo $\mathbf{Z}(M) = \emptyset$.
Também para $\big(I\!N\,;\top\big)$, se $a \top b = a^b \ \forall\ a, b \in I\!N$, temos $\mathbf{Z}(I\!N) = \emptyset$.

■

II.1.14 Definição.

Seja $\big(M\,;\top\big)$ 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 $\big(M\,;\top\big)$ é uma estrutura *comutativa*, as noções de identidade (neutro) "à esquerda", "à direita" e "bilateral" são as mesmas.

II.1.15 Exemplos.

a) a_1) O número 1 é a identidade de $\big(\mathbb{N}\,;\,\cdot\,\big)$.

a_2) A estrutura $\big(\mathbb{N}\,;\,+\,\big)$ não possui elemento neutro $(0 \notin \mathbb{N}\ !)$

a_3) 1 é a única identidade à direita de $\big(\mathbb{N}\,;\,\top\big)$ se $a \top b = a^b \ \ \forall\, a,b \in \mathbb{N}$. $\big(\mathbb{N}\,;\,\top\big)$ não possui identidade bilateral.

a_4) 0 é a única identidade à direita de $\big(\mathbb{Z}\,;\,\top\big)$ se $a \top b = a-b \ \ \forall\, a,b \in \mathbb{Z}$. $\big(\mathbb{Z}\,;\,\top\big)$ não possui identidade bilateral.

a_5) 2 e -3 são as identidades à esquerda de $\big(\mathbb{Z}\,;\,\top\big)$, quando

$$a \top b = a^2b + ab - 5b \ \ \forall\, a,b \in \mathbb{Z} :$$

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 $M = \big\{\,\nabla, \spadesuit, \heartsuit, \clubsuit\,\big\}$.

b_1) 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* $\big(M\,;\,\top\big)$.

b_2) 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* $\big(M\,;\,\top\big)$.

b_3) 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* $\big(M\,;\top\big)$.

∎

II.1.16 Observação.

Seja $\big(M\,;\top\big)$ *uma estrutura algébrica,* $e' \in M$ *uma identidade à esquerda,* $e'' \in M$ *uma identidade à direita de* $\big(M\,;\top\big)$. *Então*

$$e' = e'' \quad \textit{é a identidade bilateral de } \big(M\,;\top\big)\ .$$

Particularmente, se $\big(M\,;\top\big)$ 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* $\big(M\,;\top\big)$ (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 $\big(M\,;\top\big)$ *uma estrutura algébrica com identidade bilateral* e, *digamos.*

$$\textit{Então} \quad e \in \mathbf{Z}(M)\ .$$

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 $\big(\, M \,;\, \top \,\big)$ 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 $\big(\, M \,;\, \top \,\big)$ é dito um *monóide*, se possuir uma identidade bilateral.

II.1.19 Exemplos.

a) $\big(\, I\!N \,;\, + \,\big)$ e $\big(\, I\!N \,;\, \cdot \,\big)$ são os semigrupos dos *números naturais aditivo* e dos *números naturais multiplicativo*.
Ambos estes semigrupos são comutativos. $\big(\, I\!N \,;\, \cdot \,\big)$ é um monóide.
$\big(\, I\!N \,;\, + \,\big)$ não possui identidade (lembrar: $0 \notin I\!N$).

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 $\big(\, M \,;\, \top \,\big)$ é um monóide comutativo. Sua identidade é $e = 5$.
Se substituirmos $M = (0, 5]$ pelo intervalo aberto $M' = (0, 5)$,
$\big(\, M' \,;\, \top \,\big)$ será um semigrupo comutativo sem identidade.

c) A estrutura algébrica $\big(\, I\!N \,;\, \top \,\big)$ com

$$a \top b = a^b \quad \forall\, a, b \in I\!N$$

não é um semigrupo.

d) A estrutura algébrica $\big(\, \mathbb{Z} \,;\, \top \,\big)$ 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

$$a \top (b \top c) = \frac{a \cdot \frac{bc}{5}}{5} = \frac{abc}{25} = \frac{\frac{ab}{5} \cdot c}{5} = (a \top b) \top c\ .$$

$e \top b = \dfrac{eb}{5} = b \ \ \forall\, b \in M$ significa $e = 5$. Isto mostra que o semigrupo $\big(\, M\, ; \top \,\big)$ é um monóide. Além disso, $\big(\, M'\, ; \top \,\big)$ 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

$$M = A^A, \quad \textit{o conjunto de todas as aplicações de } A \textit{ em si mesmo}\,.$$

Considerando-se para todas as $\psi, \varphi \in M$ a aplicação composta

$$\psi \circ \varphi\ ,$$

definida por $(\psi \circ \varphi)(a) = \psi\big(\varphi(a)\big) \quad \forall\ a \in A$, 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,

$$\big(\, A^A ; \circ \,\big) \ \textit{é uma estrutura algébrica com uma composição interna.}$$

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

$$\big(\, A^A ; \circ \,\big)$$

é um *semigrupo*. Além disso, $\delta_A \circ \varphi = \varphi \circ \delta_A = \varphi \quad \forall\, \varphi \in A^A$.
Logo, $\left(A^A ; \circ \right)$ possui a identidade δ_A e é portanto um monóide.

$\left(A^A ; \circ \right)$ chama-se o *monóide de todas as aplicações de A em A*.

II.1.21 Observação.

Para $|A| \geq 2$, o monóide

$$\left(A^A ; \circ \right) \quad \textit{não é comutativo} .$$

Demonstração: Seja, digamos, A decomposto como $A = \{a, b\} \cup X$ com $X = A \backslash \{a, b\}$, 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 $\qquad (\psi \circ \varphi)(a) = \psi\left(\varphi(a)\right) = \psi(a) = b$, porém

$$\left(\varphi \circ \psi\right)(a) = \varphi\left(\psi(a)\right) = \varphi(b) = a .$$

Portanto, $(\psi \circ \varphi)(a) \neq \left(\varphi \circ \psi\right)(a)$ e segue $\qquad \psi \circ \varphi \neq \varphi \circ \psi$.

∎

II.1.22 Exemplo.

Para os elementos φ, ψ do monóide $\left(I\!R^{I\!R} ; \circ \right)$ definidos por

$$\varphi(t) = \operatorname{sen} t \quad \text{e} \quad \psi(t) = t^2 \quad \forall\, t \in I\!R$$

temos

$$(\psi \circ \varphi)(t) = \psi\left(\varphi(t)\right) = (\operatorname{sen} t)^2 = \operatorname{sen}^2 t \text{ , porém}$$

$$\left(\varphi \circ \psi\right)(t) = \varphi\left(\psi(t)\right) = \operatorname{sen}(t^2) .$$

De fato vale para o centro do monóide $\left(A^A ; \circ \right)$:

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 $|A| = \left|A^A\right| = 1$. 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 $\psi(x) = x_0 \;\; \forall\, x \in A$, vemos

$$\big(\varphi \circ \psi\big)\,(x_0) = \varphi\,\big(\psi(x_0)\big) = \varphi(x_0) \neq x_0 \quad \text{porém} \quad (\psi \circ \varphi)(x_0) = \psi\,\big(\varphi(x_0)\big) = x_0\;.$$

Logo, $\big(\varphi \circ \psi\big)\,(x_0) \neq (\psi \circ \varphi)(x_0)$ e daí $\varphi \circ \psi \neq \psi \circ \varphi$. Portanto, $\varphi \notin \mathbf{Z}(A^A)$.

■

II.1.24 Proposição.

Seja $\big(\,M\,;\top\big)$ um semigrupo e $\emptyset \neq X \subseteq M$. Então $\mathbf{C}_M(X)$ é $\top$-fechado, i.e.

$$c_1\,, c_2 \in \mathbf{C}_M(X) \quad \Longrightarrow \quad c_1 \top c_2 \in \mathbf{C}_M(X)\;.$$

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, $\big(\,M\,;\top\big)$ 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 $\varphi, \psi, \omega \in I\!R^{I\!R}$, definidas por

$$\varphi(t) = t^2\;, \quad \psi(t) = \left|t^3\right| \quad \text{e} \quad \omega(t) = t^3 \quad \forall\, t \in I\!R\;,$$

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 $\left(I\!R^{I\!R} ; \circ \right)$ *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 $\left(M \, ; \top \right)$ 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 $\left(M \, ; \top \right)$ 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 $r \in \left(M \, ; \top \right)$ *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) $\big(\forall\, x, x' \in M :\ r \top x = r \top x' \implies x = x'\big) \iff$
$\iff \big(\forall\, x, x' \in M :\ \lambda_r(x) = \lambda_r(x') \implies x = x'\big)$
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 $M = \big\{\nabla, \spadesuit, \heartsuit, \clubsuit\big\}$ 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 $\big(\mathbb{N}\,;\top\big)$ 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 $\big(\, M\,;\top\,\big)$ *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 concluimos $r_2 \top x = r_2 \top x'$. 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 $\big(\, M\,;\top\,\big)$ 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.

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 $\big(M\,;\top \big)$ *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 conseqüência de a) e b).

∎

II.1.34 Observação.

Seja $\big(M\,;\top \big)$ *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 $\big(M\,;\top \big)$ *um monóide,* e *sua identidade e seja* $u \in M$. *Sejam* λ_u, ξ_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) " $\Longrightarrow$ ": 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 $\xi_u \in \mathbf{Sob}(M,M)$.

" $\Longleftarrow$ ": 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) $\big(\mathbb{Z}\,;\cdot \big)$ temos

$$\mathbf{R}(\mathbb{Z}) = \mathbb{Z}\backslash\{0\} \quad \text{enquanto} \quad \mathbf{U}(\mathbb{Z}) = \{1,-1\} \ .$$

II.1.37 Proposição.

Seja $A \neq \emptyset$ *um conjunto. No monóide* $\big(A^A\,;\circ \big)$ *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 $\big(M\,;\top\big)$ um monóide, e sua identidade. Então os conjuntos

$$\mathbf{U}'(M), \quad \mathbf{U}''(M) \quad e \quad \mathbf{U}(M)$$

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*

$$\widehat{u_1 \top u_2} = \hat{u}_2 \top \hat{u}_1 \ .$$

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

$$(y_2 \top y_1) \top (u_1 \top u_2) \ = \ y_2 \top (y_1 \top u_1) \top u_2 \ =$$
$$= (y_2 \top e) \top u_2 \ = \ y_2 \top u_2 \ = \ e \ .$$

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 conseqüência de a) e b).

■

II.1.39 Definição.

Um monóide $\big(\,M\,;\,\top\,\big)$ 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 $\big(\,M\,;\,\top\,\big)$ *temos que*

$$\big(\,\mathbf{U}(M)\,;\,\top\,\big) \quad \textit{é um grupo.}$$

II.1.41 Exemplos.

a) Para todo conjunto $A \neq \emptyset$, temos que

$$\big(\,\mathbf{U}(A^A)\,;\,\circ\,\big) = \big(\,\mathbf{S}_A\,;\,\circ\,\big) \quad \text{é um grupo.}$$

b) Para o monóide $\big(\,\mathbb{Z}\,;\,\cdot\,\big)$, temos que

$$\big(\,\mathbf{U}(\mathbb{Z})\,;\,\cdot\,\big) = \big(\,\{1,-1\}\,;\,\cdot\,\big) \quad \text{é um grupo.}$$

II.1.42 Definição.

Se $A \neq \emptyset$ é um conjunto, o grupo

$$\big(\,\mathbf{S}_A\,;\,\circ\,\big)$$

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 $\big(\,M\,;\,\top\,\big)$ é dito *comutativo* ou *abeliano* se

$$a \top b = b \top a \qquad \forall\ a, b \in M$$

(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.

$$(\mathbf{P}\,;\,\cdot\,) \quad \text{é um grupo abeliano .}$$

c) Se $i = \sqrt{-1}$ indica uma solução (formal) da equação $x^2 + 1 = 0$, temos que

$$(\{1, -1, i, -i\}\,;\,\cdot\,) \quad \text{é um grupo abeliano,}$$

Sua tábua 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 $\left(M\,;\, \top_1, \top_2 \,, \ldots, \top_r \right)$ uma estrutura algébrica com r composições internas $\top_1, \top_2 \,, \ldots, \top_r \in M^{M\times M}$. Um subconjunto $S \subseteq M$ chama-se

uma *subestrutura de* $\left(M\,;\, \top_1, \top_2 \,, \ldots, \top_r \right)$, se

i) $S \neq \emptyset$

ii) Para todos os $a, b \in S$ temos

$$a \top_1 b \in S, \quad a \top_2 b \in S \quad , \ldots, \; a \top_r b \in S \,.$$

Abreviado:

$$a \top_i b \in S \qquad \forall\, a, b \in S \qquad \forall\, i = 1, 2 \,, \ldots, r$$

Isto significa portanto que S é fechado com respeito às composições internas definidas em M.

Indicamos isto por

$$\left(S\,;\, \top_1, \top_2 \,, \ldots, \top_r \right) \leq \left(M\,;\, \top_1, \top_2 \,, \ldots, \top_r \right) \,,$$

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 $\top$ em M:

$$\left(S\,;\, \top \right) \leq \left(M\,;\, \top \right) \iff a \top b \in S \quad \forall\, a, b \in S \,.$$

Se $\left(M\,;\, \top \right)$ é um semigrupo, uma subestrutura $\left(S\,;\, \top \right) \leq \left(M\,;\, \top \right)$ chama-se também um *sub-semigrupo* de M.

II.2.2 Exemplos.

a) Para $\left(\mathbb{Z}\,;\, + \,,\, \cdot \right)$ temos que

a_1) $\left(\mathbb{N}\,;\, + \,,\, \cdot \right) \leq \left(\mathbb{Z}\,;\, + \,,\, \cdot \right)$

a$_2$) Para $S = \{-10, -11, -12, -13\,, \ldots\}$ temos $\big(S\,; + \big) \ \leq \ \big(\mathbb{Z}\,; + \big)$

a$_3$) $S = \{\ldots, -5, -3, -1, 1, 3, 5\,, \ldots\}$, o subconjunto dos números ímpares de $\mathbb{Z}$; é uma subestrutura de $\big(\mathbb{Z}\,; \cdot \big)$, porém, não é uma subestrutura de $\big(\mathbb{Z}\,; + \big)$.

b) O conjunto $\mathbb{P} = \{2, 3, 5, 7, 11\,, \ldots\}$, dos números primos, não é uma subestrutura, nem de $\big(\mathbb{N}\,; + \big)$ nem de $\big(\mathbb{N}\,; \cdot \big)$.

c) Se a estrutura $\big(M\,; \top \big)$ possuir um elemento neutro bilateral, digamos e, então

$$\big(\{e\}; \top \big) \quad \text{é uma subestrutura de } \big(M\,; \top \big).$$

■

II.2.3 Proposição.

Seja $\big(M\,; \top \big)$ *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* $\big(M\,; \top \big)$:

$$\big(\mathbf{R}'(M); \top \big) \leq \big(M\,; \top \big)\ , \qquad \big(\mathbf{R}''(M); \top \big) \leq \big(M\,; \top \big)\ ,$$
$$\big(\mathbf{R}(M); \top \big) \leq \big(M\,; \top \big)\ .$$

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* $\big(M\,; \top \big)$ *com*

$$\mathbf{U}'(M) \subseteq \mathbf{R}'(M), \quad \mathbf{U}''(M) \subseteq \mathbf{R}''(M), \qquad \mathbf{U}(M) \subseteq \mathbf{R}(M)\ ,$$

i.e.

$$\big(\mathbf{U}'(M); \top \big) \leq \big(\mathbf{R}'(M); \top \big) \leq \big(M\,; \top \big)\ ,$$
$$\big(\mathbf{U}''(M); \top \big) \leq \big(\mathbf{R}''(M); \top \big) \leq \big(M\,; \top \big)\ ,$$
$$\big(\mathbf{U}(M); \top \big) \leq \big(\mathbf{R}(M); \top \big) \leq \big(M\,; \top \big)\ .$$

c) *Para qualquer conjunto* $\emptyset \neq X \subseteq M$ *temos que os centralizadores*

$$\mathbf{C}_M(X) \quad \text{são subestruturas de } M, \text{ i.e. } \big(\mathbf{C}_M(X); \top \big) \leq \big(M\,; \top \big)$$

Demonstração: Ver II.1.31, II.1.33 e II.1.38

■

II.2.4 Observação.

Seja $\big(M\,;\, \top_1, \top_2\ ,\dots,\ \top_r \big)$ *uma estrutura algébrica com* r *composições internas. Seja* $\mathfrak{S} \subseteq \mathbf{2}^M$ *uma família de subestruturas de* M *tal que* $\bigcap\limits_{S\in\mathfrak{S}} S \neq \emptyset$. *Então*

$$\bigcap_{S\in\mathfrak{S}} S \quad \text{\textit{é uma subestrutura de} } M\ .$$

$\bigcap\limits_{S\in\mathfrak{S}} S$ *é a* **maior** *subestrutura de* M, *contida em todas as* $S \in \mathfrak{S}$.

Demonstração: Por hipótese temos $\bigcap\limits_{S\in\mathfrak{S}} S \neq \emptyset$. Sejam $a, b \in \bigcap\limits_{S\in\mathfrak{S}} S$. Isto significa $a, b \in S \quad \forall\ S \in \mathfrak{S}$. Segue $a \top_i b \in S \quad \forall\ S \in \mathfrak{S}$ e todos os $i = 1, 2\ ,\dots, r$. Mas então $a \top_i b \in \bigcap\limits_{S\in\mathfrak{S}} S \quad \forall\, i = 1, 2\ ,\dots, r$. Logo,

$$\bigcap_{S\in\mathfrak{S}} S \leq M\ .$$

■

II.2.5 Definição.

Seja $\big(M\,;\, \top_1, \top_2\ ,\dots,\ \top_r \big)$ 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 $\big(M\,;\, \top_1, \top_2\ ,\dots,\ \top_r \big)$ **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 $\big(M\,;\, \top_1, \top_2\ ,\dots,\ \top_r \big)$ 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* $\left(M\,;\, \top_1, \top_2\,, \ldots, \top_r \right)$.

II.2.6 Exemplo.

a) A subestrutura de $\left(I\!N\,;\, + \right)$ gerada pelo conjunto $X = \{6, 15\}$ é

$$\langle X \rangle = \{6, 12, 15, 18, 21, 24, 27, 30\,, \ldots\} = \{6k + 15\ell > 0 \mid k, \ell \in I\!N_0\}\ .$$

b) $\langle I\!P \rangle = \left(I\!N\,;\, \cdot \right)$, i.e. o conjunto dos números primos $X = I\!P$ é um sistema de geradores para o monóide múltiplicativo $I\!N$ dos números naturais.

Demonstração: a) Ponhamos $E = \{6k + 15\ell > 0 \mid k, \ell \in I\!N_0\}$. 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 $k, \ell \in I\!N_0$. 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.

$\blacksquare$

Relações de congruência e estruturas quocientes

II.2.7 Definição.

Seja $\left(M\,;\, \top_1, \top_2\,, \ldots, \top_r \right)$ uma estrutura algébrica. Uma relação de equivalência $\kappa \in \mathbf{Eq}(M)$ chama-se uma

relação de congruência da estrutura $\left(M\,;\, \top_1, \top_2\,, \ldots, \top_r \right)$,

se para todos os $a, a', b, b' \in M$ tivermos as seguintes compatibilidades de κ com as composições $\top_1, \top_2\,, \ldots, \top_r$:

$$\text{Se} \quad \begin{cases} a\ \kappa\ a' \\ b\ \kappa\ b' \end{cases} \quad \text{então} \quad \begin{cases} a \top_1 b & \kappa & a' \top_1 b'\,, \\ a \top_2 b & \kappa & a' \top_2 b'\,, \\ \vdots & \vdots & \vdots \\ a \top_r b & \kappa & a' \top_r b'\,. \end{cases}$$

Mais abreviadamente:

$$\begin{cases} a\ \kappa\ a' \\ b\ \kappa\ b' \end{cases} \quad \Longrightarrow \quad a \top_i b \quad \kappa \quad a' \top_i b' \qquad\qquad \forall\, i = 1, 2\ , \ldots , r\ .$$

Por

$$\mathbf{Cg}\big(\, M\, ;\ \top_1\ , \ldots , \top_r\, \big)$$

indicamos o *conjunto de todas as relações de congruência* da estrutura algébrica $\big(\, M\, ; \top_1\ , \ldots , \top_r\, \big)$. Assim temos

$$\mathbf{Cg}\big(\, M\, ;\ \top_1\ , \ldots , \top_r\, \big) \subseteq \mathbf{Eq}(M)\ .$$

Para uma relação de congruência κ temos portanto:

Se	$a\ \ \kappa\ \ a'$
e	$b\ \ \kappa\ \ b'$
então	$a \top_i b\ \ \kappa\ \ a' \top_i b' \qquad \forall\, i = 1, 2\ , \ldots , r\ .$

Isto significa que duas congruências modulo κ podemos $\top_i$-compor verticalmente, sem destruir a κ-equivalência do resultado - como se as congruências fossem duas igualdades.

Claro que temos

$$\mathbf{Cg}\big(\, M\, ;\ \top_1 , \top_2\ , \ldots , \top_r\, \big) = \bigcap_{i=1}^{r} \mathbf{Cg}\big(\, M\, ;\ \top_i\, \big)\ .$$

II.2.8 Exemplo.

Para toda estrutura algébrica $\big(\, M\, ; \top_1 , \top_2\ , \ldots , \top_r\, \big)$ temos

$$\delta_M \in \mathbf{Cg}\big(\, M\, ;\ \top_1 , \top_2\ , \ldots , \top_r\, \big) \quad \text{e} \quad M \times M \in \mathbf{Cg}\big(\, M\, ;\ \top_1 , \top_2\ , \ldots , \top_r\, \big)\ ,$$

i.e. tanto a relação da igualdade como a relação universal em M são exemplos de relações de congruência. Particularmente,

$$\mathbf{Cg}\big(\, M\, ;\ \top_1 , \top_2\ , \ldots , \top_r\, \big) \neq \emptyset\ .$$

II.2.9 Exemplos.

Seja $\big(\, M\, ; \top_1 , \top_2\, \big) = \big(\, \mathbb{Z}\, ; +\ ,\ \cdot\, \big)$.

a) *Para as relações de equivalência* $\equiv_n$ (ver I.1.26) *vale de fato*

$$\equiv_n \in \mathbf{Cg}\big(\,\mathbb{Z}\,;\ +\,,\ \cdot\,\big) = \mathbf{Cg}\big(\,\mathbb{Z}\,;\ +\,\big) \cap \mathbf{Cg}\big(\,\mathbb{Z}\,;\ \cdot\,\big)\ .$$

b) *Seja* $\varepsilon \in \mathbf{Eq}(\mathbb{Z})$ *definida pela partição*

$$\mathfrak{P}_\varepsilon = \big\{\{x \in \mathbb{Z} \mid x \geq 0\}\ ,\ \{x \in \mathbb{Z} \mid x < 0\}\ \big\}\ .$$

Então $\varepsilon \notin \mathbf{Cg}\big(\,\mathbb{Z}\,;\ +\,\big)$.

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, $\equiv_n \in \mathbf{Cg}\big(\,\mathbb{Z}\,;\ +\,\big)$.

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, $\equiv_n \in \mathbf{Cg}\big(\,\mathbb{Z}\,;\ \cdot\,\big)$.

Assim, $\equiv_n \in \mathbf{Cg}\big(\,\mathbb{Z}\,;\ +\,\big) \cap \mathbf{Cg}\big(\,\mathbb{Z}\,;\ \cdot\,\big) = \mathbf{Cg}\big(\,\mathbb{Z}\,;\ +\,,\ \cdot\,\big)$.

b) Temos por exemplo $\begin{cases} -8 \ \ \varepsilon \ -2 \\ \ \ 6 \ \ \varepsilon \ \ 3 \end{cases}$. Porém $-2 = -8 + 6 \quad \not\varepsilon \quad -2 + 3 = 1$.

Logo, esta $\varepsilon \in \mathbf{Eq}(\mathbb{Z})$ não é compatível com a adição em $\mathbb{Z}$.

∎

As relações de congruência da estrutura algébrica $\big(\,\mathbb{Z}\,;+\,\big)$ podem ser completamente descritas. De fato, não existem outras além das $\equiv_n$:

II.2.10 Teorema.

$$\mathbf{Cg}\big(\,\mathbb{Z}\,;\ +\,\big) \ = \ \big\{\equiv_n \,\big|\, n = 0, 1, 2, 3\,, \ldots\big\}\ ,$$

i.e. as relações de congruência de $\big(\,\mathbb{Z}\,;+\,\big)$ *são exatamente as congruências* mod n.

(O mesmo vale a forteriori para $\mathbf{Cg}\big(\,\mathbb{Z}\,;\ +\,,\ \cdot\,\big)$)

Demonstração: Sabemos $\big\{\equiv_n \,\big|\, n = 0, 1, 2, 3\,, \ldots\big\} \subseteq \mathbf{Cg}\big(\,\mathbb{Z}\,;\ +\,\big)$, devido a II.2.9 a).

Seja dado uma qualquer $\kappa \in \mathbf{Cg}\big(\mathbb{Z};\ +\big)$. 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 $\begin{cases} a-b\ \kappa\ 0 \\ \quad b\ \ \kappa\ \ b \end{cases}$, 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 $0 \mod \kappa$:

2) Para todo $x \in \bar{0}$ temos também $-x \in \bar{0}$: De fato: De $\begin{cases} \ \ x\ \ \kappa\ \ 0 \\ -x\ \kappa\ -x \end{cases}$ concluimos $x + (-x)\ \kappa\ 0 + (-x)$, ou seja, $0\ \ \kappa\ -x$. Isto significa que, se $\bar{0} \neq \{0\}$, então $\bar{0}$ contém algum número natural: $\bar{0}\ \cap\ I\!N \neq \emptyset$.

Caso I: Se $\bar{0} = \{0\}$, vamos ter $\kappa = \delta_{\mathbb{Z}} =\ \equiv_0$.

Caso II: Neste caso, $\bar{0}\ \cap\ I\!N \neq \emptyset$. 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

$$kn = \pm n \pm n \pm \ldots \pm n\ \ \kappa\ \ 0 + 0 +\ \ldots\ + 0 = 0\ . \quad \text{Logo,}$$

$$\bar{0} \supseteq \{\ kn \mid k \in \mathbb{Z}\}\ .$$

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 $\begin{cases} \quad x\ \kappa\ 0 \\ -kn\ \kappa\ 0 \end{cases}$ e segue $r = x - kn\ \ \kappa\ \ 0 + 0 = 0$. Logo, $r \in \bar{0}$ com $0 \le r < n$. Como n foi escolhido como número natural *mínimo* em $\bar{0}$, concluimos $r = 0$ 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 $\big(M\,;\, \top_1, \top_2, \ldots, \top_r\big)$ *uma estrutura algébrica com* r *composições internas. Seja* $\kappa \in \mathbf{Cg}\big(M\,;\, \top_1, \ldots, \top_r\big)$ *e considere o conjunto quociente* M/κ*. Definindo-se para todos os* $\bar{a}, \bar{b} \in M/\kappa$ *e todos os* $i = 1, 2, \ldots, r$:

$$\bar{a}\ \bar{\top}_i\ \bar{b} = \overline{a \top_i b}\ ,$$

temos que $\bar{\top}_1, \bar{\top}_2, \ldots, \bar{\top}_r$ *são composições internas bem definidas no conjunto quociente* M/κ*.*

A estrutura algébrica

$$\big(M/\kappa;\ \bar{\top}_1,\ \bar{\top}_2, \ldots,\ \bar{\top}_r\big)$$

chama-se a *estrutura quociente* $M \mod \kappa$*.*

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, concluimos $a \top_i b\ \ \kappa\ \ a' \top_i b'$. Segue

$$\bar{a'}\ \bar{\top}_i\ \bar{b'} = \overline{a' \top_i b'} = \overline{a \top_i b} = \bar{a}\ \bar{\top}_i\ \bar{b}\ .$$

Portanto, a definição de $\bar{\top}_i$ independe da escolha do representante das classes de equivalência. Assim, $\bar{\top}_i \in (M/\kappa)^{M/\kappa \times M/\kappa}$ são composições internas bem definidas de M/κ.

■

II.2.12 Exemplo.

Para a estrutura $\big(\mathbb{Z}\,;\, +\,,\ \cdot\big)$ e qualquer uma das $\equiv_n \in \mathbf{Cg}\big(\mathbb{Z}\,;\ +\,,\ \cdot\big)$ temos a estrutura quociente

$$\big(\mathbb{Z}/\!\equiv_n;\ \bar{+}\,,\ \bar{\cdot}\,\big) = \big(\{\bar{a} \mid a \in \mathbb{Z}\};\ \bar{+}\,,\ \bar{\cdot}\,\big)\ ,$$

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

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$

$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{2}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Homomorfismos e Isomorfismos

II.2.13 Definição.

Sejam $\big(M\,;\top_1,\top_2\,,\ldots,\top_r\big)$ e $\big(N\,;\perp_1,\perp_2\,,\ldots,\perp_r\big)$ duas estruturas algébricas com r composições internas, cada:

$$\top_1,\top_2\,,\ldots,\top_r \in M^{M\times M} \quad \text{e} \quad \perp_1,\perp_2\,,\ldots,\perp_r \in N^{N\times N}$$

(a composição interna $\perp$ é lida: "bot"). Uma aplicação $\varphi \in N^M$ é denominada

um *homomorfismo de* $\big(M\,;\top_1,\top_2\,,\ldots,\top_r\big)$ *em* $\big(N\,;\perp_1,\perp_2\,,\ldots,\perp_r\big)$,

se para todos os $a, b \in M$ tivermos

$$\begin{aligned} \varphi(a \top_1 b) &= \varphi(a) \perp_1 \varphi(b), \\ \varphi(a \top_2 b) &= \varphi(a) \perp_2 \varphi(b), \\ &\cdots\cdots \\ \varphi(a \top_r b) &= \varphi(a) \perp_r \varphi(b) \,. \end{aligned}$$

Mais conciso:

$$\varphi(a \top_i b) = \varphi(a) \perp_i \varphi(b), \quad \forall\, i = 1, 2\ , \ldots , r, \quad \forall\, a, b \in M\ .$$

II.2.14 Exemplos.

a) Para $\big(M\,;\top \big) = \big(I\!N\,;+ \big)$ e $\big(N\,;\perp \big) = \big(I\!N\,;\cdot \big)$ temos:
A aplicação $\varphi \in I\!N^{I\!N}$ com $\varphi(a) = 2^a \quad \forall\, a \in I\!N$ é um homomorfismo.

b) Para $\big(M\,;\top \big) = \big(Z\!\!\!Z\,;+ \big)$ e $\big(N\,;\perp \big) = \big(\{1,-1\}\,;\cdot \big)$ temos: A aplicação $\varphi \in \{1,-1\}^{Z\!\!\!Z}$ com $\varphi(a) = (-1)^a \quad \forall\, a \in Z\!\!\!Z$ é um homomorfismo.

II.2.15 Definição.

Um homomorfismo φ da estrutura algébrica $\big(M\,;\top_1, \top_2\ , \ldots , \top_r \big)$ na estrutura algébrica $\big(N\,;\perp_1, \perp_2\ , \ldots , \perp_r \big)$ 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* $\big(M\,;\top_1, \top_2\ , \ldots , \top_r \big)$, se
$M = N$ e $\top_1 = \perp_1,\ \ \top_2 = \perp_2\ , \ldots , \top_r = \perp_r$.

v) um *automorfismo de* $\big(M\,;\top_1, \top_2\ , \ldots , \top_r \big)$, se φ é um endomorfismo bijetor ($=$ um isomorfismo de $\big(M\,;\top_1, \top_2\ , \ldots , \top_r \big)$ sobre si mesmo).

II.2.16 Exemplos.

a) Sejam $\big(M\,;\top \big) = \big(I\!N\,;\cdot \big)$ e $\big(N\,;\perp \big) = \big(I\!R\,;+ \big)$. A aplicação $\varphi \in I\!R^{I\!N}$ definida por

$$\varphi(x) = \lg x \qquad \forall\, x \in I\!N\ ,$$

é um monomorfismo que não é epimorfismo.

b) Sejam $\big(M\,;\top \big) = \big(Z\!\!\!Z\,;\cdot \big)$ e $\big(N\,;\perp \big) = \big(I\!N_0\,;\cdot \big)$. A aplicação $\varphi \in I\!N_0^{Z\!\!\!Z}$ definida por

$$\varphi(x) = |x| \qquad \forall\, x \in Z\!\!\!Z\ ,$$

é um epimorfismo mas não é monomorfismo.

c) Sejam $\big(M\,;\top\big)=\big(I\!R;+\big)$ e $\big(N\,;\perp\big)=(\mathbf{P};\,\cdot\,)$ onde
$$\mathbf{P}=\{x\in I\!R \mid x>0\}.$$
A aplicação $\varphi\in\mathbf{P}^{I\!R}$ definida por

$$\varphi(x)=10^x \qquad \forall\, x\in I\!R\ ,$$

é um isomorfismo.

d) A aplicação $\varphi\in Z\!\!\!Z^{Z\!\!\!Z}$ definida por

$$\varphi(x)=2x \qquad \forall\, x\in Z\!\!\!Z\ ,$$

é um endomorfismo injetor de $\big(Z\!\!\!Z\,;+\big)$, mas não é um automorfismo.

e) A aplicação $\varphi\in Z\!\!\!Z^{Z\!\!\!Z}$ definida por

$$\varphi(x)=-x \qquad \forall\, x\in Z\!\!\!Z\ ,$$

é um automorfismo de $\big(Z\!\!\!Z\,;+\big)$.

f) Seja $\big(M\,;\top\big)=\big(I\!R;\,\cdot\,\big)$. A aplicação $\varphi\in I\!R^{I\!R}$, definida por

$$\varphi(x)=x^3 \qquad \forall\, x\in I\!R\ ,$$

é um automorfismo de $\big(M\,;\top\big)$.

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

$$\varphi(x)=\frac{x^2}{4} \qquad \forall\, x\in M\ ,$$

é um automorfismo de $\big(M\,;\top\big)$, pois $\forall\, a,b\in M$:

$$\varphi(a\top b)=\tfrac{(a\top b)^2}{4}=\frac{\left(\frac{ab}{4}\right)^2}{4}=\tfrac{(ab)^2}{64}=$$
$$=\frac{\frac{a^2}{4}\cdot\frac{b^2}{4}}{4}=\frac{\varphi(a)\cdot\varphi(b)}{4}=\varphi(a)\top\varphi(b)\ .$$

■

II.2.17 Observação.

Sejam $\left(M;\top_1,\top_2,\ldots,\top_r\right)$, $\left(N;\perp_1,\perp_2,\ldots,\perp_r\right)$ *e* $\left(P;*_1,*_2,\ldots,*_r\right)$ *três estruturas algébricas com* r *composições internas, cada. Sejam* $\varphi\in N^M$ *e* $\psi\in P^N$ *homomorfismos. Então a aplicação composta*

$$\psi\circ\varphi \quad \textit{é um homomorfismo de } M \textit{ em } P.$$

Demonstração: Temos para todos os $a,b\in M$ e todos os $i=1,2,\ldots,r$:

$$(\psi\circ\varphi)(a\top_i b)=\psi\big(\varphi(a\top_i b)\big)=\psi\big(\varphi(a)\perp_i\varphi(b)\big)=$$

$$=\psi\big(\varphi(a)\big)\ *_i\ \psi\big(\varphi(b)\big)=(\psi\circ\varphi)(a)\ *_i\ (\psi\circ\varphi)(b)\,.$$

∎

II.2.18 Observação.

Sejam $\left(M;\top_1,\top_2,\ldots,\top_r\right)$ *e* $\left(N;\perp_1,\perp_2,\ldots,\perp_r\right)$ *duas estruturas algébricas com* r *composições internas, cada.*

$$\begin{gathered}\textit{Se } \varphi: M\longrightarrow N \textit{ é um isomorfismo de}\\ \left(M;\top_1,\top_2,\ldots,\top_r\right) \textit{ sobre } \left(N;\perp_1,\perp_2,\ldots,\perp_r\right), \textit{ então}\\ \varphi^{-1}: N\longrightarrow M \textit{ é um isomorfismo de}\\ \left(N;\perp_1,\perp_2,\ldots,\perp_r\right) \textit{ sobre } \left(M;\top_1,\top_2,\ldots,\top_r\right).\end{gathered}$$

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 $i=1,2,\ldots,r$:

$$\varphi^{-1}(c\perp_i c')=\varphi^{-1}\big(\varphi(a)\perp_i\varphi(a')\big)=\varphi^{-1}\big(\varphi(a\top_i a')\big)=$$

$$=a\top_i a'=\varphi^{-1}(c)\top_i\varphi^{-1}(c')\,.$$

∎

II.2.19 Definição.

Duas estruturas $\left(M;\top_1,\top_2,\ldots,\top_r\right)$ e $\left(N;\perp_1,\perp_2,\ldots,\perp_r\right)$ chamam-se *isomorfas*, denotado por

$$\left(M;\top_1,\top_2,\ldots,\top_r\right)\cong\left(N;\perp_1,\perp_2,\ldots,\perp_r\right)\ ,$$

se existe um isomorfismo de $\big(M\,;\, \top_1\,,\, \top_2\,,\ldots,\, \top_r\,\big)$ sobre $\big(N\,;\, \perp_1\,,\, \perp_2\,,\ldots,\, \perp_r\,\big)$.

II.2.20 Exemplos.

a) Seja $\mathbf{P} = \{x \in I\!R \mid x > 0\}$. Temos

$$\big(I\!R;\, + \big) \cong (\mathbf{P};\, \cdot\,)\,.$$

Para $0 < a \in I\!R,\ a \neq 1,$ as aplicações $\varphi_a \in \mathbf{P}^{I\!R}$ com

$$\varphi_a(x) = a^x \quad \forall\, x \in I\!R$$

são isomorfismos de $\big(I\!R;\, + \big)$ sobre $(\mathbf{P};\, \cdot\,)$.
Suas inversas $\varphi_a^{-1} \in I\!R^{\mathbf{P}}$ 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

$$\big(M\,;\, \top \big) \quad \text{e} \quad \big(N\,;\, \perp \big)\,,$$

definidas pelas composições internas

$$a \top b = \tfrac{ab}{5} \quad \forall\, a,b \in M \qquad \text{e} \qquad a \perp b = \tfrac{ab}{7} \quad \forall\, a,b \in N$$

são dois monóides. A aplicação

$$\varphi \in N^M \quad \text{definida por } \varphi(x) = \tfrac{7}{5}x \quad \forall\, x \in M$$

é um isomorfismo de $\big(M\,;\, \top \big)$ sobre $\big(N\,;\, \perp \big)$. Portanto

$$\big(M\,;\, \top \big) \cong \big(N\,;\, \perp \big)\,.$$

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 $\big(M\,;\, \top_1\,,\, \top_2\,,\ldots,\, \top_r\,\big)$, $\big(N\,;\, \perp_1\,,\, \perp_2\,,\ldots,\, \perp_r\,\big)$ *e* $\big(P\,;\, *_1, *_2\,,\ldots,\, *_r\,\big)$ *três estruturas algébricas com* r *composições internas, cada.*

a) *Sempre* $\big(M\,;\, \top_1\,,\, \top_2\,,\ldots,\, \top_r\,\big) \cong \big(M\,;\, \top_1\,,\, \top_2\,,\ldots,\, \top_r\,\big)$.

b) *Se* $\big(\, M\,;\, \top_1\,,\, \top_2\,, \ldots\,,\, \top_r\,\big) \cong \big(\, N\,;\, \perp_1\,,\, \perp_2\,, \ldots\,,\, \perp_r\,\big)$,
então $\big(\, N\,;\, \perp_1\,,\, \perp_2\,, \ldots\,,\, \perp_r\,\big) \cong \big(\, M\,;\, \top_1\,,\, \top_2\,, \ldots\,,\, \top_r\,\big)$.

c) *Se* $\big(\, M\,;\, \top_1\,,\, \top_2\,, \ldots\,,\, \top_r\,\big) \cong \big(\, N\,;\, \perp_1\,,\, \perp_2\,, \ldots\,,\, \perp_r\,\big)$ *e*
$\big(\, N\,;\, \perp_1\,,\, \perp_2\,, \ldots\,,\, \perp_r\,\big) \cong \big(\, P\,;\, *_1, *_2\,, \ldots\,,\, *_r\,\big)$,
então $\big(\, M\,;\, \top_1\,,\, \top_2\,, \ldots\,,\, \top_r\,\big) \cong \big(\, P\,;\, *_1, *_2\,, \ldots\,,\, *_r\,\big)$.

Demonstração: a) segue, pois a aplicação identica δ_M é um isomorfismo de $\big(\, M\,;\, \top_1\,,\, \top_2\,, \ldots\,,\, \top_r\,\big)$ sobre si mesma.
b) Se φ é um isomorfismo de $\big(\, M\,;\, \top_1\,,\, \top_2\,, \ldots\,,\, \top_r\,\big)$ sobre $\big(\, N\,;\, \perp_1\,,\, \perp_2\,, \ldots\,,\, \perp_r\,\big)$, então φ^{-1} é um isomorfismo de $\big(\, N\,;\, \perp_1\,,\, \perp_2\,, \ldots\,,\, \perp_r\,\big)$ sobre $\big(\, M\,;\, \top_1\,,\, \top_2\,, \ldots\,,\, \top_r\,\big)$
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

isomorfia 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 $\big(\, M\,;\, \top_1\,,\, \top_2\,, \ldots\,,\, \top_r\,\big) \cong \big(\, N\,;\, \perp_1\,,\, \perp_2\,, \ldots\,,\, \perp_r\,\big)$ são duas estruturas isomorfas, então, particularmente os conjuntos $M \sim N$ são equipotentes.
Também podemos pensar ao contrário:
Numa estrutura algébrica $\big(\, M\,;\, \top_1\,,\, \top_2\,, \ldots\,,\, \top_r\,\big)$ podemos substutuir o conjunto M por qualquer conjunto equipotente, como mostra

II.2.22 Proposição.

Seja $\big(\, M\,;\, \top_1\,,\, \top_2\,, \ldots\,,\, \top_r\,\big)$ *uma estrutura algébrica,* $N \sim M$ *um conjunto equipotente com* M *e seja* $\varphi \in \mathbf{Bij}\,(M,N)$.
Definindo-se composições internas $\perp_1\,,\, \perp_2\,, \ldots\,,\, \perp_r \in N^{N\times N}$ *por*

$$c \perp_i d = \varphi\left(\varphi^{-1}(c) \top_i \varphi^{-1}(d)\right) \quad \forall\; c, d \in N\;,$$

temos que

$$\big(\, N\,;\, \perp_1\,,\, \perp_2\,, \ldots\,,\, \perp_r\,\big)$$

é uma estrutura algébrica que é isomorfa com

$$\left(M\,;\, \top_1\,,\, \top_2\,,\, \ldots\,,\, \top_r \right)\ ,$$

sendo que a bijeção φ *dada torna-se um isomorfismo de* $\left(M\,;\, \top_1\,,\, \top_2\,,\, \ldots\,,\, \top_r \right)$ *sobre* $\left(N\,;\, \perp_1\,,\, \perp_2\,,\, \ldots\,,\, \perp_r \right)$.

Demonstração: Para todos os $a, b \in M$ e todos os $i = 1, 2, \ldots, r$ temos com esta definição das $\perp_1, \perp_2, \ldots, \perp_r$ de fato:

$$\varphi(a \top_i b) = \varphi\left(\varphi^{-1}\left(\varphi(a)\right) \top_i \varphi^{-1}\left(\varphi(b)\right)\right) = \varphi(a) \perp_i \varphi(b)\ .$$

∎

II.2.23 Exemplos.

a) Queremos definir uma composião interna $\perp$ no intervalo real $N = \left(-\frac{\pi}{2}, \frac{\pi}{2}\right)$ tal que

$$\left(N\,;\, \perp \right) \cong \left(\mathbb{R}\,;\, + \right)\ .$$

Tendo em vista que $\varphi \in N^{\mathbb{R}}$ com $\varphi(x) = \operatorname{arctg} x \quad \forall\ x \in \mathbb{R}$, é uma bijeção de $\mathbb{R}$ sobre N, definamos para todos os $c, d \in N$:

$$c \perp d = \operatorname{arctg}\left(\operatorname{tg}(c) + \operatorname{tg}(d)\right)\ .$$

Temos $\quad \forall\ a, b \in \mathbb{R}$:

$$\varphi(a+b) = \operatorname{arctg}(a+b) = \operatorname{arctg}\left(\operatorname{tg}\left(\operatorname{arctg}(a)\right) + \operatorname{tg}\left(\operatorname{arctg}(b)\right)\right) =$$

$$= \operatorname{arctg}(a) \perp \operatorname{arctg}(b) = \varphi(a) \perp \varphi(b)\ .$$

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 $\left(M\,;\, \top \right)$ 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 $\left(N\,;\, \perp \right)$ seja um monóide isomorfo com $\left(M\,;\, \top \right)$ e tal que $e_N = -8$ seja o elemento neutro de $\left(N\,;\, \perp \right)$.

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 $c, d \in N$:

$$\varphi\left(\varphi^{-1}(c) \top \varphi^{-1}(d)\right) = \varphi\left((-\tfrac{c}{4}+1) \top (-\tfrac{d}{4}+1)\right) =$$

$$= -4 \cdot \frac{\left(-\frac{c}{4}+1\right)\left(-\frac{d}{4}+1\right)}{3} + 4 = -\tfrac{cd}{12} + \tfrac{c}{3} + \tfrac{d}{3} + \tfrac{8}{3}\,.$$

Portanto, uma possível composição $\perp$ em $N = [-8, 4)$, tal que

$$\left(\, M\,;\, \top \right) \cong \left(\, N\,;\, \perp \right) \text{ com identidade } e_N = -8$$

é dada por

$$c \perp d = -\frac{cd}{12} + \frac{c}{3} + \frac{d}{3} + \frac{8}{3} \qquad \forall\; c, d \in N\;.$$

O TEOREMA GERAL DO HOMOMORFISMO E ESTRUTURAS SIMPLES

II.2.24 Teorema.

Seja $\left(\, M\,;\, \top_1, \top_2\;, \ldots, \top_r \right)$ *uma estrutura algébrica,* $\kappa \in \mathbf{Cg}\left(\, M\,;\; \top_1, \top_2\;, \ldots, \top_r \right)$ *e* $\left(\, M/\kappa;\; \bar{\top}_1,\; \bar{\top}_2\;, \ldots,\; \bar{\top}_r \right)$ *a estrutura quociente* $M \mod \kappa$.
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
$\left(\, M\,;\, \top_1, \top_2\;, \ldots, \top_r \right)$ sobre $\left(\, M/\kappa;\; \bar{\top}_1,\; \bar{\top}_2\;, \ldots,\; \bar{\top}_r \right)$.

Demonstração: É só preciso mostrar que γ é um homomorfismo. Isto segue, pois $\forall\; a, b \in M$ e todos os $i = 1, 2\;, \ldots, r$:

$$\gamma(a \top_i b) = \overline{a \top_i b} = \bar{a}\;\; \bar{\top}_i\; \bar{b} = \gamma(a)\;\; \bar{\top}_i\; \gamma(b)\;.$$

∎

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 $\big(\,M\,;\top_1,\top_2\,,\ldots,\top_r\,\big)$ *e* $\big(\,N\,;\perp_1,\perp_2\,,\ldots,\perp_r\,\big)$ *duas estruturas algébricas com* r *composições internas, cada.*
Seja φ *um homomorfismo de* $\big(\,M\,;\top_1,\top_2\,,\ldots,\top_r\,\big)$ *em* $\big(\,N\,;\perp_1,\perp_2\,,\ldots,\perp_r\,\big)$.
Seja κ_φ *a relação de equivalência associada ao* φ : $\forall\ a,a'\in M$:

$$a\ \kappa_\varphi\ a' \iff \varphi(a)=\varphi(a')\ .$$

Então valem:

a) $\varphi(M)$ *é uma subestrutura de* $\big(\,N\,;\perp_1,\perp_2\,,\ldots,\perp_r\,\big)$.

b) $\kappa_\varphi\in\mathbf{Cg}\big(\,M\,;\ \top_1,\top_2\,,\ldots,\top_r\,\big)$

c) *Existe um único isomorfismo* ψ *da estrutura quociente* $\big(\,M/\kappa_\varphi\,;\ \bar{\top}_1,\ \bar{\top}_2,\ldots,\ \bar{\top}_r\,\big)$ *sobre a imagem* $\big(\,\varphi(M)\,;\perp_1,\perp_2\,,\ldots,\perp_r\,\big)$, *tal que* $\varphi=\psi\circ\gamma$.
Particularmente,

$$\big(\,M/\kappa_\varphi\,;\ \bar{\top}_1,\ \bar{\top}_2\,,\ldots,\ \bar{\top}_r\,\big)\cong\big(\,\varphi(M)\,;\perp_1,\perp_2\,,\ldots,\perp_r\,\big)\ .$$

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 $\forall\ i=1,2\,,\ldots,r$:

$$b\perp_i b'=\varphi(a)\perp_i\varphi(a')=\varphi(a\top_i a')\in\varphi(M)\ .$$

Logo $\varphi(M)$ é uma subestrutura de $\big(\,N\,;\perp_1,\perp_2\,,\ldots,\perp_r\,\big)$.

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 $i=1,2\,,\ldots,r$:

$$\varphi(a\top_i c)=\varphi(a)\perp_i\varphi(c)=\varphi(a')\perp_i\varphi(c')=\varphi(a'\top_i c')$$

e portanto $a \top_i c \ \kappa_\varphi \ a' \top_i c'$. Isto significa $\kappa_\varphi \in \mathbf{Cg}\big(M\,;\ \top_1\ ,\ldots,\top_r \big)$.
c) Por I.2.29, existe uma única bijeção $\psi :\ M/\kappa_\varphi \ \longrightarrow\ \varphi(M)$ 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 $i = 1, 2\ ,\ldots, r$:

$$\psi(\bar{a}\ \bar{\top}_i\ \bar{a'}) = \psi(\overline{a \top_i a'}) = \varphi(a \top_i a') = \varphi(a) \perp_i \varphi(a') = \psi(\bar{a}) \perp_i \psi(\bar{a'})\ .$$

■

Pelo teorema geral do homomorfismo,

as imagens homomórficas de uma estrutura $\big(M\,; \top_1, \top_2\ ,\ldots, \top_r \big)$ são essencialmente determinadas *pelo conhecimento de suas relações de congruência*, i.e. pelo conjunto $\mathbf{Cg}\big(M\,;\ \top_1, \top_2\ ,\ldots, \top_r \big)$.

Toda estrutura sempre possui as congruências *triviais, a relação da igualdade e a relação universal*, i.e. $\big\{ \delta_M\,,\ M \times M \big\} \subseteq \mathbf{Cg}\big(M\,;\ \top_1, \top_2, \ldots, \top_r \big)$.
As estruturas quocientes (i.e. as imagens homomórficas) modulo estas duas congruências triviais são

$$\big(M/\delta_M\,;\ \bar{\top}_1,\ \bar{\top}_2, \ldots,\ \bar{\top}_r \big) \cong \big(M\,; \top_1, \top_2, \ldots, \top_r \big)$$

e

$$\big(M/M \times M\,;\ \ \bar{\top}_1,\ \bar{\top}_2, \ldots,\ \bar{\top}_r \big) \cong \big(\{e\}\,; \perp_1, \perp_2, \ldots, \perp_r \big)\ ,$$

onde $\big(\{e\}\,; \perp_1, \perp_2, \ldots, \perp_r \big)$ é uma estrutura algébrica trivial, definida num conjunto unitário $\{e\}$ com as r composições $\perp_1 = \perp_2 = \ldots = \perp_r$ 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 $\big(M\,; \top_1, \top_2\ ,\ldots, \top_r \big)$:

II.2.26 Definição.

Uma estrutura algébrica

$$\big(\, M\,;\, \top_1\,,\, \top_2\;,\ldots,\, \top_r\,\big) \text{ é dita } \textit{simples},$$

se $|M| \geq 2$ e se

$$\mathbf{Cg}\big(\, M\,;\; \top_1\;,\ldots,\, \top_r\,\big) = \big\{\delta_M\;,\; M\times M\big\}\;\;,$$

i.e. se as únicas relações de congruência dela fôrem a relação da igualdade e a relação universal.

II.2.27 Exemplos.

a) Se $|M| = 2$, certamente, $\big(\, M\,;\, \top_1\,,\, \top_2\;,\ldots,\, \top_r\,\big)$ será uma estrutura simples, pois $|\mathbf{Eq}(M)| = 2$ neste caso.

b) $\big(\, \mathbb{Z}\,;\, +\;,\;\cdot\,\big)$ não é uma estrutura simples, pois ela tem as infinitas relações de congruência distintas $\equiv_n$ com $n = 0, 1, 2, 3, \ldots$ (ver II.2.9 a))

II.2.28 Exemplo.

$$\big(\, \mathbb{R};\, +\;,\;\cdot\,\big) \textit{ é uma estrutura simples.}$$

Demonstração: Devemos mostrar $\mathbf{Cg}\big(\, \mathbb{R};\; +\;,\;\cdot\,\big) \;=\; \big\{\delta_{\mathbb{R}}\;,\; \mathbb{R}\times\mathbb{R}\big\}$: Seja dada $\delta_{\mathbb{R}} \neq \kappa \in \mathbf{Cg}\big(\, \mathbb{R};\; +\;,\;\cdot\,\big)$ 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 $\left\{\begin{array}{c} a\;\kappa\;b \\ -b\;\kappa\;-b \end{array}\right.$ segue $a - b\;\;\kappa\;\;0$, mas $a - b \neq 0$. Coloquemos $c = \frac{1}{a-b}$. De $\left\{\begin{array}{r} a{-}b\;\kappa\;0 \\ c\;\kappa\;c \end{array}\right.$ 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, $\mathbf{Cg}\big(\, \mathbb{R};\; +\;,\;\cdot\,\big) \;=\; \big\{\delta_{\mathbb{R}}\;,\; \mathbb{R}\times\mathbb{R}\big\}$ e vemos que $\big(\, \mathbb{R};\, +\;,\;\cdot\,\big)$ é uma estrutura simples.

Entretanto temos

II.2.29 Exemplo.

$$\textit{A estrutura } \big(\, I\!R ; + \,\big) \textit{ não é simples.}$$

Demonstração: Basta dar um exemplo de uma relação $\kappa \in \mathbf{Cg}\big(\, I\!R;\ + \,\big)$ com $\delta_{I\!R} \neq \kappa \neq I\!R \times I\!R$: Definamos para todos os $a, b \in I\!R$

$$a\ \kappa\ b \iff a - b \in \mathbb{Z}\ .$$

É fácil mostrar que $\kappa \in \mathbf{Cg}\big(\, I\!R;\ + \,\big)$.

Temos $\frac{1}{2}\ \ \not\kappa\ \ \frac{1}{3}\ \ \kappa\ \ \frac{4}{3}$. Portanto, $\delta_{I\!R} \neq \kappa \neq I\!R \times I\!R$.

∎

Associatividade, comutatividade, identidades e inversos sob homomorfismos

II.2.30 Proposição.

Sejam $\big(\, M \,;\, \top \big)$ *e* $\big(\, N \,;\, \perp \big)$ *duas estruturas algébricas e* $\varphi \in N^M$ *um homomorfismo.*

a) *Suponha* $\big(\, M \,;\, \top \big)$ *é comutativa. Então a subestrutura imagem* $\varphi(M)$ *de* $\big(\, N \,;\, \perp \big)$ *é comutativa também.*

b) *Se* $\big(\, M \,;\, \top \big)$ *é um semigrupo, então a subestrutura imagem* $\varphi(M)$ *de* $\big(\, N \,;\, \perp \big)$ *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, $\big(\, \varphi(M) ;\, \perp \big)$ 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

$$b \perp (c \perp d) = \varphi(x) \perp \big(\varphi(y) \perp \varphi(z)\big) = \varphi(x) \perp \varphi(y \top z) =$$

$$= \varphi\big(x \top (y \top z)\big) = \varphi((x \top y) \top z) = \varphi(x \top y) \perp \varphi(z) =$$
$$= \big(\varphi(x) \perp \varphi(y)\big) \perp \varphi(z) = (b \perp c) \perp d$$

Logo, $\big(\,\varphi(M)\,;\,\perp\big)$ é semigrupo também.

∎

II.2.31 Proposição.

Sejam $\big(\,M\,;\,\top\big)$ *e* $\big(\,N\,;\,\perp\big)$ *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* $\big(\,\varphi(N)\,;\,\perp\big)$.

b) *Suponha* $\big(\,M\,;\,\top\big)$ *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*
$$\varphi(u) \in \mathbf{U}'\big(\varphi(M)\big) \qquad \big[\varphi(u) \in \mathbf{U}''\big(\varphi(M)\big)\,,\ \ \varphi(u) \in \mathbf{U}\big(\varphi(M)\big)\big].$$

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 $\varphi(u) \in \mathbf{U}'\big(\varphi(M)\big)$.
("à direita" e "bilateral" é tratado da mesma forma).

Particularmente, um *epi*morfismo $\varphi\ :\ M \ \longrightarrow\ N$ leva identidades e inversos de $\big(\,M\,;\,\top\big)$ a identidades e inversos correspondentes de $\big(\,N\,;\,\perp\big)$.

∎

§ 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

$$\textit{um monóide } \big(M\,;\top\big) \textit{ no qual } \mathbf{U}(M)=M,$$

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 $\big(G;\,\cdot\,\big)$ 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

$$\left(\,\mathbf{S}_A\,;\,\circ\,\right)\ , \qquad \textit{o grupo simétrico sobre } A.$$

Este é o grupo das unidades do monóide $\left(\,A^A\,;\,\circ\,\right)$ de todas as aplicações do conjunto A em si mesmo.

b) $\left(\,\mathbb{Z}\,;\,+\,\right)$, o grupo aditivo dos inteiros.

c) $\left(\,\mathbf{P}\,;\,\cdot\,\right)$, o grupo múltiplicativo dos números reais positivos.

d) O grupo múltiplicativo $\left(\,\{1,-1\}\,;\,\cdot\,\right)$

e) Para qualquer monóide $\left(\,M\,;\,\top\,\right)$: O grupo

$$\left(\,\mathbf{U}(M)\,;\,\top\,\right)\ , \quad \text{consistindo dos elementos inversíveis de } \left(\,M\,;\,\top\,\right)$$

■

Os grupos simétricos

No monóide $\left(\,A^A\,;\,\circ\,\right)$ 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

$$\pi(x) = \begin{cases} b & \text{se } x = a \\ a & \text{se } x = b \\ x & \text{se } x \neq a, b \end{cases} \qquad \text{e} \quad \sigma(x) = \begin{cases} c & \text{se } x = a \\ a & \text{se } x = c \\ x & \text{se } x \neq a, c \end{cases}$$

temos

$$(\pi \circ \sigma)(a) = \pi\big(\sigma(a)\big) = \pi(c) = c\ ,$$

enquanto

$$(\sigma \circ \pi)(a) = \sigma\big(\pi(a)\big) = \sigma(b) = b\ .$$

Portanto, $\sigma \circ \pi \neq \pi \circ \sigma$.

■

II.3.4 Proposição.

Sejam A e B conjuntos equipotentes. Então

$$\big(\,\mathbf{S}_A\,;\,\circ\,\big) \cong \big(\,\mathbf{S}_B\,;\,\circ\,\big)\ ,$$

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

$$\Omega(\pi_1 \circ \pi_2) = \varphi \circ (\pi_1 \circ \pi_2) \circ \varphi^{-1} = \varphi \circ \pi_1 \circ (\varphi^{-1} \circ \varphi) \circ \pi_2 \circ \varphi^{-1} =$$

$$= (\varphi \circ \pi_1 \circ \varphi^{-1}) \circ (\varphi \circ \pi_2 \circ \varphi^{-1}) = \Omega(\pi_1) \circ \Omega(\pi_2)\ .$$

Portanto, Ω é um homomorfismo do grupo simétrico $\big(\,\mathbf{S}_A\,;\,\circ\,\big)$ em $\big(\,\mathbf{S}_B\,;\,\circ\,\big)$.

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 $\pi_1, \pi_2 \in \mathbf{S}_A$, concluimos

$$\varphi \circ \pi_1 \circ \varphi^{-1} = \varphi \circ \pi_2 \circ \varphi^{-1}\ .$$

Daí por múltiplicação por φ à direita e por φ^{-1} à esquerda,

$$\text{segue } \varphi \circ \pi_1 = \varphi \circ \pi_2 \text{ e finalmente } \pi_1 = \pi_2 .$$

Isto mostra a injetividade de Ω.
Portanto, Ω é um isomorfismo de $\big(\,\mathbf{S}_A\,;\,\circ\,\big)$ sobre $\big(\,\mathbf{S}_B\,;\,\circ\,\big)$.

■

Por exemplo

$$\big(\,\mathbf{S}_{\{1,2,3,4\}}\,;\,\circ\,\big) \cong \big(\,\mathbf{S}_{\{\ \triangledown,\spadesuit,\heartsuit,\clubsuit\,\}}\ ;\,\circ\,\big)\ .$$

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 $A = \{1, 2, 3\ , \ldots,\ n\}$ e escrevemos

$$\mathbf{S}_{\{1,2,3\ ,\ldots,\ n\}} = \mathbf{S}_n\ .$$

O grupo

$$\big(\,\mathbf{S}_n\,;\,\circ\,\big)$$

chama-se *o grupo simétrico de grau* n. Por I.2.34 temos

$$|\mathbf{S}_n| = n!\ .$$

Os $n!$ elementos $\pi, \sigma, \ldots$ 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 $\pi(k) = i_k\ ,\quad \sigma(k) = j_k\ \ \forall\ k = 1, 2, 3\ , \ldots,\ n$),
com a regra de múltiplicação

$$\sigma \circ \pi = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ j_1 & j_2 & j_3 & \cdots & j_n \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ i_1 & i_2 & i_3 & \cdots & i_n \end{pmatrix} =$$

$$= \begin{pmatrix} i_1 & i_2 & i_3 & \cdots & i_n \\ j_{i_1} & j_{i_2} & j_{i_3} & \cdots & j_{i_n} \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ i_1 & i_2 & i_3 & \cdots & i_n \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ j_{i_1} & j_{i_2} & j_{i_3} & \cdots & j_{i_n} \end{pmatrix}.$$

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 $\big(\mathbf{S}_3\,;\,\circ\big)$ 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

.

■

II.3.6 Definição.

Um subconjunto H de um grupo $\big(G;\cdot\big)$ 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 $\big(G;\cdot\big)$ que ainda são fechadas a inversos.

II.3.7 Exemplos.

a) Sempre existem os subgrupos triviais $\{1\}$ e G em cada grupo G.

b) $\mathbb{Z} \leq \big(\mathbb{R};+\big)$.

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 $\big(\mathbb{Z};+\big)$.

e) A subestrutura $\big(\mathbb{N};+\big)$ de $\big(\mathbb{Z};+\big)$ 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

$$\mathfrak{S}(G) = \big\{ H \mid H \text{ é subgrupo de } G \big\} \ .$$

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 $\big(\mathbf{S}_3 \, ; \circ \big)$ é

$$\mathfrak{S}(\mathbf{S}_3) = \big\{ \{\mathbf{1}\}, \ \mathbf{S}_3, \ \{\mathbf{1}, \tau_{_1}\}, \ \{\mathbf{1}, \tau_{_2}\}, \ \{\mathbf{1}, \tau_{_3}\}, \ \{\mathbf{1}, \sigma, \ \rho\} \big\} \ .$$

■

O GRUPO DOS AUTOMORFISMOS DE UMA ESTRUTURA ALGÉBRICA

II.3.10 Proposição.

Seja $\big(M \, ; \top_{_1}, \top_{_2} \ , \ldots , \ \top_{_r} \big)$ *uma estrutura algébrica com* r *composições internas. Seja* $\big(\mathbf{S}_M \, ; \circ \big)$ *o grupo simétrico sobre o conjunto* M. *O conjunto*

$$\mathbf{A} = \Big\{ \alpha \in \mathbf{S}_M \mid \alpha(a \top_{_i} b) = \alpha(a) \top_{_i} \alpha(b) \ \ \forall \, a, b \in M \ \ \forall \, i = 1, 2 \, , \ldots , \ r \Big\} \ ,$$

forma um subgrupo de $\mathbf{S}_M$, *i.e.*

$$\big(\mathbf{A} \, ; \circ \big) \leq \big(\mathbf{S}_M \, ; \circ \big) .$$

Demonstração: 1) Para a permutação identica $\mathbf{1} = \delta_{_M} \in \mathbf{S}_M$ temos certamente $\mathbf{1} \in \mathbf{A}$, pois $\mathbf{1}(a \top_{_i} b) = a \top_{_i} b = \mathbf{1}(a) \top_{_i} \mathbf{1}(b) \quad \forall \, a, b \in M \quad \forall \, i = 1, 2 \, , \ldots , \ r$.
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 $\left(M\,; \top_1, \top_2 \;, \ldots, \;\top_r \right)$ uma estrutura algébrica com r composições internas. O subgrupo

$$\left(\mathbf{A}\,; \circ \right) \quad \text{do grupo simétrico} \; \left(\mathbf{S}_M\,; \circ \right)$$

chama-se

$$\textit{o grupo dos automorfismos de } \left(M\,; \top_1, \top_2 \;, \ldots, \;\top_r \right) .$$

Mais detalhado, escreve-se também

$$\left(\mathbf{A}\,; \circ \right) = \left(\mathbf{aut}(M; \top_1, \top_2 \;, \ldots, \;\top_r); \circ \right)$$

ou simplesmente

$$\mathbf{A} = \mathbf{aut}(M; \top_1, \top_2 \;, \ldots, \;\top_r) .$$

O grupo $\mathbf{A}$ dos automorfismos da estrutura $\left(M\,; \top_1, \top_2 \;, \ldots, \;\top_r \right)$ consiste portanto das *permutações de M que são compatíveis* com todas as composições internas $\top_1, \top_2 \;, \ldots, \;\top_r$ definidas em M.

II.3.12 Proposição.

Sejam

$$\left(M\,; \top_1, \top_2 \;, \ldots, \;\top_r \right) \cong \left(N\,; \bot_1, \bot_2 \;, \ldots, \;\bot_r \right)$$

duas estruturas algébricas isomorfas. Então seus grupos de automorfismos

$$\left(\mathbf{aut}(M; \top_1, \top_2 \;, \ldots, \;\top_r); \circ \right) \quad e \quad \left(\mathbf{aut}(N; \bot_1, \bot_2 \;, \ldots, \;\bot_r); \circ \right) .$$

são isomorfos.

Demonstração: Seja $\varphi : M \longrightarrow N$ um isomorfismo de $(M; \top_1, \top_2 \;, \ldots, \;\top_r)$ sobre $(N; \bot_1, \bot_2 \;, \ldots, \;\bot_r)$ e defina

$$\Omega : \mathbf{aut}(M; \top_1, \top_2 \;, \ldots, \;\top_r) \longrightarrow \mathbf{aut}(N; \bot_1, \bot_2 \;, \ldots, \;\bot_r)$$

por

$$\Omega(\alpha) = \varphi \circ \alpha \circ \varphi^{-1} \quad \forall\, \alpha \in \mathbf{aut}(M; \top_1, \top_2 \;, \ldots, \;\top_r) .$$

Afirmamos que Ω é um isomorfismo procurado entre os grupos

$$\left(\mathbf{aut}(M; \top_1, \top_2 \;, \ldots, \;\top_r); \circ \right) \quad \text{e} \quad \left(\mathbf{aut}(N; \bot_1, \bot_2 \;, \ldots, \;\bot_r); \circ \right) .$$

De fato temos $\Omega(\alpha) \in \mathbf{aut}(N; \perp_1, \perp_2 \ , \ldots , \ \perp_r) \quad \forall\, \alpha \in \mathbf{aut}(M; \top_1, \top_2 \ , \ldots , \ \top_r)$, pois $\Omega(\alpha)$ é composta dos isomorfismos

$$N \ \stackrel{\varphi^{-1}}{\longrightarrow} M \ \stackrel{\alpha}{\longrightarrow} M \ \stackrel{\varphi}{\longrightarrow} N \ .$$

Isto significa

$$\Omega \in \mathbf{aut}(N; \perp_1, \perp_2 \ , \ldots , \ \perp_r)^{\mathbf{aut}(M; \top_1, \top_2 \ , \ldots, \ \top_r)} \ .$$

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 $\varepsilon_{_H}$ e $\eta_{_H}$ por

$$a\, \varepsilon_{_H}\, b \iff ab^{-1} \in H \qquad e \qquad a\, \eta_{_H}\, b \iff a^{-1}b \in H \ ,$$

temos

a) $\varepsilon_{_H}, \eta_{_H} \in \mathbf{Eq}(G)$.

b$_1$) *Para todo $g \in G$, a classe de equivalência de $g \mod \varepsilon_{_H}$ é o conjunto $Hg = \{ xg \mid x \in H \} \subseteq G$ e o conjunto quociente de $G \mod \varepsilon_{_H}$ é*

$$G/\varepsilon_{_H} = \{ Hg \mid g \in G \} \ .$$

b$_2$) *Para todo $g \in G$, a classe de equivalência de $g \mod \eta_{_H}$ é o conjunto $gH = \{ gx \mid x \in H \} \subseteq G$ e o conjunto quociente de $G \mod \eta_{_H}$ é*

$$G/\eta_{_H} = \{ gH \mid g \in G \} \ .$$

Observamos que as classes de equivalência Hg de $G \mod \varepsilon_{_H}$ chamam-se as *classes laterais à direita* de $G \mod H$, enquanto as gH de $G \mod \eta_{_H}$ chamam-se as *classes laterais à esquerda* de $G \mod H$.

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.
b$_1$) Seja $\bar{g}$ a classe de equivalência de $g \mod \varepsilon_H$. A afirmação b$_1$) 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 b$_2$) 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 tábua de multiplicação em II.3.5)

$$G/\varepsilon_H = \Big\{\, Hg \;\Big|\; g \in G \Big\} = \Big\{\{1,\tau_1\},\ \{1,\tau_1\}\circ\tau_2,\ \{1,\tau_1\}\circ\tau_3\Big\} =$$

$$= \Big\{\{1,\tau_1\},\ \{\tau_2,\tau_1\circ\tau_2\},\ \{\tau_3,\tau_1\circ\tau_3\}\Big\} = \Big\{\{1,\tau_1\},\ \{\tau_2,\rho\},\ \{\tau_3,\sigma\}\Big\}\ ,$$

enquanto

$$G/\eta_H = \Big\{\, gH \;\Big|\; g \in G \Big\} = \Big\{\{1,\tau_1\},\ \tau_2\circ\{1,\tau_1\},\ \tau_3\circ\{1,\tau_1\}\Big\} =$$

$$= \Big\{\{1,\tau_1\},\ \{\tau_2,\tau_2\circ\tau_1\},\ \{\tau_3,\tau_3\circ\tau_1\}\Big\} = \Big\{\{1,\tau_1\},\ \{\tau_2,\sigma\},\ \{\tau_3,\rho\}\Big\}$$

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

$$\begin{cases} \rho \ \ \varepsilon_H \ \ \rho \\ \mathbf{1} \ \ \varepsilon_H \ \ \tau_1 \end{cases} \qquad \text{obtemos} \quad \rho\circ\mathbf{1} = \rho \quad \not\varepsilon_H \quad \tau_3 = \rho\circ\tau_1\ .$$

Portanto, $\varepsilon_H \notin \mathbf{Cg}\big(\,\mathbf{S}_3\,;\ \circ\,\big)$.

Multiplicando-se as η_H-equivalências

$$\begin{cases} \mathbf{1} \ \ \eta_H \ \ \tau_1 \\ \rho \ \ \eta_H \ \ \rho \end{cases} \qquad \text{obtemos} \quad \mathbf{1}\circ\rho = \rho \quad \not\eta_H \quad \tau_2 = \tau_1\circ\rho\ .$$

Portanto, também $\eta_H \notin \mathbf{Cg}\big(\,\mathbf{S}_3\,;\ \circ\,\big)$.

∎

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) $\Longrightarrow$ a)": Se $Hg = gH \quad \forall\, g\in G$ temos também $G/\varepsilon_H = \big\{\,Hg \;\big|\; g\in G\big\} = \big\{\,gH \;\big|\; g\in G\big\} = G/\eta_H$ e daí $\varepsilon_H = \eta_H$.
"a) $\Longrightarrow$ b)": Suponhamos $\varepsilon_H = \eta_H$, i.e.

$$G/\varepsilon_H = \big\{\,Hg \;\big|\; g\in G\big\} = \big\{\,yH \;\big|\; y\in G\big\} = G/\eta_H\ .$$

Para todo $g\in G$ existe portanto $y\in G$ com $Hg = yH$.
De $g\in gH \cap Hg = gH\cap yH$ concluimos $yH = gH$ 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 $\big(\,G;\,\cdot\,\big)$, é preciso determinar ou descrever o conjunto $\mathbf{Cg}\big(\,G;\ \cdot\,\big)$ de suas relações de congruência.
Uma relação de congruência $\kappa\in\mathbf{Cg}\big(\,G;\ \cdot\,\big)$ do grupo G é um elemento

$$\kappa \in \mathbf{Eq}(G) \subseteq \mathbf{2}^{G\times G}\ ,$$

tal que $\forall\ a, a', b, b' \in G$:

$$\begin{cases} a\ \kappa\ a' \\ b\ \kappa\ b' \end{cases} \quad\Longrightarrow\quad a\cdot b = a'\cdot b'\ .$$

Como podemos conseguir uma descrição de $\mathbf{Cg}\big(\,G;\ \cdot\,\big)$?

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* $g^{-1}Hg = \left\{ g^{-1}xg \;\middle|\; x \in H \right\}$.

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)": $\forall\ x \in H,\ \ g \in G$ 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 $g^{-1}xg \in H \quad \forall\, x \in H,\ \ g \in G$.

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) concluimos $Hg = gH \quad \forall\, g \in G$, 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) $\kappa_{_N} \in \mathbf{Cg}\big(\, G;\ \cdot\ \big)$.

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 $y = bb'^{-1} \in N$. Como N é subgrupo normal de G, concluimos $ay \in aN = Na$ 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 $\kappa_{_N} \in \mathbf{Cg}\big(\, G;\ \cdot\ \big)$.

Se $N_1 \neq N_2$, digamos $N_1 \not\leq N_2$, vamos ter algum $x \in N_1 \backslash N_2$. 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

$$\big\{\, \kappa_{_N} \;\big|\; N \in \mathfrak{N}(G) \big\} \subseteq \mathbf{Cg}\big(\, G;\ \cdot\ \big) \;.$$

Mas também ao contrário vale: Toda relação de congruência de $\big(\, G;\cdot\ \big)$ é induzida por um subgrupo normal de G da forma descrita em II.3.18:

II.3.19 Proposição.

Seja G um grupo, $\kappa \in \mathbf{Cg}\big(\, G;\ \cdot\,\big)$ uma relação de congruência. Então

a) $N_\kappa = \big\{\, x \in G \;\big|\; x\ \kappa\ 1 \,\big\}$ *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

$$\big\{\, \kappa_{N} \;\big|\; N \in \mathfrak{N}(G) \,\big\} = \mathbf{Cg}\big(\, G;\ \cdot\,\big) \quad \text{e temos a}$$

II.3.20 Conseqüência.

Seja G um grupo. Entre o conjunto $\mathfrak{N}(G)$ dos subgrupos normais de G e o conjunto $\mathbf{Cg}\big(\, G;\ \cdot\,\big)$ 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

$$\kappa \longrightarrow N_\kappa \quad \forall\ \kappa \in \mathbf{Cg}\big(\, G;\ \cdot\,\big)\ .$$

Particularmente, $\mathfrak{N}(G)$ *e* $\mathbf{Cg}\big(G;\,\cdot\,\big)$ *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 $\big(G;\,\cdot\,\big)$ *é simples, se e somente se*

$$G \neq \{1\} \quad e \quad \mathfrak{N}(G) = \big\{\{1\}\ ,\ G\big\}\ .$$

■

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 $G/\kappa_N = \big\{\, Ng \;\big|\; g\in G\big\}$ como

$$G/N = G/\kappa_N\ .$$

$\big(G/N\,;\,\cdot\,\big)$ é a estrutura quociente com a multiplicação induzida (ver II.2.11).

II.3.22 Observação.

Seja $\big(G;\,\cdot\,\big)$ *um grupo,* $N \trianglelefteq G$ *e*

$$G/N = \big\{\, Ng \;\big|\; g\in G\big\}$$

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 canónico* $\gamma \in (G/N)^G$ *é a aplicação dada por*

$$\gamma(g) = Ng \quad \forall\ g\in G\ .$$

c) *A estrutura quociente* $\big(G/N\,;\,\cdot\,\big)$ *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 $\big(G/N\,;\,\cdot\,\big)$ chama-se portanto *o grupo quociente de* $G \mod N$.

Demonstração: Abreviamos $\bar{g} = Ng$,

a) Se $a,b\in G$, esta multiplicação indicada é

$$\bar{a}\cdot\bar{b} = (Na)(Nb) = Nab = \overline{ab}$$

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 $(Na)^{-1} = \big(\gamma(a)\big)^{-1} = \gamma(a^{-1}) = Na^{-1}$. Isto mostra que Na^{-1} é o inverso bilateral de Na.

■

II.3.23 Observação.

Sejam $\big(\,G\,;\,\cdot\,\big)$ *e* $\big(\,L\,;\,*\,\big)$ *grupos e* $\varphi\in L^G$ *um homomorfismo.*
Seja $\kappa_{_\varphi}$ *a relação de congruência associada ao* φ, *i.e.*

$$a\ \kappa_{_\varphi}\ b \iff \varphi(a) = \varphi(b)\ .$$

Então valem:

a) $\qquad N_{\kappa_\varphi} = \big\{\,x\in G\ \big|\ x\ \kappa_{_\varphi}\ 1_{_G}\big\} = \big\{\,x\in G\ \big|\ \varphi(x) = 1_{_L}\big\} \trianglelefteq G.$

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

$$\mathrm{Nuc}\,\varphi = \big\{\,x\in G\ \big|\ \varphi(x) = 1_{_L}\big\}$$

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) $a\ \kappa_{_\varphi}\ b \iff \varphi(a) = \varphi(b) \iff \varphi(a)\varphi(b^{-1}) = \varphi(b)\varphi(b^{-1}) \iff$
$\iff \varphi(ab^{-1}) = \varphi(bb^{-1}) = \varphi(1_{_G}) = 1_{_L} \iff ab^{-1}\in N_{\kappa_\varphi}.$

■

II.3.24 Observação.

Se $\big(G;\cdot\big)$ *e* $\big(L;*\big)$ *são grupos e* $\varphi\in L^G$ *um homomorfismo, então*

a) $\varphi(G)$ *é um subgrupo de* $(L;\ *\ )$.

b) $\mathrm{Nuc}\,\varphi \trianglelefteq G$.

a) $\kappa_{\varphi} = \kappa_{\mathrm{Nuc}\,\varphi}$

Demonstração: a) Certamente, $\varphi(G)$ é uma subestrutura de $\big(L;*\big)$. 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 $\big(G;\cdot\big)$ *e* $\big(L;*\big)$ *dois grupos. Seja* $\varphi\in L^G$ *um homomorfismo de* $\big(G;\cdot\big)$ *em* $\big(L;*\big)$. *Seja* $\mathrm{Nuc}\ \varphi = \big\{x\in G \bigm| \varphi(x)=1_L\big\}$ *o núcleo do* φ. *Então valem:*

a) $\varphi(G)=\big\{\varphi(x) \bigm| x\in G\big\}$ *é um subgrupo de* $(L;\ *\ )$.

b) $\mathrm{Nuc}\,\varphi$ *é um subgrupo normal de* G.

c) *Existe um único isomorfismo* ψ *do grupo quociente* $\big(G/\mathrm{Nuc}\,\varphi;\cdot\big)$ *sobre o subgrupo imagem* $\big(\varphi(G);*\big)$, *de tal maneira que* $\varphi=\psi\circ\gamma$.
Particularmente,
$$\big(G/\mathrm{Nuc}\,\varphi;\cdot\big)\cong\big(\varphi(G);*\big)\ .$$

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** $\mathrm{Nuc}\,\varphi$ **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:

a) *O grupo quociente G/N é abeliano.*

b) *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 *a 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 $\big(G\,;\cdot \big)$ *um grupo e* $x\in G$ *um elemento fixo. Então:*

a) *A aplicação* $\varphi_x \in G^{\mathbb{Z}}$ *definida por*

$$\varphi_x(m) = x^m \qquad \forall\, m \in \mathbb{Z}\ ,$$

é um homomorfismo do grupo $\big(\mathbb{Z}\,;+ \big)$ *em* $\big(G\,;\cdot \big)$

b) *A imagem de* φ_x*, indicada por*

$$\langle x\rangle = \varphi_x(\mathbb{Z}) = \big\{\, x^m \,\big|\, m \in \mathbb{Z} \big\}\ ,$$

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*

$$\mathrm{Nuc}\,\varphi_x = U_n = \{nk \mid k \in \mathbb{Z}\} = \big\{\, m \in \mathbb{Z} \,\big|\, x^m = 1 \big\} \le \mathbb{Z}$$

e vale o isomorfismo

$$\mathbb{Z}/U_n = \mathbb{Z}/\mathrm{Nuc}\,\varphi_x \cong \varphi_x(\mathbb{Z}) = \langle x\rangle\ .$$

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 $\big(G\,;\cdot \big)$ 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 $\mathbf{o}(x)$ 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 $\big(\mathbb{Z} ; + \big)$. Portanto temos:

A menos de isomorfismo, *os grupos cíclicos são exatamente o grupo* $\big(\mathbb{Z} ; + \big)$ *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 $n \in I\!N$ e consideremos a matriz

$$x = \begin{pmatrix} \cos\frac{2\pi}{n} & \operatorname{sen}\frac{2\pi}{n} \\ -\operatorname{sen}\frac{2\pi}{n} & \cos\frac{2\pi}{n} \end{pmatrix} .$$

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 $m \in \mathbb{Z}$:

$$\varphi_x(m) = x^m = \begin{pmatrix} \cos\frac{2\pi}{n} & \operatorname{sen}\frac{2\pi}{n} \\ -\operatorname{sen}\frac{2\pi}{n} & \cos\frac{2\pi}{n} \end{pmatrix}^m = \begin{pmatrix} \cos\frac{2\pi m}{n} & \operatorname{sen}\frac{2\pi m}{n} \\ -\operatorname{sen}\frac{2\pi m}{n} & \cos\frac{2\pi m}{n} \end{pmatrix}$$

e

$$\operatorname{Nuc}\varphi_x = \left\{ m \in \mathbb{Z} \;\middle|\; x^m = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\} = n\mathbb{Z} .$$

Portanto,

$$\left\langle \begin{pmatrix} \cos\frac{2\pi}{n} & \operatorname{sen}\frac{2\pi}{n} \\ -\operatorname{sen}\frac{2\pi}{n} & \cos\frac{2\pi}{n} \end{pmatrix} \right\rangle$$

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 $\big(A; +\,,\ \cdot\,\big)$ é denominada um *anel*, se

i) $\big(A; +\big)$ é um grupo comutativo.

ii) $\big(A; \cdot\,\big)$ 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) $\big(\mathbb{Z}; +\,,\ \cdot\,\big)$ é um anel, o *anel dos números inteiros.*

b) $\big(\mathbb{R}; +\,,\ \cdot\,\big)$ é o *anel dos números reais.*

c) Seja $\big(A; +\big)$ um grupo comutativo aditivo.
Definindo-se uma *multiplicação trivial* em A por $ab = 0 \quad \forall\ a, b \in A$, temos que $\big(A; +\,,\ \cdot\,\big)$ é um anel.
Particularmente, se $\big(\{0\}; +\big)$ é um grupo com um só elemento,
$\big(\{0\}; +\,,\ \cdot\,\big)$ é *o anel unitário com um só elemento.*

d) Seja

$$A = \mathbf{M}_2(\mathbb{R}) = \left\{ \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \;\middle|\; a_{11}, a_{12}, a_{21}, a_{22} \in \mathbb{R} \right\}\ ,$$

o conjunto das (2×2)-matrizes com entradas reais.
Definindo-se para todas as

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix},\ \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \in A$$

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 $\big(\mathbf{M}_2(I\!R);+\,,\,\cdot\,\big)$ 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 $X, Y \in \mathfrak{A}$:

$$X + Y = (X \cup Y) \backslash (X \cap Y) \qquad \text{e} \qquad X \cdot Y = X \cap Y ,$$

temos que $\big(\mathfrak{A}\,;+\,,\,\cdot\,\big)$ 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 $\big(A;+\,,\,\cdot\,\big)$ *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 $(x\cdot 0 + x\cdot 0) + \big(-(x\cdot 0)\big) = x\cdot 0 + \big(-(x\cdot 0)\big)$. Portanto também $x\cdot 0 + \big(x\cdot 0 + \big(-(x\cdot 0)\big)\big) = x\cdot 0 + \big(-(x\cdot 0)\big)$. Mas $x\cdot 0 + \big(-(x\cdot 0)\big) = 0$, 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 $\big(A;+\,,\,\cdot\,\big)$ é dito um *subanel de* A, se

i) S é um subgrupo de $\big(A;+\big)$.

ii) S é um subsemigrupo de $\big(A;\cdot\big)$.

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 $\frac{1}{2}\mathbb{Z} = \{ \frac{1}{2}k \mid k \in \mathbb{Z} \} = \{0, \pm\frac{1}{2}, \pm 1, \pm\frac{3}{2}, \pm 2, \ldots\}$ 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

$$\textit{a subestrutura } \ (\varphi(A); + , \cdot) \ \textit{ de } \ (L; + , \cdot) \ \textit{ é um anel}.$$

(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

$$x(y+z)=\varphi(a)\big(\varphi(b)+\varphi(c)\big)=\varphi(a)\varphi(b+c)=\varphi\big(a(b+c)\big)=$$
$$=\varphi(ab+ac)=\varphi(ab)+\varphi(ac)=\varphi(a)\varphi(b)+\varphi(a)\varphi(c)=xy+xz\ .$$

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 $\kappa\in\mathbf{Cg}\big(A;\,+\,,\,\cdot\big)$, é um elemento

$$\kappa\in\mathbf{Eq}(A)\subseteq\mathbf{2}^{A\times A}\ ,$$

tal que $\forall\ a,a',b,b'\in A$:

$$\begin{cases} a\ \kappa\ a' \\ b\ \kappa\ b' \end{cases}\quad\Longrightarrow\quad a+b\ \ \kappa\ \ a'+b'\qquad \text{e}\qquad a\cdot b\ \ \kappa\ \ a'\cdot b'\ .$$

Se κ é uma relação de congruência do anel $\big(A;+\,,\,\cdot\big)$ e γ é o epimorfismo canónico de A sobre A/κ, vemos por II.4.6 que a estrutura quociente $\big(A/\kappa;+\,,\,\cdot\big)$ é de fato um anel.

$\big(A/\kappa;+\,,\,\cdot\big)$ 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 $\big(A;+\,,\,\cdot\big)$, é preciso determinar ou descrever o conjunto $\mathbf{Cg}\big(A;\,+\,,\,\cdot\big)$ de suas relações de congruência (ver II.2.24/25).

Se $\big(A;+\,,\,\cdot\big)$ 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 $\big(A;+\big)$ é normal nele (ver II.3.18). Logo

$$\kappa_S\in\mathbf{Cg}\big(A;\,+\big)\ .$$

Além disso, sabemos que toda relação de congruência de $\big(A;+\big)$ é assim obtida. Problemas vamos ter em geral quanto à compatibilidade de κ_S com a multiplicação:

Considerando-se em $\big(I\!\!R; + , \cdot \big)$ o subanel $Z\!\!\!Z$ dos números inteiros e a relação

$$a \, \kappa_{Z\!\!\!Z} \, b \iff a - b \in Z\!\!\!Z \qquad (a, b \in I\!\!R) \, ,$$

temos

$$\begin{cases} \frac{1}{2} \, \kappa_{Z\!\!\!Z} \, \frac{3}{2} \\ \frac{1}{4} \, \kappa_{Z\!\!\!Z} \, \frac{5}{4} \end{cases} , \qquad \text{mas } \frac{1}{8} = \frac{1}{2} \cdot \frac{1}{4} \, \not\kappa_{Z\!\!\!Z} \, \frac{3}{2} \cdot \frac{5}{4} = \frac{15}{8} \, .$$

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 $\big(A; + \big)$, 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 $\Im(A)$ indicamos *o conjunto de todos os ideais de* A.

Escrever $I \in \Im(A)$ significa o mesmo quanto $I \trianglelefteq A$.

Os *ideais* de um anel são portanto uma categoria especial de subanéis - da mesma forma que os *subgupos normais* de um grupo são uma categoria especial de subgrupos.

II.4.8 Exemplos.

a) Para qualquer anel A temos $\{0\}$, $A \in \Im(A)$, i. e. os subgrupos aditivos triviais $\{0\}$ e A são ideais de A, os chamados *ideais triviais*.

b) Seja $\big(A; + , \cdot \big) = \big(Z\!\!\!Z; + , \cdot \big)$ e $n \in I\!\!N_0$.
Para os subanéis $U_n = \big\{ nk \bigm| k \in Z\!\!\!Z \big\}$ de $\big(Z\!\!\!Z; + , \cdot \big)$ temos de fato

$$U_n \in \Im(Z\!\!\!Z) \, .$$

c) O subanel $\mathbb{Z}$ de $\left(\mathbb{R};+,\cdot\right)$ 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 $\left(A;+,\cdot\right)$ *um anel e* $I \trianglelefteq A$. *Definindo-se para todos os* $a,b\in A$:

$$a\ \kappa_I\ b \iff a-b\in I\ , \quad \textit{temos}$$

a) $\kappa_I \in \mathbf{Cg}\left(A;\,+,\cdot\right)$.

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 $\kappa_I \in \mathbf{Cg}\left(A;\,+\right)$. 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

$$ab-a'b' = a(b-b')+(a-a')b'\in I \qquad \text{e portanto} \quad ab\ \kappa_I\ a'b'\ .$$

Vemos que $\kappa_I \in \mathbf{Cg}\left(A;\,+,\cdot\right)$.

■

Também ao contrário vale: Toda relação de congruência de A é induzida por um ideal de A :

II.4.10 Proposição.

Seja $\left(A;+,\cdot\right)$ *um anel,* $\kappa \in \mathbf{Cg}\left(A;\,+,\cdot\right)$ *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 $\big(A; + \big)$. 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* $\mathbf{Cg}\big(A;\, + \,,\, \cdot \big)$ *das suas relações de congruência, existe uma correspondência biunívoca, estabelecida por*

$$I \longrightarrow \kappa_I \quad \forall\, I \in \mathfrak{I}(A)\,,$$

cuja inversa é

$$\kappa \longrightarrow I_\kappa \quad \forall\, \kappa \in \mathbf{Cg}\big(A;\, + \,,\, \cdot \big) \,.$$

Particularmente, $\mathfrak{I}(A)$ *e* $\mathbf{Cg}\big(A;\, + \,,\, \cdot \big)$ *são conjuntos equipotentes.*

Além disso,

$$\{0\} \longrightarrow \kappa_{\{0\}} = \delta_A \qquad \text{e} \qquad A \longrightarrow \kappa_A = A \times A \,,$$

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 $\big(A; + \,,\, \cdot \big)$ *é simples, se e somente se*

$$A \neq \{0\} \quad \text{e} \;\; \mathfrak{I}(A) = \big\{ \{0\} \;,\; A \big\} \,.$$

∎

II.4.13 Observação.

Seja $\big(A;+\,,\,\cdot\big)$ *um anel,* $I \trianglelefteq A$ *e* κ_I *é a congruência associada ao* I.

a) *A classe de equivalência* $\bar{a}$ *do elemento* $a \in A \mod \kappa_I$ *é*

$$\bar{a} = a + I = \big\{ a + x \bigm| x \in I \big\} \ .$$

b) *O anel quociente* A/κ_I *é*

$$A/\kappa_I = \big\{ a+I \bigm| a \in A \big\} \ .$$

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 $\big(A;+\,,\,\cdot\big)$ *um anel,* $I \trianglelefteq A$ *e*

$$A/I = \big\{ a+I \bigm| a \in A \big\}$$

o anel quociente de $A \mod I$. *Então*

a) *A adição e multiplicação induzidas em* A/I *são dadas por*

$$\begin{array}{c} (a+I) \ + \ (b+I) = (a+b) + I \\ (a+I) \cdot (b+I) = ab + I \end{array} \qquad \forall\ a+I,\ b+I \in A/I\ .$$

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 $\big(A;+\,,\,\cdot\big)$ *e* $\big(L;+\,,\,\cdot\big)$ *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*

$$I_{\kappa_\varphi} = \big\{\,x\in A\ \big|\ x\ \kappa_{\varphi}\ 0_{A}\big\} = \big\{\,x\in A\ \big|\ \varphi(x) = 0_{L}\big\}\ .$$

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

$$\mathrm{Nuc}\,\varphi = \big\{\,x\in A\ \big|\ \varphi(x) = 0_{L}\big\}$$

e se chama o *núcleo do homomorfismo* φ

Demonstração: a) Temos $\varphi(0_{A}) = 0_{L}$. Logo, $I_{\kappa_\varphi} = \big\{\,x\in A\ \big|\ x\ \kappa_{\varphi}\ 0_{A}\big\} = \big\{\,x\in A\ \big|\ \varphi(x) = \varphi(0_{A})\big\} = \big\{\,x\in A\ \big|\ \varphi(x) = 0_{L}\big\}$.

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 $\big(A;+\,,\,\cdot\big)$ *e* $\big(L;+\,,\,\cdot\big)$ *são anéis e* $\varphi\in L^A$ *um homomorfismo, então*

a) $\varphi(A)$ *é um subanel de* $\big(L;+\,,\,\cdot\big)$.

b) $\mathrm{Nuc}\,\varphi \trianglelefteq A$.

c) $\kappa_{\varphi} = \kappa_{\mathrm{Nuc}\,\varphi}$

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 $\big(A;+\,,\,\cdot\big)$ *e* $\big(L;+\,,\,\cdot\big)$ *dois anéis. Seja* $\varphi\in L^A$ *um homomorfismo de* $\big(A;+\,,\,\cdot\big)$ *em* $\big(L;+\,,\,\cdot\big)$. *Então valem:*

a) *A imagem* $\varphi(A) = \big\{\varphi(x)\;\big|\;x\in A\big\}$ *é um subanel de* $\big(L;+\,,\,\cdot\big)$.

b) *O núcleo* $\mathrm{Nuc}\,\varphi = \big\{x\in A\;\big|\;\varphi(x)=0_{L}\big\}$ *é um ideal de* A.

c) *Existe um único isomorfismo* ψ *do anel quociente* $\big(A/\mathrm{Nuc}\,\varphi;+\,,\,\cdot\big)$ *sobre o subanel imagem* $\big(\varphi(A);+\,,\,\cdot\big)$, *de tal maneira que* $\varphi=\psi\circ\gamma$. Particularmente,

$$\big(A/\mathrm{Nuc}\,\varphi;+\,,\,\cdot\big)\cong\big(\varphi(A);+\,,\,\cdot\big)\ .$$

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** $\mathrm{Nuc}\,\varphi$ **associado ao homomorfismo** φ.

II.4.18 Definição.

Um anel $\big(A; + , \cdot\big)$ 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 $\big(A; \cdot\big)$ é um monóide.

b) *anel comutativo*, se $ab = ba$ para todos os $a, b \in A$. Isto significa que o semigrupo $\big(A; \cdot\big)$ é comutativo.

c) *anel comutativo com identidade* se A tem as propriedades de a) e b) simultâneamente. Isto significa portanto que $\big(A; \cdot\big)$ 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) $\big(\mathbb{Z}; + , \cdot\big)$, o anel dos números inteiros é um domínio de integridade porém não é um corpo.

b) $\big(\mathbb{R}; + , \cdot\big)$, o anel dos números reais, é um corpo.

c) O anel $\big(2\mathbb{Z}; + , \cdot\big)$ dos números inteiros pares é um anel comutativo sem elemento identidade.

d) Seja $\big(A; +\big)$ um grupo comutativo aditivo.

O anel $\big(A; + , \cdot\big)$ com a mutiplicação 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

$$A = \mathbf{M}_2(I\!R)$$

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 $\big(\mathfrak{A}\,;+\,,\,\cdot\,\big)$ sobre o conjunto E ($\mathfrak{A} = \mathbf{2}^E$ 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 $E = \big\{b\big\}$ um conjunto unitário, temos que $\mathfrak{A} = \big\{\emptyset\,,\,E\big\}$ é um corpo com 2 elementos.

(Provar estas asserções !) ∎

Pelos nossos conhecimentos podemos afirmar:

II.4.20 Observação.

a) *Todo corpo* $\big(C; +\,,\,\cdot\,\big)$ *é um domínio de integridade*

b) *Todo domínio de integridade* $\big(A; +\,,\,\cdot\,\big)$ *é um anel comutativo com identidade*

c) *Um anel comutativo com identidade A é um domínio de integridade, se e somente se* $\forall\, a, b \in A$:

$$ab = 0 \implies a = 0 \;\; ou \;\; b = 0\,.$$

Demonstração: a) Observe $\mathbf{U}(C;\,\cdot\,) \subseteq \mathbf{R}(C;\,\cdot\,)$.

b) Vale por definição.

c) Se $\mathbf{R}(A;\,\cdot\,) = A\backslash\{0\}$ e tendo em vista que $\mathbf{R}(A)$ é multiplicativamente fechado, concluimos $ab \neq 0$ sempre se $a \neq 0 \neq b$.
Reciprocamente, se $\mathbf{R}(A) \subsetneqq A\setminus\{0\}$, 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 $A = \mathbb{Z}/(6) = \big(\{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}; + \,, \,\cdot \big)$ 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 $B = Cpt_E(A)$. 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 $\big(\mathfrak{A}; + \,, \cap \big)$ (observe que $\emptyset$ é o elemento nulo de $\mathfrak{A}$!).

∎

Ideais principais em anéis comutativos com identidade

II.4.23 Observação.

Seja $\big(A; + \,, \,\cdot \big)$ *um anel comutativo com elemento identidade* 1 *e seja* $a \in A$ *um qualquer elemento. Então*

$$aA = \big\{ ax \;\big|\; x \in A \big\}$$

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 $\big(A; +\,,\,\cdot\,\big) = \big(\mathbb{Z}; +\,,\,\cdot\,\big)$

$$(6) = I_6 = 6\mathbb{Z} = \big\{\, 6x \;\big|\; x \in \mathbb{Z} \big\}$$

é o ideal principal de $\mathbb{Z}$ gerado por 6. Observamos

$$(6) = (-6)\ .$$

b) Seja E um conjunto, $\mathfrak{A} = \mathbf{2}^E$ e seja $\big(\mathfrak{A}\,; +\,,\,\cdot\,\big)$ o anel de Boole sobre E, as composições de $\mathfrak{A}$ sendo

$$X + Y = (X \cup Y) \backslash (X \cap Y)\ , \quad X \cdot Y = X \cap Y \quad \forall\, X, Y \in \mathfrak{A}\ .$$

O ideal principal de $\mathfrak{A}$ gerado por $A \in \mathfrak{A}$, é

$$A\mathfrak{A} = (A) = \big\{\, AX \;\big|\; X \in \mathfrak{A} \big\} = \big\{\, A \cap X \;\big|\; X \in \mathfrak{A} \big\} =$$
$$= \big\{\, Y \;\big|\; Y \subseteq A \big\} = \mathbf{2}^A \trianglelefteq \mathbf{2}^E\ .$$

■

Em qualquer anel (comutativo com elemento identidade) temos

$$\big\{\, (a) \;\big|\; a \in A \big\} \subseteq \mathfrak{I}(A)\ ,$$

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
$$\mathfrak{A} = \mathbf{2}^{I\!N}$$
sobre os números naturais (ou sobre qualquer conjunto infinito) temos que
$$\mathfrak{F} = \{\, X \mid |X| < \infty \,\} \ ,$$
a família dos subconjuntos finitos de $I\!N$, forma um ideal (demonstração ?).
$\mathfrak{F}$ não pode ser um ideal principal de $\big(\mathbf{2}^{I\!N}; + \,,\, \cdot\,\big)$:
Para qualquer $F \in \mathfrak{F}$ e $X \in \mathfrak{A}$ temos $|FX| = |F \cap X| \le |F|$.
Como $\mathfrak{F}$ contém subconjuntos *de tamanho finito arbitrário*, isto significa que $(F) = F\mathfrak{A} = \mathbf{2}^F \underset{\neq}{\subseteq} \mathfrak{F}$, 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 $j \in I\!N \setminus F$.

■

Portanto: Só excepcionalmente vamos ter
$$\big\{\, (a) \;\big|\; a \in A \big\} = \ \mathfrak{I}(A) \ .$$
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 $\big(A; + \,,\, \cdot\,\big)$ 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 $\big(\mathbb{Z}\,; + \,,\, \cdot\,\big)$ 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 $\kappa_{_J}$ 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

$$\big\{ (a) \bigm| a \in \mathbb{Z} \big\} = \mathfrak{I}(\mathbb{Z}) .$$

■

Anéis simples e Corpos

A propriedade da simplicidade (i.e. $A \neq \{0\}$ e $\mathfrak{I}(A) = \big\{\{0\}\ ,\ A\big\}$) tem uma caracterização transparente, se A é um anel comutativo com elemento identidade. Esta queremos mencionar:

II.4.28 Proposição.

Seja $\big(A; +\ ,\ \cdot\ \big)$ *um anel* **comutativo com elemento identidade** 1.
Equivalentes são:

a) $\big(A; +\ ,\ \cdot\ \big)$ *é simples*

b) $\big(A; +\ ,\ \cdot\ \big)$ *é um corpo*

Demonstração: "a) $\Rightarrow$ b)": Seja $\big(A; +\ ,\ \cdot\ \big)$ simples. Isto significa $\mathfrak{I}(A) = \big\{\{0\}\ ,\ A\big\}$ com $A \neq \{0\}$. Seja dado $0 \neq a \in A$ e considere o ideal principal

$$(a) = aA = \big\{ ax \bigm| x \in A \big\} .$$

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 $\mathbf{U}(A;\ \cdot\ ) = A \backslash \{0\}$ e vemos que A é um corpo.

"b) $\Rightarrow$ a)": Seja $\big(A; +\ ,\ \cdot\ \big)$ 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 $y \in A$ concluimos agora $y = y \cdot 1 \in I$. Isto significa $I = A$ e daí $\mathfrak{I}(A) = \big\{\{0\}\ ,\ A\big\}$. Vemos a simplicidade de A.

■

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.

a) Seja p um número primo. Então o ideal principal $P = (p)$ de $\big(\mathbb{Z}; + , \cdot\big)$ é um ideal primo.

b) O ideal $I = (6)$ de $\mathbb{Z}$ não é um ideal primo.

c) Em qualquer anel comutativo com identidade temos que o ideal trivial

$$P = A \quad \text{é um ideal primo.}$$

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 distribuido para dois fatores, concluimos 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 $\big(A; +\,,\,\cdot\big)$ *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* $A\backslash J$ *é multiplicativamente fechado.*

Demonstração: "a) $\Longleftrightarrow$ c)": J é um ideal primo $\Longleftrightarrow$

$$\Longleftrightarrow \ (\ \forall\, a,b \in A: \ \ ab \in J \ \Rightarrow \ a \in J \ \text{ ou } \ b \in J)$$
$$\Longleftrightarrow \ (\ \forall\, a,b \in A: \ \ a \notin J \ \text{ e } \ b \notin J \ \Rightarrow \ ab \notin J\ )$$
$$\Longleftrightarrow \ (\ \forall\, a,b \in A: \ \ a,b \in A\backslash J \ \Rightarrow \ ab \in A\backslash J\ )\ .$$

"a) $\Rightarrow$ b)": Seja J é um ideal primo de A e sejam

$$a+J,\ b+J \in A/J \quad \text{tais que} \ \ (a+J)(b+J) = J$$

(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, concluimos $a \in J$ 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, concluimos $a+J = J$ 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 $\big(A; + \,,\, \cdot \big)$ 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 $\big(A; + \,,\, \cdot \big)$ *um anel comutativo com identidade e* $J \trianglelefteq A$. *Então são equivalentes*:

a) $\big(A/J ; + \,,\, \cdot \big)$ *é um corpo.*

b) J *é um ideal maximal de* A.

Demonstração: Certamente,

$$A/J \text{ é um anel comutativo cujo elemento identidade é } 1{+}J$$

(a classe $0{+}J = J$ é seu elemento nulo).
Por II.4.28, a afirmação da proposição pode ser substituida por:

$$A/J \textit{ é um anel simples, se e somente se } J \textit{ é um ideal maximal em } A.$$

"a) $\Rightarrow$ b)": Seja A/J um anel simples. Particularmente temos $|A/J| \geq 2$ e portanto, $J \underset{\neq}{\subseteq} A$.
Suponha, $J \leq X \trianglelefteq A$ e $X \neq A$. Segue que

$$X/J = \big\{\, x{+}J \;\big|\; x{\in}X \,\big\}$$

é um ideal de A/J com $\{J\} = J/J \leq X/J \neq A/J$ (detalhar!). Pela simplicidade de A/J concluimos 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 $Y = J + (a) = \left\{ j + ax \;\middle|\; j \in J,\ x \in A \right\}$ 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 $by_1 = y_1 b = j_1 b + a(x_1 b) \in J + (a) = Y$. Portanto, Y é um ideal de A e vemos $J < Y \trianglelefteq A$.

Pela maximalidade de J concluimos $Y = A$. 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 $\left(\mathbb{Z}\,; + , \cdot \right)$ *o anel dos números inteiros e* $n \in \mathbb{N}_0$. *Então são equivalentes*:

a) $\left(\mathbb{Z}/(n); + , \cdot \right)$ *é um corpo.*

b) $n = p$ *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 $(p) \subsetneqq \mathbb{Z}$. Suponha $(p) \leq X \trianglelefteq \mathbb{Z}$ 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 concluimos que $\mathbb{Z}/(p)$ é um corpo.

∎

II.4.36 Exemplos.

a) No anel quociente $\mathbb{Z}/(10)$ temos

$$\mathbf{U}\left(\mathbb{Z}/(10)\right) = \{\bar{1}, \bar{3}, \bar{7}, \bar{9}\} \ ,$$

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

$$\begin{array}{lclclcl}
\bar{1}\bar{x} = \bar{1} & \longleftarrow & \bar{x} = \bar{1} & \qquad & \bar{6}\bar{x} = \bar{1} & \longleftarrow & \bar{x} = \bar{2} \\
\bar{2}\bar{x} = \bar{1} & \longleftarrow & \bar{x} = \bar{6} & & \bar{7}\bar{x} = \bar{1} & \longleftarrow & \bar{x} = \bar{8} \\
\bar{3}\bar{x} = \bar{1} & \longleftarrow & \bar{x} = \bar{4} & & \bar{8}\bar{x} = \bar{1} & \longleftarrow & \bar{x} = \bar{7} \\
\bar{4}\bar{x} = \bar{1} & \longleftarrow & \bar{x} = \bar{3} & & \bar{9}\bar{x} = \bar{1} & \longleftarrow & \bar{x} = \bar{5} \\
\bar{5}\bar{x} = \bar{1} & \longleftarrow & \bar{x} = \bar{9} & & \overline{10}\bar{x} = \bar{1} & \longleftarrow & \bar{x} = \overline{10}
\end{array}$$

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 $\left(\mathbf{2}^E; + , \cap\right)$ 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 $\big(A;+\,,\,\cdot\big)$ 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.

a) Os elementos idempotentes de $\mathbb{Z}/6\mathbb{Z}$ são $\{\bar{0},\bar{1},\bar{3},\bar{4}\}$.

b) Num anel de Boole, todo elemento é idempotente.

c) 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 $\big(A;+\,,\,\cdot\big)$ *um anel comutativo com elemento identidade* 1 *e seja* $e\in A$ *um elemento idempotente. Então:*

a) *Também* $1-e$ *é idempotente, vale* $e(1-e)=0$ *e* $1-(1-e)=e$.

b) *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 $e(1-e) = e-e^2 = e-e = 0$. $\quad 1-(1-e)=e$ é claro.

b) Segue, pois $e(1-e)=0$ e $e\neq 0,1$.

II.4.40 Exemplos.

a) Os pares de elementos idempotentes do anel $A=\big(\mathbb{Z}/(10);+\,,\,\cdot\big)$ 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 $A = \big(\mathbb{Z}/(100); + \,,\, \cdot \big)$ são

$$\{\bar{0},\ \bar{1}\} \quad \text{e} \quad \{\overline{25},\ \bar{1}-\overline{25}\} = \{\overline{25},\ \overline{76}\}\ .$$

c) Os pares de elementos idempotentes do anel $A = \big(\mathbb{Z}/(105); + \,,\, \cdot \big)$ são

$$\{\bar{0},\ \bar{1}\},\ \{\overline{70},\ \bar{1}-\overline{70}\} = \{\overline{70},\ \overline{36}\}\ ,$$

$$\{\overline{21},\ \bar{1}-\overline{21}\} = \{\overline{21},\ \overline{85}\} \quad \text{e} \quad \{\overline{15},\ \bar{1}-\overline{15}\} = \{\overline{15},\ \overline{91}\}\ .$$

∎

II.4.41 Proposição.
Seja $\big(A; + \,,\, \cdot \big)$ *um anel comutativo com identidade* 1 *e* I *um ideal de* A. *Equivalentes são*:

a) *O anel* I *possui uma identidade* e.

b) *Existe um ideal* J *de* A *tal que*

$$A = I + J \quad e \quad I \cap J = \{0\}\ .$$

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

$$x = (1-e)a \text{ para algum } a \in A \text{ e daí } x = ex = e(1-e)a = 0 \cdot a = 0.$$

Logo, $I \cap J = \{0\}$.
Temos $1 = e + (1-e)$ e para todo $y \in A$:

$$y = 1 \cdot y = ey + (1-e)y \quad \text{com} \quad ey \in I; \quad (1-e)y \in J\ .$$

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, $\mathfrak{A} = \mathbf{2}^E$ e considere o anel de Boole $\big(\mathfrak{A}\,;+\,,\,\cdot\,\big)$. Seja $A \in \mathfrak{A}$ e considere o ideal principal

$$\mathfrak{I} = A\mathfrak{A} = \mathbf{2}^A \trianglelefteq \mathfrak{A}.$$

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 $\mathfrak{J} = (E \setminus A)\mathfrak{A} = \mathbf{2}^{E \setminus A} \trianglelefteq \mathfrak{A}$ 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.