Matemática Discreta para Ciência da Computação

P. Blauth Menezes

blauth@inf.ufrgs.br

Departamento de Informática Teórica

Instituto de Informática / UFRGS

Matemática Discreta para Ciência da Computação

P. Blauth Menezes

9 – Álgebras e Homomorfismos

9 Álgebras e Homomorfismos

◆ Já foi introduzido que

- Álgebra, desde a sua origem até a sua forma atual
  - ∗ refere-se a cálculos
- Desenvolvida de forma informal ou formal
  - ∗ praticamente em todos os níveis de escolaridade
  - ∗ ex: operações aritméticas (adição, multiplicação…) sobre $\mathbf{R}$
- Álgebras, em CC, destaca-se a partir de 1950
  - ∗ Teoria dos Autômatos e Linguagens Formais
- De certa forma, toda a CC é construída sobre álgebras
  - ∗ Álgebra: denominação alternativa para a Matemática Discreta

- **Assim, o estudo mais amplo de álgebras**
  - central no contexto da Matemática Discreta
- **Alguns exemplos de álgebras já introduzidos**
  - Álgebra de Conjuntos
    - $*$ conjuntos e as operações sobre conjuntos (união,…)
  - Álgebra de Funções
    - $*$ funções e composição de funções
  - Álgebra de Proposições
    - $*$ proposições e conetivos lógicos (e, negação,…)
- **Seguindo a mesma linha de raciocínio**
  - Álgebra de Relações, Álgebra de Funções Parciais, ...

◆ Conceito formal de álgebra

- simples
- mas com um nível de abstração relativamente alto
  - ∗ para caracterizar todos os tipos de álgebras

◆ O conceito é construindo do concreto para o abstrato

- inicialmente são introduzidos alguns exemplos

◆ Exemplos acima são de álgebras grandes

- operações definidas sobre coleções (e não conjuntos)

◆ Neste capítulo

- ênfase às álgebras pequenas

◆ Homomorfismo de Álgebras

- conceito tão importante quanto o de álgebra
- são funções (álgebras pequenas)
  - mapeiam álgebras (estruturalmente similares)
  - preservando as estruturas

- morfismo
  - alguma forma de mapeamento (relação, função, …)
  - entre duas estruturas similares

- *homo*
  - preserva a estrutura

- noção de homomorfismo é desenvolvida gradativamente

◆ Estudo mais formal de álgebra

- conceito de operação
- principais propriedades das operações

◆ Importantes álgebras e homomorfismos

- fecho de Kleene
- grafo (visto como álgebra)
- categoria (vista como álgebra)

9 – Álgebras e Homomorfismos

9.1 Operações Binárias
9.2 Propriedades das Operações Binárias
9.3 Grupóides, Semigrupos, Monóides, Grupos
9.4 Importantes Propriedades dos Monóides e Grupos
9.5 Homomorfismos
9.6 Monóide Livre Gerado e Fecho de Kleene
9.7 Grafos
9.8 Categorias

9.1 Operações Binárias

- **Operação (pequena): função parcial**
  - já foi introduzido
- **De especial interesse para a Computação e Informática**
  - operações binárias
    - domínio: produto cartesiano
  - operações internas a um conjunto A
    - domínio e contra-domínio são definidos sobre A
  - operações fechadas
    - total

Def: Operação Binária, Interna, Fechada

A, B e C conjuntos

Operação Binária

$$\oplus: A \times B \to C$$

Operação Interna ao conjunto A

- domínio e contra-domínio são definidos em A
  - o próprio A ou
  - conjunto resultante do produto cartesiano sobre A

- operação binária interna ao conjunto A

$$\oplus: A \times A \to A$$

Operação Fechada: operação total (*função*)

Exp: Operação binária? interna? fechada?

Divisão nos reais. div: $\mathbf{R} \times \mathbf{R} \rightarrow \mathbf{R}$

$$\text{div}\langle x, y\rangle = x/y$$

Quadrado nos naturais. quadrado: $\mathbf{N} \rightarrow \mathbf{N}$

$$\text{quadrado}(n) = n^2$$

Elemento. $1 = \{ * \}$ conjunto unitário. zero: $1 \rightarrow \mathbf{N}$

$$\text{zero}\langle * \rangle = 0$$

União. A conjunto. $\cup$: $\mathbf{P}(A) \times \mathbf{P}(A) \rightarrow \mathbf{P}(A)$

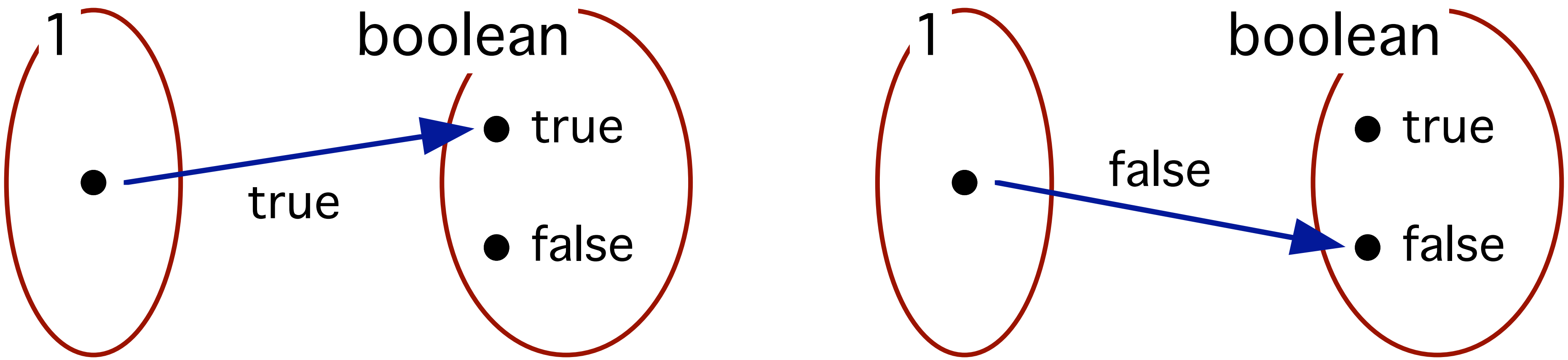
Obs: Elemento de Conjunto como Função

Função zero: $1 \rightarrow \mathbf{N}$ tal que $zero\langle * \rangle = 0$

- forma de identificar um elemento de um conjunto por uma função
- se 1 é conjunto unitário fixo, e A conjunto qualquer

$$\#A = \#\{ f \mid f : 1 \rightarrow A \text{ é função } \}$$

- exemplo



9 – Álgebras e Homomorfismos

9.2 Propriedades das Operações Binárias

- **Principais propriedades das operações binárias, internas e fechadas**
  - Comutativa *
  - Associativa *
  - Elemento neutro *
  - Elemento inverso

* introduzidas anteriormente: Álgebra de Conjuntos & Lógica

Def: Comutativa, Associativa, Elemento Neutro, Elemento Inverso

$\oplus$: $A \times A \rightarrow A$ operação binária, interna e fechada

Comutativa

$$(\forall a \in A)(\forall b \in A)\ (\ a \oplus b = b \oplus a\ )$$

Associativa

$$(\forall a \in A)(\forall b \in A)(\forall c \in A)\ (\ a \oplus (b \oplus c) = (a \oplus b) \oplus c\ )$$

Elemento Neutro

$$(\exists e \in A)(\forall a \in A)\ (\ a \oplus e = e \oplus a = a\ )$$

Elemento Inverso

$$(\forall a \in A)(\exists \underline{a} \in A)\ (\ a \oplus \underline{a} = \underline{a} \oplus a = e\ )$$

◆ Associativa ???

- precedência na aplicação do operando *não* é importante
- parênteses podem ser omitidos

$$a \oplus b \oplus c$$

◆ Elemento Neutro

- satisfazer *simultaneamente* à esquerda e à direita é fundamental

$$(\exists e \in A)(\forall a \in A)\ (\ a \oplus e = e \oplus a = a\ )$$

- divisão nos reais
  - ∗ possui neutro à direita — número um
  - ∗ *não* possui neutro à esquerda

Exp: Propriedades da União

A conjunto. $\cup$: $\mathbf{P}(A) \times \mathbf{P}(A) \rightarrow \mathbf{P}(A)$

- Comutativa?
- Associativa?
- Elemento neutro? (qual ?)
- Elemento inverso?

Exp: Propriedades da Adição

$+: \mathbf{N} \times \mathbf{N} \rightarrow \mathbf{N}$

- comutativa
- associativa
- elemento neutro (zero)

$+: \mathbf{Z} \times \mathbf{Z} \rightarrow \mathbf{Z}$

- comutativa
- associativa
- elemento neutro
- elemento inverso

$$n + {}^{-}n = {}^{-}n + n = 0$$

Exp: Propriedades da Multiplicação

$*: \mathbf{N} \times \mathbf{N} \to \mathbf{N}$

- comutativa, associativa e elemento neutro (um)

$*: \mathbf{R} \times \mathbf{R} \to \mathbf{R}$

- comutativa, associativa e elemento neutro
- se considerada *sem o zero*
  - elemento inverso

$$x * 1/x = 1/x * x = 1$$

9 – Álgebras e Homomorfismos

9.3 Grupóides, Semigrupos, Monóides, Grupos

◆ Exemplo de álgebra

- operação binária e interna $\oplus$: $A \times A \to A$
- usualmente denotada como um par ordenado

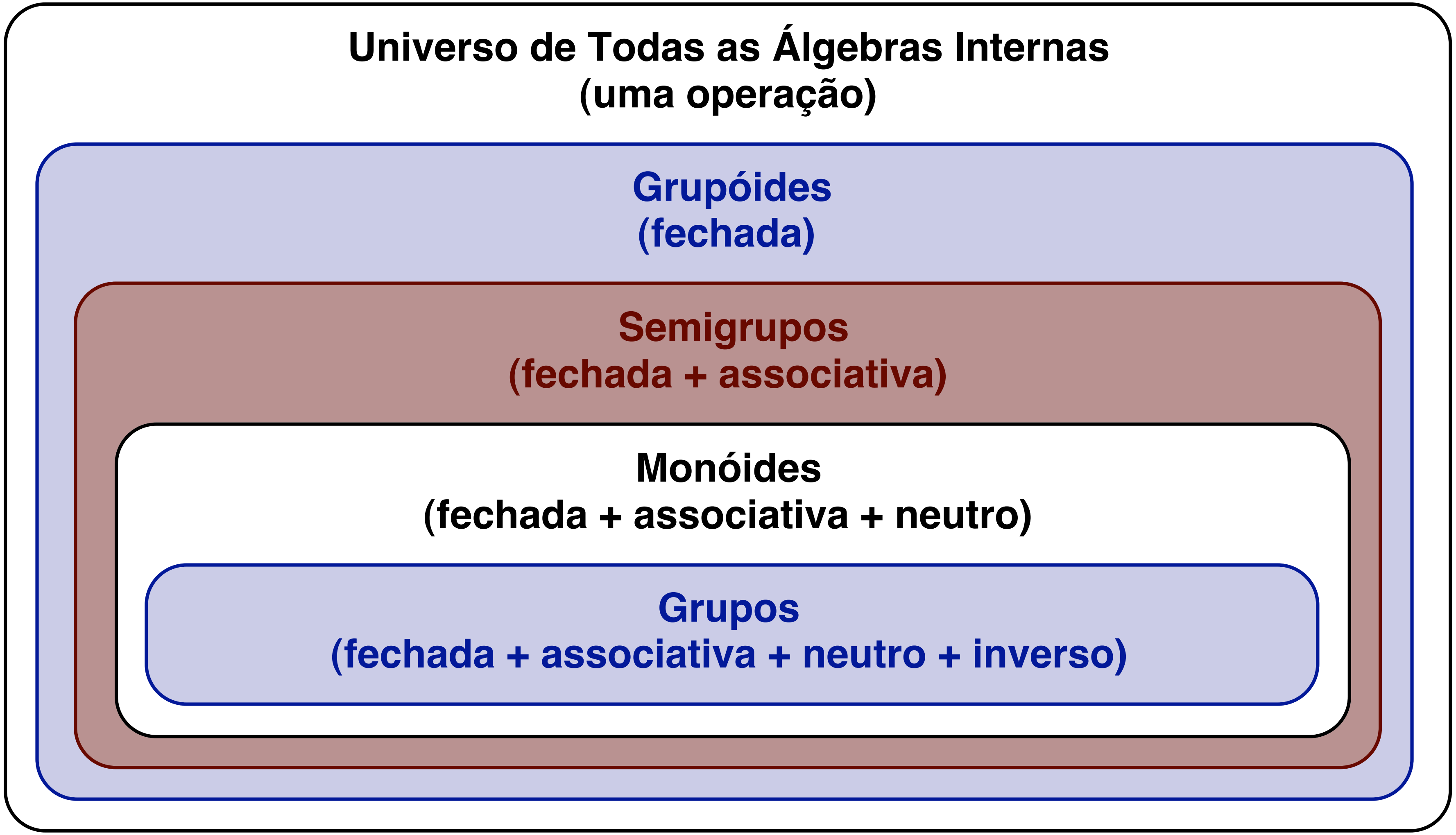
$$\langle A, \oplus \rangle$$

- álgebra interna
  * operação $\oplus$ é interna
- conjunto suporte da álgebra interna $\langle A, \oplus \rangle$
  * conjunto A

- **Operações binárias e internas são especialmente importantes para Computação e Informática**
- **Tipos mais importantes de álgebras internas com uma única operação binária**
  - se a operação for comutativa, é dita abeliana

Tipo de Álgebra	Fechada	Associativa	Elemento Neutro	Elemento Inverso
Grupóide	✔			
Semigrupo	✔	✔		
Monóide	✔	✔	✔	
Grupo	✔	✔	✔	✔

◆ Hierarquia entre estes tipos de álgebras



Def: Grupóide, Semigrupo, Monóide, Grupo

Grupóide: álgebra interna $\langle A, \oplus \rangle$

- $\oplus: A \times A \rightarrow A$ operação (binária e interna)
- fechada

Semigrupo: álgebra interna $\langle A, \oplus \rangle$

- $\langle A, \oplus \rangle$ grupóide
- associativa

Monóide: álgebra interna $\langle A, \oplus \rangle$ ou $\langle A, \oplus, e \rangle$

- $\langle A, \oplus \rangle$ semigrupo
- elemento neutro

Grupo: álgebra interna $\langle A, \oplus \rangle$ ou $\langle A, \oplus, e \rangle$

- $\langle A, \oplus \rangle$ monóide
- elemento inverso

Def: Grupóide, Semigrupo, Monóide, Grupo

Se a operação for comutativa

- Grupóide Comutativo ou Grupóide Abeliano
- Semigrupo Comutativo ou Semigrupo Abeliano
- Monóide Comutativo ou Monóide Abeliano
- Grupo Comutativo ou Grupo Abeliano

Exp: Grupóide, Semigrupo, Monóide: Concatenação

Σ alfabeto não-vazio, operação de concatenação

$$\text{conc}: \Sigma^* \times \Sigma^* \to \Sigma^*$$

- fechada
- associativa
- elemento neutro (palavra vazia ε)

Portanto, a álgebra interna $\langle \Sigma^*, \text{conc} \rangle$ é simultaneamente

- grupóide
- semigrupo
- monóide

Não é

- grupo (e se o alfabeto for vazio?)
- comutativa (e se o alfabeto for vazio ou unitário?)

Exp: Grupóide, Semigrupo, Monóide: União e Intersecção

A conjunto, operações de união e de intersecção

$$\cup: \mathbf{P}(A) \times \mathbf{P}(A) \to \mathbf{P}(A) \quad \text{e} \quad \cap: \mathbf{P}(A) \times \mathbf{P}(A) \to \mathbf{P}(A)$$

- fechadas
- associativas
- elemento neutro ($\varnothing$ e A)
- comutativas

Portanto álgebras internas $\langle \mathbf{P}(A), \cup \rangle$ e $\langle \mathbf{P}(A), \cap \rangle$ são simultaneamente

- grupóides abelianos
- semigrupos abelianos
- monóides abelianos

Exp: Grupóide, Semigrupo, Monóide: União e Intersecção

Se união e intersecção

- definidas sobre todos os conjuntos
- constituem grupóides?

Se o conjunto suporte A for vazio,

- $\langle \mathbf{P}(A), \cup \rangle$ e $\langle \mathbf{P}(A), \cap \rangle$
- constituem grupos?

Exp: Grupóide, Semigrupo, Monóide, Grupo: Adição e Multiplicação

Simultaneamente grupóides abelianos, semigrupos abelianos e monóides abelianos (qual o elemento neutro ?)

- $\langle \mathbf{N}, + \rangle$ e $\langle \mathbf{N}, * \rangle$
- $\langle \mathbf{Z}, + \rangle$ e $\langle \mathbf{Z}, * \rangle$
- $\langle \mathbf{R}, + \rangle$ e $\langle \mathbf{R}, * \rangle$

Grupos abelianos

- $\langle \mathbf{Z}, + \rangle$ adição nos inteiros
- $\langle \mathbf{R}, + \rangle$ adição nos reais
- $\langle \mathbf{R} - \{ 0 \}, * \rangle$ multiplicação nos reais *sem o zero*

Exp: Grupóide, Semigrupo, Monóide, Grupo: Unitário

Simultaneamente grupóide abeliano, semigrupo abeliano, monóide abeliano e grupo abeliano

Unitário. $\langle \{ * \}, ! \rangle$, operação $!: \{ * \} \times \{ * \} \to \{ * \}$

- fechada
- associativa
- comutativa
- elemento neutro (o único elemento do suporte)
- elemento inverso (por quê?)
- *única* op. com origem em $\{ * \} \times \{ * \}$ e destino em $\{ * \}$ (por quê?)

Menor monóide (em termos do cardinal do conjunto suporte)

- unitário

Exp: Grupóide, Semigrupo: Vazio

Simultaneamente grupóide abeliano e semigrupo abeliano

Vazio. $\langle \varnothing, \varnothing \rangle$, operação vazia $\varnothing: \varnothing \times \varnothing \to \varnothing$

- fechada
- associativa (por quê?)
- comutativa
- *única* operação com origem em $\varnothing \times \varnothing$ e destino em $\varnothing$ (por quê?)

Menor grupóide (em termos do cardinal do conjunto suporte)

- vazio

Exp: Álgebra Não-Grupóide

A conjunto não-vazio. *Não* são grupóides (por que?)

- Subtração nos naturais: $\langle \mathbf{N}, - \rangle$
- Divisão nos reais: $\langle \mathbf{R}, / \rangle$
- Produto cartesiano no conjunto das partes $\langle \mathbf{P}(A), \times \rangle$

Exp: Álgebra Não-Semigrupo

São grupóides, mas *não* são semigrupos (operações não-associativas)

- Subtração nos inteiros: $\langle \mathbf{Z}, - \rangle$
- Divisão nos reais sem o zero: $\langle \mathbf{R} - \{ 0 \}, / \rangle$

Exp: Álgebra Não-Monóide

Vazio. Semigrupo abeliano $\langle \varnothing, \varnothing \rangle$

- operação $\varnothing: \varnothing \times \varnothing \to \varnothing$
- *não* possui elemento neutro
  - ∗ suporte de um monóide *não* pode ser vazio

Adição e Multiplicação. Excluindo-se, respectivamente, 0 e 1

- $\langle \mathbf{N} - \{ 0 \}, + \rangle$ e $\langle \mathbf{N} - \{ 1 \}, * \rangle$
- $\langle \mathbf{R} - \{ 0 \}, + \rangle$ e $\langle \mathbf{R} - \{ 1 \}, * \rangle$

Exp: Álgebra Não-Grupo

Adição e Multiplicação.

- $\langle \mathbf{N}, + \rangle$ adição nos inteiros
- $\langle \mathbf{R}, * \rangle$ multiplicação nos reais

União e Intersecção. A conjunto *não-vazio*

- $\langle \mathbf{P}(A), \cup \rangle$
- $\langle \mathbf{P}(A), \cap \rangle$

Concatenação. Σ alfabeto *não-vazio*

- $\langle \Sigma^*, \mathrm{conc}, \varepsilon \rangle$

9 – Álgebras e Homomorfismos

9.4 Importantes Propriedades dos Monóides e Grupos

- **Elemento neutro em um monóide é único???**

  - Técnicas de Demonstração - prova por absurdo

*0 é o único elemento neutro da adição em **N***

Teorema: Elemento Neutro de um Monóide é Único

$\langle A, \oplus, e \rangle$ monóide. Então, $e \in A$ é o *único* elemento neutro do monóide

Prova: (*por absurdo*)

$\langle A, \oplus, e \rangle$ monóide. Suponha que e *não* é o único elemento neutro

- existe um outro elemento neutro $\underline{e}$, diferente de e

Então (suponha $a \in A$)

- e é neutro
  - $a = e \oplus a = a \oplus e$
  - para $a = \underline{e}$ tem-se que $\underline{e} = e \oplus \underline{e} = \underline{e} \oplus e$
- $\underline{e}$ é neutro
  - $a = \underline{e} \oplus a = a \oplus \underline{e}$
  - para $a = e$ tem-se que $e = \underline{e} \oplus e = e \oplus \underline{e}$
- transitividade da igualdade
  - $e = \underline{e}$
  - *contradição!!!* foi suposto que $e \neq \underline{e}$

É absurdo supor que o elemento neutro de $\langle A, \oplus, e \rangle$ *não* é único

Logo, o elemento neutro é único

◆ Teorema a seguir

- importante propriedade dos grupos
- generaliza a intuição sobre operações como a adição nos reais
  - ∗ se $x + 3 = y + 3$
  - ∗ então, $x = y$
- propriedade cancelamento

Teorema: Propriedade de Cancelamento dos Grupos

$\langle A, \oplus \rangle$ um grupo satisfaz à propriedade de cancelamento, ou seja, simultaneamente:

- Cancelamento à direita

$$(\forall a \in A)(\forall x \in A)(\forall y \in A)\,(\, x \oplus a = y \oplus a \rightarrow x = y\,)$$

- Cancelamento à esquerda:

$$(\forall a \in A)(\forall x \in A)(\forall y \in A)\,(\, a \oplus x = a \oplus y \rightarrow x = y\,)$$

Prova:

Cancelamento à direita. Suponha que $x \oplus a = y \oplus a$

- $x =$ elemento neutro
- $x \oplus e =$ elemento inverso
- $x \oplus (a \oplus \underline{a}) =$ associatividade
- $(x \oplus a) \oplus \underline{a} =$ hipótese
- $(y \oplus a) \oplus \underline{a} =$ associatividade
- $y \oplus (a \oplus \underline{a}) =$ elemento inverso
- $y \oplus e =$ elemento neutro
- y

- Portanto, $x = y$

Cancelamento à esquerda. A prova é análoga (exercício)

Teorema Elemento Inverso em um Grupo é Único

$\langle A, \oplus \rangle$ grupo. Então, para qualquer $a \in A$, o elemento inverso de a é *único*

Prova:

Exercício

9 – Álgebras e Homomorfismos

9.5 Homomorfismos

- **Homomorfismo de álgebras (já foi afirmado)**
  - é constituído por funções (no caso de álgebras pequenas)
  - mapeiam álgebras de um *mesmo tipo*
  - preservando as suas estruturas
- **Como estruturas (abelianas ou não) são preservadas por homomorfismos de**
  - Grupóides?
  - Semigrupos?
  - Monóides?
  - Grupos?

◆ Monomorfismo, epimorfismo e isomorfismo?

- seria de se esperar que os conceitos fossem naturalmente estendidos para mapeamentos de álgebras
- somente o de isomorfismo pode ser estendido

Obs: Monomorfismo, Epimorfismo e Isomorfismo de Álgebras

Isomorfismo

- baseado na existência de um morfismo inverso
- pode ser naturalmente estendido para as estruturas algébricas

Monomorfismo e epimorfismo

- necessitam de noções e conceitos baseados em Teoria das Categorias (fogem do escopo da disciplina)

Estruturas algébricas isomorfas

- se existe um isomorfismo entre tais estruturas
- são consideradas basicamente a mesma

iguais a menos de isomorfismo

- e, obrigatoriamente

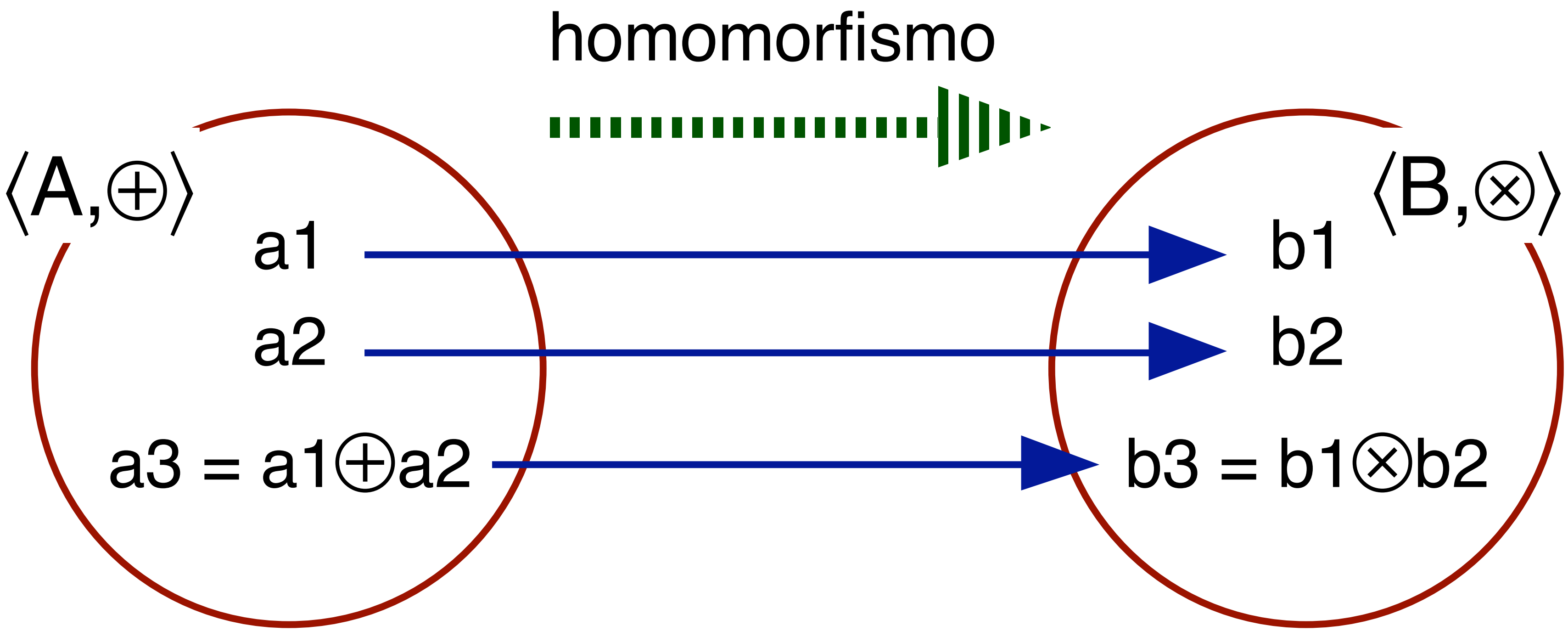
possuem as mesmas propriedades

9 – Álgebras e Homomorfismos

9.5.1 Homomorfismo: Grupóides e Semigrupos

◆ Homomorfismo de grupóides

- função entre os conjuntos suportes
- preserva a operação



◆ Homomorfismo de semigrupos

- é como um homomorfismo de grupóides
- preserva operação $\Rightarrow$ preserva associatividade

Def: Homomorfismo de Grupóides

$\langle A, \oplus \rangle$ e $\langle B, \otimes \rangle$ grupóides

$$h: \langle A, \oplus \rangle \to \langle B, \otimes \rangle$$

função entre os conjuntos suportes $h: A \to B$ tal que

$$(\forall a_1 \in A)(\forall a_2 \in A)(\, h\langle a_1 \oplus a_2 \rangle = h\langle a_1 \rangle \otimes h\langle a_2 \rangle \,)$$

◆ Notação

$$h: \langle A, \oplus \rangle \to \langle B, \otimes \rangle$$

- e *não* simplesmente como função $h: A \to B$
- destaca o fato de que se trata de um morfismo entre álgebras

Exp: Homomorfismo de Grupóides: Identidade, Inclusão

$\langle A, \oplus \rangle$, $\langle \mathbf{N}, + \rangle$ e $\langle \mathbf{Z}, + \rangle$ grupóides

Identidade. Função identidade $id_A: A \to A$ induz

$$id_{\langle A, \oplus \rangle}: \langle A, \oplus \rangle \to \langle A, \oplus \rangle$$

Inclusão. Função inclusão $inc_{\mathbf{N},\mathbf{Z}}: \mathbf{N} \to \mathbf{Z}$ induz

$$inc_{\langle \mathbf{N},+ \rangle, \langle \mathbf{Z},+ \rangle}: \langle \mathbf{N}, + \rangle \to \langle \mathbf{Z}, + \rangle$$

- **Termos identidade e inclusão**
  - consideram *toda a estrutura* do grupóide
  - e não apenas o conjunto suporte

Exp: Morfismo Não-Homomorfismo de Grupóides

A um conjunto e $\langle \mathbf{P}(A), \cup \rangle$, $\langle \mathbf{P}(A), \cap \rangle$ grupóides

Morfismo induzido pela identidade $id_{\mathbf{P}(A)}: \mathbf{P}(A) \to \mathbf{P}(A)$ *não* é, em geral, um homomorfismo de grupóides

$$id_{\mathbf{P}(A)}: \langle \mathbf{P}(A), \cup \rangle \to \langle \mathbf{P}(A), \cap \rangle$$

Exemplo: $A = \{ a, b \}$, $\mathbf{P}(A) = \{ \varnothing, \{ a \}, \{ b \}, \{ a, b \} \}$

- São diferentes
  - $*$ $id_{\mathbf{P}(A)}\langle \{ a \} \cup \{ b \} \rangle = id_{\mathbf{P}(A)}\langle \{ a, b \} \rangle = \{ a, b \}$
  - $*$ $id_{\mathbf{P}(A)}\langle \{ a \} \cup \{ b \} \rangle = id_{\mathbf{P}(A)}\langle \{ a \} \rangle \cap id_{\mathbf{P}(A)}\langle \{ b \} \rangle = \{a\} \cap \{b\} = \varnothing$

Exercício: função inclusão (não-identidade) a qual induz um morfismo não-homomorfismo de grupóides

Exp: Homomorfismo de Grupóides: Concatenação

$\Sigma_1 = \{ a, b, c \}$ e $\Sigma_2 = \{ r, s \}$ alfabetos

$\langle \Sigma_1^*, conc_1 \rangle$ e $\langle \Sigma_2^*, conc_2 \rangle$ grupóides

Função $f: \Sigma_1 \to \Sigma_2$ tal que (função entre *alfabetos*)

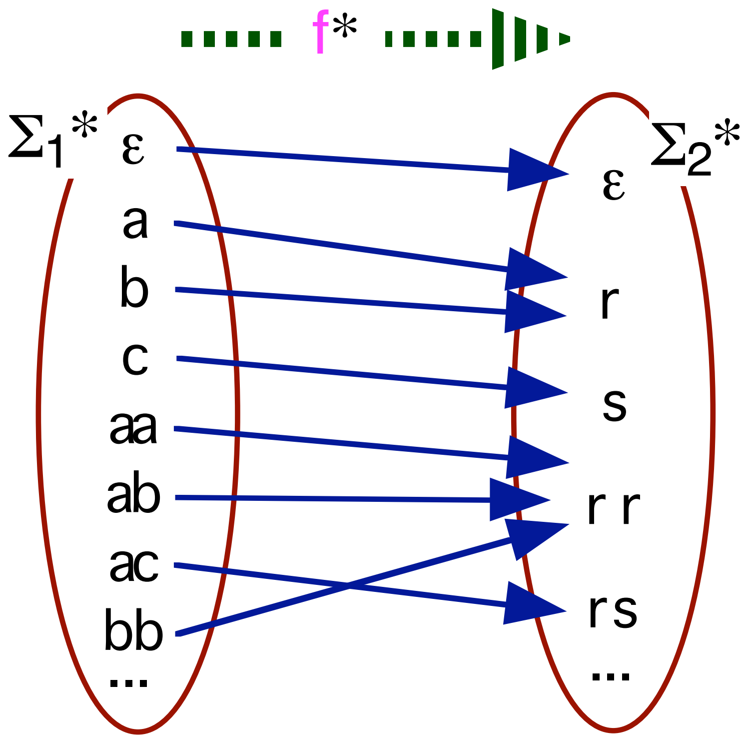
- $f\langle a \rangle = r$
- $f\langle b \rangle = r$
- $f\langle c \rangle = s$

induz canonicamente o homomorfismo de grupóides (mapeia *palavras*)

$$f^*: \langle \Sigma_1^*, conc_1 \rangle \to \langle \Sigma_2^*, conc_2 \rangle$$

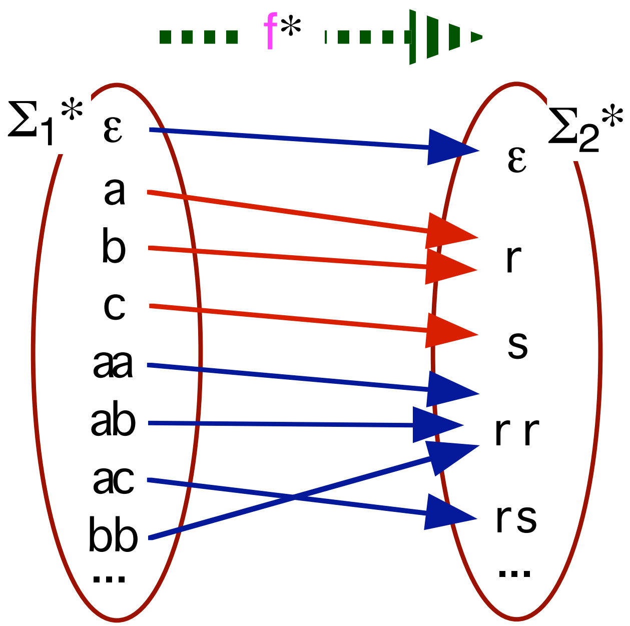
indutivamente definido

- $f^*\langle \varepsilon \rangle = \varepsilon$
- para qualquer $x \in \Sigma_1$, vale $f^*\langle x \rangle = f\langle x \rangle$
- se $x \in \Sigma_1$ e $w \in \Sigma_1^*$, então $f^*\langle x\, w \rangle = f\langle x \rangle\, f^*\langle w \rangle$



Exemplo:

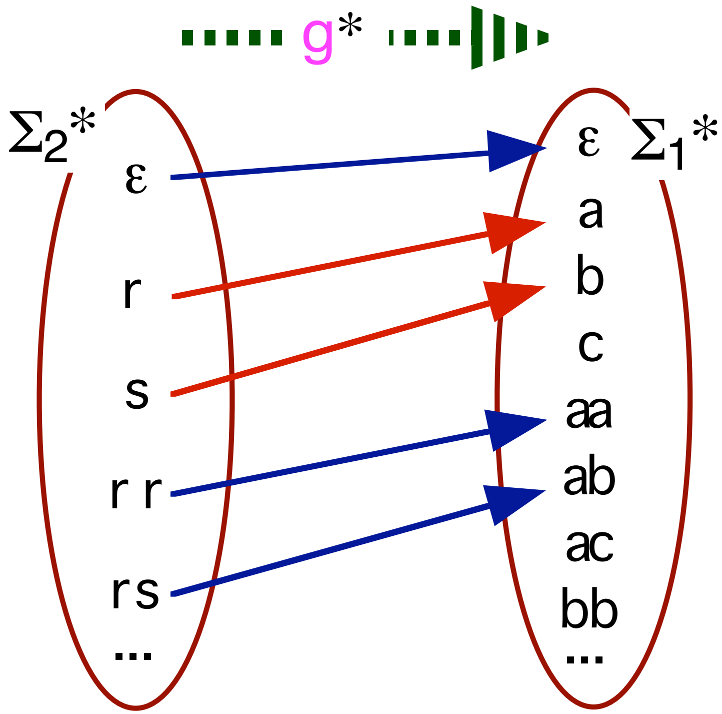
- $f^*\langle abc \rangle =$
- $f\langle a \rangle\ f^*\langle bc \rangle =$
- $f\langle a \rangle\ f\langle b \rangle\ f^*\langle c \rangle =$
- $f\langle a \rangle\ f\langle b \rangle\ f\langle c \rangle\ f^*\langle \varepsilon \rangle =$
- $r\,r\,s\,\varepsilon = r\,r\,s$



Função entre alfabetos $g: \Sigma_2 \to \Sigma_1$

- $g\langle r\rangle = a$
- $g\langle s\rangle = b$

induz o homomorfismo de grupóides



Def: Isomorfismo de Grupóides

$h: \langle A, \oplus \rangle \rightarrow \langle B, \otimes \rangle$ é um Isomorfismo de Grupóides se e somente se

- h possui um homomorfismo de grupóides inverso
  $g: \langle B, \otimes \rangle \rightarrow \langle A, \oplus \rangle$

$$g \circ h = id_{\langle A, \oplus \rangle} \quad \text{e} \quad h \circ g = id_{\langle B, \oplus \rangle}$$

Exp: Isomorfismo de Grupóides

$\langle \{ a \}^*, \text{conc} \rangle$ e $\langle \mathbf{N}, + \rangle$ grupóides

$$h: \{ a \} \to \mathbf{N}$$

- tal que $h\langle a \rangle = 1$

induz o homomorfismo de grupóides indutivamente definido

$$h^*: \langle \{ a \}^*, \text{conc} \rangle \to \langle \mathbf{N}, + \rangle$$

- $h^*\langle \varepsilon \rangle = 0$
- $h^*\langle a \rangle = h\langle a \rangle$
- se $w \in \{ a \}^*$, então $h^*\langle a\,w \rangle = h\langle a \rangle + h^*\langle w \rangle$

Exp: ...Isomorfismo de Grupóides

Mapeia cada palavra no seu correspondente tamanho

$$h^*\langle aaa\rangle = h\langle a\rangle + h^*\langle aa\rangle = h\langle a\rangle + h\langle a\rangle + h^*\langle a\rangle =$$

$$h\langle a\rangle + h\langle a\rangle + h\langle a\rangle + h^*\langle \varepsilon\rangle = 1 + 1 + 1 + 0 = 3$$

Homomorfismo induzido $h^*: \langle \{ a \}^*, \text{conc}\rangle \to \langle \mathbf{N}, +\rangle$

- é isomorfismo de grupóides (qual o homomorfismo inverso?).

Logo, $\langle \Sigma^*, \text{conc}\rangle$ e $\langle \mathbf{N}, +\rangle$ são

iguais a menos de isomorfismo

- base unária para os naturais e a operação de adição

Obs: Base de Sistemas Numéricos

Base decimal

- base dos sistemas numéricos usualmente adotada na Matemática
  - ∗ origem: número de dedos das duas mãos

- base complicada para representação em sistemas computadores
  - ∗ computador: usa base binária
  - ∗ os dois valores possíveis de um bit: 0 e 1 ou qq alfabeto binário

Exemplo anterior: base unária para os naturais e a adição

Estudo de bases

- Arquitetura de Computadores e Aritmética Computacional

Exercício: base binária para os números naturais e a adição

◆ Dois teoremas importantes

- composição de hom. de grupóides é hom. de grupóides
- hom. de grupóides preservam a propriedade associativa

Teorema: Composição de Homomorfismo de Grupóides

$\langle A, \oplus \rangle$, $\langle B, \otimes \rangle$ e $\langle C, \nabla \rangle$ grupóides

$f: \langle A, \oplus \rangle \to \langle B, \otimes \rangle$ e $g: \langle B, \otimes \rangle \to \langle C, \nabla \rangle$ hom. de grupóides

$$g \circ f: \langle A, \oplus \rangle \to \langle C, \nabla \rangle$$

induzido pela composição das funções $f: A \to B$ e $g: B \to C$

$$g \circ f: A \to C$$

é homomorfismo de grupóides

Prova:

Suponha $f: \langle A, \oplus \rangle \to \langle B, \otimes \rangle$ e $g: \langle B, \otimes \rangle \to \langle C, \nabla \rangle$ hom. de grupóides

Como a composição de funções é uma função

- mostrar que $g \mathbin{\mathbf{o}} f: \langle A, \oplus \rangle \to \langle C, \nabla \rangle$ é hom. de grupóides
- basta mostrar que preserva a operação

Para quaisquer $a_1 \in A$ e $a_2 \in A$

- $g \mathbin{\mathbf{o}} f\langle a_1 \oplus a_2 \rangle =$ definição de composição
- $g\langle f\langle a_1 \oplus a_2 \rangle\rangle =$ f hom. de grupóides
- $g\langle f\langle a_1 \rangle \otimes f\langle a_2 \rangle\rangle =$ g hom. de grupóides
- $g\langle f\langle a_1 \rangle\rangle \nabla g\langle f\langle a_2 \rangle\rangle =$ definição de composição
- $g \mathbin{\mathbf{o}} f\langle a_1 \rangle \nabla g \mathbin{\mathbf{o}} f\langle a_2 \rangle$

Portanto $g \mathbin{\mathbf{o}} f: \langle A, \oplus \rangle \to \langle C, \nabla \rangle$ é hom. de grupóides

Teorema: Hom de Grupóides Preserva a Associatividade

Sejam $\langle A, \oplus \rangle$ e $\langle B, \otimes \rangle$ grupóides e $f: \langle A, \oplus \rangle \to \langle B, \otimes \rangle$ hom. de grupóides

Se $\langle A, \oplus \rangle$ *ou* $\langle B, \otimes \rangle$ é semigrupo

- então $f: \langle A, \oplus \rangle \to \langle B, \otimes \rangle$ preserva a associatividade

Prova:

Caso 1: $\langle A, \oplus \rangle$ é semigrupo

Como $\oplus$ é associativa, para quaisquer $a \in A$, $b \in A$ e $c \in A$

$$f\langle a \oplus (b \oplus c)\rangle = f\langle (a \oplus b) \oplus c\rangle$$

Como $f: \langle A, \oplus \rangle \to \langle B, \otimes \rangle$ preserva a operação

- $f\langle a \oplus (b \oplus c)\rangle = f\langle (a \oplus b) \oplus c\rangle \Leftrightarrow$
- $f\langle a\rangle \otimes f\langle (b \oplus c)\rangle = f\langle (a \oplus b)\rangle \otimes f\langle c\rangle \Leftrightarrow$
- $f\langle a\rangle \otimes (f\langle b\rangle \otimes f\langle c\rangle) = (f\langle a\rangle \otimes f\langle b\rangle) \otimes f\langle c\rangle$

Logo, preserva a associatividade

Caso 2: $\langle B, \otimes \rangle$ é semigrupo

Para quaisquer $a \in A$, $b \in A$ e $c \in A$

- $f\langle a \oplus (b \oplus c) \rangle =$ — f preserva a operação
- $f\langle a \rangle \otimes f\langle b \oplus c \rangle =$ — f preserva a operação
- $f\langle a \rangle \otimes (f\langle b \rangle \otimes f\langle c \rangle) =$ — $\otimes$ é associativa
- $(f\langle a \rangle \otimes f\langle b \rangle) \otimes f\langle c \rangle =$ — f preserva a operação
- $f\langle a \oplus b \rangle \otimes f\langle c \rangle =$ — f preserva a operação
- $f\langle (a \oplus b) \oplus c \rangle$

Logo, preserva a associatividade

Portanto, hom de semigrupos é como um hom. de grupóides

- basta preservar a operação

Def: Homomorfismo de Semigrupos

$\langle A, \oplus \rangle$ e $\langle B, \otimes \rangle$ semigrupos

Homomorfismo de Semigrupos

$$h: \langle A, \oplus \rangle \to \langle B, \otimes \rangle$$

- é um homomorfismo de grupóides $h: \langle A, \oplus \rangle \to \langle B, \otimes \rangle$

Isomorfismo de semigrupos

- se e somente se h possui um hom. de semigrupos inverso

◆ Comutatividade

- raciocínio análogo
- exercício

Teorema: Hom. de Grupóides Preserva Comutatividade

$\langle A, \oplus \rangle$ e $\langle B, \otimes \rangle$ grupóides

$f: \langle A, \oplus \rangle \to \langle B, \otimes \rangle$ hom. de grupóides

Se $\langle A, \oplus \rangle$ *ou* $\langle B, \otimes \rangle$ é abeliano

- então $f: \langle A, \oplus \rangle \to \langle B, \otimes \rangle$ preserva a comutatividade

9 – Álgebras e Homomorfismos

9.1.2 Homomorfismo de Monóides

◆ Mapeamento de monóides

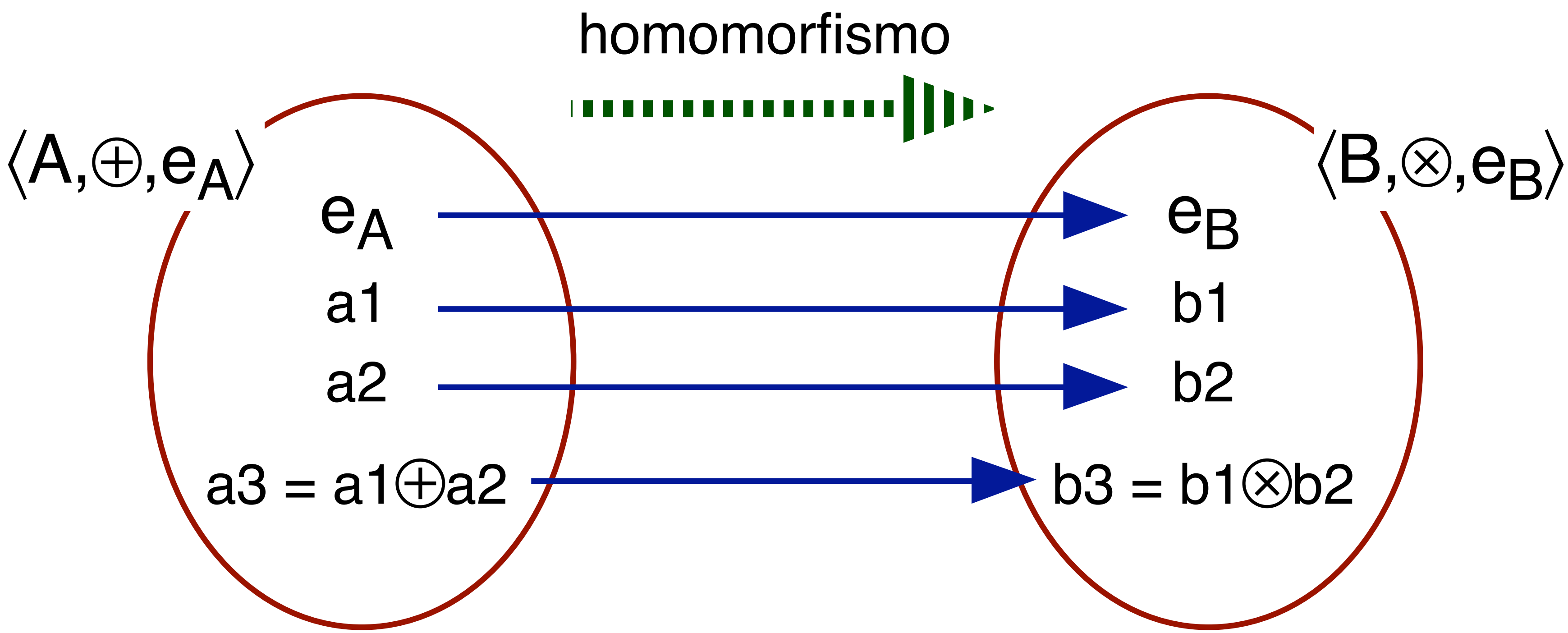
- preservar a operação
- *não* necessariamente implica preservar o elemento neutro
  - ∗ exercício

◆ Homomorfismo de monóides

- função entre os conjuntos suportes tal que, preserva
  - ∗ operação (como hom. de grupóides/semigrupos)
  - ∗ elemento neutro

◆ Homomorfismo de monóides

- função entre os conjuntos suportes
  - ∗ preserva operação (como hom. de grupóides/semigrupos)
  - ∗ preserva elemento neutro



Def: Homomorfismo de Monóides

$\langle A, \oplus, e_A \rangle$ e $\langle B, \otimes, e_B \rangle$ monóides

Homomorfismo de Monóides

$$h: \langle A, \oplus, e_A \rangle \rightarrow \langle B, \otimes, e_B \rangle$$

- hom. de semigrupos (ou grupóides) $h: \langle A, \oplus \rangle \rightarrow \langle B, \otimes \rangle$
- preserva o elemento neutro

$$h\langle e_A \rangle = e_B$$

Isomorfismo de monóides

- se e somente se possuir um hom. de monóides inverso

Exp: Homomorfismo: Identidade, Inclusão

$\langle A, \oplus, e \rangle$, $\langle \mathbf{N}, +, 0 \rangle$ e $\langle \mathbf{Z}, +, 0 \rangle$ monóides

Identidade. Função identidade $id_A: A \to A$

- induz homomorfismo identidade de monóides
- isomorfismo de monóides

$$id_{\langle A, \oplus, e \rangle}: \langle A, \oplus, e \rangle \to \langle A, \oplus, e \rangle$$

Inclusão. Função inclusão $inc_{\mathbf{N},\mathbf{Z}}: \mathbf{N} \to \mathbf{Z}$

- induz o homomorfismo inclusão de monóides abelianos

$$inc_{\langle \mathbf{N}, +, 0 \rangle, \langle \mathbf{Z}, +, 0 \rangle}: \langle \mathbf{N}, +, 0 \rangle \to \langle \mathbf{Z}, +, 0 \rangle$$

Exp: Homomorfismo: União

$A = \{ a, b \}$ e $X = \{ x, y, z \}$ conjuntos

$\langle \mathbf{P}(A), \cup, \varnothing \rangle$ e $\langle \mathbf{P}(B), \cup, \varnothing \rangle$ monóides abelianos

$$h: \langle \mathbf{P}(A), \cup, \varnothing \rangle \to \langle \mathbf{P}(X), \cup, \varnothing \rangle$$

tal que:

- $h\langle \varnothing \rangle = \varnothing$
- $h\langle \{ a \} \rangle = \{ x, y \}$
- $h\langle \{ b \} \rangle = \{ y, z \}$
- $h\langle \{ a, b \} \rangle = \{ x, y, z \}$

Preserva elemento neutro e operação

Exp: …Homomorfismo: União

Exemplificando a preservação da operação

- $h\langle \{ a \} \cup \{ b \} \rangle =$
- $h\langle \{ a, b \} \rangle =$
- $\{ x, y, z \} =$
- $\{ x, y \} \cup \{ y, z \} =$
- $h\langle \{ a \} \rangle \cup h\langle \{ b \} \rangle$

Portanto, $h\langle \{ a \} \cup \{ b \} \rangle = h\langle \{ a \} \rangle \cup h\langle \{ b \} \rangle$

Exp: Homomorfismo: Isomorfismo

O homomorfismo de grupóides (exemplo anterior)

$$h^*: \langle \{ a \}^*, \text{conc}, \varepsilon \rangle \rightarrow \langle \mathbf{N}, +, 0 \rangle$$

é um isomorfismo de monóides

- preserva operação (é hom. de grupóides)
- preserva elemento neutro

$$h^*\langle \varepsilon \rangle = 0$$

Teorema: Composição de Homomorfismo de Monóides

$\langle A, \oplus, e_A \rangle$, $\langle B, \otimes, e_B \rangle$ e $\langle C, \nabla, e_C \rangle$ monóides

$f: \langle A, \oplus, e_A \rangle \to \langle B, \otimes, e_B \rangle$ e $g: \langle B, \otimes, e_B \rangle \to \langle C, \nabla, e_C \rangle$ hom. de monóides

O homomorfismo composto

$$g \circ f: \langle A, \oplus, e_A \rangle \to \langle C, \nabla, e_C \rangle$$

- induzido pela composição das funções $f: A \to B$ e $g: B \to C$
- *é* um homomorfismo de monóides

Prova: (*direta*)

$f: \langle A, \oplus, e_A \rangle \rightarrow \langle B, \otimes, e_B \rangle$ e $g: \langle B, \otimes, e_B \rangle \rightarrow \langle C, \nabla, e_C \rangle$ hom. de monóides

Como a composição de hom. de semigrupos é hom. de semigrupos basta mostrar que $g \mathbin{\mathbf{o}} f: \langle A, \oplus, e_A \rangle \rightarrow \langle C, \nabla, e_C \rangle$ preserva elem. neutro

- $g \mathbin{\mathbf{o}} f\langle e_A \rangle =$ definição de composição
- $g\langle f\langle e_A \rangle\rangle =$ f é homomorfismo de monóides
- $g\langle e_B \rangle =$ g é homomorfismo de monóides
- e_C

Portanto, $g \mathbin{\mathbf{o}} f\langle e_A \rangle = e_C$

Logo, $g \mathbin{\mathbf{o}} f: \langle A, \oplus, e_A \rangle \rightarrow \langle C, \nabla, e_C \rangle$ é um homomorfismo de monóides

9 – Álgebras e Homomorfismos

9.1 Operações Binárias
9.2 Propriedades das Operações Binárias
9.3 Grupóides, Semigrupos, Monóides, Grupos
9.4 Importantes Propriedades dos Monóides e Grupos
9.5 Homomorfismos
  9.5.1 Grupóides e Semigrupos
  9.5.2 Monóides
  9.5.3 Grupos
9.6 Monóide Livre Gerado e Fecho de Kleene
9.7 Grafos
9.8 Categorias

9.1.3 Homomorfismo de Grupos

- **Homomorfismo de grupos**
  - como homomorfismo de grupóides
  - basta preservar a operação
- **Prova-se que, em se tratando de grupos**
  - preservar a operação
  - *implica* preservar
    - elemento neutro
    - elemento inverso

◆ Composição homs. de grupóides é hom. de grupóides

- *Implica*: composição de homs. de grupos é hom. de grupos

◆ Analogamente aos homs. Anteriores

- isomorfismo de grupos se e somente se
  - possuir um homomorfismo de grupos inverso

Teorema: Homomorfismo de Grupos $\times$ Elemento Neutro

$\langle A, \oplus, e_A \rangle$ e $\langle B, \otimes, e_B \rangle$ grupos

$f: \langle A, \oplus, e_A \rangle \rightarrow \langle B, \otimes, e_B \rangle$ homomorfismo de grupóides

Então, f preserva o elemento neutro

$$f\langle e_A \rangle = e_B$$

Prova:

Suponha $\langle A, \oplus, e_A \rangle$ e $\langle B, \otimes, e_B \rangle$ grupos e $f: \langle A, \oplus, e_A \rangle \to \langle B, \otimes, e_B \rangle$ hom. de grupóides

- $f\langle e_A \rangle \otimes f\langle e_A \rangle =$ — f é homomorfismo de grupóides
- $f\langle e_A \oplus e_A \rangle =$ — elemento neutro de $\oplus$
- $f\langle e_A \rangle =$ — elemento neutro de $\otimes$
- $f\langle e_A \rangle \otimes e_B$

Portanto, $f\langle e_A \rangle \otimes f\langle e_A \rangle = f\langle e_A \rangle \otimes e_B$. Pela propriedade do cancelamento

$$f\langle e_A \rangle = e_B$$

Logo, f preserva o elemento neutro

Teorema: Homomorfismo de Grupos × Elemento Inverso

$\langle A, \oplus, e_A \rangle$ e $\langle B, \otimes, e_B \rangle$ grupos

$f: \langle A, \oplus, e_A \rangle \rightarrow \langle B, \otimes, e_B \rangle$ homomorfismo de grupóides

Então f preserva o elemento inverso

$$(\forall a \in A)\ (\ f\langle \underline{a} \rangle = \underline{f\langle a \rangle}\ )$$

Prova:

Suponha $\langle A, \oplus, e_A \rangle$ e $\langle B, \otimes, e_B \rangle$ grupos, $f: \langle A, \oplus, e_A \rangle \rightarrow \langle B, \otimes, e_B \rangle$ homomorfismo de grupóides e qualquer $a \in A$

• $f\langle \underline{a} \rangle \otimes f\langle a \rangle =$	f é homomorfismo de grupóides
• $f\langle \underline{a} \oplus a \rangle =$	elemento inverso de $\oplus$
• $f\langle e_A \rangle =$	f preserva elemento neutro
• $e_B =$	elemento inverso de $\otimes$
• $\underline{f\langle a \rangle} \otimes f\langle a \rangle$	f é homomorfismo de grupóides

Portanto, $f\langle \underline{a} \rangle \otimes f\langle a \rangle = \underline{f\langle a \rangle} \otimes f\langle a \rangle$. Pela propriedade do cancelamento

$$f\langle \underline{a} \rangle = \underline{f\langle a \rangle}$$

Logo, f preserva o elemento inverso

9 – Álgebras e Homomorfismos

9.6 Monóide Livre Gerado e Fecho de Kleene

◆ Já foi visto

- para um alfabeto Σ, a álgebra interna $\langle \Sigma^*, \text{conc}, \varepsilon \rangle$ é monóide
- Σ^* pode ser indutivamente definido a partir do alfabeto Σ

◆ Definição indutiva

- *Base de Indução*
  - $\varepsilon \in \Sigma^*$
  - para qualquer $x \in \Sigma$, tem-se que $x \in \Sigma^*$

- *Passo de Indução*
  - se u e v são palavras de Σ^*, então a concatenação $u\,v \in \Sigma^*$

◆ O raciocínio pode ser aplicado a um conjunto A qq

- não necessariamente é um alfabeto (não finito)
- passo de indução
  - considera a palavra vazia ε como elemento neutro

$$\text{se } u \in A^*, \text{ então } u\,\varepsilon = \varepsilon\,u = u$$

◆ Monóide livre

- tipo especial e importante de monóide
- conjunto suporte A^* é (livremente) gerado por um conjunto A

Def: Monóide Livre, Fecho de Kleene

A conjunto

Monóide Livre Gerado por A ou Monóide Livremente Gerado por A

$$\langle A^*, \text{conc}, \varepsilon \rangle$$

- conjunto suporte A^* = Fecho de Kleene de A
- A é denominado de Gerador

Base de Indução

- $\varepsilon \in A^*$
- para qualquer $x \in A$, tem-se que $x \in A^*$

Passo de Indução

- se u e v são palavras de A^*, então a concatenação $u\,v \in A^*$

◆ Portanto

- conjunto de todas as palavras sobre um alfabeto
  - ⁎ conjunto suporte do monóide livremente gerado pelo alfabeto
  - ⁎ Fecho de Kleene do alfabeto

- linguagem formal (como Pascal)
  - ⁎ subconjunto do Fecho de Kleene do alfabeto

◆ Condições para que monóide livre seja abeliano???

Exp: Homomorfismo – Monóides Livres

$\Sigma_1 = \{ a, b, c \}$ e $\Sigma_2 = \{ r, s \}$ alfabetos

$\langle \Sigma_1^*, \ conc_1, \varepsilon \rangle$ e $\langle \Sigma_2^*, conc_2, \varepsilon \rangle$ monóides

Canonicamente induzidos por funções nos geradores

- $f: \Sigma_1 \to \Sigma_2$ função
  - $f\langle a \rangle = r$
  - $f\langle b \rangle = r$
  - $f\langle c \rangle = s$
- $g: \Sigma_2 \to \Sigma_1$ função
  - $g\langle r \rangle = a$
  - $g\langle s \rangle = b$

Exp: …Homomorfismo – Monóides Livres

$\sum_1 = \{ a, b, c \}$ e $\sum_2 = \{ r, s \}$ alfabetos

Homomorfismo não induzido por função entre os geradores

- $h\langle\varepsilon\rangle = \varepsilon$
- $h\langle a\rangle = rr$
- $h\langle b\rangle = rs$
- $h\langle c\rangle = ss$
- se $x \in \Sigma_1$ e $w \in \Sigma_1{}^*$, então $h\langle x\,w\rangle = h\langle x\rangle\, h\langle w\rangle$

- exemplo
  - $h\langle abc\rangle =$
  - $h\langle a\rangle\, h\langle bc\rangle =$
  - $h\langle a\rangle\, h\langle b\rangle\, h\langle c\,\varepsilon\rangle =$
  - $h\langle a\rangle\, h\langle b\rangle\, h\langle c\rangle\, h\langle\varepsilon\rangle =$
  - $rr\,rs\,ss\,\varepsilon =$
  - $rr\,rs\,ss$

9 – Álgebras e Homomorfismos

9.7 Grafos

- **Até o momento, as álgebras apresentadas**
  - uma única operação
  - definida sobre um único conjunto
- **Freqüentemente, álgebras**
  - mais de uma operação
  - operações definidas sobre mais de um conjunto

◆ Álgebras polissortidas

- definidas sobre mais de um conjunto
- termo sorte: gênero, classe ou espécie

◆ Álgebras monossortidas

- definidas sobre um único conjunto

◆ Noção de grafo

- informalmente apresentada: estudo das endorrelações
- toda endorrelação pode ser vista como um grafo
  - ∗ e conseqüentemente, como uma álgebra
- nem todo grafo pode ser visto como uma endorrelação
  - ∗ exercício

- **Grafos são importantes para Computação e Informática**
- **Estudo de Grafos é brevemente apresentado**
- **Ênfase grafos**
  - grafos pequenos
    - nodos e arcos constituem conjuntos
  - grafos direcionados
    - arcos possuem sentido

◆ Grafo visto como álgebra

- nodos e arcos
  - ∗ conjuntos sobre os quais as operações são definidas
  - ∗ álgebra polissortida

- origem e destino
  - ∗ operações unárias fechadas (*não*-internas)
  - ∗ associam, para cada arco, o nodo origem e destino

Def: Grafo

Grafo Pequeno Direcionado ou simplesmente Grafo G

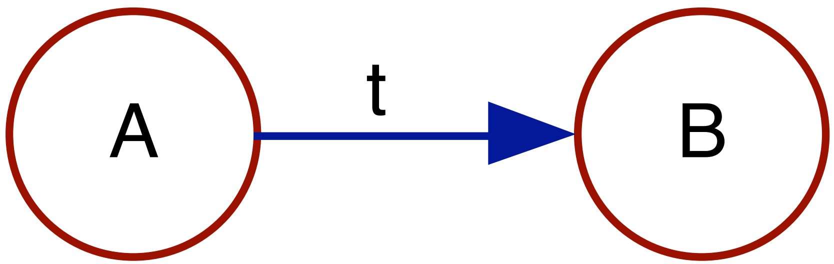
- álgebra polissortida

$$G = \langle V, T, orig, dest \rangle$$

- V conjunto de Nodos ou Vértices
- T conjunto de Arcos, Arestas ou Setas
- $orig: T \to V$ e $dest: T \to V$
  - ∗ operações totais (funções)
  - ∗ denominadas Origem e Destino

◆ Notação

- arco t tal que $orig\langle t \rangle = A$ e $dest\langle t \rangle = B$
- denotado por $t: A \to B$
- representado na forma de diagrama



Exp: Grafo

Arco único. $G_1 = \langle \{ A, B \}, \{ t \}, orig_1, dest_1 \rangle$

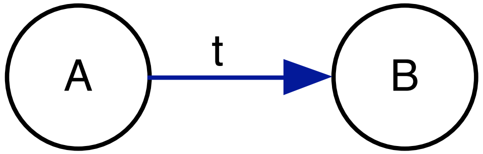
- $orig\langle t \rangle = A$
- $dest\langle t \rangle = B$

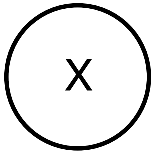
Nodo isolado. $G_2 = \langle \{ X \}, \varnothing, orig_2, dest_2 \rangle$

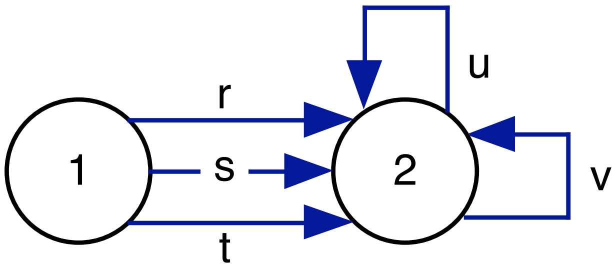
- $orig_2 \colon \varnothing \to \{ X \}$ e $dest_2 \colon \varnothing \to \{ X \}$
- funções vazias

Arcos paralelos. $G_3 = \langle \{ 1, 2 \}, \{ r, s, t, u, v \}, \partial 0_3, \partial 1_3 \rangle$

- arcos paralelos: mesmos nodos origem e destino







◆ Multigrafo

- freqüentemente, grafos com arcos paralelos são ditos multigrafos

◆ Homomorfismo de grafos

- preserva a estrutura dos grafos,
- ao mapear os nodos e arcos
  - ∗ deve preservar as operações origem e destino
- mapeamento de um arco
  - ∗ de acordo com o mapeamento dos seus nodos origem e destino

Def: Homomorfismo de Grafos

$G_1 = \langle V_1, T_1, orig_1, dest_1 \rangle$ e $G_2 = \langle V_2, T_2, orig_2, dest_2 \rangle$ grafos

$$h: G_1 \to G_2$$

par de funções

$$h = \langle h_V, h_T \rangle$$

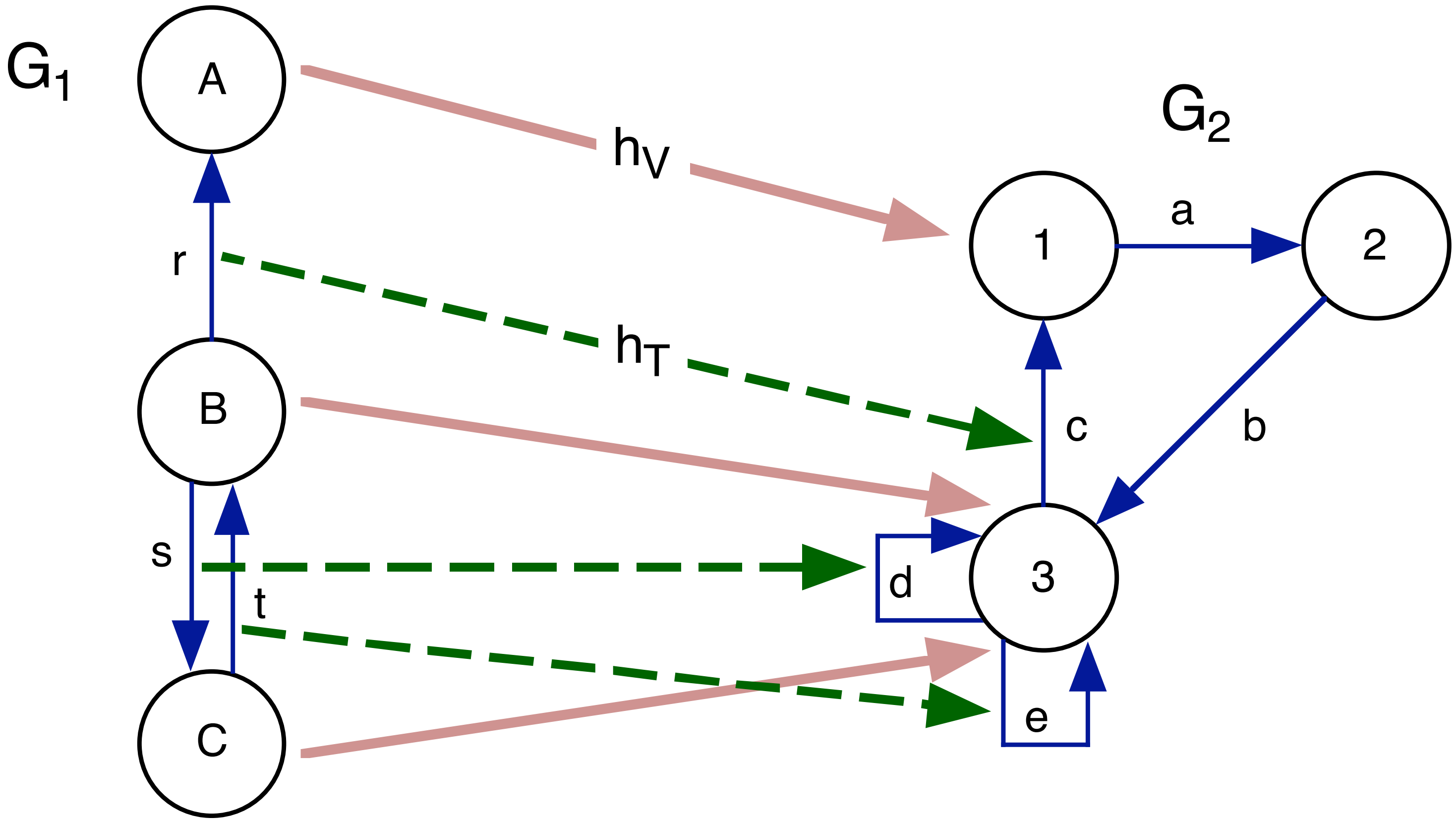
onde

$$h_V: V_1 \to V_2 \quad \text{e} \quad h_T: T_1 \to T_2$$

tais que

$$orig_2 \circ h_T = h_V \circ orig_1 \quad \text{e} \quad dest_2 \circ h_T = h_V \circ dest_1$$

Exp: Homomorfismo de Grafos



- existe mais algum homomorfismo de grafos de G_1 para G_2?
- existe pelo menos um morfismo de G_2 para G_1?

Teorema: Composição de Homomorfismos de Grafos

Sejam $f: G_1 \to G_2$ e $g: G_2 \to G_3$ homomorfismos de grafos

$$g \circ f: G_1 \to G_3$$

tal que $g \circ f = \langle g_V \circ f_V, g_T \circ f_T \rangle$, é um homomorfismo de grafos

Prova: (*direta*)

Seja $t: A \to B$ arco de G_1. Então

- $t: A \to B$ é arco de G_1 $\Rightarrow$
- $f_T(t): f_V(A) \to f_V(B)$ é arco de G_2 (f é hom. de grafos) $\Rightarrow$
- $g_T(f_T(t)): g_V(f_V(A)) \to g_V(f_V(B))$ é arco de G_3 (g é hom. de grafos)

Logo, $g \circ f$ é homomorfismo de grafos

9 – Álgebras e Homomorfismos

9.8 Categorias

- **Em um primeiro momento, Teoria das Categorias pode ser vista como**
  - generalização da álgebra de funções
  - principal operação: composição de funções
- **Categoria é uma estrutura abstrata**
  - constituída de objetos e setas entre os objetos
  - com uma propriedade fundamental
    - composicionalidade das setas

Categoria	Objetos	Setas	Composição
conjuntos e funções	conjuntos	funções (totais)	composição de funções
figuras	figuras	transform. de figuras	construtor de transform. “complexas”
um programa funcional	tipos de dados	operações	construtor operações não-primitivas
espaços vetoriais	espaços vetoriais	transforma. lineares	composição de transformações lineares
grafos	grafos	homomorfismo de grafos	composição homomorfismo de grafos
lógica	proposições	provas	transitividade das provas
uma máquina de estados	estados	transições	construtor de computações
conjuntos parcialmente ordenados	conjuntos parcialmente ordenados	funções monotônicas	composição de funções monotônicas
um conjunto parcialmente ordenado	elementos do conjunto	pares da relação de ordem parcial	transitividade da relação de ordem parcial

◆ Qq modificação sobre objetos, setas ou composição

- nova categoria

Exp: Conjuntos e Funções

Substituição das funções (totais) por funções parciais

- nova categoria
  - ∗ conjuntos e funções parciais
  - ∗ com diferentes propriedades
- produto cartesiano
  - ∗ generalizado categorialmente
  - ∗ diferente nas duas categorias

◆ Objeto, seta e composição

- não necessariamente possuem estruturas
  - ⁎ que lembrem as da Teoria dos Conjuntos

Exp: Conjunto Parcialmente Ordenado como Categoria

$$
\begin{tikzcd}
0 \arrow[loop above, "0 \leq 0"] \arrow[r, "0 \leq 1"] \arrow[rr, bend right, "(0 \leq 2) = (1 \leq 2) \circ (0 \leq 1)"'] & 1 \arrow[loop above, "1 \leq 1"] \arrow[r, "1 \leq 2"] & 2 \arrow[loop above, "2 \leq 2"]
\end{tikzcd}
$$

- objetos - não possuem qualquer estrutura (elementos de conjunto)
- setas - pares de elementos
- composição - transitividade da relação

◆ Uma mesma estrutura, simultaneamente

- pode constituir uma categoria por si só
  - conj. parcialmente ordenado como categoria

- ou ser objeto de uma categoria
  - categoria dos conj. parcialmente ordenados
  - (conjuntos parcialmente ordenados e funções monotônicas)

Exp: Categoria dos Conjuntos Parcialmente Ordenados

- pode ser vista como uma categoria de categorias
  - uma categoria
  - cujos objetos são conjuntos parcialmente ordenados vistos como categorias

◆ Teoria das Categorias e Ciência da Computação

- possuem muito em comum
- são enriquecidas mutuamente
  - ∗ a partir de visões e abordagens de um campo sobre o outro

◆ Entre as características que motivam o seu uso

- destaca-se a expressividade de suas construções
- observado nas Diretrizes Curriculares do MEC para Cursos de Computação e Informática

Teoria das Categorias possui construções cujo poder de expressão não possui, em geral, paralelo em outras teorias. Esta expressividade permite formalizar idéias mais complexas de forma mais simples, bem como propicia um novo ou melhor entendimento das questões relacionadas com toda a Ciência da Computação. Como Teoria das Categorias é uma ferramenta nova, para exemplificar, vale a pena estabelecer um paralelo com a linguagem Pascal: Teoria das Categorias está para a Teoria dos Conjuntos assim como Pascal está para a linguagens Assembler.

- **Apenas o conceito de categoria (como álgebra) é apresentado**
  - estudo de suas propriedades e aplicações
    - não é objetivo desta disciplina
- **Categoria é basicamente um grafo**
  - eventualmente grande
  - arcos são componíveis, formando caminhos
  - cada nodo possui um endoarco especial: identidade

Def: Categoria

Uma álgebra polissortida

$$\mathbf{C} = \langle \mathrm{Ob}_{\mathbf{C}}, \mathrm{Mor}_{\mathbf{C}}, \mathrm{orig}, \mathrm{dest}, \iota, \circ \rangle$$

- $\mathrm{Ob}_{\mathbf{C}}$ - coleção de Objetos
- $\mathrm{Mor}_{\mathbf{C}}$ - coleção de Morfismos ou Setas
- $\mathrm{orig}: \mathrm{Mor}_{\mathbf{C}} \to \mathrm{Ob}_{\mathbf{C}}$ e $\mathrm{dest}: \mathrm{Mor}_{\mathbf{C}} \to \mathrm{Ob}_{\mathbf{C}}$
  - ∗ operações fechadas e totais Origem e Destino
  - ∗ um morfismo f tal que $\mathrm{orig}(f) = A$ e $\mathrm{dest}(f) = B$ é denotado por

$$f: A \to B$$

* $\mathbf{o}: (\mathrm{Mor}\mathcal{C})^2 \to \mathrm{Mor}\mathcal{C}$ - operação Composição
  * cada par de morfismos

$$\langle f: A \to B, g: B \to C \rangle$$

  * é associado a um morfismo

$$g \mathbf{o} f: A \to C$$

  * deve satisfazer a propriedade associativa

$$(h \mathbf{o} g) \mathbf{o} f = h \mathbf{o} (g \mathbf{o} f)$$

* $\iota: \mathrm{Ob}\mathcal{C} \to \mathrm{Mor}\mathcal{C}$ - operação Identidade
  * cada objeto A é associado a um morfismo

$$\iota_A: A \to A$$

  * deve satisfazer a propriedade da identidade (suponha $f: A \to B$)

$$f \mathbf{o} \iota_A = \iota_B \mathbf{o} f = f$$

Exp: Categoria $\mathbf{Set}$

$$\mathbf{Set} = \langle \mathrm{Ob}_{\mathbf{Set}}, \mathrm{Mor}_{\mathbf{Set}}, \mathrm{orig}, \mathrm{dest}, \iota, \mathbf{o} \rangle$$

- $\mathrm{Ob}_{\mathbf{Set}}$ - coleção de todos os conjuntos
- $\mathrm{Mor}_{\mathbf{Set}}$ - coleção de todas as funções (totais)
- orig: $\mathrm{Mor}_{\mathbf{Set}} \to \mathrm{Ob}_{\mathbf{Set}}$ e dest: $\mathrm{Mor}_{\mathbf{Set}} \to \mathrm{Ob}_{\mathbf{Set}}$
  - ∗ para qualquer função f com domínio em A e codomínio em B,

$$\mathrm{orig}(f) = A \text{ e } \mathrm{dest}(f) = B$$

- $\mathbf{o}$: $(\mathrm{Mor}_{\mathbf{Set}})^2 \to \mathrm{Mor}_{\mathbf{Set}}$
  - ∗ operação de composição de funções (é associativa)
- ι: $\mathrm{Ob}_{\mathbf{Set}} \to \mathrm{Mor}_{\mathbf{Set}}$ - operação identidade
  - ∗ cada conjunto A é associado à função identidade id_A: $A \to A$

$$\iota\langle A \rangle = id_A$$

Exp: Categoria **Mon**

- objetos: todos os monóides
- morfismos: todos os homomorfismos de monóides
- composição: composição de homomorfismos de monóides
- identidade: dada pelo homomorfismo identidade de cada monóide

◆ Análogamente, as categorias

- grupóides e correspondentes homomorfismos
- semigrupos e corrrespondentes homomorfismos
- grupos e corrrespondentes homomorfismos

Exp: Categoria **Gr**

- objetos: todos os grafos
- morfismos: todos os homomorfismos de grafos
- composição: composição de homomorfismos de grafos
- identidade: dada pelo homomorfismo identidade de cada grafo

Exp: As "Menores" Categorias

Categoria Vazia (justifique cada componente)

$$\langle \varnothing, \varnothing, \varnothing, \varnothing, \varnothing, \varnothing \rangle$$

Categoria **1**

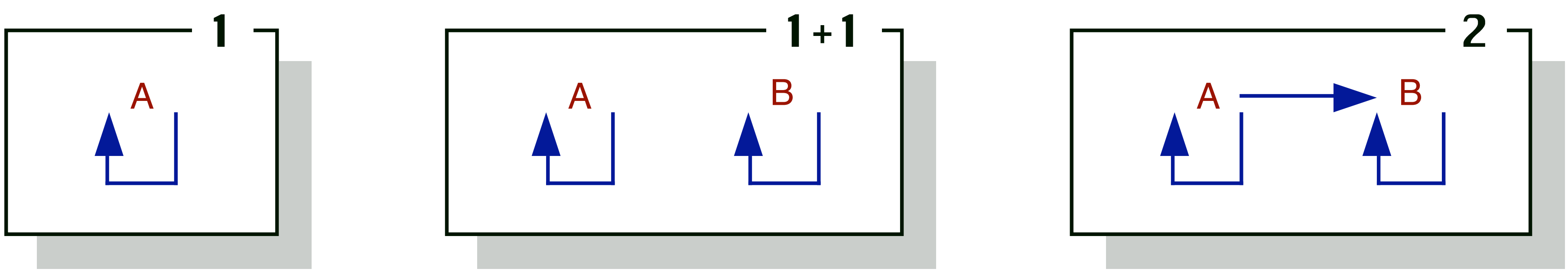
- um objeto e um morfismo (identidade desse objeto)

Categoria **1+1**

- dois objetos e dois morfismos (identidade)

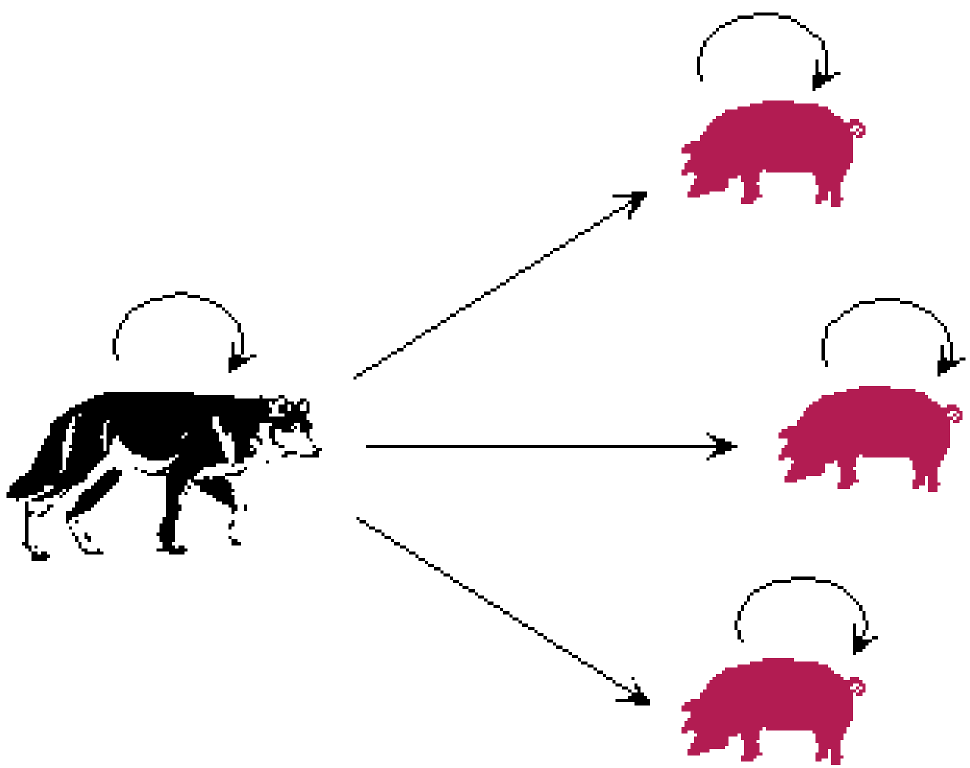
Categoria **2**

- dois objetos e três morfismos (sendo dois identidade)



EXEMPLO Categoria Três Porquinhos e o Lobo Mau

3 porquinhos P_1, P_2 e P_3, o lobo mau L e os morfismos “persegue” com origem no lobo mau e destino em cada um dos porquinhos, além dos morfismos identidade "outra atividade qualquer"



Matemática Discreta para Ciência da Computação

P. Blauth Menezes

Matemática Discreta para Ciência da Computação

P. Blauth Menezes

blauth@inf.ufrgs.br

Departamento de Informática Teórica

Instituto de Informática / UFRGS