Axiomas da Categoria dos Conjuntos

Pedro G. Mattos

$$\mathbb{0} \qquad \mathbb{1} \qquad \mathbb{2} \qquad \mathbb{N}$$

$$+ \qquad \times \qquad \geqslant \qquad \overset{\dashleftarrow}{\twoheadrightarrow}$$

Sumário

Categoria dos Conjuntos 3
Lista dos axiomas 3

0 Vazio 4

1 Ponto 4
1.0 Elementos 4
1.1 Valores de transformações em elementos e funtorialidade 4

2 Soma 5
2.1 O axioma da soma e notações 5
2.2 Propriedades algébricas da soma 6
2.3 Soma de transformações 6

3 Par 7
3.1 Monomorfismos, contenção e subconjuntos 7
3.2 Transformação indicadora e objeto indicador 9
3.3 O par e o axioma da bivalência 9
3.4 Imagem inversa e imagem direta 10
3.5 União e interseção 10
3.6 Definição de subconjunto a partir de proposição lógica? 10

4 Produto 10
4.1 O axioma do produto e notações 10
4.2 Propriedades algébricas do produto 11
4.3 Produto de transformações e transposição de argumentos 11
4.4 Epimorfismos e transformações sobrejetivas 12

5 Exponencial 12
5.1 O axioma da exponencial e notações 13
5.2 Propriedades algébricas da exponencial 14
5.3 Representação de transformações em ${}^{E}B$ 15
5.4 Representação de subconjuntos em ${}^{C}2$ 16

6 Infinito 17
6.1 Axioma do infinito e construções básicas 17
6.1.1 Composição iterada de dinâmica 19
6.2 Aritmética 20
6.2.1 Adição 20
6.2.2 Multiplicação 20
6.2.3 Potenciação 20

7 Escolha 21

Referências 22

Categoria dos Conjuntos

A *negação lógica* de uma proposição P será denotada por "$\bar{P}$" (lê-se "não é verdade que P"), a *conjunção lógica* de proposições P e P' por "$P \sqcap P'$" (lê-se "P e P'"), a *disjunção lógica* de P e P' por "$P \sqcup P'$" (lê-se "P ou P'"), a *implicação lógica* por $P \Rightarrow P'$ (lê-se "P implica que P'") e a *equivalência lógica* por $P \Leftrightarrow P'$ (lê-se "P é equivalente a P'" ou "P se, e somente se, P'"). O *quantificador universal* de um predicado P sobre uma variável x é denotado por "$\prod_x xP$" (lê-se "para todo x, xP"), e o *quantificador existencial* de P sobre x, por "$\coprod_x xP$" (lê-se "para algum x, xP" ou "existe x tal que xP"). Vamos usar também as abreviações "$\prod_{xP} xP'$" para "$\prod_x [xP \Rightarrow xP']$" e "$\coprod_{xP} xP'$" para "$\coprod_x [xP \sqcap xP']$". Denotaremos a *igualdade* por "$=$" e a *desigualdade* por "$\neq$". De modo geral vamos evitar notação lógica, optando pelas frases equivalente em língua portuguesa.

Uma *categoria* é formalizada como uma teoria formal da lógica de primeira ordem com igualdade na qual as variáveis podem ser de dois tipos: *objetos*, ou *morfismos* (também chamados *setas*).[1] A cada morfismo f está associado um objeto C chamado *domínio* de f e um objeto C' chamado *contradomínio* de f. Denota-se $f: C \to C'$ e diz-se que "f é um morfismo de C para C'". Dados morfismos $f: C \to C'$ e $f': C' \to C''$, existe um morfismo chamado *composição* de f com f' cujo domínio é C e cujo contradomínio é C'', denotado $f' \circ f: C \to C''$. A composição é associativa: dados morfismos $f: C \to C'$, $f': C' \to C''$ e $f'': C'' \to C'''$, vale

$$f'' \circ (f' \circ f) = (f'' \circ f') \circ f.$$

Dado um objeto C, existe um morfismo $\mathrm{I}_C: C \to C$ chamado *identidade* de C. A identidade satisfaz, para todo morfismo $f: C \to C'$, $f \circ \mathrm{I}_C = f$ e $\mathrm{I}_{C'} \circ f = f$.

Lista dos axiomas

A seguir, listamos brevemente os dez axiomas da Teoria Elementar da Categoria de Conjuntos, inicialmente propostos por Lawvere (cf. [Law64; LR03]).

A *Categoria dos Conjuntos* é uma categoria que satisfaz:

AXIOMA 0. Existe objeto inicial $\mathbb{0}$ (*vazio*).

AXIOMA 1. Existe objeto terminal $\mathbb{1}$ (*ponto*).

AXIOMA 1.0. $\mathbb{0} \neq \mathbb{1}$.

AXIOMA 1.1 O ponto $\mathbb{1}$ separa transformações.

AXIOMA +. Existe *soma* $C \xrightarrow{\iota_0} C + C' \xleftarrow{\iota_1} C'$.

AXIOMA 2. O *par* $\mathbb{2} \coloneqq \mathbb{1} + \mathbb{1} \xleftarrow{1} \mathbb{1}$ é objeto indicador.

AXIOMA ×. Existe *produto* $C \xleftarrow{\pi_0} C \times C' \xrightarrow{\pi_1} C'$.

AXIOMA >. Existe *exponencial* ${}^{E}B \times E \xrightarrow{\epsilon} B$.

AXIOMA ∞. Existe *infinito contável* $\mathbb{1} \xrightarrow{0} \mathbb{N} \xrightarrow{\Vdash} \mathbb{N}$.

AXIOMA 10. (Escolha) Todo epimorfismo tem inversa à direita.

A Categoria dos Conjuntos é denotada $\mathfrak{S}$, seus *objetos* C são denominados *conjuntos* e seus *morfismos* $f: C \to C'$, *transformações* (ou *funções*). A classe de transformações de um conjunto C para um conjunto C' é denotada $\mathfrak{S}(C, C')$.

1. Podemos mais simplesmente considerar as variáveis representando somente morfismos, assim como na teoria de conjuntos tradicional de ZFC as variáveis representam conjuntos. Para isso, em vez de falar de um objeto C falamos de seu morfismo identidade I_C.

0 Vazio

Axioma 0 (Vazio)**.** Existe objeto inicial $\mathbb{0}$, que satisfaz: para todo conjunto C, existe única transformação $\iota_C^{\mathbb{0}} : \mathbb{0} \to C$. Um objeto inicial é chamado um (*conjunto*) *vazio*.

Um objeto inicial não é único por definição, mas todos eles são isomorfos entre si. Por isso, trataremos $\mathbb{0}$ como único ao usar o artigo definido na expressão "*o* vazio".

Proposição 0.0. *A transformação* $\iota_{\mathbb{0}}^{\mathbb{0}} : \mathbb{0} \to \mathbb{0}$ *é a identidade* $\mathrm{I}_{\mathbb{0}}$.

Demonstração. Segue da unicidade de $\iota_{\mathbb{0}}^{\mathbb{0}}$. ■

1 Ponto

Axioma 1 (Ponto)**.** Existe objeto terminal $\mathbb{1}$, que satisfaz: para todo conjunto C, existe única transformação $\pi_{\mathbb{1}}^{C} : C \to \mathbb{1}$. Um objeto terminal é chamado um (*conjunto*) *ponto*.

Esse objeto terminal não é único por definição, mas todos eles são isomorfos entre si. Por isso, trataremos ele como único ao usar o artigo definido na expressão "*o* ponto".

Proposição 1.1. *A transformação* $\pi_{\mathbb{1}}^{\mathbb{1}} : \mathbb{1} \to \mathbb{1}$ *é a identidade* $\mathrm{I}_{\mathbb{1}}$.

1.0 Elementos

Definição 1. Seja C um conjunto. Um *elemento* de C é uma transformação $x : \mathbb{1} \to C$. Denota-se $x \in C$.

Para garantir a não trivialidade da teoria, enunciamos o seguinte axioma.

Axioma 1.0 (Não-degeneração)**.** O vazio não é isomorfo ao ponto:

$$\mathbb{0} \not\equiv \mathbb{1}.$$

Sem esse axioma, o vazio poderia ter elementos, o que implicaria que todos conjuntos são isomorfos.

Proposição 1.2. *O conjunto vazio* $\mathbb{0}$ *não tem elementos.*

Demonstração. Por definição de $\mathbb{0}$, existe única transformação $\iota_{\mathbb{1}}^{\mathbb{0}} : \mathbb{0} \to \mathbb{1}$ e, por definição de $\mathbb{1}$, existe única transformação $\pi_{\mathbb{1}}^{\mathbb{0}} : \mathbb{0} \to \mathbb{1}$. Isso significa que $\iota_{\mathbb{1}}^{\mathbb{0}} = \pi_{\mathbb{1}}^{\mathbb{0}}$. Chamemos essa transformação de f.

Suponha, por absurdo, que exista $x : \mathbb{1} \to \mathbb{0}$. Então a composição $f \circ x : \mathbb{1} \to \mathbb{1}$ seria igual à identidade $\mathrm{I}_{\mathbb{1}}$ (pois existe única tal transformação pela definição de $\mathbb{1}$) e a composição $x \circ f : \mathbb{0} \to \mathbb{0}$ seria igual à identidade $\mathrm{I}_{\mathbb{0}}$ (pois existe única tal transformação pela definição de $\mathbb{0}$), o que mostra que x seria um isomorfismo entre $\mathbb{0}$ e $\mathbb{1}$, contradizendo o AXIOMA 1.0. ■

1.1 Valores de transformações em elementos e funtorialidade

Definição 2. Sejam $f : C \to C'$ uma transformação e $x \in C$ um elemento. O *valor de* f *em* x é o elemento

$$f(x) := f \circ x : \mathbb{1} \to C'.$$

Proposição 1.3. *Sejam* $C \xrightarrow{f} C' \xrightarrow{f'} C''$ *transformações. Para todo elemento* $x \in C$,

$$(f' \circ f)(x) = f'(f(x)).$$

Demonstração. Segue da associatividade da composição de transformações e da definição de valor da transformação em um elemento. ■

O próximo axioma estabelece a propriedade fundamental das transformações, que diz que transformações são iguais quando ela são iguais em todos elementos.

Axioma 1.1 (Elementariedade)**.** O objeto terminal $\mathbb{1}$ separa transformações $C \xrightarrow{f,f'} C'$.

Isto é: se os valores das transformações f e f' são iguais em todo elemento $x \in C$ (ou seja, $f(x) = f'(x)$), então elas são iguais (ou seja, $f = f'$).

$$\begin{tikzcd} \mathbb{1} \arrow[r, "x"] & C \arrow[r, shift left, "f"] \arrow[r, shift right, "f'"'] & C' \end{tikzcd}$$

Essa é a propriedade fundamental das transformações. Ela não é satisfeita por qualquer morfismo em uma categoria. De fato, ela não pode nem mesmo ser enunciada em uma categoria qualquer pois o conceito de elemento não necessariamente existe.

Proposição 1.4. *Um conjunto S separa transformações $C \xrightarrow{f,f'} C'$ se, e somente se, não é vazio.*

Notação 1. O AXIOMA 1.1 nos permite definir uma transformação $f : C \to C'$ somente definindo o valor de f em cada elemento $x \in C$. Denotamos isso por

$$\begin{aligned} f : C &\longrightarrow C' \\ c &\longmapsto f(c), \end{aligned}$$

em que $f(c)$ representa a definição do valor de f num elemento qualquer $c \in C$. Nos referimos a essa definição como a *definição elementar* de f e dizemos que a expressão acima define f *elementarmente*.

2 Soma

2.1 O axioma da soma e notações

O próximo axioma estabelece a primeira maneira que temos de criar um novo conjunto a partir de conjuntos dados.

Axioma + (Soma)**.** Sejam C, C' conjuntos. Existem a *soma*[2] $C + C'$ e as *inclusões canônicas* $\iota_0^{C,C'} : C \to C + C'$ e $\iota_1^{C,C'} : C \to C + C'$, que satisfazem: para todas transformações $f : C \to X$ e $f' : C' \to X$, existe única transformação $\begin{cases} f \\ f' \end{cases} : C + C' \to X$ tal que

$$\begin{cases} f \\ f' \end{cases} \circ \iota_0^{C,C'} = f$$
$$\begin{cases} f \\ f' \end{cases} \circ \iota_1^{C,C'} = f'.$$

2. Também chamada *união disjunta*.

Isso equivale ao seguinte diagrama ser comutativo:

$$\begin{tikzcd}
C \arrow[r, "\iota_0^{C,C'}"] \arrow[dr, "f"'] & C + C' \arrow[d, dashed, "\begin{cases} f \\ f' \end{cases}"] & C' \arrow[l, "\iota_1^{C,C'}"'] \arrow[dl, "f'"] \\
& X &
\end{tikzcd}$$

Quando não houver ambiguidade, as inclusões canônicas serão denotadas $\iota_0 \coloneqq \iota_C \coloneqq \iota_0^{C,C'}$ e $\iota_1 \coloneqq \iota_{C'} \coloneqq \iota_1^{C,C'}$ e a soma será resumidamente denotada

$$C \xrightarrow{\iota_0} C + C' \xleftarrow{\iota_1} C'.$$

Notação 2. Usando o AXIOMA 1.1, a transformação $\begin{cases} f \\ f' \end{cases}$ pode ser definida elementarmente para cada $e \in C + C'$. Denotamos isso por

$$\begin{aligned} \begin{cases} f \\ f' \end{cases} : C + C' &\longrightarrow X \\ e &\longmapsto \begin{cases} f(e) & e \in C \\ f'(e) & e \in C'. \end{cases} \end{aligned}$$

Proposição 2.1 (Unicidade da soma)**.** *A soma $C \xrightarrow{\iota_0} C + C' \xleftarrow{\iota_1} C'$ é única a menos de isomorfismo.*

2.2 Propriedades algébricas da soma

A proposição a seguir estabelece propriedades básicas da soma em relação a $\mathbb{0}$.

Proposição 2.2 (Propriedades algébricas da soma)**.** *A soma $+$ satisfaz:*

1. *(Identidade) Para todo conjunto C,*

$$\mathbb{0} + C \equiv C \equiv C + \mathbb{0}.$$

2. *(Comutatividade) Para todos conjuntos C, C',*

$$C + C' \equiv C' + C.$$

3. *(Associatividade) Para todos conjuntos C, C', C'',*

$$(C + C') + C'' \equiv C + (C' + C'').$$

2.3 Soma de transformações

Dadas transformações $f : D \to C$ e $f' : D' \to C'$, podemos formar a *soma de f e f'* usando a propriedade universal da soma para definir

$$f + f' \coloneqq \begin{cases} \iota_C \circ f \\ \iota_{C'} \circ f' \end{cases},$$

dada pelo diagrama

$$\begin{tikzcd}
D \arrow[r, "\iota_D"] \arrow[d, "f"'] & D + D' \arrow[d, dashed, "f+f'"] & D' \arrow[l, "\iota_{D'}"'] \arrow[d, "f'"] \\
C \arrow[r, "\iota_C"'] & C + C' & C' \arrow[l, "\iota_{C'}"]
\end{tikzcd}$$

Definindo $f + f'$ elementarmente, temos

$$\begin{aligned} f + f' : D + D' &\longrightarrow C + C' \\ e &\longmapsto \begin{cases} \iota_C(f(e)) & e \in D \\ \iota_{C'}(f'(e)) & e \in D'. \end{cases} \end{aligned}$$

3 Par

Antes de falar sobre o par e o axioma da bivalência, vamos definir transformações injetivas e subconjuntos.

3.1 Monomorfismos, contenção e subconjuntos

Monomorfismos são morfismos que são canceláveis à esquerda.

Definição 3. Um *monomorfismo* é um morfismo $C \xrightarrow{i} C'$ tal que, para todo objeto X e todos morfismos $X \xrightarrow{x,x'} C$, se $i \circ x = i \circ x'$, então $x = x'$.

Definição 4. Uma *transformação injetiva* é uma transformação $i : C \to C'$ tal que, para todos $x, x' \in C$, se $i(x) = i(x')$, então $x = x'$. Denota-se $i : C \rightarrowtail C'$.

Proposição 3.1. *Valem as seguintes propriedades:*

1. *Os monomorfismos da categoria de conjuntos são as transformações injetivas.*
2. *Seja C um conjunto. Toda transformação $\iota : \mathbb{0} \to C$ é um epimorfismo.*
3. *Seja $C \xrightarrow{\iota_0} C + C' \xleftarrow{\iota_1} C'$ uma soma. As inclusões canônicas ι_0 e ι_1 são monomorfismos.*
4. *Seja C um conjunto. Todo elemento $x : \mathbb{1} \to C$ é um monomorfismo.*

Demonstração.
1. Todo monomorfismo é uma transformação injetiva por definição. Toda transformação injetiva é um monomorfismo por causa do AXIOMA 1.1.
2. Exercício.
3. Exercício.
4. Exercício. ∎

Para definirmos subconjuntos de um conjunto C, vamos nos basear na ideia intuitiva de suconjunto e usar a inclusão canônica associada a cada subconjunto. Diferentes transformações injetivas podem representar o mesmo subconjunto, e por isso é necessário considerar uma relação de equivalência para definir mais precisamente um subconjunto.

Definição 5 (Inclusão de transformações injetivas). Seja C um conjunto. A relação de *inclusão entre transformações injetivas* é definida como: uma transformação injetiva $i : D \rightarrowtail C$ está *incluída* em uma

transformação injetiva $i' : D' \rightarrowtail C$ precisamente quando, para alguma transformação $j : D \to D'$, vale
$$i \circ j = i'.$$
Denota-se $i \subseteq_C i'$.

Poderíamos de fato definir essa relação entre quaisquer transformações $f : D \to C$ e $f' : D' \to C$. A relação de *inclusão* $f \subseteq_C f'$ significa que, para alguma transformação $g : D \to D'$ vale
$$f \circ g = f'.$$
De certa forma, essa propriedade imita as relações aritméticas de ordem de divisão da aritmética dos números naturais. No caso geral, se f' não for monomorfismo, a transformação g não precisa ser única. A relação dual (invertendo a orientação das setas) formaliza a noção de que $f' = g \circ f$ é *determinada* por f.

Note que tal j da definição é injetiva por causa da seguinte proposição.

Proposição 3.2. *Sejam $i : D \to C$ um monomorfismo e $f : D \to C$ e $j : D' \to D$ morfismos tais que $f \circ j = i$. Então j é monomorfismo. (Em geral, f não precisa ser monomorfismo.)*

A relação de inclusão $\subseteq_C$ é reflexiva e transitiva.

Proposição 3.3 ($\subseteq_C$ é pré-ordem)**.** *Seja C um conjunto.*

1. *(Reflexividade) Para toda transformação injetiva $i : D \rightarrowtail C$ vale que $i \subseteq_C i$.*
2. *(Transitividade) Para todas transformações injetivas $i : D \rightarrowtail C$, $i' : D' \rightarrowtail C$ e $i'' : D'' \rightarrowtail C$ vale que, se $i \subseteq_C i'$ e $i' \subseteq_C i''$, então $i \subseteq_C i''$.*

Porém, ela nem sempre é antissimétrica. Por isso, definimos a relação de equivalência associada à inclusão como segue. Com respeito às classes dessa equivalência, a inclusão se torna antissimétrica, portanto uma relação de ordem.

Definição 6. Seja C um conjunto. A relação de *equivalência entre transformações injetivas* é definida como: uma transformação injetiva $i : D \rightarrowtail C$ é *equivalente* a uma transformação injetiva $i' : D' \rightarrowtail C$ precisamente quando, $i \subseteq_C i'$ e $i' \subseteq_C i$. Denota-se $i \simeq_C i'$.

Proposição 3.4 ($\simeq_C$ é equivalência)**.** *Seja C um conjunto.*

1. *(Reflexividade) Para toda transformação injetiva $i : D \rightarrowtail C$, $i \equiv_C i$.*
2. *(Simetria) Para todas transformações injetivas $i : D \rightarrowtail C$ e $i' : D' \rightarrowtail C$ vale que $i \simeq_C i'$ se, e somente se, $i' \simeq_C i$.*
3. *(Transitividade) Para todas transformações injetivas $i : D \rightarrowtail C$, $i' : D' \rightarrowtail C$ e $i'' : D'' \rightarrowtail C$ vale que, se $i \simeq_C i'$ e $i' \simeq_C i''$, então $i \simeq_C i''$.*

Em geral, pode existir um isomorfismo entre D e D' sem que i e i' sejam equivalentes. A proposição caracteriza a equivalência em termos de um isomorfismo entre D e D'.

Proposição 3.5 (Caracterização da equivalência)**.** *Seja C um conjunto. Para todas transformações injetivas $i : D \to C$ e $i' : D' \to C$, vale que $i \simeq_C i'$ se, e somente se, existem $j : D \to D'$ e $j' : D' \to D$ tais que $i \circ j = i'$, $i' \circ j' = i$, $j' \circ j = \mathrm{I}_D$ e $j \circ j' = \mathrm{I}_{D'}$.*

Demonstração. Se existem tais j e j', então por definição $i \simeq_C i'$. Reciprocamente, suponhamos que $i \simeq_C i'$ e sejam $j : D \to D'$ e $j' : D' \to D$ tais que $i \circ j = i'$ e $i' \circ j' = i$. Nesse caso vale que $i \circ j \circ j' = i' \circ j' = i$ e $i' \circ j' \circ j = i \circ j = i'$. Como i e i são injetivas, segue então que $j' \circ j = \mathrm{I}_D$ e $j \circ j' = \mathrm{I}_{D'}$. ∎

Dessa forma, usando a relação de equivalência $\simeq_C$, pensamos em um subconjunto S de C, denotado por $S \subseteq C$, como a classe de equivalência de transformações injetivas $i\colon D \to C$. Denotamos um elemento representante dessa equivalência com o abuso de notação $\iota_S\colon S \to C$ (isso é um abuso de notação pois S denota tanto a tanto a classe de equivalência como o domínio S).

3.2 Transformação indicadora e objeto indicador

Definição 7. Um *indicador* (*de subconjunto*)[3] é um conjunto V e um elemento $\mathrm{t} \in V$ que satisfazem: para todo conjunto C e todo subconjunto $S \subseteq C$, existe única transformação $\chi_S\colon C \to V$ tal que

$$\chi_S \circ \iota_S = \mathrm{t} \circ \pi^S_{\mathbb{1}}.$$

Tal χ_S é denominada *transformação indicadora*[4] de S relativa a C.

Isso equivale ao seguinte diagrama ser comutativo:

$$\begin{tikzcd} & S \arrow[dl, "\iota_S"'] \arrow[dr, "\pi^S_{\mathbb{1}}"] & \\ C \arrow[dr, dashed, "\chi_S"'] & & \mathbb{1} \arrow[dl, "\mathrm{t}"] \\ & V & \end{tikzcd}$$

Em particular, para qualquer elemento $x \in S$, vale que

$$\chi_S \circ \iota_S(x) = \mathrm{t} \circ \pi^S_{\mathbb{1}}(x) = \mathrm{t},$$

ou seja, $x \in S$ se, e somente se, “$\chi_S(x) = \mathrm{t}$”.

3.3 O par e o axioma da bivalência

Usando a soma, podemos criar novos conjuntos a partir dos que já temos. Em particular, $\mathbb{0} + \mathbb{1} \equiv \mathbb{1} \equiv \mathbb{1} + \mathbb{0}$ (pois $\mathbb{0}$ é uma identidade para a soma de acorco com PROPOSIÇÃO 2.2), portanto o novo conjunto mais simples desses é a soma de $\mathbb{1}$ com $\mathbb{1}$, que definiremos depois da proposição.

Definição 8. Um *par* é um conjunto $\mathbb{2} \coloneqq \mathbb{1} + \mathbb{1}$. O *zero* de $\mathbb{2}$ é o elemento $0 \coloneqq \iota^{\mathbb{1},\mathbb{1}}_0 : \mathbb{1} \to \mathbb{2}$ e o *um* de $\mathbb{2}$ é o elemento $1 \coloneqq \iota^{\mathbb{1},\mathbb{1}}_1 : \mathbb{1} \to \mathbb{2}$.

Na notação resumida da soma temos

$$\mathbb{1} \xrightarrow{0} \mathbb{1} + \mathbb{1} \xleftarrow{1} \mathbb{1}.$$

Esse conjunto não é único por definição, mas todos eles são isomorfos entre si. Por isso, trataremos ele como único ao usar o artigo definido na expressão “*o* par”.

Proposição 3.6. *O par $\mathbb{2}$ cossepara transformações.*

$$\begin{tikzcd} C' \arrow[r, shift left, "f"] \arrow[r, shift right, "f'"'] & C \arrow[r, "t"'] & \mathbb{2} \end{tikzcd}$$

3. Usualmente chamado *classificador de subobjeto*.
4. Também chamada *transformação característica*.

A proposição a seguir afirma que o par tem exatamente dois elementos. Note que essa definição não depende da definição do número dois (2) em si, ele pode ser feita puramente dentro da lógica[5].

Proposição 3.7. *O par* $\mathbb{2}$ *tem exatamente dois elementos,* 0 *e* 1.

Axioma 2 (Bivalência)**.** O par $\mathbb{2}$ com o elemento $1 \in \mathbb{2}$ é um indicador de subconjunto.

$$\begin{tikzcd} & S \arrow[dl, "\iota_S"'] \arrow[dr, "\pi_{\mathbb{1}}^S"] & \\ C \arrow[dr, dashed, "\chi_S"'] & & \mathbb{1} \arrow[dl, "1"] \\ & \mathbb{2} & \end{tikzcd}$$

3.4 Imagem inversa e imagem direta

3.5 União e interseção

3.6 Definição de subconjunto a partir de proposição lógica?

4 Produto

4.1 O axioma do produto e notações

Axioma $\times$ (Produto)**.** Sejam C, C' conjuntos. Existem o *produto* $C \times C'$ e as *projeções canônicas* $\pi_0^{C,C'} : C \times C' \to C$ e $\pi_1^{C,C'} : C \times C' \to C'$, que satisfazem: para todas transformações $f : X \to C$ e $f' : X \to C'$, existe única transformação $(f, f') : X \to C \times C'$ tal que

$$\pi_0^{C,C'} \circ (f, f') = f$$
$$\pi_1^{C,C'} \circ (f, f') = f'.$$

Isso equivale ao seguinte diagrama ser comutativo:

$$\begin{tikzcd} & X \arrow[dl, "f"'] \arrow[d, dashed, "{(f,f')}"] \arrow[dr, "f'"] & \\ C & C \times C' \arrow[l, "\pi_0^{C,C'}"] \arrow[r, "\pi_1^{C,C'}"'] & C' \end{tikzcd}$$

Quando não houver ambiguidade, as projeções canônicas serão denotadas $\pi_0 \coloneqq \pi_C \coloneqq \pi_0^{C,C'}$ e $\pi_1 \coloneqq \pi_{C'} \coloneqq \pi_1^{C,C'}$, e o prduto será resumidamente denotado

$$C \xleftarrow{\pi_0} C \times C' \xrightarrow{\pi_1} C'.$$

5. Da seguinte forma: dizemos que "um conjunto C tem exatamente 2 elementos" quando vale

$$\bigsqcup_{x \in C} \bigsqcup_{x' \in C} [x \neq x' \sqcap \prod_{y \in C} [y = x \sqcup y = x']].$$

Note que a primeira sentença da disjunção dentro dos colchetes externos afirma que C tem no mínimo 2 elementos, enquanto que a segunda afirma que C tem no máximo 2 elementos.

Em geral, dados elementos $c \in C$ e $c' \in C'$ e transformação $f : C \times C' \to Y$, omitiremos os parênteses na notação do valor de f em (c, c'), denotando

$$f(c, c') \coloneqq f((c, c')).$$

Notação 3. Usando o AXIOMA 1.1, a transformação (f, f') pode ser definida elementarmente em cada elemento de X. Denotamos isso por

$$\begin{aligned} (f, f') : X &\longrightarrow C \times C' \\ x &\longmapsto (f(x), f'(x)). \end{aligned}$$

4.2 Propriedades algébricas do produto

O produto satisfaz as seguintes propriedades com relação a $\mathbb{0}$, $\mathbb{1}$ e $+$. As primeiras três propriedades são análogas às propriedades algébricas da soma, e as outras duas relacionam o produto com a soma e a identidade da soma.

Proposição 4.1 (Propriedades algébricas do produto). *O produto $\times$ satisfaz:*

1. *(Identidade) Para todo conjunto C,*

$$\mathbb{1} \times C \equiv C \equiv C \times \mathbb{1}.$$

2. *(Comutatividade) Para todos conjuntos C, C',*

$$C \times C' \equiv C' \times C.$$

3. *(Associatividade) Para todos conjuntos C, C', C'',*

$$(C \times C') \times C'' \equiv C \times (C' \times C'').$$

4. *(Nulidade) Para todo conjunto C,*

$$\mathbb{0} \times C \equiv \mathbb{0} \equiv C \times \mathbb{0}.$$

5. *(Distributividade) Para todos conjuntos C, C', D,*

$$(C + C') \times D \equiv (C \times D) + (C' \times D).$$

Proposição 4.2 (Unicidade do produto). *O produto $C \xleftarrow{\pi_0} C \times C' \xrightarrow{\pi_1} C'$ é único a menos de isomorfismo.*

4.3 Produto de transformações e transposição de argumentos

Dadas transformações $f : D \to C$ e $f' : D' \to C'$, podemos formar o produto delas usando a propriedade universal do produto para definir

$$f \times f' \coloneqq (f \circ \pi_D, f' \circ \pi_{D'}).$$

$$\begin{tikzcd} D \arrow[d, "f"'] & D \times D' \arrow[l, "\pi_D"'] \arrow[r, "\pi_{D'}"] \arrow[d, dashed, "f \times f'"] & D' \arrow[d, "f'"] \\ C & C \times C' \arrow[l, "\pi_C"] \arrow[r, "\pi_{C'}"'] & C' \end{tikzcd}$$

Definindo $f \times f'$ elementarmente, temos

$$\begin{aligned} f \times f' :\ D \times D' &\longrightarrow C \times C' \\ (d, d') &\longmapsto (f(d), f'(d')). \end{aligned}$$

Podemos também definir a *transposição de argumentos* $\mathrm{T}_{C,C'} :\ C \times C' \to C' \times C$ por

$$\mathrm{T}_{C,C'} \coloneqq (\pi_1^{C,C'}, \pi_0^{C,C'}),$$

definida elementarmente por

$$\begin{aligned} \mathrm{T}_{C,C'} :\ C \times C' &\longrightarrow C' \times C \\ (c, c') &\longmapsto (c', c). \end{aligned}$$

$$\begin{tikzcd} & C \times C' \arrow[dl, "\pi_1^{C,C'}"'] \arrow[d, dashed, "\mathrm{T}_{C,C'}"] \arrow[dr, "\pi_0^{C,C'}"] & \\ C' & C' \times C \arrow[l, "\pi_0^{C',C}"] \arrow[r, "\pi_1^{C',C}"'] & C \end{tikzcd}$$

O análogo (ou dual) para a soma da transposição de argumentos do produto não é relevante, pois se resume à transformação identidade em $C + C'$.

4.4 Epimorfismos e transformações sobrejetivas

Epimorfismos são morfismos que são canceláveis à direita.

Definição 9. Um *epimorfismo* é um morfismo $p :\ C \to C'$ tal que, para todo objeto X e todos morfismos $f, f' :\ C \to X$, se $f \circ p = f' \circ p$, então $f = f'$.

Definição 10. Uma *transformação sobrejetiva* é uma transformação $p :\ C \to C'$ tal que, para todo $e' \in C$, existe $e \in C$ satisfazendo $p(e) = e'$. Denota-se $p :\ C \twoheadrightarrow C'$.

Proposição 4.3. *Valem as seguintes propriedades:*

1. *Os epimorfismos da categoria dos conjuntos são as transformações sobrejetivas.*
2. *Seja C um conjunto. Toda transformação $\pi :\ C \to \mathbb{1}$ é um epimorfismo.*
3. *Seja $C \xleftarrow{\pi_0} C \times C' \xrightarrow{\pi_1} C'$ um produto. As projeções canônicas π_0 e π_1 são epimorfismos.*

5 Exponencial

A exponencial de conjuntos é uma forma de representar a classe de transformações $\mathfrak{S}(E, B)$ de um conjunto E para um conjunto B dentro da teoria de conjuntos, através de um conjunto denotado ${}^{E}B$, a exponencial de E e B. Além do conjunto ${}^{E}B$, também é necesssária uma transformação de avaliação, que, para cada elemento $g \in {}^{E}B$ e elemento $e \in E$, retorna um elemento $g(e) \in B$. A transformação avaliação permite tratarmos o elemento $g \in {}^{E}B$ como uma transformação de E para B, calculando seu valor em cada elemento de E.

Por fim, esses objetos devem satisfazer uma propriedade universal muito comumente usada na matemática: dada uma transformação $f :\ X \times E \to B$, podemos definir, para cada $x \in X$, uma transformação $f_x : E \to B$ por $f_x(e) \coloneqq f(x,e)$. Pensamos em cada transformação f_x como um elemento de ${}^E B$. Então, podemos definir uma família de transformações $f_\bullet : X \to {}^E B$ tal que, para cada $x \in X$, $f_\bullet(x) \coloneqq f_x$. Essa família é uma indexação em X das transformações $f_x \in {}^E B$.

A construção explicada acima é tão comumente usada e intuitiva na matemática que é costume usar o abuso de notação $f = f_\bullet$ e, para cada $(x,e) \in X \times E$, $f(x,e) = f_x(e)$. Essa propriedade caracteriza um objeto exponencial.

5.1 O axioma da exponencial e notações

Axioma ⩾ (Exponencial)**.** Sejam E, B conjuntos. Existem a *exponencial* ${}^E B$ e a *avaliação canônica* $\epsilon : {}^E B \times E \to B$, que satisfazem: para toda transformação $f : X \times E \to B$, existe única transformação $f_\bullet : X \to {}^E B$ tal que

$$f = \epsilon \circ (f_\bullet \times \mathrm{I}_C). \tag{1}$$

Isso equivale ao seguinte diagrama ser comutativo:

$$\begin{tikzcd} & X \times E \arrow[dl, dashed, "f_\bullet \times \mathrm{I}_E"'] \arrow[d, "f"] & & X \arrow[d, dashed, "f_\bullet"'] \\ {}^E B \times E \arrow[r, "\epsilon"'] & B & & {}^E B \end{tikzcd}$$

A exponencial será resumidamente denotada

$${}^E B \times E \xrightarrow{\epsilon} B.$$

O valor da avaliação ϵ em um elemeto $(g,e) \in {}^E B \times E$ será denotado

$$g(e) \coloneqq \epsilon(g,e) \in B$$

e o valor da transformação $f_\bullet$ em um elemento $x \in X$ será denotado

$$f_x \coloneqq f_\bullet(x) \in {}^E B,$$

de modo que a FÓRMULA (1) se torna, para cada $(x,e) \in X \times E$,

$$\begin{aligned} f(x,e) &= \epsilon \circ (f_\bullet \times \mathrm{I}_E)(x,e) \\ &= \epsilon(f_\bullet(x), \mathrm{I}_E(e)) \\ &= \epsilon(f_x, e) \\ &= f_x(e). \end{aligned}$$

Notação 4. Usando o axioma AXIOMA 1.1, dada uma transformação $f : X \times E \to B$, a transformação $f_\bullet$ pode ser definida elementarmente para cada $x \in X$. Denotamos isso por

$$\begin{aligned} f_\bullet : X &\longrightarrow {}^E B \\ x &\longmapsto f_x \coloneqq f_\bullet(x) : E \longrightarrow B \\ &\qquad\qquad\qquad\qquad e \longmapsto f_x(e) \coloneqq \epsilon(f_x, e) = f(x,e) \end{aligned}$$

ou, de modo mais simples, omitindo as definições de notação,

$$\begin{aligned} f_\bullet : X &\longrightarrow {}^E B \\ x &\longmapsto f_x : E \longrightarrow B \\ &\qquad\qquad e \longmapsto f(x,e). \end{aligned}$$

Proposição 5.1 (Unicidade da exponencial)**.** *A exponencial* ${}^{E}B \times E \xrightarrow{\epsilon} B$ *é única a menos de isomorfismo.*

A "recíproca" do AXIOMA > também está bem definida na teoria apenas pela existência do produto: dada qualquer transformação $F\colon X \to {}^{E}B$, podemos definir a transformação $f := \epsilon \circ (F \times \mathrm{I}_C)$, elementarmente dada por

$$\begin{aligned} f\colon X \times E &\longrightarrow B \\ (x, e) &\longmapsto F(x)(e), \end{aligned}$$

que satisfaz automaticamente o diagrama

$$\begin{tikzcd} & X \times E \arrow[dl, "F\times \mathrm{I}_E"'] \arrow[d, dashed, "f"] \\ {}^{E}B \times E \arrow[r, "\epsilon"'] & B \end{tikzcd} \qquad \begin{tikzcd} X \arrow[d, "F"'] \\ {}^{E}B \end{tikzcd}$$

A unicidade de f segue do AXIOMA 1.1, pois o diagrama acima define ela nos elementos $(x, e) \in X \times E$.

5.2 Propriedades algébricas da exponencial

A exponencial satisfaz as seguintes propriedades com relação a $\mathbb{0}$, $\mathbb{1}$, $+$ e $\times$.

Proposição 5.2 (Propriedades algébricas da exponencial)**.** *A exponencial satisfaz:*

1. *Para todo conjunto B,*
$${}^{\mathbb{0}}B \equiv \mathbb{1}.$$
2. *(Absorção à direita para $\mathbb{1}$) Para todo conjunto E,*
$${}^{E}\mathbb{1} \equiv \mathbb{1}.$$
3. *(Identidade à esquerda para $\mathbb{1}$) Para todo conjunto B*
$${}^{\mathbb{1}}B \equiv B.$$
4. *(Absorção à direita para $\mathbb{0}$) Para todo conjunto $E \not\equiv \mathbb{0}$,*
$${}^{E}\mathbb{0} \equiv \mathbb{0}.$$
5. *(Exponenciação à esquerda) Para todos conjuntos B, E, E',*
$${}^{E+E'}B \equiv {}^{E}B \times {}^{E'}B$$
6. *(Distributividade exponencial) Para todos conjuntos B, E, E',*
$${}^{E\times E'}B \equiv {}^{E'}({}^{E}B)$$

5.3 Representação de transformações em ${}^{E}B$

Seja E um conjunto, e denotemos o único elemento de $\mathbb{1}$ por $0 \in \mathbb{1}$ (esse elemento coincide com a identidade $\mathrm{I}_{\mathbb{1}}$). Existe um isomorfismo entre E e $\mathbb{1} \times E$. Isso ocorre pelo seguinte.

Pela propriedade universal do produto de conjuntos, o seguinte diagrama comuta:

$$\begin{tikzcd}
 & E \arrow[dl, "\pi_{\mathbb{1}}^{E}"'] \arrow[d, dashed, "(\pi_{\mathbb{1}}^{E}{,}\mathrm{I}_E)"] \arrow[dr, "\mathrm{I}_E"] & \\
\mathbb{1} & \mathbb{1} \times E \arrow[l, "\pi_0^{\mathbb{1},E}"] \arrow[r, "\pi_1^{\mathbb{1},E}"'] & E
\end{tikzcd}$$

A transformação $(\pi_{\mathbb{1}}^{E}, \mathrm{I}_E)$ é definida elementarmente por

$$\begin{aligned}
(\pi_{\mathbb{1}}^{E}, \mathrm{I}_E) \colon E &\longrightarrow \mathbb{1} \times E \\
e &\longmapsto (0, e).
\end{aligned}$$

Essa transformação é um isomorfismo, pois tem inversa

$$\begin{aligned}
\pi_1^{\mathbb{1},E} \colon \mathbb{1} \times E &\longrightarrow E \\
(0, e) &\longmapsto e = \pi_1^{\mathbb{1},E}(0, e).
\end{aligned}$$

De fato, a relação $\pi_1^{\mathbb{1},E} \circ (\pi_{\mathbb{1}}^{E}, \mathrm{I}_E) = \mathrm{I}_E$ vale pela definição de $(\pi_{\mathbb{1}}^{E}, \mathrm{I}_E)$; por outro lado, para todo $(0, e) \in E$ vale que

$$(\pi_{\mathbb{1}}^{E}, \mathrm{I}_E) \circ \pi_1^{\mathbb{1},E}(0, e) = (\pi_{\mathbb{1}}^{E}, \mathrm{I}_E)(e) = (0, e) = \mathrm{I}_{\mathbb{1}\times E}(0, e),$$

portanto $(\pi_{\mathbb{1}}^{E}, \mathrm{I}_E) \circ \pi_1^{\mathbb{1},E} = \mathrm{I}_{\mathbb{1}\times E}$.

O isomorfismo $E \equiv \mathbb{1} \times E$ faz com que cada transformação $f \colon E \to B$ possa ser associada à transformação $\dot{f} \coloneqq f \circ \pi_1^{\mathbb{1},E} \colon \mathbb{1} \times E \to B$, definida elementarmente por

$$\begin{aligned}
\dot{f} \colon \mathbb{1} \times E &\longrightarrow B \\
(0, e) &\longmapsto f(e).
\end{aligned}$$

A associação contrária é dada para cada $h \colon \mathbb{1} \times E \to B$ por $\hat{h} \coloneqq h \circ \pi_1^{\mathbb{1},E} \colon E \to B$, definida elementarmente por

$$\begin{aligned}
\hat{h} \colon E &\longrightarrow B \\
e &\longmapsto h(0, e).
\end{aligned}$$

Consideremos agora o diagrama da exponencial ${}^{E}B \times E \xrightarrow{\epsilon} B$ com $X = \mathbb{1}$ e $h \colon \mathbb{1} \times E \to B$:

$$\begin{tikzcd}
 & \mathbb{1} \times E \arrow[dl, dashed, "h_{\bullet}\times\mathrm{I}_E"'] \arrow[d, "h"] & \mathbb{1} \arrow[d, dashed, "h_{\bullet}"'] \\
{}^{E}B \times E \arrow[r, "\epsilon"'] & B & {}^{E}B
\end{tikzcd}$$

Seja $f \colon E \to B$. Note que vale $(\dot{f}_{\bullet} \times \mathrm{I}_E) \circ (\pi_{\mathbb{1}}^{E}, \mathrm{I}_E) = (\dot{f}_{\bullet} \circ \pi_{\mathbb{1}}^{E}, \mathrm{I}_E)$. Podemos então substituir no lugar de h nesse diagrama a transformação $\dot{f} \colon \mathbb{1} \times E \to B$ e, usando o isomorfismo $(\pi_{\mathbb{1}}^{E}, \mathrm{I}_E) \colon E \to \mathbb{1} \times E$, obtemos o diagrama

$$\begin{tikzcd} & E \arrow[dl, dashed, "(\dot{f}_{\bullet}\circ\pi_{\mathbb{1}}^{E},\mathrm{I}_E)"'] \arrow[d, "f"] & \mathbb{1} \arrow[d, dashed, "\dot{f}_{\bullet}"'] \\ {}^{E}B \times E \arrow[r, "\epsilon"'] & B & {}^{E}B \end{tikzcd}$$

Para cada elemento $e \in E$, o diagrama determina que

$$f(e) = \epsilon \circ (\dot{f}_{\bullet}\pi_{\mathbb{1}}^{E}, \mathrm{I}_E)(e) = \epsilon(\dot{f}_{\bullet}, e) = \dot{f}_{\bullet}(e),$$

ou seja, $\dot{f}_{\bullet}$ é uma representação de f em ${}^{E}B$. Esse comentários provam a seguinte proposição.

Proposição 5.3. *Sejam E, B conjuntos e $f : E \to B$. Existe único elemento $f' \in {}^{E}B$ tal que, para todo $e \in E$,*

$$f(e) = f'(e).$$

Nesse caso $f' = \dot{f}_{\bullet}$.

Demonstração. Como demonstrado acima, basta tomar $f' \coloneqq \dot{f}_{\bullet}$. ■

Analogamente, também é válida a representação contrária.

Proposição 5.4. *Sejam E, B conjuntos e $h \in {}^{E}B$. Existe única transformação $h' : E \to B$ tal que, para todo $e \in E$,*

$$h(e) = \epsilon(h, e) = h'(e).$$

5.4 Representação de subconjuntos em ${}^{C}\mathbb{2}$

Consideremos o caso da exponencial ${}^{C}\mathbb{2} \times C \xrightarrow{\epsilon} \mathbb{2}$. Nesse caso específico, temos o seguinte diagrama:

$$\begin{tikzcd} & \mathbb{1} \times C \arrow[dl, dashed, "f_{\bullet}\times\mathrm{I}_C"'] \arrow[d, "f"] & \mathbb{1} \arrow[d, dashed, "f_{\bullet}"'] \\ {}^{C}\mathbb{2} \times C \arrow[r, "\epsilon"'] & \mathbb{2} & {}^{C}\mathbb{2} \end{tikzcd}$$

Usando a identificação $\mathbb{1} \times C \equiv C$, isso significa que, dada $f : C \to \mathbb{2}$, existe única $f_{\bullet} : \mathbb{1} \to {}^{C}\mathbb{2}$ tal que $\epsilon \circ (f_{\bullet} \times \mathrm{I}_C) = f$, ou seja, tal que para todo $c \in C$ vale

$$f(c) \text{ “=” } f(0, c) = f_0(c).$$

Isso mostra que as transformações $f : C \to \mathbb{2}$ podem ser unicamente representadas por elementos $f_0 \in {}^{C}\mathbb{2}$.

Lembremos agora do diagrama de classificador de subobjeto:

$$\begin{tikzcd} & S \arrow[dl, "\iota_S"'] \arrow[dr, "\mathbb{1}_S"] & \\ C \arrow[dr, dashed, "\chi_S"'] & & \mathbb{1} \arrow[dl, "1"] \\ & \mathbb{2} & \end{tikzcd}$$

Se tomarmos $f = \chi_S$, obtemos que, para cada subconjunto $\iota_S : S \to C$, existe única $\chi_{S_{\bullet}} : \mathbb{1} \to {}^{C}\mathbb{2}$ tal que, $\epsilon \circ (\chi_{S_{\bullet}} \times \mathrm{I}_C) = \chi_S$; ou seja, para todo $c \in C$,

$$\chi_{S_{\bullet}}(c) = \chi_S(c).$$

6 Infinito

O axioma do infinito é o modo de formalizar o conjunto dos números naturais e o processo de definição recursiva, que tem como uma de suas consequências a indução matemática. Além da existência de um conjunto $\mathbb{N}$ que representa os números naturais, há também uma transformação sucessor em $\mathbb{N}$ e o elemento inicial $0 \in \mathbb{N}$. A propriedade universal que caracteriza esses objetos tem um caráter intrinsecamente dinâmico: a transformação sucessor nos permite determinar, para qualquer transformação $f : C \to C$ (dinâmica) e qualquer ponto $x_0 \in C$ (condição inicial), uma sequência em C que representa a órbita de x_0 sob a ação de f, a qual entendemos que é definida recursivamente pela regra

$$x_{n+1} = f(x_n).$$

6.1 Axioma do infinito e construções básicas

Axioma ∞ (Infinito)**.** Existem o *infinito contável* $\mathbb{N}$ (ou *conjunto dos números naturais*), o *zero* $0 \in \mathbb{N}$ e a transformação *sucessor* $\Vdash : \mathbb{N} \to \mathbb{N}$, que satisfazem: para todo conjunto C, toda transformação $f : C \to C$ e todo elemento $x_0 \in C$, existe única transformação $x : \mathbb{N} \to C$ tal que

$$\begin{aligned} x(0) &= x_0 \\ x \circ \Vdash &= f \circ x. \end{aligned}$$

Isso é equivalente a dizer que o seguinte diagrama comuta:

$$\begin{tikzcd}
& \mathbb{N} \arrow[r, "\Vdash"] \arrow[dd, dashed, "x"'] & \mathbb{N} \arrow[dd, dashed, "x"] \\
\mathbb{1} \arrow[ur, "0"] \arrow[dr, "x_0"'] & & \\
& C \arrow[r, "f"'] & C
\end{tikzcd}$$

Notação 5. Em geral omitiremos os parênteses no aplicação de $\Vdash$ a um número natural $n \in \mathbb{N}$, denotando $\Vdash n \coloneqq \Vdash(n)$.

Definição 11. Um *número natural* é um elemento $n \in \mathbb{N}$. O *um* é o número $1 \coloneqq \Vdash 0$, o sucessor do zero, e o *dois* é o número $2 \coloneqq \Vdash 1$, o sucessor do um.

A notação $\Vdash$ tem um propósito duplo: de certa forma representa uma seta (sem ponta) orientada para a direita, indicando que o sucessor de um número n é o próximo número à direita de n na usual representação linear horizontal de $\mathbb{N}$ orientada para a direita; e também relembra (grosseiramente) os símbolos "1+" na representação do sucessor de n usando a adição + e o número 1, isto é,

$$\Vdash n = 1 + n.$$

A transformação $x : \mathbb{N} \to C$ que aparece no AXIOMA ∞ é o que se denomina uma sequência em C.

Definição 12. Seja C um conjunto. Uma *sequência* em C é uma transformação $x : \mathbb{N} \to C$. Para cada $n \in \mathbb{N}$, denota-se $x_n \coloneqq x \circ n$ e $(x_n)_{n \in \mathbb{N}} \coloneqq x$.

Considerando cada $n \in \mathbb{N}$, a condição do AXIOMA ∞ se torna

$$\begin{aligned} x(0) &= x_0, \\ x_{\Vdash n} &= f(x_n), \end{aligned}$$

o que deixa claro que x é a órbita de x_0 sob a ação da dinâmica f.

O seguinte lema é uma versão "mais geral" do AXIOMA ∞. A intuição dinâmica por trás é imaginar que agora a dinâmica f depende não somente do ponto em C, mas também do tempo em $\mathbb{N}$. Isso é uma versão discreta de um sistema não-autônomo de equações diferenciais, e a demonstração envolve o mesmo tipo de argumento para reduzir um sistema não autônomo a um sistema autônomo.

Proposição 6.1 (Recursão não-autônoma)**.** *Para toda transformação $f\colon \mathbb{N} \times C \to C$ e todo elemento $x_0 \in C$, existe única sequência $x\colon \mathbb{N} \to C$ tal que*

$$\begin{aligned} x(0) &= x_0, \\ x \circ \Vdash &= f \circ (\mathrm{I}_{\mathbb{N}}, x); \end{aligned}$$

ou seja, para cada $n \in \mathbb{N}$,

$$\begin{aligned} x(0) &= x_0, \\ x_{\Vdash n} &= f(n, x_n). \end{aligned}$$

Demonstração. Defina $D \coloneqq \mathbb{N} \times C$, $y_0 \coloneqq (0, x_0)$ e

$$\begin{aligned} g\colon \mathbb{N} \times C &\longrightarrow \mathbb{N} \times C \\ (n, c) &\longmapsto (\Vdash n, f(n, c)). \end{aligned}$$

Pelo AXIOMA ∞ para D, g e y_0, existe única sequência $y\colon \mathbb{N} \to D$ tal que

$$\begin{aligned} y(0) &= y_0, \\ y \circ \Vdash &= g \circ y; \end{aligned}$$

ou seja, para cada $n \in \mathbb{N}$,

$$\begin{aligned} y(0) &= y_0, \\ y_{\Vdash n} &= g(y_n). \end{aligned}$$

Tomando as projeções $\pi_0^{\mathbb{N},C}\colon \mathbb{N} \times C \to \mathbb{N}$ e $\pi_1^{\mathbb{N},C}\colon \mathbb{N} \times C \to C$ da sequência y, obtemos sequências $i\colon \mathbb{N} \to \mathbb{N}$ e $x\colon \mathbb{N} \to C$ tais que, para todo $n \in \mathbb{N}$,

$$y_n = (\pi_0^{\mathbb{N},C}(y_n), \pi_1^{\mathbb{N},C}(y_n)) = (i_n, x_n),$$

e que satisfazem

$$\begin{aligned} (i(0), x(0)) &= y(0) = y_0 = (0, x_0), \\ (i_{\Vdash n}, x_{\Vdash n}) &= y_{\Vdash n} = g(y_n) = g(i_n, x_n) = (\Vdash i_n, f(i_n, x_n)). \end{aligned}$$

Pela unicidade do AXIOMA ∞, deve valer $i = \mathrm{I}_{\mathbb{N}}$. Portanto a sequência x é única e satisfaz, para cada $n \in \mathbb{N}$,

$$\begin{aligned} x(0) &= x_0, \\ x_{\Vdash n} &= f(n, x_n). \end{aligned}$$

∎

Proposição 6.2. *Existe uma única transformação* $\dashv\colon \mathbb{N} \to \mathbb{N}$ *(denominada transformação* predecessor*) tal que*

$$\begin{aligned} \dashv(0) &= 0 \\ \dashv \circ \Vdash &= \mathrm{I}_{\mathbb{N}}; \end{aligned}$$

ou seja, para cada $n \in \mathbb{N}$,

$$\begin{aligned} \dashv(0) &= 0 \\ \dashv \circ \Vdash n &= n. \end{aligned}$$

A definição de conjunto infinito de Dedekind-Peano vale para $\mathbb{N}$. Essa definição diz que um conjunto ser infinito significa que existe um bijeção entre ele e um subconjunto próprio dele.

Proposição 6.3 ($\mathbb{N}$ é infinito)**.** *Vale* $\mathbb{1} + \mathbb{N} \equiv \mathbb{N}$ *e a transformação sucessor* $\Vdash$ *é injetiva e não é sobrejetiva.*

Podemos também provar o postulado do Peano para indução (matemática).

Proposição 6.4 (Indução matemática)**.** *Seja* $C \subseteq \mathbb{N}$ *um subconjunto tal que*

- *(Caso zero)* $0 \in C$;
- *(Caso sucessor) Para todo* $n \in \mathbb{N}$, *se* $n \in C$ *então* $\Vdash n \in C$.

Então $C = \mathbb{N}$.

Demonstração. Note que temos a inclusão canônica $\iota_C\colon C \to \mathbb{N}$ e que $C = \mathbb{N}$ quer dizer que ι_C é isomorfismo. Devemos portanto achar uma inversa $x\colon \mathbb{N} \to C$ para ι_C. A inversa será definida recursivamente usando o AXIOMA ∞. Pelo CASO SUCESSOR, podemos definir uma transformação $s\colon C \to C$ tal que

$$\iota_A \circ s = \Vdash \circ \iota_C.$$

Pelo CASO ZERO, temos $0 \in C$. Portanto segue do AXIOMA ∞ para C, s e 0 que existe única sequência $x\colon \mathbb{N} \to C$ tal que

$$\begin{aligned} x(0) &= 0 \\ x \circ \Vdash &= s \circ x \end{aligned}$$

Então segue que $\iota_C \circ x(0) = \iota_C(0) = 0$ e

$$(\iota_C \circ x) \circ \Vdash = \iota_C \circ s \circ x = \Vdash \circ \iota_C \circ x = \Vdash \circ (\iota_C \circ x),$$

logo segue por unicidade (do AXIOMA ∞) que $\iota_C \circ x = \mathrm{I}_{\mathbb{N}}$. Por outro lado, vale

$$\iota_C \circ (x \circ \iota_C) = (\iota_C \circ x) \circ \iota_C = \mathrm{I}_{\mathbb{N}} \circ \iota_C = \iota_C \circ \mathrm{I}_C.$$

Como ι_C é injetiva (monomorfismo), segue que $x \circ \iota_C = \mathrm{I}_C$. Concluímos então que x é inversa de ι_C e portanto que $C = \mathbb{N}$. ■

6.1.1 Composição iterada de dinâmica

Consideremos um conjunto C e uma transformação $f\colon C \to C$. O diagrama da exponencial nesse caso fica

$$\begin{tikzcd} & \mathbb{1} \times C \arrow[dl, dashed, "f. \times \mathrm{I}_C"'] \arrow[d, "f"] & \mathbb{1} \arrow[d, dashed, "f."'] \\ {}^{C}C \times C \arrow[r, "\epsilon"'] & C & {}^{C}C \end{tikzcd}$$

$$
\begin{tikzcd}
 & X \times C \arrow[dl, dashed, "f_\bullet \times \mathrm{I}_C"'] \arrow[d, "f"] \\
{}^{C}C \times C \arrow[r, "\epsilon"'] & C
\end{tikzcd}
\qquad
\begin{tikzcd}
X \arrow[d, dashed, "f_\bullet"'] \\
{}^{C}C
\end{tikzcd}
$$

O seguinte resultado permite representar a composição iterada de uma dinâmica $f : C \to C$ no conjunto de transformações ${}^{C}C$.

Proposição 6.5 (Composições iteradas de transformação)**.** *Sejam C um conjunto e $f : C \to C$ uma transformação. Existe única sequência $f^{(\cdot)} : \mathbb{N} \to {}^{C}C$ tal que*

$$
\begin{aligned}
f^{(\cdot)}(0) &= \mathrm{I}_C, \\
f^{(\cdot)} \circ \Vdash &= \epsilon(f_\bullet, f^{(\cdot)} \circ \Vdash);
\end{aligned}
$$

ou seja, para cada $n \in \mathbb{N}$, e denotando $f^n := f^{(\cdot)}(n)$,

$$
\begin{aligned}
f^0 &= \mathrm{I}_C \\
f^{\Vdash n} &= f \circ f^n.
\end{aligned}
$$

6.2 Aritmética

Para definir as operações aritméticas usuais em $\mathbb{N}$, vamos usar a composição iterada de transformações (PROPOSIÇÃO 6.5).

6.2.1 Adição

Definição 13 (Adição)**.** Definimos a adição $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ (denotada $n + n'$) indutivamente a partir da sucessão $\Vdash : \mathbb{N} \to \mathbb{N}$: para cada $n' \in \mathbb{N}$,

1. se $n = 0$, define-se $0 + n' := n'$;
2. se $\Vdash n$, define-se $(\Vdash n) + n' := \Vdash(n' + n)$.

Proposição 6.6 (Propriedades algébricas da adição)**.**

6.2.2 Multiplicação

Definição 14 (Multiplicação)**.** Definimos a multiplicação $\times : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ (denotada $n \times n'$) indutivamente a partir da adição $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$: para cada $n' \in \mathbb{N}$,

1. se $n = 0$, define-se $0 \times n' := 0$;
2. se $\Vdash n$, define-se $(\Vdash n) \times n' := n' + (n' \times n)$.

Proposição 6.7 (Propriedades algébricas da multiplicação)**.**

6.2.3 Potenciação

Definição 15 (Potenciação)**.** Definimos a potenciação $\hat{} : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ (denotada $n^{n'}$) indutivamente a partir da multiplicação $\times : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$: para cada $n \in \mathbb{N}$,

1. se $n' = 0$, define-se $n^0 := 1$;
2. se $\Vdash n'$, define-se $n^{\Vdash n} := n \times n^{n'}$.

Proposição 6.8 (Propriedades algébricas da potenciação)**.**

7 Escolha

Axioma 10 (Escolha)**.** Todo epimorfismo tem inversa à direita.

$$C \underset{\twoheadrightarrow}{\overset{\leftarrow\text{-}\text{-}\text{-}}{\rightleftarrows}} C'$$

Referências

[Law64] F. W. Lawvere. "An Elementary Theory of the Category of Sets". *Proceedings of the National Academy of Science of the U.S.A.* 52.6 (1964), pp. 1506–1511 [Citado na p. 3].

[LR03] F. W. Lawvere e R. Rosebrugh. "Sets for Mathematics". Cambridge University Press, 2003 [Citado na p. 3].