1. O CONJUNTO DOS NÚMEROS NATURAIS E OS AXIOMAS DE PEANO

Neste capítulo apresentaremos os números naturais. Primeiro será apresentada brevemente parte histórica e sua importância, após isso, enunciaremos os axiomas. Depois definiremos uma adição, uma multiplicação e uma relação de ordem, bem como listaremos algumas propriedades básicas e faremos sua demonstração. As referências básicas desse capítulo são **domingues-2009** e **ferreira**.

1.1. Um pouco de história

Uma possível narrativa para o início do trabalho com números seria à de associação à controle de rebanho por pastores, embora essa narrativa não seja definitiva **roque**. Essa iniciação com números pode ter seguido dois caminhos possíveis, foram mantidos ou não foram mantidos. Isso porque alguns conhecimentos foram perdidos ao longo do tempo, enquanto outros foram mantidos e desenvolvidos, Nesse sentido não é possível estabelecer uma matemática definitiva e uma única evolução **roque**.

Em

Os números naturais foram os que mais resistiram ao tempo na sua formalização. Uma tentativa que na época não ficou muito difundida foi, em 1888 por Dedekind, a formalização dos naturais. No entando, apenas no ano seguinte, pelo italiano Giuseppe Peano, a formalização ficou amplamente difundida. O trabalho de Peano utilizou o de Dedekind como base. CITAR

O autor que teve grande contribuição no desenvolvimento dessa área, **peano** fundamentou a sua aritmética com 9 axiomas, como extraído abaixo e com 3 conceitos primitivos.

ARITHMETICES PRINCIPIA.

§ 1. De numeris et de additione.

Explicationes.

Signo N significatur *numerus (integer positivus).*
» 1 » *unitas.*
» $a+1$ » *sequens* a, sive a *plus* 1.
» $=$ » *est aequalis*. Hoc ut novum signum considerandum est, etsi logicae signi figuram habeat.

Axiomata.

1. $1 \varepsilon \mathrm{N}.$
2. $a \varepsilon \mathrm{N} \,.\supset.\, a=a.$
3. $a, b, c \varepsilon \mathrm{N} \,.\supset:\, a=b \,.=.\, b=a.$
4. $a, b \varepsilon \mathrm{N} \,.\supset\therefore\, a=b \,.\, b=c :\supset.\, a=c.$
5. $a=b \,.\, b \varepsilon \mathrm{N} :\supset.\, a \varepsilon \mathrm{N}.$
6. $a \varepsilon \mathrm{N} \,.\supset.\, a+1 \varepsilon \mathrm{N}.$
7. $a, b \varepsilon \mathrm{N} .\supset:\, a=b \,.=.\, a+1=b+1.$
8. $a \varepsilon \mathrm{N} \,.\supset.\, a+1 -= 1.$
9. $k \varepsilon \mathrm{K} \therefore 1 \varepsilon k \therefore x \varepsilon \mathrm{N} \,.\, x \varepsilon k :\supset_x .\, x+1 \varepsilon k :: \supset .\, \mathrm{N} \supset k.$

Definitiones.

10. $2=1+1;\ 3=2+1;\ 4=3+1;$ etc.

CITAR

"Ao cirar um jogo, é importante que suas regras sejam suficientes e consistentes. Por *suficiente* queremos dizer que as regras devem estabelecer o que é permitido fazer em qualquer situação que possa viar a ocorrer no desenrolar de uma partida do jogo. Por *consistente* queremos dizer que as regras não devem contradizer-se, ou sua aplicação levar a situações contraditórias."**barbosa**.

Para nós, as peças do jogo serão o conceito de um, o conceito de número natural, e o conceito da relação sucessor. As regras do jogo, naturalmente serão os axiomas que relacionarão esses 3 conceitos primitivos. Nessa analogia, as peças não são muito importantes.

1.2. Axiomas

O nosso estudo dos números naturais será iniciado pela sua apresentação em 3 conceitos primitivos, como os de Peano, e 5 axiomas (ao invés de 9), que são:

Axioma 1. *Existe um conjunto de exatamente todos os números naturais, que será denotado por $\mathbb{N}$, e existe uma função $s : \mathbb{N} \to \mathbb{N}$, que é a relação "sucessor".*

Axioma 2. *Um é um número natural, isto é, $1 \in \mathbb{N}$.*

Axioma 3. *Um não é sucessor de nenhum número, isto é, $1 \notin Im(s)$ ou ainda, $\nexists x \in \mathbb{N} : s(x) = 1$.*

Axioma 4. *s é injetora, isto é, $s(x) = s(y) \implies x = y$ [1].*

Axioma 5. *Se $\mathbb{S}$ é um subconjunto de $\mathbb{N}$, caso $1 \in \mathbb{S}$ e se para todo k em $\mathbb{S}$ $s(k)$ também esteja em $\mathbb{S}$, então $\mathbb{S} = \mathbb{N}$, isso é o mesmo que colocar: $\mathbb{S} \subseteq \mathbb{N} \land 1 \in S \land (k \in \mathbb{S} \implies s(k) \in \mathbb{S}) \implies \mathbb{S} = \mathbb{N}$.*

Este último axioma é chamado de axioma da indução finita.

Conforme os axiomas aprsentados, deve ser notado que o conjunto $\mathbb{N}$ (na nossa axiomatização) não tem o 0 (zero) que é, usualmente, o neutro da soma em $\mathbb{N}$. O intuito de construir a partir do 1 é pela questão que às vezes surge em diversas situações: "0 é um número natural?". Em diversos locais, dizem que pode ser e pode não ser. É dito que fica a critério de conveniência, embora para nós, seja 'inconveniente' perder o neutro da soma (que aparecerá sua primeira vez em $\mathbb{Z}$).

Justificamos essa escolha pois essa dificuldade na ausência do zero terá algumas implicações, que poderão ser observadas na nossa construção. Além disso, a bibliografia

[1] Vale notar a contra-positiva que estabelece, nesse caso: $x \neq y \implies s(x) \neq s(y)$

principal trata o zero como um número natural, então a construção será necessariamente com essas adaptações, o que na visão do autor, é algo positivo para o desenvolvimento do trabalho, mas o resultado final em certo ponto de vista fica prejudicado, pois fica mais "remendado".

Observemos também que o próprio Peano começou originalmente pelo 1 e somente depois colocou o 0 como o primeiro número natural.

Para comerçarmos nosso desenvolvimento, podemos notar que o axioma 2 garante $\mathbb{N} \neq \emptyset$. Além dele, como $1 \in \mathbb{N}$ e pelo axioma 1 temos que $s(s(1)) \in \mathbb{N}$. Analogamente, $s(s(s(1))) \in \mathbb{N}$.

Em seguida apresentamos um lema que será necessário para ampliação de nosso ferramental inicial.

Lema 1.1. *Nenhum número natural é seu próprio sucessor* $x \in \mathbb{N} \implies x \neq s(x)$.

Demonstração: Faremos por indução. Seja $\mathbb{S} = \{x \in \mathbb{N} : x \neq s(x)\}$ Os axiomas 2 e 3 garantem que $1 \in \mathbb{S}$.
Supondo que $\exists k \in \mathbb{S} : k \neq s(k)$, queremos provar que o sucessor de k é diferente do sucessor do sucessor de k, isto é, $s(k) \neq s(s(k))$. Como $k \neq s(k)$ e s é injetora pelo axioma 4, concluímos que $s(k) \neq s(s(k))$. ∎

Teorema 1.1. *Todo número natural, exceto o* 1 *é sucessor de algum outro número natural, que é único, isto é,* $\forall x(x \in \mathbb{N} \wedge x \neq 1 \implies \exists! y : s(y) = x)$.

Demonstração: A prova é feita por indução. Seja $\mathbb{S} = \{x \in \mathbb{N} : x \neq 1 \implies (\exists! y \in \mathbb{N} : s(y) = x)\}$.
sabemos que $1 \in \mathbb{S}$ porque $x = 1$ torna o antecedente falso, onde podemos concluir qualquer coisa. Suponhamos que existe um k em $\mathbb{S}$, queremos mostrar que $s(k) \in \mathbb{S}$.
É imediato que $s(k) \in \mathbb{S}$ pois, se $k \in \mathbb{S}$, para o sucessor $s(k)$ existe um número k tal que
$$\underbrace{s(k)}_{\text{Da regra de } \mathbb{S}} = \underbrace{s(k)}_{\text{Axioma 5}}.$$
A unicidade de y também é imediata, pois $s(a) = s(b) = k \implies a = b$ pela injetividade de s axioma 4. ∎

Observação 1.1. Diremos que o número y é antecessor de $x = s(y)$. Além disso vale notar que s conforme definida no axioma 1 não é sobrejetora somente pelo fato de o contradomínio ser $\mathbb{N}$. Mas se considerarmos o caso restrito para $\mathbb{N} \setminus \{1\}$ teremos que s é uma *bijeção*.

1.3. A adição

A adição em $\mathbb{N}$ é a que mais intuitivamente está relacionada com a contagem e união de coisas discretas.

Definição 1.1. *Adição Sejam $x, y \in \mathbb{N}$. A adição entre x e y, denotada por $x+y$ é definida com as seguintes condições:*

(i) $x + 1 = s(x)$;

(ii) $x + s(y) = s(x + y)$.

Às vezes poderemos fazer referência à operação de adição com o nome de soma.

Lema 1.2. *O 1 comuta com qualquer número na soma, isto é,*$\forall x, x + 1 = 1 + x$

Demonstração: Seja $\mathbb{S} = \{x \in \mathbb{N} : x+1 = 1+x\}$. O 1 está em $\mathbb{S}$ pois $1+1 = 1+1$. sabendo que existe um k em $\mathbb{S}$, queremos provar que $s(k)$ também está em $\mathbb{S}$. Como $s(k) + 1 = s(s(k)) = s(k + 1) = s(1 + k) = 1 + s(k)$. Portanto $s(k)$ também está em $\mathbb{S}$ sempre que k também está, o que pelo princípio de indução $\mathbb{S} = \mathbb{N}$. ■

Abaixo veremos algumas propriedades básicas sobre a adição no conjunto $\mathbb{N}$.

Proposição 1.1. *Sejam $a, b, c, d \in \mathbb{N}$ valem:*

(i) Associativa: $(a + b) + c = a + (b + c)$;

(ii) Comutativa: $a + b = b + a$;

(iii) Fechamento: $a + b \in \mathbb{N}$;

(iv) Lei do cancelamento: $a + c = b + c \implies a = b$;

(v) $a + b \neq a$;

(vi) Inexistência de neutro: $\nexists e \in \mathbb{N} : \forall a, a + e = e + a = a$.

Demonstração:

(i) Associativa:
Seja $\mathbb{S} = \{x \in \mathbb{N} : (a + b) + x = a + (b + x)\}$. Para o 1 temos então $(a + b) + 1 = s(a + b) = a + s(b) = a + (b + 1)$, o que mostra que o 1 está em $\mathbb{S}$. Mostraremos que

$k \in \mathbb{S} \implies s(k) \in \mathbb{S}$, pois: $(a+b)+s(k) = s((a+b)+k) = s(a+(b+k)) = a + s(b+k) = a+(b+s(k))$, o que, pelo princípio de indução $\mathbb{S} = \mathbb{N}$.

Com isso tomamos a liberdade natural de omitir os parênteses na soma.

(ii) Comutativa:
Consideremos o conjunto $\mathbb{S} = \{x \in \mathbb{N} : a + x = x + a\}$. O $1 \in \mathbb{S}$ pois $a + 1 = 1 + a$ conforme o lema 1.2. Provemos então que se $k \in \mathbb{S}$ então $s(k) \in \mathbb{S}$, pois $a + s(k) = s(a+k) = s(k+a) = k + s(a) = k + a + 1 = k + 1 + a = s(k) + a$

(iii) Fechamento:
Seja $\mathbb{S} = \{x \in \mathbb{N} : a + x \in \mathbb{N}\}$. Obviamente o 1 está em $\mathbb{S}$. Suponhamos então que existe $k \in \mathbb{S}$, queremos saber se isso garante que $s(k) \in \mathbb{S}$. Temos então que $a + k \in \mathbb{N}$, já para $a + s(k) = a + k + 1 = (a + k) + 1 = s(a + k) \in \mathbb{S}$ pelo axioma 1 a função tem domínio e contradomínio $\mathbb{N}$.

(iv) Lei do cancelamento:
Seja $\mathbb{S} = \{x \in \mathbb{N} : x + b = x + c \implies b = c\}$, vamos provar que $\mathbb{S} = \mathbb{N}$. Obviamente o 1 está em $\mathbb{S}$ pois $1 + b = 1 + c \iff b + 1 = c + 1$ e pelo axioma da injetividade, se dois elementos tem sucessores iguais, eles próprios são iguais. Agora consideremos se vale que $(k + b = k + c \implies b = c) \implies (s(k) + b = s(k) + c \implies b = c)$.
$s(k)+b = s(k)+c \iff (k+b)+1 = (k+c)+1$, o que pelo mesmo motivo anterior, concluímos que $k + b = k + c$, e pela nossa hipótese concluímos que $b = c$.

(v) $a + b \neq a$;
Consideremos quatro casos:

(1) $a = 1 \wedge b = 1$
Temos $a + b = a \iff 1 + 1 = 1 \Rightarrow\!\Leftarrow$.

(2) $a = s(x) \wedge b = 1$
Temos $a + b = a \iff s(x) + 1 = s(x) \iff s(s(x)) = s(x) \Rightarrow\!\Leftarrow$.

(3) $a = 1 \wedge b = s(y)$
Temos $a + b = a \iff 1 + s(y) = 1 \iff s(1 + y) = 1 \Rightarrow\!\Leftarrow$.

(4) $a = s(x) \wedge b = s(y)$
Temos $a + b = a \iff s(x) + s(y) = s(x) \iff x + 1 + y + 1 = x + 1 \iff s(1 + y) = 1 \Rightarrow\!\Leftarrow$.

(vi) Inexistência de neutro:
Como consequência da demonstração anterior, temos que não existe neutro na adição, isto é, $a + e = e + a = a$.

■

Podemos observar que como não existe neutro, não poderemos aplicar descuidadamente as outras propriedades, por exemplo: não poderíamos ter provado que $a \neq a + 1$ usando a lei do corte e supondo que fossem iguais, assim: $a = a + 1 \implies 0 = 1$, porque isso não faz sentido no nosso desenvolvimento.

A multiplicação toma seu lugar como uma operação de redução da soma. É verdade que sem a notação do sistema posicional, o que nos possibilitaria interpretar $10 = s(9)$, dizer que a multiplicação é um resumo ou simplificação da computação da soma não faz muito sentido. Não faremos o uso do sistema posicional aqui em $\mathbb{N}$.

1.4. A multiplicação

Definição 1.2. *Multiplicação Sejam $x, y \in \mathbb{N}$. A multiplicação entre x e y, denotada por $x \cdot y$ é definida com as seguintes condições:*

(i) $x \cdot 1 = x$;

(ii) $x \cdot s(y) = x + x \cdot y$.

Observação 1.2. Com o intuito de omitir parênteses que seriam usados demais de outro modo, estebeleceremos a seguinte convenção:

$$x + y \cdot z := x + (y \cdot z) \text{ [2]}$$
$$x \cdot y + z := (x \cdot y) + z;$$
$$x \cdot y := xy$$

Enunciaremos abaixo algumas propriedades da multiplicação.

Proposição 1.2. *Sejam $a, b, c, d \in \mathbb{N}$ valem:*

(i) *Elemento neutro:* $\exists! e \in \mathbb{N} : a \cdot e = e \cdot a = a$; [3].

(ii) *Distributiva à esquerda:* $a \cdot (b + c) = ab + ac$;

(iii) *Associativa:* $(a \cdot b) \cdot c = a \cdot (b \cdot c)$;

(iv) *Distributiva à direita:* $(a + b) \cdot c = ac + bc$;

(v) *Comutativa:* $a \cdot b = b \cdot a$;

[2] := é o símbolo que representa que o que está à esquerda é por definição igual ao que está à direita
[3] Se for observada a definição de multiplicação, esse número pode ser o 1

(vi) Lei do cancelamento: $a \cdot b = a \cdot c \implies b = c$;

(vii) $a \cdot b = 1 \implies a = b = 1$.

Demonstração:

(i) Elemento neutro:
Seja $\mathbb{S} = \{x \in \mathbb{N} : 1 \cdot x = x \cdot 1\}$. O 1 está em $\mathbb{S}$ pois $1 \cdot 1 = 1 \cdot 1$. Supondo que $k \in \mathbb{S}$ podemos concluir que $s(k) \in \mathbb{S}$? Temos $1 \cdot s(k) = 1 + 1 \cdot k = 1 + k \cdot 1 = 1 + k = s(k) = s(k) \cdot 1$.
Além disso, sejam e_1, e_2 dois elementos neutros. Então $e_1 = e_1 \cdot e_2 = e_2 \implies e_1 = e_2$, portanto o neutro é único. Além disso a definição de multiplicação nos diz que é o 1 quem é o neutro.

(ii) Distributiva à esquerda:
Seja $\mathbb{S} = \{x \in \mathbb{N} : a(b + x) = ab + ax\}$. O 1 está em $\mathbb{S}$ pois $a(b+1) = a(s(b)) = a + ab = a \cdot 1 + ab$. Supondo que existe um $k \in \mathbb{S}$, queremos concluir que $s(k)$ também está em $\mathbb{S}$. Como $a(b + s(k)) = a(s(b + k)) = a + (a(b + k)) = a + (ab + ak) = ab + a + ak = ab + a \cdot s(k)$. Pelo axioma 5 tem-se que $\mathbb{S} = \mathbb{N}$.

(iii) Associativa:
Seja $\mathbb{S} = \{x \in \mathbb{N} : a(bx) = (ab)x\}$. Sabemos que o 1 está em $\mathbb{S}$ pois $a(b \cdot 1) = a(b) = ab = (ab) \cdot 1$. Agora suponhamos que exista um $k \in \mathbb{S}$, consideremos $s(k)$, para ver se ele está ou não em $\mathbb{S}$. Temos $a(b \cdot s(k)) = a(b + bk) = ab + abk = (ab) \cdot s(k)$, o que pelo axioma 5 tem-se que $\mathbb{S} = \mathbb{N}$.

(iv) Distributiva à direita: Seja $\mathbb{S} = \{x \in \mathbb{N} : (a + b)x = ax + bx\}$. Temos que o $1 \in \mathbb{S}$ pois $(a + b)1 = a + b = a \cdot 1 + b \cdot 1$. Provemos que se $k \in \mathbb{S}$ temos que $s(k) \in \mathbb{S}$. Consideremos então: $(a + b)s(k) = (a + b)(k + 1) = (a + b)k + (a + b) \cdot 1 = ak + bk + a + b = a + ak + b + bk = a \cdot s(k) + b \cdot s(k)$. Pelo axioma 5 tem-se que $\mathbb{S} = \mathbb{N}$.

(v) Comutativa:
Seja $\mathbb{S} = \{x \in \mathbb{N} : ax = xa\}$. Com certeza o 1 está em $\mathbb{S}$, porque 1 é o neutro da multiplicação. Agora vejamos se $k \in \mathbb{S}$ acarreta que $s(k) \in \mathbb{S}$. Temos então: $a \cdot s(k) = a(k + 1) = ak + a = 1 \cdot a + ka = (1 + k)a = s(k) \cdot a$. Pelo axioma 5 tem-se que $\mathbb{S} = \mathbb{N}$.

(vi) Lei do cancelamento:
Seja $\mathbb{S} = \{x \in \mathbb{N} : xb = xc \implies b = c\}$. O 1 está em $\mathbb{S}$ pois $1b = 1c \implies b = c$. Provemos que $k \in \mathbb{S} \implies s(k) \in \mathbb{S}$. Temos que $s(k) \cdot b = s(k) \cdot c \iff b + bk = c + ck \iff b = c$. Pelo axioma 5 tem-se que $\mathbb{S} = \mathbb{N}$.

(vii) $a \cdot b = 1 \implies a = b = 1$. Consideremos que o a ou o b podem ser igual (ou iguais) a 1. Sem perda de generalidade, seja $a = 1$. Temos que $1 \cdot b = 1 \implies b = 1$ pois 1 é o elemento neutro. Portanto se algum a ou se b forem iguais a 1, obrigatoriamente o outro deverá ser, para que a igualdade ocorra. Consideremos um último caso, se $a \neq 1 \wedge b \neq 1$. Então existem x e y naturais tais que $a = s(x)$ e $b = s(y)$. Assim, $ab = 1 \iff (x+1)(y+1) = 1 \implies 1 + y + 1 + x = 1 \implies s(y+1+x) = 1$, o que obviamente não pode ocorrer de acordo com o axioma 3.

■

Nesse desenvolvimento, as propriedades ficaram semelhantes à como seria se fosse incluído o 0. As propriedades associativa e comutativa já eram presentes na soma. Agora no produto, temos um elemento neutro que não há para a soma, além da distributiva que pode ser aplicada com soma e produto. Na nossa lei do cancelamento, não precisamos especificar que o termo a ser cancelado é diferente de zero.

Até agora dispomos de uma soma e um produto em $\mathbb{N}$, mas isso ainda não nos possibilita comparar dois elementos de $\mathbb{N}$. Numa situação simplificada poderíamos legitimamente perguntar se a qunatidade x ou quantidade y é maior ou tem mais. Para essas perguntas, podemos utilizar uma relação de ordem.

Uma relação de ordem em um conjunto em geral não precisa ser única, embora para os fins deste trabalho, as relações de odem em todos os conjuntos que definiremos será a relação de ordem usual, o que poderemos chamar de "a"relação de ordem, ao invés de "uma"relação de ordem.

1.5. A relação de ordem

Definição 1.3. *Sejam $x, y \in \mathbb{N}$. Definiremos a relação $\leq$ entre x e y, denotado por $x \leq y$, e diremos que x se relaciona com y através de '$\leq$' quando $x = y \vee x + n = y, n \in \mathbb{N}$.*

Observação 1.3. Deve ser notado que quando $x \leq y$ uma e apenas uma das seguintes situações pode ocorrer $x = y$ ou $x + n = y, n \in \mathbb{N}$. Isso é devido à propriedade 1.1

Definição 1.4. *Vamos usar a relação $<$ entre x e y dessa forma: $x < y$, para dizer que $x \leq y$ mas $x \neq y$, o que é devido à observação anterior.*

Proposição 1.3. *Sejam $a, b, c, d \in \mathbb{N}$ valem:*

(i) Reflexiva: $a \leq a$;

(ii) Antissimétrica: $a \leq b \wedge b \leq a \implies a = b$;

(iii) Transitiva: $a \leq b \wedge b \leq c \implies a \leq c$*;*

(iv) Totalidade: $a \leq b \vee b \leq a$*;*

(v) Compatível com adição: $a \leq b \iff a + c \leq b + c$*;*

(vi) Compatível com multiplicação: $a \leq b \iff ac \leq bc$*.*

Demonstração:

(i) Reflexiva:
É imediato que $a = a \implies a \leq a$.

(ii) Antissimétrica:
Se $a = b$ não há nada a provar. Consideremos que sejam diferentes. Então $a \leq b \iff b = a + n$ e também, como $b \leq a \iff a = b + m$, substituindo, temos $b = (b + m) + n \implies b = b + r$ para algum r natural, o que não pode ocorrer.

(iii) Vamos considerar 4 casos:

(1) $a = b = c$
Temos $a = c \implies a \leq c$

(2) $a = b < c$
Temos $b + n = c \implies a + n = c \implies a \leq c$

(3) $a < b = c$
Temos $a + n = b = c \implies a \leq c$

(4) $a < b < c$
Temos $a + m = b \wedge b + n = c \implies (a + m) + n = c \implies a \leq c$

(iv) Totalidade: TODO

(v) Compatível com adição:
Seja $a \leq b$. Se $a = b$ teremos que $a + c = b + c$ porque a adição é uma função! Consideremos agora $a < b$. Então $b = a + m \implies b + c = a + m + c \implies a + c < b + c$.

(vi) Compatível com multiplicação:
É análogo ao caso da compatibilidade com a adição.

■

Essa é uma relação de ordem pois tem as propriedades i, ii e iii.

2. O CONJUNTO DOS NÚMEROS INTEIROS

Neste capítulos faremos a construção dos números inteiros. A bibliografia principal continua sendo FERREIRA e DOMINGUES. Será apresentado uma relação de equivalência que servirá para criar $\mathbb{Z}$. Depois definiremos uma adição e um produto que tenha algumas propriedades que já tinham em $\mathbb{N}$, isto é, queremos "estender"$\mathbb{N}$.

Devemos observar que em $\mathbb{N}$ temos que a subtração, tal como conhecemos no ensino básico, não é uma operação (no sentido da álgebra), pois a subtração não está definida para quaisquer dois elementos de $\mathbb{N}$ tal que o resultado esteja em $\mathbb{N}$.

Com o objetivo de contornar esse problema, queremos criar um novo conjunto a partir de $\mathbb{N}$ tal que a subtração também seja uma operação. Veremos que isso é possível, tal conjunto será denotado por $\mathbb{Z}$ e chamaremos ele de conjunto dos *números inteiros*.

Nos números naturais, poderíamos ter definido uma função que tivesse o intuito de fazer o inverso da soma, que seria a subtração denotada por "$-$". Seguindo esse raciocínio poderíamos mostrar que $9-3=8-2=7-1$. Concluiríamos com base nessas igualdades, que $9+2=8+3$ e $8+1=7+2$, o que em ambos os casos, os resultados são números naturais.

Além disso, queremos expressar um número inteiro apenas com números naturais, sem ter que assumir mais que $\mathbb{N}$, a lógica e a teoria de conjuntos que já foram assumidas. Além disso, tentar dar significado à expressões do tipo $3-5, 4-8, 2-3$ que nesses exemplos não são números naturais.

A maneira como expressaremos será através de uma relação binária $\sim$ sobre $\mathbb{N}\times\mathbb{N}$ definida desse modo: $(a,b)\sim(c,d) \iff a+d=b+c$.

Teorema 2.1. *A relação $\sim$ é de equivalência.*

Demonstração:

(i) Reflexiva: $(a,b)\sim(a,b) \iff a+b=b+a$.

(ii) Simetria: $(a,b)\sim(c,d) \iff (c,d)\sim(a,b)$
Temos $a+d=b+c=c+b=d+a \iff (c,d)\sim(a,b)$.

(iii) Transitiva: $(a,b) \sim (c,d) \wedge (c,d) \sim (e,f) \implies (a,b) \sim (e,f)$.
Temos $(a,b) \sim (c,d) \iff a+d = b+c$
e também que $(c,d) \sim (e,f) \iff c+f = d+e$.
Somando os dois primeiros termos entre si, e os dois segundos termos entre si, e igualando os resultados, temos:
$a+d+(c+f) = b+c+(d+e) \iff a+f = b+e \iff (a,b) \sim (e,f)$.

■

Definição 2.1. *O conjunto quociente* $\mathbb{N} \times \mathbb{N}/\sim = \{\overline{(a,b)} : (a,b) \in \mathbb{N} \times \mathbb{N}\}$ *será chamado de* conjunto dos números inteiros *e será denotado, conforme já anunciado, por* $\mathbb{Z}$ *.*

Observação 2.1. Utilizaremos a mesma notação para adição e multiplicação de números inteiros, que utilizamos nos números naturais. Inicialmente para o desenvolvimento do texto, sempre que $x, y \in \mathbb{N}$ entenderemos a soma $x+y$ como sendo executada em $\mathbb{N}$. Caso $x, y \in \mathbb{Z}$ entenderemos a soma $x+y$ sendo executada em $\mathbb{Z}$. Posteriormente justificaremos a escolha de utilizar os mesmos símbolos sendo que os conjuntos são diferentes. Isso se repetirá com a multiplicação e coma a relação de ordem.

Com essa definição de número inteiro podemos interpretar, a nível de ensino básico, que o número $\overline{(a,b)}$ é $a-b$. Embora caso fôssemos definir subtração em $\mathbb{N}$, ela não seria uma operação, pois estaria definida apenas quando $a > b$.

Proposição 2.1. *Podemos considerar uma "lei do corte"dentro do par ordenado, isto é, se* $a, b, k \in \mathbb{N}$ *vale que:* $\overline{(a+k, b+k)} = \overline{(a,b)}$

Demonstração: A demonstração é imediata, vemos que os elementos (os pares ordenados) representam a mesmo conjunto pois $a+k+b = b+k+a$. ■

2.1. A adição em $\mathbb{Z}$

Tínhamos a adição em $\mathbb{N}$. Vamos definir uma adição em $\mathbb{Z}$, se possível, mantendo algumas propriedades da adição em $\mathbb{N}$. Veremos que a maneira como definiremos garante isso.

Definição 2.2. *Dados* $\overline{(a,b)}$ *e* $\overline{(c,d)}$ *em* $\mathbb{Z}$ *, definimos a adição* $\overline{(a,b)} + \overline{(c,d)}$ *pelo número* $\overline{(a+c, b+d)}$*.*

Proposição 2.2. *A operação de adição está bem definida em* $\mathbb{Z}$ *. Isto é, a adição em* $\mathbb{Z}$ *não depende do representante das classes envolvidas na adição. Podemos expressar isso assim* *também:* $a, a', b, b', c, c', d, d' \in \mathbb{N}$, $\overline{(a,b)} = \overline{(a',b')} \wedge \overline{(c,d)} = \overline{(c',d')} \implies \overline{(a,b)} + \overline{(c,d)} = \overline{(a',b')} + \overline{(c',d')}$.

Demonstração: Vamos desenvolver as duas somas e mostrar que são iguais. Consideremos $\overline{(a,b)} + \overline{(c,d)} = \overline{(a+c, b+d)}$. Considerando agora a segunda soma temos: $\overline{(a',b')} + \overline{(c',d')} = \overline{(a'+c', b'+d')}$. Precisamos agora apenas mostrar que $(a+c, b+d) \sim (a'+c', b'+d')$, isso mostrará que $\overline{(a+c, b+d)} = \overline{(a'+c', b'+d')}$. Como $\overline{(a,b)} = \overline{(a',b')} \iff a+b' = b+a'$. Também como $\overline{(c,d)} = \overline{(c',d')} \iff c+d' = d+c'$ teremos então que $(a+b')+(c+d') = (b+a')+(d+c') \iff (a+c)+(b'+d') = (b+d)+(a'+c') \iff (a+c, b+d) \sim (a'+c', b'+d')$. ■

Proposição 2.3. *Sejam* $\overline{(a,b)}, \overline{(c,d)}, \overline{(e,f)}$ *números inteiros quaisquer, para a adição valem as seguintes propriedades:*

(i) Associativa: $\left(\overline{(a,b)} + \overline{(c,d)}\right) + \overline{(e,f)} = \overline{(a,b)} + \left(\overline{(c,d)} + \overline{(e,f)}\right)$;

(ii) Comutativa: $\overline{(a,b)} + \overline{(c,d)} = \overline{(c,d)} + \overline{(a,b)}$;

(iii) Elemento neutro: $\exists!\overline{(x,y)} \in \mathbb{Z} : \overline{(x,y)} + \overline{(a,b)} = \overline{(a,b)} + \overline{(x,y)} = \overline{(a,b)}$;

(iv) Lei do cancelamento: $\overline{(a,b)} + \overline{(c,d)} = \overline{(a,b)} + \overline{(e,f)} \implies \overline{(c,d)} = \overline{(e,f)}$

(v) Simétrico: $\forall\overline{(a,b)}\exists!\overline{(c,d)} : \overline{(a,b)} + \overline{(c,d)} = \overline{(c,d)} + \overline{(a,b)} = 0$;

(vi) Fechamento: $\overline{(a,b)} + \overline{(c,d)} \in \mathbb{Z}$

Demonstração:

(i) Associativa: $\left(\overline{(a,b)} + \overline{(c,d)}\right) + \overline{(e,f)} = \overline{(a+c, b+d)} + \overline{(e,f)} = \overline{(a+c+e, b+d+f)} = \overline{(a+(c+e), b+(d+f))} = \overline{(a,b)} + (\overline{(c+e, d+f)})$.

(ii) Comutativa: $\overline{(a,b)} + \overline{(c,d)} = \overline{(a+c, b+d)} = \overline{(c+a, d+b)} = \overline{(c,d)} + \overline{(a,b)}$;

(iii) Elemento neutro: $\exists!\overline{(x,y)} \in \mathbb{Z} : \overline{(x,y)} + \overline{(a,b)} = \overline{(a,b)} + \overline{(x,y)} = \overline{(a,b)}$;
Consideremos $\overline{(1,1)}$, vamos mostrar que ele é neutro pela esquerda. Temos que $\overline{(1,1)} + \overline{(a,b)} = \overline{(1+a, 1+b)}$. Provemos que $\overline{(1+a, 1+b)} \sim \overline{(a,b)}$. Temos então que $(1+a)+b = (1+b)+a$, o que sempre ocorre, portanto $\overline{(1,1)}$ é neutro pela esquerda. Analogamente prova-se que é pela direita, e além disso, todo elemento neutro para uma operação é único, conforme o teorema **??**, o que conclui nossa prova. Denotaremos o elemento neutro da adição de 0 e chamaremos de zero.

(iv) Lei do cancelamento: $\overline{(a,b)} + \overline{(c,d)} = \overline{(a,b)} + \overline{(e,f)} \implies \overline{(c,d)} = \overline{(e,f)}$. Temos $\overline{(a,b)} + \overline{(c,d)} = \overline{(a,b)} + \overline{(e,f)} \iff \overline{(a+c, b+d)} = \overline{(a+e, b+f)} \iff (a+c)+(b+f) = (b+d)+(a+e) \iff c+f = d+e \iff \overline{(c,d)} = \overline{(e,f)}$. A comutatividade garante a lei do cancelamento à esquerda e à direita.

(v) Simétrico: $\forall\overline{(a,b)}\exists!\overline{(c,d)} : \overline{(a,b)} + \overline{(c,d)} = \overline{(c,d)} + \overline{(a,b)} = 0$;
Consideremos então $\overline{(a,b)}$, mostraremos que $\overline{(b,a)}$ é tal que $\overline{(a,b)} + \overline{(b,a)} = \overline{(1,1)}$. Temos que $\overline{(a+b, b+a)} = \overline{(1,1)}$ porque $a + b + 1 = b + a + 1$, o que sempre ocorre. Considerando qualquer $\overline{(c,d)}$ tal que $\overline{(a,b)} + \overline{(c,d)} = \overline{(1,1)}$ teremos que $\overline{(a,b)} + \overline{(c,d)} = \overline{(a,b)} + \overline{(b,a)} \iff \overline{(c,d)} = \overline{(b,a)}$ pela lei do cancelamento da adição. Com isso, fica opcional a utilização da notação $-$ na frente do número, desse modo: $-\overline{(a,b)}$ para representar o simétrico de $\overline{(a,b)}$, porque ele existe e é único.

(vi) Fechamento: $\overline{(a,b)} + \overline{(c,d)} \in \mathbb{Z}$: Essa é imediata pois $a + c \in \mathbb{N} \wedge b + d \in \mathbb{N} \implies \overline{(a+c, b+d)} \in \mathbb{Z}$.

■

Com essas propriedades, podemos ver que a comutatividade, associatividade e fechamento são mantidos, com a diferença que agora trabalhamos com números inteiros e não naturais. Indo além, é possível ver que o elemento neutro da soma e o simétrico surgem naturalmente, embora não possamos dizer que o neutro em $\mathbb{Z}$ é $(0,0)$, pois nenhuma das coordenadas desse par ordenado são números naturais, não obstante qualquer $k \in \mathbb{N}$ temos que $(k,k) = 0 \in \mathbb{Z}$. E por último e não menos importante, temos agora um simétrico para a soma, o que em $\mathbb{N}$ não tem análogo.

2.2. A multiplicação em $\mathbb{Z}$

Novamente, podemos entender a multiplicação em $\mathbb{Z}$ como tentativa de estensão de $\mathbb{N}$ e, portanto, a multiplicação como uma notação resumida da soma.

Definição 2.3. *Dados $\overline{(a,b)}$ e $\overline{(c,d)}$ em $\mathbb{Z}$, definimos a multiplicação $\overline{(a,b)} \cdot \overline{(c,d)}$ pelo número $\overline{(a \cdot c + b \cdot d, a \cdot d + b \cdot c)}$.*

Observação 2.2. Poderemos omitir o símbolo da operação de multiplicação "$\cdot$"que fizemos nos naturais, quando não houver ambiguidade.

Teorema 2.2. *A operação de multiplicação está bem definida em $\mathbb{Z}$. Isto é, a multiplicação em $\mathbb{Z}$ não depende do representante das classes envolvidas na multiplicação. Equivale a dizer que, se*
$a, a', b, b', c, c', d, d' \in \mathbb{N} \wedge \overline{(a,b)} = \overline{(a',b')} \wedge \overline{(c,d)} = \overline{(c',d')} \implies \overline{(a,b)} \cdot \overline{(c,d)} = \overline{(a',b')} \cdot \overline{(c',d')}$.

Demonstração: Comecemos pela definição de multiplicação, $\overline{(a,b)} = \overline{(a',b')}$ e $\overline{(c,d)} = \overline{(c',d')}$ teremos os produtos: $\overline{(a,b)} \cdot \overline{(c,d)} = \overline{(ac+bd, ad+bc)}$ e $\overline{(a',b')} \cdot \overline{(c',d')} = \overline{(a'c'+b'd', a'd'+b'c')}$.

Vamos considerar agora as igualdades das classes, temos:
$\overline{(a,b)} = \overline{(a',b')} \iff a+b' = b+a'$ disso concluímos que $(a+b')c' = (b+a')c'$ e que $(a+b')d' = (b+a')d'$.
Considerando $\overline{(c,d)} = \overline{(c',d')} \iff c+d' = d+c'$, temos que $a(c+d') = a(d+c')$ e também que $b(c+d') = b(d+c')$.

Das igualdades que obtemos no parágrafo anterior, colocaremos na ordem de aparecimento as duas últimas de cada caso, embora apliquemos as distributivas e talvez troquemos o primeiro com o segundo termo da igualdade.

$$\begin{aligned} ac' + b'c' &= bc' + a'c' \\ bd' + a'd' &= ad' + b'd' \\ ac + ad' &= ad + ac' \\ bd + bc' &= bc + bd' \end{aligned}$$

Vamos agora somar a colona à esquerda, depois a coluna à direita, e colocar na mesma equação, assim:

$$ac' + b'c' + bd' + a'd' + ac + ad' + bd + bc' = bc' + a'c' + ad' + b'd' + ad + ac' + bc + bd'$$

Cancelando os termos ac', bd', ad', bc' ficamos com:

$$\begin{aligned} b'c' + a'd' + ac + bd &= a'c' + b'd' + ad + +bc \\ ac + bd + a'd' + b'c' &= ad + bc + a'c' + b'd' \end{aligned}$$

Com isso provamos que $(ac+bd, ad+bc) \sim (a'c'+b'd', a'd'+b'c')$, o que nos mostra que a classe é a mesma, então o produto não depende do representante da classe, que pode, portanto, ser arbitrário. ■

Proposição 2.4. *Sejam $\overline{(a,b)}, \overline{(c,d)}, \overline{(e,f)}$ números inteiros quaisquer, para a multiplicação valem as seguintes propriedades:*

(i) Associativa: $\left(\overline{(a,b)} \cdot \overline{(c,d)}\right) \cdot \overline{(e,f)} = \overline{(a,b)} \cdot \left(\overline{(c,d)} \cdot \overline{(e,f)}\right)$;

(ii) Comutativa: $\overline{(a,b)} \cdot \overline{(c,d)} = \overline{(c,d)} \cdot \overline{(a,b)}$;

(iii) Elemento neutro: $\exists! \overline{(x,y)} \in \mathbb{Z} : \overline{(x,y)} \cdot \overline{(a,b)} = \overline{(a,b)} \cdot \overline{(x,y)} = \overline{(a,b)}$;

(iv) Lei do cancelamento: $\overline{(a,b)} \cdot \overline{(c,d)} = \overline{(a,b)} \cdot \overline{(e,f)} \implies \overline{(c,d)} = \overline{(e,f)}$

(v) Fechamento: $\overline{(a,b)} \cdot \overline{(c,d)} \in \mathbb{Z}$

(vi) Lei do anulamento do produto: $\overline{(a,b)} \cdot \overline{(c,d)} = 0 \implies \overline{(a,b)} = 0 \vee \overline{(c,d)} = 0$;

(vii) Distributivas: $\overline{(a,b)} \cdot \left(\overline{(c,d)} + \overline{(e,f)}\right) = \left(\overline{(a,b)} \cdot \overline{(c,d)}\right) + \left(\overline{(a,b)} \cdot \overline{(e,f)}\right)$

Demonstração:

(i) Associativa:

$$\begin{aligned}
\left(\overline{(a,b)} \cdot \overline{(c,d)}\right) \cdot \overline{(e,f)} &= \overline{(ac+bd, ad+bc)} \cdot \overline{(e,f)} \\
&= \overline{((ac+bd)e + (ad+bc)f, (ac+bd)f + (ad+bc)e} \\
&= \overline{(ace+bde+adf+bcf, acf+bdf+ade+bce)} \\
&= \overline{(ace+adf+bcf+bde, acf+ade+bce+bdf)} \\
&= \overline{(a(ce+df)+b(cf+de), a(cf+de)+b(ce+df))} \\
&= \overline{(a,b)} \cdot \overline{(ce+df, cf+de)} \\
&= \overline{(a,b)} \cdot \left(\overline{(c,d)} \cdot \overline{(e,f)}\right)
\end{aligned}$$

(ii) Comutativa:

$$\begin{aligned}
\overline{(a,b)} \cdot \overline{(c,d)} &= \overline{(ac+bd, ad+bc)} \\
&= \overline{(ca+db, bc+da)} \\
&= \overline{(c,d)} \cdot \overline{(a,b)}
\end{aligned}$$

(iii) Elemento neutro: Consideremos o número $\overline{(2,1)}$. Vamos mostrar que ele é neutro pela direita. Temos $\overline{(a,b)} \cdot \overline{(2,1)} = \overline{(2a+b, a+2b)} = \overline{(a,b)}$, essa última igualdade é porque $a+a+2b = b+2a+b$. Analogamente se mostra que é neutro pela esquerda. A unicidade é garantido pelo teorema **??**.

(iv) Lei do cancelamento: Por hipótese temos

$$\begin{aligned}
\overline{(a,b)} \cdot \overline{(c,d)} &= \overline{(a,b)} \cdot \overline{(e,f)} \\
\overline{(ac+bd, ad+bc)} &= \overline{(ae+bf, af+be)}
\end{aligned}$$

O que equivale a:

$$ac+bd+af+be = ad+bc+ae+bf$$

Como $\overline{(a,b)} \neq 0$, $a \neq b$. Suponhamos sem perda de generalidade que $a > b$, temos que $a = b+m$ para algum m natural. Substituindo na equação ficamos com

$$\begin{aligned}
(b+m)(c+f)+b(d+e) &= (b+m)(d+e)+b(c+f) \\
bc+bf+mc+mf+bd+be &= bd+be+md+me+bc+bf
\end{aligned}$$

Cancelando os termos bc, bf, bd, be ficamos com

$$\begin{aligned} mc + mf = md + me &\iff \\ m(c+f) = m(d+e) &\iff \\ c + f = d + e &\iff \\ (c,d) &\sim (e,f) \end{aligned}$$

$$\therefore \overline{(c,d)} = \overline{(e,f)}$$

(v) Fechamento: $\overline{(a,b)} \cdot \overline{(c,d)} \in \mathbb{Z}$ Temos $\overline{(a,b)} \cdot \overline{(c,d)} = \overline{(ac+bd, ad+bc)}$. Como $ac + bd \in \mathbb{N}$ e também $ad + bc \in \mathbb{N}$ temos $\overline{(ac+bd, ad+bc)} \in \mathbb{Z}$.

(vi) Lei do anulamento do produto: $\overline{(a,b)} \cdot \overline{(c,d)} = 0 \implies \overline{(a,b)} = 0 \vee \overline{(c,d)} = 0$; TODO

(vii) Distributiva: primeiro vamos mostrar a distributiva à esquerda.

$$\begin{aligned} \overline{(a,b)} \cdot \left(\overline{(c,d)} + \overline{(e,f)}\right) &= \overline{(a,b)} + (\overline{(c,d)} + \overline{(e,f)}) \\ &= \overline{(a(c+e) + b(d+f), a(d+f) + b(c+e)} \\ &= \overline{(ac + ae + bd + bf, ad + af + bc + be)} \\ &= \overline{(ac+bd, ad+bc)} + \overline{(ae+bf, af+be)} \\ &= \left(\overline{(a,b)} \cdot \overline{(c,d)}\right) + \left(\overline{(a,b)} \cdot \overline{(e,f)}\right) \end{aligned}$$

Pela comutatividade do produto em $\mathbb{Z}$ e pela distributiva à esquerda, a distributiva a direita está também provada.

■

Lema 2.1. $\forall \overline{(a,b)} \in \mathbb{Z} : \overline{(a,b)} \cdot 0 = 0$

Demonstração: Temos que $\overline{(a,b)} \cdot 0 = \overline{(a,b)} \cdot \overline{(1,1)} = \overline{(a+b, a+b)} = 0$. ■

2.3. Relação de ordem

Definição 2.4. *Dados $\overline{(a,b)}$ e $\overline{(c,d)}$ em $\mathbb{Z}$, definimos a relação de ordem $\leq$ e dizemos que $\overline{(a,b)}$ é menor do que ou igual a $\overline{(c,d)}$ quando $a + d \leq b + c$ e denotamos por $\overline{(a,b)} \leq \overline{(c,d)}$.*

Proposição 2.5. *Sejam $\overline{(a,b)}, \overline{(c,d)}, \overline{(e,f)}$ números inteiros quaisquer, para a relação de ordem valem as seguintes propriedades:*

(i) Reflexiva:
$\overline{(a,b)} \leq \overline{(a,b)}$

(ii) Antissimétrica:
$\overline{(a,b)} \leq \overline{(c,d)} \wedge \overline{(c,d)} \leq \overline{(a,b)} \implies \overline{(a,b)} = \overline{(c,d)}$

(iii) Transitiva:
$\overline{(a,b)} \leq \overline{(c,d)} \wedge \overline{(c,d)} \leq \overline{(e,f)} \implies \overline{(a,b)} \leq \overline{(e,f)}$

(iv) Totalidade:
$\overline{(a,b)} \leq \overline{(c,d)} \vee \overline{(c,d)} \leq \overline{(a,b)}$

(v) Compatível com a adição:
$\overline{(a,b)} \leq \overline{(c,d)} \implies \overline{(a,b)} + \overline{(e,f)} \leq \overline{(c,d)} + \overline{(e,f)}$

(vi) Compatível com a multiplicação:
$\overline{(a,b)} \leq \overline{(c,d)} \wedge 0 = \overline{(1,1)} \leq \overline{(e,f)} \implies \overline{(a,b)} \cdot \overline{(e,f)} \leq \overline{(c,d)} \cdot \overline{(e,f)}$.

Demonstração:

(i) Reflexiva:
De fato ocorre que $a + b \leq b + a \therefore \overline{(a,b)} \leq \overline{(a,b)}$.

(ii) Antissimétrica:

$$\overline{(a,b)} \leq \overline{(c,d)} \wedge \overline{(c,d)} \leq \overline{(a,b)}$$
$$a + d \leq c + b \wedge c + b \leq d + a$$

O que, pela antissimetria em $\mathbb{N}$ temos que $a + d = c + b$, então $(a,b) \sim (c,d)$ e $\overline{(a,b)} = \overline{(c,d)}$.

(iii) Transitiva:

$$\overline{(a,b)} \leq \overline{(c,d)} \wedge \overline{(c,d)} \leq \overline{(e,f)} \iff$$
$$a + d \leq b + c \wedge c + f \leq d + e \iff$$
$$a + d + f \leq b + c + f \wedge c + f + b \leq d + e + b \iff$$
$$a + d + f \leq d + e + b \iff$$
$$a + f \leq b + e \iff \therefore \overline{(a,b)} \leq \overline{(e,f)}.$$

(iv) Totalidade:

$$\overline{(a,b)} \leq \overline{(c,d)} \vee \overline{(c,d)} \leq \overline{(a,b)}$$
$$a + d \leq b + c \vee c + b \leq d + a$$

Pela totalidade em $\mathbb{N}$ temos que sempre pelo menos uma das proposições disjuntas pelo $\vee$ ocorre.

(v) Compatível com a adição:

$$\overline{(a,b)} \leq \overline{(c,d)}$$
$$\overline{(a,b)} + \overline{(e,f)} + \overline{(f,e)} \leq \overline{(c,d)} + \overline{(e,f)} + \overline{(f,e)}$$

O que pela lei do cancelamento, temos

$$\overline{(a,b)} + \overline{(e,f)} \leq \overline{(c,d)} + \overline{(e,f)}.$$

(vi) Compatível com a multiplicação:
Por hipótese temos $\overline{(a,b)} \leq \overline{(c,d)}$ e $0 = \overline{(1,1)} \leq \overline{(e,f)}$. Isso nos garante que $e > f$ pois $a + f < 1 + e$. Seja então $e = f + m$ para algum m natural. Consideremos agora o que queremos provar:

$$\begin{aligned}
\overline{(a,b)} \cdot \overline{(e,f)} \leq \overline{(c,d} \cdot \overline{(e,f)} &\iff \\
\overline{(ae+bf, af+be)} \leq \overline{(ce+df, cf+de)} &\iff \\
ae + bf + cf + de \leq af + be + ce + df &\iff Já_f oi_p rovado?? \\
am + dm \leq bm + cm &\iff \\
(a+d)m \leq (b+c)m &\iff \\
a + d \leq b + c &
\end{aligned}$$

■

2.4. Imersão de $\mathbb{N}$ em $\mathbb{Z}$

Teorema 2.3. *Seja a função* $f : \mathbb{N} \to \mathbb{Z}, f(k) \mapsto f(k+1, 1)$. *Essa função tem as propriedades a seguir:*

(i) $f(a+b) = f(a) + f(b)$*;*

(ii) $f(a \cdot b) = f(a) \cdot f(b)$*;*

(iii) $a \leq b \implies f(a) \leq f(b)$*.*

Demonstração:

(i) $f(a+b) = f(a) + f(b)$

$$\begin{aligned} f(a+b) &= \overline{(a+b+1,1)}. \\ &= \overline{(a+1+b+1,1+1)} \\ &= f(a)+f(b). \end{aligned}$$

(ii) $f(a \cdot b) = f(a) \cdot f(b)$;

$$\begin{aligned} f(a \cdot b) &= \overline{(ab+1,1)} \\ &= \overline{(ab+a+b+1+1,a+1+b+1)} \\ &= \overline{((a+1)(b+1)+1,(a+1)1+1(b+1))} \\ &= \overline{(a+1,1)} \cdot \overline{(b+1,1)} \\ &= f(a)+f(b). \end{aligned}$$

(iii) $a \leq b \implies f(a) \leq f(b)$
Se $a = b$ então $f(a) = f(b)$ é óbvio. Suponhamos, por outro lado, $a \neq b$. Então $a < b \iff b = a + m$ para algum $m \in \mathbb{N}$. Temos então $f(a) = \overline{(a+1,1)}$ e $f(b) = f(a+m) = \overline{(a+m+1,1)}$. Vemos que $\overline{(a+1,1)} \leq \overline{(a+m+1,1)}$ porque $a+1+1 \leq 1+a+m+1$.

■

Observação 2.3. A partir de agora, tomaremos a liberdade de escrever os números inteiros com a notação usual de $\mathbb{N}$, isto é $1 = \overline{(2,1)}, 2 = \overline{(3,1)}, 3 = \overline{(4,1)}$ e assim por diante, além de representar o $\overline{(1,2)} = -1$, $\overline{(1,3)} = -2$, $\overline{(4,1)} = -3$ analogamente, ad infinitum.

A imersão de $\mathbb{N}$ em $\mathbb{Z}$ permite-nos interpretar $\mathbb{N}$ como um subconjunto de $\mathbb{Z}$, embora pela nossa construção fique evidente que isso não ocorra, nos termos de elementos dos conjuntos. Mas, por outro lado, as operações de adição e multiplicação e a relação de ordem funcionam analogamente em $\mathbb{Z}$, ou seja, o objetivo inicial de construir mantendo certa semelhança funcionou.

Essa é uma parte importante da construção dos números inteiros. Em geral não importa o que é um número, mas apenas o que conseguimos fazer com ele, as regras do jogo. Por outro lado, a construção do conjunto dos números inteiros mostra-nos que, se existir um conjunto $\mathbb{N}$, a lógica e a teoria de conjuntos elementar que assumimos até agora, então existe um conjunto $\mathbb{Z}$ que podemos manipular com as regras mostradas.

Num ponto de vista mais algébrico, num estudo básico de gradução, não interessa o que são e como são definidas as operações de soma e produto, mas, admitindo que exista um conjunto A com uma operação de soma e uma operação de produto, ambas tendo certas propriedades, é possível provar teoremas sem levar em conta a *natureza* dos entes matemáticos envolvidos.

A construção de $\mathbb{Z}$, a apresentação e prova das proposições apresentadas caminham nesse sentido de permitir uma abstração do conjunto, para que não seja mais necessário trabalhado com pares ordenados (ainda mais sem o 0 em $\mathbb{N}$!).

Poderíamos desenvolver alguns tópicos importantes levando em conta a natureza dos nossos números inteiros, que são pares ordenados. Isso é satisfatório, se conseguirmos provar o que queremos. Por outro lado, tratar com conjuntos genéricos permite uma abstração e uma generalização, mostrando que certas características não dependem de um conjunto específico, porque um conjunto está inexoravelmente ligado às propriedades que esse conjunto tem (claro que dependendo do que se assume como basilar). As abstrações permitem formar conclusões dependendo de apenas algumas caracterísitcas/propriedades do conjunto.

3. O CONJUNTO DOS NÚMEROS RACIONAIS

3.1. Ideias iniciais e objetivos

No capítulo anterior, conseguimos criar um conjunto cuja soma tivesse elemento neutro e que todo elemento tivesse um elemento simétrico nessa mesma operaçao. Neste capítulo vamos tentar construir um conjunto tal que para a multiplicação, dado qualquer elemento, seja também possível encontrar um simétrico. Para isso a bibliografia utilizada será DOMINGUES e FERREIRA.

O conjunto que criaremos será chamado de conjunto dos números racionais e será denotado por $\mathbb{Q}$.

3.2. Definição do conjunto

Para criar os racionais, vamos utilizar o mesmo artifício das classes de equivalência num subconjunto do produto cartesiano. O produto cartesiano que precisaremos excluirá o neutro da soma em $\mathbb{Z}$ da segunda cordenada, que será justificado no tempo devido.

$$\mathbb{Z} \times \mathbb{Z}^* = \{(a, b) : a \in \mathbb{Z} \wedge b \in \mathbb{Z}^*\}$$

Sobre $\mathbb{Z} \times \mathbb{Z}$ vamos considerar a relação definida por $(a, b) \sim (c, d) \iff ad = bc$. Muito, muito analogamente à criação de $\mathbb{Z}$.

Teorema 3.1. *A relação $\sim$ é de equivalência.*

Demonstração:

(i) Reflexiva: $(a, b) \sim (a, b) \iff a \cdot b = b \cdot a$.

(ii) Simetria: $(a, b) \sim (c, d) \iff (c, d) \sim (a, b)$
Temos $a \cdot d = b \cdot c = c \cdot b = d \cdot a \iff (c, d) \sim (a, b)$.

(iii) Transitiva: $(a, b) \sim (c, d) \wedge (c, d) \sim (e, f) \implies (a, b) \sim (e, f)$.
Temos $(a, b) \sim (c, d) \iff a \cdot d = b \cdot c$
e também que $(c, d) \sim (e, f) \iff c \cdot f = d \cdot e$.

Multiplicando os dois primeiros termos entre si, e os dois segundos termos entre si, e igualando os resultados, temos:
$(a \cdot d) \cdot (c \cdot f) = (b \cdot c) \cdot (d \cdot e) \iff a \cdot f = b \cdot e \iff (a, b) \sim (e, f)$.

■

Observação 3.1. Ao invés de utilizar a notação ostensiva de pares ordenados como utilizamos nos inteiros, passaremos a utilizar a notação de fração, que consiste em separar os elementos do par, na ordem, por uma barra horizontal, denotada $\frac{a}{b}$ ou por uma barra inclinada denotada assim: a/b, em ambos os casos representam $\overline{(a, b)} \in \mathbb{Q}$.

Definição 3.1. *Os números racionais são o conjunto $\mathbb{Z} \times \mathbb{Z}^*/\sim$, que será denotado por $\mathbb{Q}$.*

Claro que com essa definição, os números de $\mathbb{Q}$ são classes de equivalência em $\mathbb{Z} \times \mathbb{Z}$, então quando escrevermos que $\frac{a}{b}$ ou a/b e dissermos que eles são números racionais, estaremos afirmando também que $a \in \mathbb{Z}$ e que $b \in \mathbb{Z}^*$.

3.3. Adição em $\mathbb{Q}$

Definição 3.2. *Adição em $\mathbb{Q}$ Sejam $x = \dfrac{a}{b}$ e $y = \dfrac{c}{d}$ números racionais. Chamamos de adição entre x e y, denotada por $x + y$ que é definido como $\dfrac{ad + bc}{bd}$.*

Proposição 3.1. *A operação de adição está bem definida.*

Demonstração: DEMONSTRACAO A operação de adição está bem definida. ■

Proposição 3.2. *A adição em $\mathbb{Q}$ é associativa, comutativa, tem elemento neutro, cada elemento tem um único simétrico, atende a lei do cancelamento e é fechada em $\mathbb{Q}$.*

Proposição 3.3. *Para a adição valem as seguintes propriedades:*

(i) Associativa;

(ii) Comutativa;

(iii) Existe um elemento neutro;

(iv) Todo elemento tem um simétrico;

(v) Lei do cancelamento;

(vi) Fechamento;

Proposição 3.4. *Sejam* $\frac{a}{b}, \frac{c}{d}, \frac{e}{f}$ *números racionais quaisquer, para a adição valem as seguintes propriedades:*

(i) Associativa: $\left(\frac{a}{b} + \frac{c}{d}\right) + \frac{e}{f} = \frac{a}{b} + \left(\frac{c}{d} + \frac{e}{f}\right)$

(ii) Comutativa: $\frac{a}{b} + \frac{c}{d} = \frac{c}{d} + \frac{a}{b}$

(iii) Elemento neutro: $\exists!\frac{x}{y} : \frac{x}{y} + \frac{c}{d} = \frac{c}{d}$

(iv) Simétrico: $\forall\frac{a}{b}\exists!\frac{x}{y} : \frac{a}{b} + \frac{x}{y} = \frac{0}{1}$

(v) Lei do cancelamento: $\frac{a}{b} + \frac{c}{d} = \frac{a}{b} + \frac{e}{f} \implies \frac{c}{d} = \frac{e}{f}$.

(vi) Fechamento: $\frac{a}{b} + \frac{c}{d} \in \mathbb{Q}$.

Demonstração:

(i) Associativa: $\left(\frac{a}{b} + \frac{c}{d}\right) + \frac{e}{f} = \frac{a}{b} + \left(\frac{c}{d} + \frac{e}{f}\right)$

(ii) Comutativa: $\frac{a}{b} + \frac{c}{d} = \frac{c}{d} + \frac{a}{b}$

(iii) Elemento neutro: $\exists!\frac{x}{y} : \frac{x}{y} + \frac{c}{d} = \frac{c}{d}$

(iv) Simétrico: $\forall\frac{a}{b}\exists!\frac{x}{y} : \frac{a}{b} + \frac{x}{y} = \frac{0}{1}$

(v) Lei do cancelamento: $\frac{a}{b} + \frac{c}{d} = \frac{a}{b} + \frac{e}{f} \implies \frac{c}{d} = \frac{e}{f}$.

(vi) Fechamento: $\frac{a}{b} + \frac{c}{d} \in \mathbb{Q}$.

■

3.4. Multiplicação

Definição 3.3. *Sejam* $\frac{a}{b}$ *e* $\frac{c}{d}$ *números racionais quaisquer. A multiplicação de* $\frac{a}{b}$ *por* $\frac{c}{d}$ *será denotada por* $\frac{a}{b} \cdot \frac{c}{d}$ *e é definida por* $\frac{ac}{bd}$.

Proposição 3.5. *A multiplicação em* $\mathbb{Q}$ *está bem definida.*

Proposição 3.6. *Sejam* $\frac{a}{b}, \frac{c}{d}, \frac{e}{f}$ *números racionais quaisquer, para a multiplicação valem as seguintes propriedades:*

(i) Associativa: $\left(\frac{a}{b} \cdot \frac{c}{d}\right) \cdot \frac{e}{f} = \frac{a}{b} \cdot \left(\frac{c}{d} \cdot \frac{e}{f}\right)$

(ii) Comutativa: $\frac{a}{b} \cdot \frac{c}{d} = \frac{c}{d} \cdot \frac{a}{b}$

(iii) Elemento neutro: $\exists! \frac{x}{y} : \frac{x}{y} \cdot \frac{c}{d} = \frac{c}{d}$

(iv) Simétrico: $\forall \frac{a}{b} \exists! \frac{x}{y} : \frac{a}{b} \cdot \frac{x}{y} = \frac{0}{1}$

(v) Lei do cancelamento: $\frac{a}{b} \cdot \frac{c}{d} = \frac{a}{b} \cdot \frac{e}{f} \implies \frac{c}{d} = \frac{e}{f}$.

(vi) Fechamento: $\frac{a}{b} \cdot \frac{c}{d} \in \mathbb{Q}$.

Demonstração:

(i) Associativa:
$\left(\frac{a}{b} \cdot \frac{c}{d}\right) \cdot \frac{e}{f} =$
$\left(\frac{a}{b} \cdot \frac{c}{d}\right) \frac{e}{f} =$
$\frac{ace}{bdf} = \frac{a}{b} \cdot \frac{ce}{df} =$
$\frac{a}{b} \cdot \left(\frac{c}{d} \cdot \frac{e}{f}\right)$

(ii) Comutativa:
$\frac{a}{b} \cdot \frac{c}{d} =$
$\frac{ac}{bd} =$
$\frac{ac}{db} =$
$\frac{c}{d} \cdot \frac{a}{b}$

(iii) Elemento neutro: $\exists! \frac{x}{y} : \frac{x}{y} \cdot \frac{c}{d} = \frac{c}{d}$
Consideremos o $1/1$. Afirmamos que ele é o neutro do produto, pois: $(1c/1d) = c/d$. Assim, provamos que é neutro pela esquerda. Pela direita é evidente pela comutatividade do produto em $\mathbb{Z}$. A unicidade é dada pelo teorema **??**.

(iv) Simétrico: $\forall \frac{a}{b} \exists! \frac{x}{y} : \frac{a}{b} \cdot \frac{x}{y} = \frac{0}{1}$ Consideremos o elemento $\frac{b}{a}$. Mostraremos que ele é o simétrico de $\frac{a}{b}$ pois ocorre que $\frac{a}{b} \cdot \frac{b}{a} = \frac{ab}{ba} = \frac{1}{1}$ pois $ab \cdot 1 = ba \cdot 1$.

(v) Lei do cancelamento:
$\frac{a}{b} \cdot \frac{c}{d} = \frac{a}{b} \cdot \frac{e}{f} \iff$
$\frac{b}{a} \cdot \frac{a}{b} \cdot \frac{c}{d} = \frac{b}{a} \cdot \frac{a}{b} \cdot \frac{e}{f} \implies$
$\implies \frac{c}{d} = \frac{e}{f}$.

(vi) Fechamento:
$\frac{a}{b} \cdot \frac{c}{d} \in \mathbb{Q}$, como $a, b, c, d \in \mathbb{Z}$, temos que $ac \in \mathbb{Z}$ e $bd \in \mathbb{Z}$. Além disso, por causa do anulamento do produto em $\mathbb{Z}$, temos que $bd = 0 \iff b = 0 \vee d = 0$, mas como originalmente $b, d \neq 0$, temos $bd \neq 0$.

∎

3.5. Relação de ordem

Definição 3.4. *Sejam $\frac{a}{b}$ e $\frac{c}{d}$ números racionais quaisquer. A relação de ordem $\leq$ entre $\frac{a}{b}$ e $\frac{c}{d}$ será denotada por $\frac{a}{b} \leq \frac{c}{d}$ e representa que $ad \leq bc$.*

Observação 3.2. Deve ser notado que a última desigualdade da definição, bem como seu produto são em $\mathbb{Z}$.

Proposição 3.7. *A relação de ordem está bem definida.*

Proposição 3.8. *Relação de ordem*

(i) Reflexiva:

(ii) Antissimétrica:

(iii) Transitiva:

(iv) Totalidade:

(v) Compatível com a adição:

(vi) Compatível com a multiplicação:

Demonstração: Demonst racao

(i) Reflexiva:

(ii) Antissimétrica:

(iii) Transitiva:

(iv) Totalidade:

(v) Compatível com a adição:

(vi) Compatível com a multiplicação:

$\blacksquare$

Teorema 3.2. *Imersão de* $\mathbb{Z}$ *em* $\mathbb{Q}$ *.*

Demonstração: PROVA RPD POJASPDOJPAOSDJOPZ<X $\blacksquare$

4. O CONJUNTO DOS NÚMEROS REAIS

CONSIDERAÇÕES FINAIS

É a parte final do texto. Deve retomar o problema inicial, revendo os objetivos e comentando se foram atingidos ou não, enunciando as principais contribuições. Sintetiza as principais idéias, bem como os resultados, avaliando pontos positivos e negativos. Geralmente inclui recomendações e/ou sugestões.

REFERÊNCIAS

APÊNDICE A - ÁLGEBRA BÁSICA

Definição 4.1. *Seja A um conjunto arbitrário. Uma operação $*$ sobre A é uma função que a cada $x, y \in A$ associa um elemento $x * y \in A$, ou seja, associa a cada 2 elementos em A a sua imagem $x * y$ que também é um elemento de A.*

Por essa definição, a adição em $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ e $\mathbb{R}$ são operações, sobre cada um desses conjuntos, cada um com sua adição. Por outro lado, a subtração em $\mathbb{N}$ não é uma operação em $\mathbb{N}$ pois $1 - 2 \neq\in \mathbb{N}$. Também a divisão não é uma operação em $\mathbb{N}$ e em $\mathbb{Z}$, pelo mesmo motivo.

Definição 4.2. *Seja A um conjunto e seja $*$ uma operação em A. Se existir um $e \in A$ tal que para qualquer $x \in A$ valer $e * x = x$ dizemos que e é elemento neutro à esquerda.*

Por analogia definimos neutro à direita.

Definição 4.3. *Seja A um conjunto, , e seja $*$ uma operação sobre A. Dizemos que a operação $*$ tem a propriedade:*

(i) *associativa, quando para quaisquer $x, y, z \in A$ é válido que $x * (y * z) = (x * y) * z$.*

(ii) *comutativa, quando para quaisquer $x, y \in A$ é válido que $x * y = y * x$.*

(iii) *do elemento neutro, quando existe $e \in A$, onde e é neutro à esquerda e à direita.*

(iv) *do elemento simétrico, quando para qualquer $x \in A$ existe algum $w \in A$, onde é válido que $x * w$ é o elemento neutro de $*$.*

(v) *do fechamento, quando para quaisquer $x, y \in A$ ocorre que $x * y \in A$.*

Em geral, nesse trabalho, o elemento neutro para a operação de adição é o 0 e o elemento neutro para a multiplicação é o 1.

Observação 4.1. A propriedade do fechamento na verdade é imediata da definição de operação, colocamos para realçar o fato de que a operação tem imagem em A e não qualquer elemento que não esteja em A.

Definição 4.4. *Sejam A um conjunto e sejam $+$ e $\cdot$ operações sobre A. Dizemos que a multiplicação é distributiva em relação a soma quando para quaisquer $x, y, z \in A$ é valido que $x \cdot (y + z) = x \cdot y + x \cdot z$.*

Frequentemente omitimos o símbolo da multiplicação.

Teorema 4.1. *Seja A um conjunto e $*$ uma operação em A. Se existir elemento neutro para $*$, então ele é único.*

Demonstração: Sejam $e_1 e e_2$ dois elementos neutros para $*$. Temos que $e_1 = e_1 * e_2 = e_2$, portanto $e_1 = e_2$. A primeira igualdade é porque e_2 é neutro à direita, a segunda igualdade é porque e_1 é neutro à esquerda. ∎

Em particular deve ser observada a comutatividade do elemento neutro com qualquer elemento, para uma dada operação.

Teorema 4.2. *Seja A um conjunto e $*$ uma operação em A. Se $*$ é associativa e tem a propriedade do elemento simétrico, então o simétrico de cada elemento é único.*

Demonstração: Seja $x \in A$, e seja y, z dois elementos simétricos de x, assim temos que $x*y = e = x*z$. Temos $y = y*e = y*(x*z) = (y*x)*z = (x*y)*z = e*z = z$. ∎

Definição 4.5. *Seja A um conjunto, e sejam $+, \cdot$ duas operações sobre A, chamadas de adição e multiplicação. Se são válidas as propriedades:*

(i) associativa da adição

(ii) comutativa da adição;

(iii) do elemento neutro para adição;

(iv) do elemento simétrico para a adição;

(v) associativa da multiplicação;

(vi) comutativa da multiplicação;

(vii) do elemento neutro da multiplicação;

(viii) da distributiva do produto em relação à soma;

dizemos que $(A, +, \cdot)$ é um anel. Quando não houver ambiguidade chama-se apenas de anel A.

Definição 4.6. *Um corpo é um anel A em que cada elemento diferente do zero aditivo tem um simétrico multiplicativo.*

Definição 4.7. *Par ordenado Dados um conjunto não vazio A e $a, b \in A$, definimos o* par ordenado (a, b) *como sendo o conjunto* $\{\{a\}, \{a, b\}\}$.

Observação 4.2. Essa definição de par ordenado visa formar conjuntos onde a "ordem"importa, isto é, $(a, b) = (c, d) \iff a = c \wedge b = d$.

Definição 4.8. *Produto Cartesiano Dado um conjunto A, o produto cartesiano de A por A, denotado por $A \times A$, é o conjunto de todos os pares ordenados compostos por elementos de A, isto é, $A \times A = \{(x, y) : x, y \in A\}$.*

Definição 4.9. *Relação binária Uma* relação binária R *num conjunto A é qualquer subconjunto do produto cartesiano $A \times A$, isto é, $R \subset A \times A$.*

Definição 4.10. *Uma relação R é chamada de* Relação de equivalência *quando possuir as seguintes propriedades:*

(i) reflexiva $aRa, \forall a \in A$;

(ii) simétrica $aRb \implies bRa, \forall a, b \in A$;

(iii) transitiva $aRb \wedge bRc \implies aRc, \forall a, b, c \in A$.

Definição 4.11. *Seja R uma relação de equivalência num conjunto A e seja $a \in A$ um elemento fixado arbitrariamente. O conjunto*

$$\bar{a} = \{x \in A : xRa\}$$

chama-se classe de equivalência de a pela relação R.

Teorema 4.3. *Sejam R uma relação de equivalência em um conjunto A e sejam a, b elementos quaisquer de A, então:*

1. $a \in \bar{a}$;

2. $\bar{a} = \bar{b} \iff aRb$;

3. $\bar{a} \neq \bar{b} \implies \bar{a} \cap \bar{b} = \emptyset$.

Definição 4.12. *Seja R uma relação de equivalência num conjunto A. O conjunto constituído das classes de equivalência em A pela relação R é denotado por A/R e denominado* conjunto quociente *de A por R.*
Assim, $A/R = \{\bar{a} : a \in A\}$.