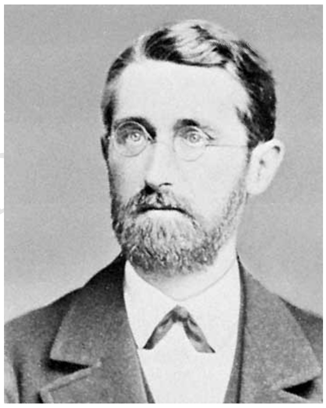
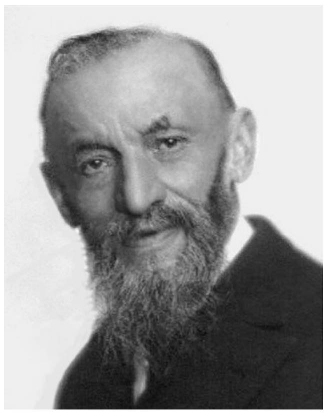
Aula 1. Números Inteiros e Principio da Boa Ordem

1.1 Fatos históricos

A noção de número real foi formalizada só em 1872 por Richard Dedekind. No seu estudo dos números reais, Dedekind apóia-se nos racionais, que, por sua vez, definem-se a partir de pares ordenados de números inteiros. Mas, afinal, o que são os números inteiros?

A noção de número natural (a partir da qual se pode explicitar a noção de inteiros) foi fundamentada com precisão pela primeira vez por Giuseppe Peano em 1889 na sua *Arithmetica Principia Nova Methodo Exposita*. O método de Peano, com leves variantes, é usado até hoje por numerosos textos, mas tem o inconveniente de ser longo e demorado. Segundo essa teoria, a definição de número natural é estabelecida a partir de três conceitos primitivos c cinco axiomas. O leitor interessado nesse ponto de vista poderá consultar o último capitulo destas notas.


Richard Dedekind (1831–1916)


Giuseppe Peano (1858–1932)

O primeiro sistema algébrico que vamos ver são os inteiros. Nesta nota, listamos os axiomas que determinam o sistema de inteiros, junto com muitas consequências simples desses axiomas. Muitas dessas consequências serão declaradas sem provas ou deixadas como exercícios; nosso principal objetivo nesta aula é pesquisar os fatos sobre os inteiros que você pode assumir com segurança em discussões posteriores.

1.2 Axiomática dos inteiros (A1–A15)

Os números inteiros formam um conjunto, que notaremos por $\mathbb{Z}$, no qual estão definidas duas operações, que chamaremos da adição e multiplicação e denotaremos por $+$ e $\cdot$. Em $\mathbb{Z}$ também está definida uma relação que permite comparar os seus elementos, a relação "menor ou igual", que indicaremos por $\leq$.

A. 1 **Propriedade Associativa:** Para toda tripla a, b, c de inteiros tem-se que

$$a + (b + c) = (a + b) + c.$$

A. 2 **Existência do Neutro:** Existe um único elemento, denominado *neutro aditivo* ou zero, que indicaremos por 0, tal que

$$a + 0 = a,$$

para todo $a \in \mathbb{Z}$.

A. 3 **Existência do Oposto:** Para cada inteiro a existe um único elemento que chamaremos *oposto* de a e indicaremos por $-a$, tal que

$$a + (-a) = 0.$$

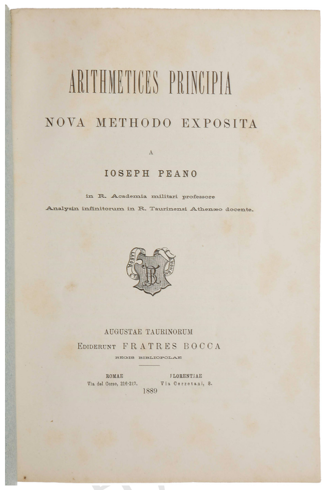
A. 4 **Propriedade Comutativa:** Para todo par a, b de inteiros tem-se que

$$a + b = b + a.$$

O próximo grupo de axiomas explicita algumas das propriedades da multiplicação.

A. 5 **Propriedade Associativa:** Para toda tripla a, b, c de inteiros tem-se que

$$a(bc) = (ab)c.$$



Arithmetices Principia, 1889

A. 6 **Existência do Neutro:** Existe um único elemento, diferente de zero, denominado *neutro multiplicativo*, que indicaremos por 1, tal que

$$1 \cdot a = a,$$

para todo $a \in \mathbb{Z}$.

A. 7 **Propriedade Cancelativa:** Para toda terna a, b, c de inteiros, com $a \neq 0$, tem-se que, se $ab = ac$, então, $b = c$.

A. 8 **Propriedade Comutativa:** Para todo par a, b de inteiros, tem-se que

$$ab = ba.$$

Agora, anunciaremos os axiomas referentes à relaço "menor ou igual" $\leq$.

A. 9 **Propriedade Reflexiva:** Para todo inteiro a tem-se que $a \leq a$.

A. 10 **Propriedade Anti-simétrica:** Dados dois inteiros t e b, se $a \leq b$ e $b \leq a$, então $a = b$

A. 11 **Propriedade Transitiva:** Para toda terna a, b, c de inteiros tem-se que, se $a \leq b$ e $b \leq c$, então $a \leq c$.

Por causa dos axiomas A.10, A.11 e A.12 temos que a relação $\leq$ é uma *relação de ordem*. Usaremos o símbolo $a < b$ para indicar que $a \leq b$, mas $a \neq b$ nesse caso, diremos que a é menor que b. No que segue, usaremos os termos "positivo" e "negativo" no seu sentido usual, isto é, para indicar que um certo número é maior ou menor que zero, respectivamente. Quando conveniente, usaremos também os sim bolos $b \geq a$ ou $b > a$ para indicar que $a \leq b$ ou $a < b$.

A. 12 **Tricotomia:** Dados dois inteiros quaisquer a, b, c tem-se que ou $a < b$ ou $a = b$ ou $b < a$.

As operações de multiplicação e soma são ligados entre-si pelo seguinte axioma chamado distribuição da some e produto.

A. 13 **Distribuição:** Para toda tripla a, b, c de inteiros, tem-se que

$$a(b + c) = ab + ac.$$

Agora, temos alguns axiomas que relacionam a ordem e operações em $\mathbb{Z}$.

A. 14 Para toda terna a, b, c de inteiros, se $a \leq b$, então $a + c \leq b + c$.

A. 15 Para toda terna a, b, c de inteiros, se $a \leq b$ e $0 \leq c$, então $ac \leq bc$.

1.3 *Propriedades*

Nessa seção vemos como provas certas propriedades naturais dos inteiros usando os axiomas acima. Primeiramente, observamos que a propriedade cancelativa vale também para adição. s

Proposição 1.1: (Propriedade cancelativa da adição)

Para toda tripla a, b, c de inteiros tem-se que, se $a + b = a + c$, então $b = c$.

Prova

Se $a + b = a + c$, somando o oposto de a ambos os lados dessa igualdade, temos que

$$(-a) + (a + b) = (-a) + (a + c).$$

Usando a propriedade associativa (A.1), temos:

$$[(-a) + (a)] + b = [(-a) + (a)] + c$$

isto é (usando A.3 – A.4),

$$0 + b = 0 + c$$

portanto (usando A.2),

$$b = c.$$

Proposição 1.2

Para todo inteiro a, tem-se que

$$a \cdot 0 = 0.$$

Prova

Como $a \cdot 0 + a \cdot 0 = a(0+0) = a \cdot 0 = a \cdot 0 + 0$, comparando o primeiro e o último termo da cadeia de igualdades acima temos que

$$a \cdot 0 + a \cdot 0 = a \cdot 0 + 0$$

Usando a propriedade cancelativa da adição (Proposição 1.1), vem imediatamente que

$$a \cdot 0 = 0.$$

Exercício 1.1: (Trabalho p/ casa)

Sejam a, b inteiros, tais que $a \cdot b = 0$.
Mostre que $a = 0$ ou $b = 0$.

Proposição 1.3: (Regra dos sinais)

Sejam a e b inteiros. Então vale:

(i) $-(-a) = a$

(ii) $(-a)(b) = -(ab) = a(-b)$

(iii) $(-a)(-b) = ab$.

Prova

Notamos inicialmente que podemos interpretar o axioma A.3 da seguinte forma: *o oposto de um elemento a é o único inteiro que verifica a equação $a + x = 0$.*

Para provar (i) basta observar que a verifica a equação $(-a) + x = 0$. Consequentemente, a é o oposto de $-a$ (que é o elemento indicado por $-(-a)$).

Para provar a primeira igualdade de (ii), basta observar que $(-a)b$ é a solução de $ab + x = 0$, já que

$$ab + (-a)b = \{(-a) + a]b = 0 \cdot b = 0.$$

Analogamente, verifique que

$$ab + a(-b) = 0.$$

Para (iii), podemos observar diretamente que aplicando (ii) temos

$$(-a) \cdot (-b) = -(a(-b)) = -(-(ab))$$

e usando também (i) no último termo segue que

$$(-a)(-b) = ab.$$

Exercício 1.2: (Trabalho p/ casa)

Seja a um inteiro. Então:

(i) Se $a \leq 0$, então $-a \geq 0$.

(ii) Se $a \geq 0$, então $-a \leq 0$.

(iii) $a^2 \geq 0$.

(iv) $1 > 0$.

1.4 *Principio da Boa Ordem (Axioma A.16)*

Um elemento $a_0 \in A$ diz-se *elemento mínimo* de A se, para todo $a \in A$, tem-se que $a_0 \leq a$ (verifique que, se existe um elemento mínimo de A, ele é único).

Usaremos os símbolos $\min A$ e $\max A$ para indicar o mínimo e o máximo de um conjunto A, quando existiram.

A. 16 **Princípio da Boa Ordem (PBO):**

Todo conjunto não-vazio de inteiros não-negativos contém um elemento mínimo.

Note que, como consequência dos axiomas A.14 e A.15, podemos provar que $0 < 1$. Porém, ainda não conseguimos demonstrar o fato obvio de que não existem inteiros ente 0 e 1. Esse é o conteúdo da próxima proposição.

Proposição 1.4

Seja a um inteiro tal que $0 \leq a \leq 1$. Então $a = 0$ ou $a = 1$.

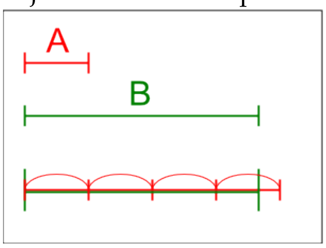
Prova

Suponhamos por absurdo que existe um inteiro a diferente de 0 e l nessas condições. Assim, o conjunto $S = \{a \in \mathbb{Z} \mid 0 < a < 1\}$ seria não-vazio e pelo Principio da Boa Ordem existe $m = \min S$.

Como $m \in S$ temos que $m > 0$ e $m < 1$. Usando o axioma A.15, multiplicando por m a segunda desigualdade obtemos $m^2 < m$. Contradição.

Proposição 1.5: (Propriedade Arquimediana)

Sejam a e b inteiros positivos. Então, existe um inteiro positivo n tal que $na > b$.



Prova

Suponhamos que a afirmação não seja verdadeira. Isso significa que, para tolo inteiro positive n o conjunto

$$S = \{b - na \mid n \in \mathbb{Z}, n > 0\}$$

ésta formado por inteiros não-negativos. Conforme o Princípio da Boa Ordem, existe $m = \min S$. Como $m \in S$, ele é da forma $m = b - ra$ para algum $r \in \mathbb{Z}$.
Consideramos então o elemento $m' = b - (r+1)a$, que também pertence a S, obtemos

$$m' = b - (r+1)a = b - ra - a = m - a < m.$$

Teríamos, então, que $m' \in S$ e $m' < m = \min S$, uma contradição.

Exercício 1.3: Trabalho p/casa

Sejam a, b, c, d inteiros, provar que

(i) Se $a \geq b$ e $c \geq 0$, então $ac \geq bc$.

(ii) Se $c > 0$ e $ac < bc$, então $a < b$.

(iii) Se $c < 0$ e $ac > bc$, então $a < b$.

(iv) $a^2 - ab + b^2 \geq 0$.