Notas de Aula - Fundamentos de matemática

Leandro F. Aurichi

A ideia deste texto não é focar em determinados conteúdos, mas sim numa forma de pensar e organizar para se tratar de problemas matemáticos. Tente encarar o texto apenas como um ponto inicial: não fique apenas com o que for apresentado aqui. Algumas sugestões: [1]

- Não leia passivamente. Papel e lápis são seus amigos;
- Tente explicar a colegas o conteúdo aqui apresentado. Procure ajuda de colegas quando algo não for claro;
- Leia as soluções apresentadas uma vez. Numa segunda, tente resolver por conta própria. Não conseguiu? Leia um pouco (mas só um pouco) e volte a tentar. Repita;
- Viu um problema e já sabe resolver? Pense em formulações alternativas. E se as condições fossem um pouco diferentes? Saberia resolver um caso mais geral?
- Tente se divertir.

[1] Obviamente, essas sugestões não funcionam para todo mundo. Dê uma chance a cada uma, veja as que parecem melhores para você - acrescente outras.

Aula 1

Um primeiro problema

Slide 2

Numa[2] república, moram 11 pessoas e só há uma geladeira. Os moradores da república resolvem criar um método para a utilização da geladeira e, usando uma corrente e diversos cadeados, querem que ocorram duas coisas:

- A geladeira só pode ser aberta quando houver pelo menos metade do moradores na casa;
- Qualquer grupo de moradores que tenha pelo menos metade dos moradores, precisa conseguir abrir a geladeira.

Desta forma, quantos cadeados e quantas chaves são necessários no mínimo para satisfazer essas duas condições?

Um caso simples

Slide 3

Antes de atacarmos o problema propriamente dito, vamos ver alguns casos mais simples:

Quantos cadeados e quantas chaves (no mínimo) precisaríamos ter se quiséssemos que qualquer morador da república pudesse abrir a geladeira?

Basta 1 cadeado e 11 chaves dele (uma cópia para cada morador).

Outro caso simples

Slide 4

Quantos cadeados e quantas chaves (no mínimo) precisaríamos ter se quiséssemos que a geladeira só fosse aberta quando todos os moradores estivessem presentes?

11 cadeados e 11 chaves (uma chave para cada cadeado, dando uma para cada morador).

Nosso problema original é bem mais complicado que esses dois casos simples. Para resolvê-lo, precisamos de algumas ideias. Várias destas ideias serão usadas no futuro, em outros problemas. Assim, vamos dar um passo de lado no nosso problema atual, mas já vamos construir maquinário que vai nos ajudar no futuro também.

Funções

Slide 5

Primeiramente, considere um grupo com 5 pessoas. Note que 6 pessoas é o menor grupo com mais da metade do total de moradores[3], logo um grupo com 5 não pode conseguir abrir a geladeira. Para que isso aconteça, precisa existir pelo menos um cadeado que esse grupo não consiga abrir. Assim, para cada grupo de 5 pessoas, precisa existir pelo menos um cadeado que esse grupo não abra.

Criando uma função

Slide 6

Temos aqui uma associação entre diferentes conjuntos: para cada grupo de 5 pessoas, fixe um cadeado que tal grupo não consegue abrir. Essa associação vai ser bastante importante, então precisamos deixá-la clara[4]. Uma associação, em matemática, nada mais é que uma função, que denotamos da seguinte maneira:

$$f : A \to B$$

Isso quer dizer que a função f associa a cada elemento de A um elemento de B (em símbolos, f associa um elemento a com $f(a)$).

Slide 7

Neste caso, chamamos A de **domínio** de f

$$\mathrm{dom}(f)$$

e B de **contradomínio** de f. O subconjunto de B formado pelos elementos que foram "atingidos" por f é chamado de **imagem** de f

$$\mathrm{Im}(f).$$

Isto[5] é, são todos os elementos de B que são da forma $f(a)$ para algum elemento a de A.
Em símbolos

$$\mathrm{Im}(f) = \{f(a) : a \in A\}.$$

Voltando ao problema

Slide 8

No nosso problema, vamos considerar uma função

$$c : G \to C$$

onde G é o conjunto de todos os grupos de 5 moradores e C é o conjunto dos cadeados. Essa associação será da seguinte forma: dado um grupo g, o cadeado $c(g)$ é um cadeado que o grupo g não consegue abrir[6].

Vejamos o que a gente consegue falar sobre essa função. Note que a gente fez uma associação abstrata. Sabemos que a cada grupo, existe um cadeado associado tal que o grupo não consegue abri-lo. Nem sabemos se existem outros cadeados nessa mesma situação. Mesmo com essa falta de informação, já podemos concluir algumas coisas.

Cadeados diferentes

Slide 9

Considere dois grupos diferentes, g_1 e g_2. Será que estes dois grupos podem estar associados ao mesmo cadeado? Colocando em símbolos, pode acontecer $g_1 \neq g_2$ e $c(g_1) = c(g_2)$? Essa é uma propriedade bastante importante sobre funções e que nos será bastante útil neste problema.

Dizemos que uma função $f : A \to B$ é **injetora** se, dados $a \neq b$, temos que $f(a) \neq f(b)$[7].

Slide 10

[2] Você pode dar uma olhada no artigo "Os problemas da geladeira e dos táxis" na revista Acta Legalicus.

[3] Sim, o mais certo seria $5,5$, mas isso implicaria serrar alguém ao meio...

[4] Usaremos ao longo do texto diversas notações. A ideia não é deixar as coisas complicadas, mas sim mais fáceis - o problema é que você precisa se acostumar com elas para aproveitar...

[5] Note que nem todo elemento de B precisa pertencer a $\mathrm{Im}(f)$. Quando temos que $\mathrm{Im}(f) = B$, dizemos que f é **sobrejetora**.

[6] Aqui convém dizer que pode existir mais de um cadeado que o grupo g não consegue abrir - mas isso não é um problema, escolhemos um só para fazer a associação.

[7] A ideia é "coisas diferentes vão para lugares diferentes".

Ou seja, estamos nos perguntando se c é injetora ou não. Sabemos que $c(g_1)$ é um cadeado que g_1 não consegue abrir. Também sabemos que $c(g_2)$ é um cadeado que g_2 não consegue abrir. Mas, como $g_1 \neq g_2$, sabemos que há pelo menos uma pessoa em g_2 que não está em g_1[8]. Juntando essa pessoa ao grupo g_1, temos um grupo de 6 pessoas. Assim, tal grupo precisa conseguir abrir a geladeira. Desta forma, se $c(g_1) = c(g_2)$, o cadeado que o grupo g_1 não abre, também não seria aberto pela sexta pessoa acrescentada ao grupo (pois ela não abre $c(g_2)$, que é o mesmo cadeado $c(g_1)$). Desta forma, os cadeados precisam ser diferentes. Ou seja, o argumento acima mostra que c é uma função injetora.

Mais uma informação

Slide 11

Com isso, já temos uma importante informação sobre o conjunto imagem da função c: ele tem a mesma quantidade de elementos que o conjunto G (o conjunto de todos os grupos de 5 pessoas). Ou seja, a solução para o nosso problema requer uma quantidade de cadeados igual ou maior que a quantidade de grupos de 5 moradores da república. Essa quantidade até poderia ser maior, pois ainda não sabemos se a tal associação fez aparecer todos os cadeados da solução.

Chaves

Slide 12

Vamos agora tentar examinar quantidade de cópias de chaves que precisamos para fazer a solução. Imagine que você é um dos moradores da república e que só você esteja nela. Agora suponha que chegou um grupo g de 5 moradores. Sabemos que o grupo não consegue abrir o cadeado $c(g)$. Mas também sabemos que g junto com você forma um grupo de 6 pessoas. Logo, vocês conseguem abrir a geladeira.

Slide 13

Assim, concluimos que você tinha uma cópia da chave do cadeado $c(g)$. Mas se entrasse outro grupo, digamos h, pelo mesmo argumento, você teria que ter uma cópia da chave de $c(h)$. E já sabemos que, se $g \neq h$, então $c(g) \neq c(h)$. Ou seja, para cada grupo de 5 moradores (excluindo você), você precisa de uma chave diferente. E o análogo vale para qualquer outro morador da casa.

Resumindo, a quantidade de chaves que cada pessoa da casa precisa carregar é, pelo menos, a quantidade de grupos de 5 outras pessoas da república.

Juntando tudo para resolver o problema

Slide 14

Já sabemos que, para resolver o problema, vamos precisar de pelo menos um cadeado para cada grupo de 5 moradores. Também sabemos que cada pessoa vai ter que carregar uma chave para cada grupo de outros 5 moradores (excluindo ela).

Note que ainda não sabemos se uma solução com tais quantidades é possível. Só sabemos, pela discussão acima, que uma solução vai ter que ter pelo menos tais quantidades. Ou seja, poderia ser que as quantidades mínimas fossem ainda maiores.

É uma situação possível

Slide 15

Vamos mostrar que existe uma solução com tais quantidades. Portanto, essa seria a melhor solução possível[9].

[8] Cuidado aqui: pode parecer que juntando os grupos g_1 e g_2 teríamos 10 pessoas. Mas pode haver pessoas em comum nos dois grupos. Assim, juntando os dois grupos temos pelos menos 6 pessoas e, no máximo, 10 pessoas.

[9] É a melhor possível sob um ponto de vista. Comprar outra geladeira seria provavelmente melhor.

Para cada grupo de 5 pessoas, compre um cadeado. No cadeado, escreva o nome das 6 pessoas que não estão no tal grupo deste cadeado. Para cada uma dessas pessoas cujo nome está no cadeado, dê uma cópia da chave deste cadeado.

Primeiro, note que as quantidades batem: o número de cadeados é o mesmo da quantidade de grupos de 5 pessoas. Note também que cada pessoa tem o nome (e portanto a chave) de cada cadeado em cujo grupo ela não está.

Slide 16

Vejamos que isso é de fato uma solução. Suponha que cheguem 6 moradores na casa. Para cada cadeado, ele só não tem o nome de 5 pessoas. Logo, uma das pessoas do grupo tem o nome escrito nele e, portanto, tal pessoa tem a chave do cadeado. Isso vale para todos os cadeados, logo o grupo consegue abrir a geladeira. Falta ver que grupos com menos de 6 pessoas não conseguem abrir. Se um grupo tiver 5 ou menos pessoas, vai haver um cadeado sem o nome de todos os integrantes do grupo. Logo, tal cadeado não vai poder ser aberto.

Colocando os números

Slide 17

Falta ver quais são as quantidades exatas. Para isso, vamos usar algumas fórmulas de contagem. Essas fórmulas serão apresentadas formalmente mais adiante. Por equanto, vamos só aplicá-las aqui sem maiores discussões.

Slide 18

Para o número de cadeados, precisamos da quantidade de combinações de 11 5 a 5:

$$\binom{11}{5} = \frac{11!}{5!6!} = \frac{11 \cdot 10 \cdot 9 \cdot 8 \cdot 7}{5 \cdot 4 \cdot 3 \cdot 2} = 462$$

Slide 19

Já para as chaves, para cada morador é necessária a quantidade de combinações de 10 5 a 5:

$$\binom{10}{5} = \frac{10!}{5!5!} = \frac{10 \cdot 9 \cdot 8 \cdot 7 \cdot 6}{5 \cdot 4 \cdot 3 \cdot 2} = 252$$

Assim, somando as chaves de todos os moradores, temos um total de 2772 chaves.

Alongamentos da Aula 1

Alongamento 1.1. Se juntamos dois grupos diferentes de até 5 pessoas cada, qual o menor grupo possível? E o maior? (em número de pessoas)

Alongamento 1.2. Exiba uma função bijetora $f : C \to S$, onde C é o conjunto de todos os grupos de 5 pessoas da república e S é o conjunto de todos os grupos de 6 pessoas da mesma república.

Exercícios da Aula 1

Exercício 1.1. Na solução apresentada, é verdade que as chaves que uma pessoa fixada carrega são todas diferentes? (note que se tivesse alguma repetida, poderíamos diminuir o total de chaves)

Exercício 1.2. Na solução apresentada, quantas cópias de cada chave existem? Quantas chaves diferentes existem?

Aula 2

Conjuntos

Slide 20

Vamos ver um pouco sobre conjunto (mas só um pouco, por enquanto).
Vimos no problema da geladeira que muitas vezes conjuntos são importantes (lá os conjuntos com 5 moradores foram fundamentais na resolução). Nesta seção vamos praticar algumas operações com conjuntos, que serão importantes nos problemas futuros.

Primeiro, vamos fixar algumas notações. Um conjunto, informalmente, é uma coleção de coisas. Vamos tentar dar uma explicação melhor no final deste curso - mas, por enquanto, vamos ficar com essa versão ingênua mesmo. Se temos um conjunto A e um elemento a deste conjunto, denotamos esta relação por

$$a \in A.$$

Lê-se a pertence a A. Para um exemplo, temos que $1 \in \mathbb{N}$, onde $\mathbb{N}$ é o conjunto dos números naturais

$$\mathbb{N} = \{0, 1, 2, 3, ...\}.$$

Inclusão

Slide 21

Podemos ter um subconjunto de um conjunto. No sentido que todos os elementos do primeiro também são elementos do segundo. Essa relação é denotada por

$$A \subset B$$

Lê-se A está contido em B. Como exemplo, temos que $\mathbb{N} \subset \mathbb{R}$, onde $\mathbb{R}$ é o conjunto dos números reais. Afinal, todo número natural é também um número real.

Algumas propriedades sobre a inclusão

Slide 22

Proposição 2.1. *Sejam A, B, C conjuntos. Valem as seguintes propriedades*[10]*:*

- $A \subset A$*;*
- *Se $A \subset B$ e $B \subset C$, então $A \subset C$;*
- *Se $A \subset B$ e $B \subset A$, então $A = B$.*

Slide 23

Demonstração.

- $A \subset A$:[11]

  Teríamos só que verificar que todo elemento de A é um elemento de A. Mas isso é imediato (certo?).

Slide 24

- Se $A \subset B$ e $B \subset C$, então $A \subset C$:

  Agora temos que verificar que todo elemento de A é também um elemento de C. Isso fica mais fácil se fixarmos um elemento de A de começo. Considere $a \in A$. Como $A \subset B$, obtemos que $a \in B$. Por sua vez, sabemos que $B \subset C$. Assim, $a \in C$, como queríamos.

Slide 25

- Se $A \subset B$ e $B \subset A$, então $A = B$:

  O grande truque aqui é: dois conjuntos são o mesmo conjunto se eles tem os mesmos elementos. Daí agora ficou simples: $A \subset B$ quer dizer que todos os elementos de A estão em B. Por sua vez, todos os elementos de B estão em A (pois também temos que $B \subset A$). □

Subconjuntos especiais

Slide 26

Quando temos um conjunto A, podemos querer tomar um subconjunto B dele, formado só com os elementos que satisfaçam uma determinada propriedade P. Adotamos a seguinte notação para isso:

$$B = \{a \in A : P(a)\}.$$

Um exemplo deixa isso mais claro. Imagine que queremos o conjunto P dos números pares. Podemos fazer isso a partir do conjunto dos números naturais:

$$P = \{n \in \mathbb{N} : n \text{ é par}\}.$$

Repare que sempre que fizermos algo do tipo temos uma inclusão automática. No caso deste último exemplo, $P \subset \mathbb{N}$.

União

Slide 27

Podemos "juntar" dois conjuntos. Se A e B são dois conjuntos, podemos criar um novo conjunto que contém todos os elementos de A e de B. Chamamos tal conjunto de **união** de A e B e denotamos por $A \cup B$.

Por exemplo, considere P o conjunto do números pares e I o conjunto dos números ímpares. Note que $\mathbb{N} = P \cup I$[12].

Intersecção

Slide 28

Também podemos criar a partir de conjuntos A e B um conjunto que tem todos os elementos em comum entre A e B. Chamamos tal conjunto de **intersecção** entre A e B e denotamos por $A \cap B$.

Por exemplo, considere P o conjunto dos números pares e T o conjunto dos números múltiplos de 3 (isto é, $T = \{0, 3, 6, 9, 12, ...\}$). Temos

$$P \cap T = \{0, 6, 12, 18, ...\}.$$

Por outro lado, se tomarmos P (conjunto dos pares) e I (conjunto dos ímpares), temos que $P \cap I$ não tem qualquer elemento, já que P e I não tem elementos em comum. Ao conjunto que não tem elementos damos o nome de **conjunto vazio** e denotamos por $\emptyset$. Assim, $P \cap I = \emptyset$.

[10] Essas propriedades podem parecer bem bobinhas. Mas serão bastante úteis no futuro. Principalmente a última.
[11] A maior dificuldade dessa demonstração é que tudo parece óbvio demais. Mas vamos com um pouco de calma.
[12] Basicamente porque todo número natural é par ou ímpar.

Vacuidade

Slide 29

Aqui há algo que causa estranhamento: $\emptyset \subset A$, para qualquer conjunto A. Para tentar aceitar isso[13], pense da seguinte forma: para que não fosse verdade que $\emptyset \subset A$, deveria existir algum elemento em $\emptyset$ que não estivesse em A.

Uma igualdade

Slide 30

Vamos apresentar uma igualdade bastante útil (há várias parecidas no Alongamento 2.1).
Proposição 2.2. *Sejam A, B e C conjuntos. Então vale a seguinte igualdade:*

$$(A \cup B) \cap (A \cup C) = A \cup (B \cap C).$$

Slide 31

Demonstração. Essa demonstração[14] fica muito mais fácil se tentarmos mostrá-la em dois pedaços. Primeiro, vamos mostrar que o conjunto da esquerda é subconjunto do da direita. Depois fazemos o contrário e, portanto, teremos a igualdade.

Slide 32

- $\subset$: Seja $x \in (A \cup B) \cap (A \cup C)$. Vamos dividir em dois casos. Primeiro, vamos fazer o caso em que $x \in A$. Neste caso é imediato que $x \in A \cup (B \cap C)$. Agora suponha que $x \notin A$. Então, como $x \in A \cup B$, $x \in B$. Analogamente, como $x \in A \cup C$, temos que $x \in C$. Ou seja, $x \in B \cap C$. Logo, temos o que queríamos.

Slide 33

- $\supset$: Seja $x \in A \cup (B \cap C)$. Novamente, fazemos dois casos. Se $x \in A$, então claramente $x \in (A \cup B) \cap (A \cup C)$. Por outro lado, se $x \notin A$, então $x \in B \cap C$. Neste caso, novamente temos que $x \in A \cup B$ e $x \in A \cup C$ como queríamos.

□

Conjuntos de conjuntos

Slide 34

Não há problema em um conjunto pertencer a outro. Na verdade, no exemplo da geladeira, fizemos exatamente isso: tínhamos um conjunto que cada elemento era um conjunto de 5 moradores. Podemos então ter um conjunto

$$A = \{1, 2, 4\}$$

e depois ter um outro conjunto que contém A como elemento:

$$B = \{7, 9, A\}.$$

Um outro jeito de representar B seria não usando a notação de A:

$$B = \{7, 9, \{1, 2, 4\}\}.$$

Que é muito diferente de

$$\{7, 9, 1, 2, 4\}.$$

Slide 35

Note, por exemplo, que o conjunto $\{7, 9, \{1, 2, 4\}\}$ tem 3 elementos, enquanto que o conjunto $\{7, 9, 1, 2, 4\}$ tem 5.

Se você estiver com dúvidas com relação a isso, tente se convencer primeiramente que 2 não é um elemento de $\{7, 9, \{1, 2, 4\}\}$.

Conjunto das partes

Slide 36

Dado um conjunto A, existe um conjunto especial, chamado de **conjunto das partes** de A, denotado por $\wp(A)$ que nada mais é que o conjunto de todos os subconjuntos de A.

Por exemplo, considere $A = \{a, b, c\}$. Assim

$$\wp(A) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}.$$

Observe que, não importa quem seja o conjunto A, sempre teremos que $\emptyset \in \wp(A)$ e também que $A \in \wp(A)$.

Mais estranhezas

Slide 37

Uma coisa estranha aqui é a seguinte: quem é $\wp(\emptyset)$? O jeito mais fácil é ir colocando um elemento por vez. Pelo comentário acima, sabemos que $\emptyset \in \wp(\emptyset)$, pois $\emptyset \in \wp(A)$ não importa o A. Mas quem mais? Pela continuação do comentário, também temos que $\emptyset \in \wp(\emptyset)$ (pois $A \in \wp(A)$ não importa o A). Mas isso a gente já sabia. Tem mais algum subconjunto de $\emptyset$? A resposta, depois de pensarmos um pouco, é não. Ou seja

$$\wp(\emptyset) = \{\emptyset\}.$$

Um erro comum aqui é achar que $\emptyset = \{\emptyset\}$. Mas tem um argumento simples para ver que tais conjuntos são diferentes. Por exemplo, $\emptyset$ tem 0 elementos, enquanto que $\{\emptyset\}$ tem um elemento (chamamos um conjunto com um único elemento de **conjunto unitário**) que é o próprio conjunto $\emptyset$.

Uniões e intersecções múltiplas

Slide 38

Podemos fazer uniões de infinitos conjuntos de uma vez. Por exemplo, se para cada $n \in \mathbb{N}$ temos um conjunto A_n, denotamos por $\bigcup_{n\in\mathbb{N}} A_n$ o conjunto com todos os elementos que pertençam a algum dos A_n's.

Analogamente, denotamos por $\bigcap_{n\in\mathbb{N}} A_n$ o conjunto que contém todos os elementos que pertençam a todos os A_n's.

Slide 39

Essa notação também serve para finitos conjuntos. Por exemplo, se A_1, A_2 e A_3 são conjuntos[15], podemos usar a notação

$$\bigcup_{n=1}^{3} A_n$$

em vez de $A_1 \cup A_2 \cup A_3$. O análogo serve para a intersecção.

[13] Digamos que isso vale por absoluta falta de testemunhas do contrário.

[14] Lembra que falamos que $X \subset Y$ e $Y \subset X$ implica $X = Y$ era importante?

[15] Mais ou menos como fazemos com somatórias.

Um pequeno resultado

Slide 40

Como exemplo, vamos provar um resultado para ver essa notação em uso:

Proposição 2.3. *Seja I um conjunto de índices. Para cada $i \in I$, considere A_i um conjunto. Se existe um conjunto X tal que cada $A_i \subset X$, então $\bigcup_{i\in I} A_i \subset X$.*

Demonstração. Precisamos tomar um elemento de $\bigcup_{i\in I} A_i$ e mostrar que ele pertence a X.

Seja $x \in \bigcup_{i\in I} A_i$. Isso quer dizer que existem um $i \in I$ tal que $x \in A_i$. Mas, por hipótese, temos que $A_i \subset X$. Assim, $x \in X$, como queríamos. □

Um exemplo de união infinita

Slide 41

Exemplo 2.4. Para cada $n \in \mathbb{N}$, considere $A_n = \{0, 1, ..., n\}$. Então $\bigcup_{n\in\mathbb{N}} A_n = \mathbb{N}$. Note que já temos que $\bigcup_{n\in\mathbb{N}} A_n \subset \mathbb{N}$. Assim, só precisamos mostrar que $\mathbb{N} \subset \bigcup_{n\in\mathbb{N}} A_n$. De fato, seja $n \in \mathbb{N}$. Note que $n \in A_n$ (pois $A_n = \{0, 1, ..., n\}$). Assim, $n \in \bigcup_{n\in\mathbb{N}} A_n$.

Diferença entre conjuntos

Slide 42

Dados A e B conjuntos, muitas vezes é útil o conjunto formado pelos elementos que estão em A mas não estão em B. Ou seja, o seguinte conjunto[16]:

$$A \setminus B = \{a \in A : a \notin B\}$$

Uma coisa "estranha" aqui é que B não precisa estar contido em A (veja o Alongamento 2.3.).

Intervalos

Slide 43

Um tipo de conjunto bastante importante é o **intervalo** de números reais. Formalmente, um subconjunto A dos reais é um intervalo se, dados $a, b \in A$ tais que $a < b$, se $c \in \mathbb{R}$ é tal que $a < c < b$, então $c \in A$. Isso quer dizer o seguinte: se um número c estrá entre dois números do intervalo, então c também está no intervalo. As notações para intervalos são as usuais:

$$[a, b] = \{x \in \mathbb{R} : a \leq x \leq b\}$$

$$[a, b[= \{x \in \mathbb{R} : a \leq x < b\}$$

$$[a, \infty[= \{x \in \mathbb{R} : a \leq x\}.$$

Slide 44

Note que o último exemplo pode parecer estranho ser um intervalo segundo a nossa definição. Mas cuidado aqui: a nossa definição de intervalo não é a de um conjunto em que todos o elementos estão entre dois números fixados. Para deixar isso mais claro, vejamos que $[1, +\infty[$ é de fato um intervalo (segundo a nossa definição). Ou seja, precisamos tomar $a, b \in [1, +\infty[$ e $c \in \mathbb{R}$ de forma que $a < c < b$ e provar que $c \in [1, +\infty[$. Note que, como $a \in [1, +\infty[$, temos que $1 \leq a$. Como $a < c$, temos que $1 < c$. Ou seja, $c \in [1, +\infty[$.[17]

[16] Lê-se A menos B.

[17] Sim, nem usamos o b aqui.

Nem tudo é intervalo

Slide 45

O seguinte conjunto não é um intervalo:

$$A = \{x \in \mathbb{R} : x \neq 0\}.$$

Um motivo para que ele não seja um intervalo: note que $-1, 1 \in A$. Note também que $-1 < 0 < 1$. Mas, $0 \notin A$. Ou seja, 0 está entre dois elementos de A mas não está em A.

Uniões e intersecções

Slide 46

Observe que a união de dois dois intervalos não necessariamente é um intervalo (ver o Alongamento 2.4). Por outro lado, com a intersecção a resposta é sempre um intervalo:

Proposição 2.5. *Sejam I e J intervalos. Então $I \cap J$ também é um intervalo.*

Demonstração. Sejam $a, b \in I \cap J$ tais que $a < b$. Seja c tal que $a < c < b$. Temos que mostrar que $c \in I \cap J$. Mas, como $a, b \in I \cap J$, então $a, b \in I$. Logo, como I é intervalo, $c \in I$. Analogamente, $c \in J$. Ou seja, $c \in I \cap J$. □

Slide 47

Na verdade, de forma análoga, se prova que a intersecção qualquer de intervalos (não só de dois) é sempre um intervalo (veja o Exercício 2.3).

Mais um fato estranho: tanto o vazio, como os conjuntos unitários são intervalos. Talvez o mais fácil seja pensar qual seria o motivo para eles não serem (teria que existir a, b, c etc.). Outro motivo é ver o que acabamos de provar e notar que:

- $\emptyset = [1, 2] \cap [3, 4]$;
- $\{1\} = [0, 1] \cap [1, 2]$.

Alongamentos da Aula 2

Alongamento 2.1. Verifique as seguintes afirmações para conjuntos A, B e C dados:

(a) $A \setminus B \subset A$;

(b) $(A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B)$;

(c) $(A \setminus B) \cap B = \emptyset$;

(d) $(A \cap B) \cup (A \cap C) = A \cap (B \cup C)$;

(e) $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$.

Alongamento 2.2. Considere $A = \{1, 2, 4\}$, $B = \{7, A\}$ e $C = \{1, 7, A, B\}$.

(a) $2 \in B$?

(b) Quantos elementos tem B?

(c) Quantos elementos tem C?

Alongamento 2.3. Sejam A, B conjuntos. Mostre que $A \setminus B = A \setminus (A \cap B)$.

Alongamento 2.4. Dê um exemplo de intervalos I e J de forma que:

(a) $I \cup J$ seja um intervalo;

(b) $I \cup J$ não seja um intervalo;

(c) $I \setminus J$ não é um intervalo;

(d) $I \setminus J$ é um intervalo;

Exercícios da Aula 2

Exercício 2.1. Seja A um conjunto. Determine $\bigcup_{B\in\wp(A)} B$.

Exercício 2.2. Determine:

(a) $\bigcup_{x\in\mathbb{R}}\{x\}$.

(b) $\bigcup_{n\in\mathbb{N}}[0,n[$.

(c) $\bigcup_{n\in\mathbb{N}}]\frac{1}{n},+\infty[$.

(d) $\bigcap_{x\in\mathbb{R}}\{x\}$

(e) $\bigcap_{n\in\mathbb{N}}[n,+\infty[$.

Exercício 2.3. Mostre que se cada I_a para $a\in A$ é um intervalo, então $\bigcap_{a\in A} I_a$ é um intervalo.

Exercício 2.4. Mostre que, dados dois intervalos I, J, se $I\cap J\neq\emptyset$, então $I\cup J$ é um intervalo.

Exercício 2.5. Para cada $n\in\mathbb{N}$, considere $A_n\subset\mathbb{R}$.

(a) Se algum $n\in\mathbb{N}$ é tal que $A_n=\emptyset$, mostre que $\bigcap_{n\in\mathbb{N}} A_n=\emptyset$.

(b) Vale a volta do item anterior? Isto é, se $\bigcap_{n\in\mathbb{N}} A_n=\emptyset$, é verdade que necessariamente para algum n, $A_n=\emptyset$?

Aula 3

Indução

Slide 48

Uma maneira de se provar coisas que valem para todos os naturais é o processo conhecido como **indução**. Basicamente, uma demonstração por indução funciona da seguinte forma:

- Provamos que certa propriedade vale para 0.
- Provamos que se a tal propriedade vale para algum $n \in \mathbb{N}$, ela precisa valer para $n+1$.

Com essas duas verificações, provamos que ela vale para todos os naturais.

Porque isso vale?

Slide 49

Pense nisso como uma sequência de peças de dominó, de forma que a primeira peça cai e que, se uma peça cair, a seguinte cai também. No final, teremos que todas as peças caem.

Um jeito formal para ver que isso vale de fato, é o uso do seguinte fato sobre os naturais:

Todo subconjunto não vazio de $\mathbb{N}$ admite mínimo.

Slide 50

Vamos ver que esse fato implica que a indução vale. Considere uma propriedade P que vale para 0. Em símbolos, dizemos que vale $P(0)$.

Suponha também que, se vale $P(n)$ para algum $n \in \mathbb{N}$, então necessariamente vale $P(n+1)$ também. Vamos mostrar então que vale $P(k)$ para todo $k \in \mathbb{N}$. Suponha que não. Então o conjunto:

$$\{k \in \mathbb{N} : \text{não vale } P(k)\}$$

é não vazio. Assim, pelo fato, tal conjunto admite mínimo. Seja m tal mínimo. Note que $m \neq 0$, já que temos que vale $P(0)$. Então $m-1 \in \mathbb{N}$ (pois $m > 0$). Note que $m-1$ não pertence ao conjunto, já que é menor que o mínimo.

Slide 51

Assim, pela definição do conjunto, vale $P(m-1)$. Mas, se vale $P(m-1)$, vale para $P((m-1)+1)$. Mas $(m-1)+1 = m$. Ou seja, vale $P(m)$, contradição.

Um exemplo

Slide 52

Vamos ver como isso funciona na prática:

Proposição 3.1. *Para todo $n \in \mathbb{N}$, vale $2^0 + 2^1 + \cdots + 2^n = 2^{n+1} - 1$*

Demonstração. Precisamos verificar a igualdade para o caso $n = 0$. Nela, só temos que calcular ambos os lados. Mas, de fato, temos $2^0 = 1 = 2^{0+1} - 1$.

Slide 53

Vamos agora supor que vale para n e provar para $n+1$. Ou seja, vamos supor que vale

$$2^0 + 2^1 + \cdots + 2^n = 2^{n+1} - 1$$

e vamos provar que vale

$$2^0 + 2^1 + \cdots + 2^n + 2^{n+1} = 2^{n+2} - 1.$$

Vamos começar pelo lado esquerdo e chegar no direito:

$$\begin{array}{rcl} 2^0 + 2^1 + \cdots + 2^n + 2^{n+1} & = & (2^0 + 2^1 + \cdots + 2^n) + 2^{n+1} \\ & \stackrel{HI}{=} & (2^{n+1} - 1) + 2^{n+1} \\ & = & 2 \cdot 2^{n+1} - 1 \\ & = & 2^{n+2} - 1 \end{array}$$

□

O HI acima indica onde usamos a hipótese de indução.

Mais um exemplo

Slide 54

Vejamos uma fórmula para somar os primeiros números ímpares.

Proposição 3.2. *Dado $N \in \mathbb{N}$, temos $\sum_{k=0}^{N}(2k+1) = (N+1)^2$.*

Demonstração.
Para o caso $N = 0$, temos que a fórmula vale (basta verificar ambos os lados).

Slide 55

Agora suponha que a fórmula vale para N e vamos provar para $N+1$. Ou seja, temos que

$$\sum_{k=0}^{N}(2k+1) = (N+1)^2$$

e temos que provar que

$$\sum_{k=0}^{N+1}(2k+1) = (N+2)^2.$$

Temos

$$\begin{array}{rcl} \sum_{k=0}^{N+1}(2k+1) & = & (\sum_{k=0}^{N} 2k+1) + 2(N+1) + 1 \\ & \stackrel{HI}{=} & (N+1)^2 + 2N + 3 \\ & = & N^2 + 2N + 1 + 2N + 3 \\ & = & (N+2)^2 \end{array}$$

□

Generalizando

Slide 56

Note que pelo argumento anterior, se a gente prova que vale para $n = 3$ e depois que se vale para n, então vale para $n+1$, conseguimos garantir que a propriedade vale para qualquer $k \geq 3$ (e não para todo $\mathbb{N}$). Obviamente, o análogo vale para qualquer k_0 que seja o primeiro que a gente prova que vale.

Exemplo

Slide 57

Isso é útil em alguns casos, como por exemplo:
Proposição 3.3. *Se $n \geq 5$, então $4n < 2^n$.*

Demonstração. Vamos provar o primeiro caso, que aqui é quando $n = 5$. De fato, temos que $4n = 20 < 32 = 2^5$.

Agora suponha que vale para n e vamos provar para $n + 1$. Temos

$$4(n+1) = 4n + 4 \overset{HI}{<} 2^n + 2^2 \overset{2<n}{<} 2^n + 2^n = 2^{n+1}.$$

□

Misturando um pouco

Slide 58

Nem sempre as afirmações envolvem só naturais:
Proposição 3.4. *Se X tem n elementos, $\wp(X)$ tem 2^n elementos.*

Demonstração. De fato, se $n = 0$, temos que $X = \emptyset$ e $\wp(X) = \{\emptyset\}$ que tem um elemento.

Slide 59

Agora suponha que vale para n e vamos provar para $n + 1$.
Então $X = \{x_1, ..., x_{n+1}\}$. Note que

$$\wp(X) = \{A \subset X : x_{n+1} \notin A\} \cup \{A \subset X : x_{n+1} \in A\}.$$

Note que os dois conjuntos acima são disjuntos e que eles têm a mesma quantidade de elementos (voce consegue fazer uma bijeção entre eles?).

Note também que $\{A \subset X : x_{n+1} \notin A\} = \wp(Y)$, onde $Y = \{x_1, ..., x_n\}$. Ou seja, por hipótese de indução, tal conjunto tem 2^n elementos. Assim, $\wp(X)$ tem $2^n + 2^n = 2^{n+1}$ elementos. □

Apertos de mão

Slide 60

Numa festa, havia $2n$ pessoas e algumas se cumprimentaram com apertos de mão. Sabe-se que a cada 3 pessoas, alguma delas não cumprimentou alguma das outras (ou seja, não tem 3 que se cumprimentaram mutuamente). Podemos concluir que houve no máximo n^2 cumprimentos.

Vamo fazer isso por indução. Se $n = 1$, o resultado é claro (tem no máximo 1 cumprimento).

Slide 61

Agora suponha que vale o resultado para n e vamos provar para $n + 1$.

Note que temos $2n + 2$ pessoas. Dessas, separe duas que se cumprimentaram (podemos supor que elas existem, caso contrário o resultado vale). Vamos chamá-las de A e B.

Por (HI), existe no máximo n^2 apertos de mão entre as outras pessoas. E, pela hipótese do problema, nenhuma das outras pessoas cumprimentou tanto A como B. Ou seja, existem no máximo $2n$ cumprimentos envolvendo alguma das outras pessoas com A ou B. Assim, a quantidade de apertos de mão é limitada por

$$n^2 + 2n + 1 = (n+1)^2$$

como queríamos.

Exercícios da Aula 3

Exercício 3.1. Mostre que para todo $n \geq 1$, temos que $3^{n+1} > 2n$.

Exercício 3.2. Mostre que $n^3 - n$ é múltiplo de 3 para todo $n \in \mathbb{N}$.

Exercício 3.3. Mostre que $n^2 - 1$ é múltiplo de 8 para todo n ímpar.

Exercício 3.4. Use a Proposição 3.4 para provar a Proposição 3.1 (precisa de uma boa ideia).

Exercício 3.5. Joãozinho tentou provar que todos os cavalos que existem têm a mesma cor. E ele fez isso por indução no número de cavalos. Começando com $n = 1$, é claro que o resultado vale. Agora, supondo que vale para n, para provar que vale para $n+1$, Joãozinho argumento da seguinte forma: pegue um conjunto com $n + 1$ cavalos e separe um cavalo. Chame tal cavalo de X. O que resta é um conjunto com n cavalos que, por hipótese de indução, todos têm a mesma cor. Mas, devolvendo X e tirando outro cavalo (digamos, Y), novamente sobram n cavalos, todos da mesma cor. Além disso, concluímos que X tem a mesma cor que os outros (pois só o Y está de fora). Ou seja, deixando X e Y junto com os outros, todos têm a mesma cor.

Joãozinho está certo?

Aula 4

Vamos agora começar a trabalhar com algumas técnicas de contagem. Em particular, vamos obter as fórmulas que usamos ao final do problema da geladeira.

Palavras

Slide 62

Fixe um conjunto A que vamos chamar de **alfabeto**. Uma **palavra** de n letras neste alfabeto nada mais é do que uma sequência de n elementos de A. Por exemplo, se[18] $A = \{1, 2, 3, 4\}$, temos que 113 e 345 são duas palavras de 3 letras de A. Note também que a ordem *importa*: $212 \neq 122$.

Slide 63

Denotaremos usualmente uma palavra p como

$$p = a_1 \cdots a_n$$

onde cada $a_i \in A$ é a i-ésima letra de p.

Contar palavras possíveis com um alfabeto fixado é simples. Por exemplo, se $|A| = k$, existem $k \cdots k = k^n$ palavras de n letras.

Mas muitas vezes não queremos *qualquer* palavra possível feita com o alfabeto. Uma restrição bastante popular é exigir que as letras sejam todas distintas. Ou seja, neste caso, temos que uma palavra $p = a_1 \cdots a_n$ é tal que cada $a_i \in A$ como antes mas, além disso, $a_i \neq a_j$ se $i \neq j$. Desta forma, voltando ao nosso exemplo inicial, temos que 123 é uma palavra válida, enquanto que 141 não é.

Um exemplo

Slide 64

Vejamos uma situação mais concreta. Imagine que tenhamos 5 livros distintos (vamos chamá-los de A, B, C, D e E) e que tenhamos 3 crianças para quem queremos distribuir os livros - mas vamos dar apenas um livro para cada uma delas[19]. De quantas maneiras podemos fazer isso? Vamos usar a ideia de alfabeto e de palavras para nos ajudar. Podemos fixar como alfabeto o conjunto dos livros $\{A, B, C, D, E\}$ e associar a cada distribuição uma palavra com letras distintas (e vice e versa) da seguinte maneira: a primeira letra indica o livro da primeira criança. A segunda, o da segunda e a terceira o da terceira. Ou seja, desta forma, basta contarmos apenas quantas palavras de 3 letras *sem repetição* são possíveis.

Slide 65

Podemos tentar exibir todas:

$$ABC\ ABD\ ABE\ ACB\ ACE\ ADE\ BAC\ BAD...$$

Mas note que já deu uma quantidade razoável.

Permutações

Slide 66

O exemplo anterior indica que pode ser interessante sabermos contar quantas palavras de k letras sem repetição são possíveis de ser feitas com um alfabeto de n letras. Vamos denotar tal quantidade por $P(n, k)$. Lê-se permutações de n k a k. Alguns lugares chamam isso de k-permutações. Outros ainda dizem que é permutação só se $k = n$ - os outros casos são chamados de arranjos.

[18] Indicamos por $|X|$ a quantidade de elementos de X.
[19] Ou seja, vão sobrar dois livros

A fórmula

Slide 67

Proposição 4.1. *Se $k \leq n$, $P(n,k) = \frac{n!}{(n-k)!}$.*

Demonstração. Vamos mostrar por indução sobre k. Se $k = 1$, é claro que só podemos formar n palavras e a igualdade vale. Agora suponha que o resultado vale para q e vamos mostrar para $q+1$. Ou seja, estamos supondo que vale $P(n,q) = \frac{n!}{(n-q)!}$ e queremos mostrar que vale $P(n,q+1) = \frac{n!}{(n-q-1)!}$. Sabemos que com q letras, temos $P(n,q)$ palavras. Podemos pensar que uma palavra de $q+1$ letras é simplesmente uma palavra de q letras seguida de mais uma letra no final. Para cada início de q letras, temos mais quantas possibilidades para o final? Já "gastamos" q letras, então ainda nos sobram $n-q$ possibilidades para esta última.

Slide 68

Ou seja:

$$\begin{aligned} P(n,q+1) &= P(n,q)(n-q) \\ &\overset{HI}{=} \frac{n!}{(n-q)!}(n-q) \\ &= \frac{n!}{(n-q)(n-q-1)!}(n-q) \\ &= \frac{n!}{(n-q-1)!} \end{aligned}$$

□

Uma convenção

Slide 69

Se $k > n$, é conveniente definir $P(n,k) = 0$ (note que isso fica coerente com a contagem de palavras).

Finalizando o exemplo dos livros

Slide 70

No nosso exemplo dos livros, temos que existem $P(5,3) = 60$ formas diferentes de distribuir os livros.

Mais um exemplo

Slide 71

Numa sala com 50 pessoas, qual a chance de duas fazerem aniversário no mesmo dia?

Vamos ter que supor vários fatos aqui[20]: todo mundo só faz aniversário num dos 365 dias do ano (ou seja, sem 29 de fevereiro) e que todos os dias são equiprováveis.

Se são 50 pessoas, há 365^{50} possibilidades de aniversários. Mas, estamos interessados em saber se há duas pessoas que fazem aniversário no mesmo dia. Ou seja, podemos contar quantas palavras de comprimento 50 existem, formadas com os dias do ano como alfabeto sem repetição: as que repetem são justamente os casos que não estamos interessados. Assim

$$P = 1 - \frac{P(365,50)}{365^{50}}$$

esse resultado é aproximadamente $0,97$.

Combinações

Slide 72

Imagine que temos que montar um grupo de 4 pessoas para uma comissão de forma que uma seja a presidente, um seja a vice, uma seja a tesoureira e o última seja a estagiária. Se temos 50 pessoas para dividir nestes 4 cargos, de quantas maneiras podemos fazer isso?

Já sabemos que isso pode ser feito através de $P(50,4) = \frac{50!}{46!} = 50 \cdot 49 \cdot 48 \cdot 47 = 5527200$.

Slide 73

Mas e se quisermos simplesmente montar uma chapa com 4 pessoas, depois elas que decidam quem faz o quê? Podemos pensar nisso como sendo uma palavra de 4 letras (cada letra uma pessoa diferente) mas que não importa qual a posição de cada letra (por exemplo, a palavra $ABCD = DBCA$). Vamos denotar tal quantidade da seguinte maneira[21]: $\left(\begin{array}{c} n \\ k \end{array} \right)$.

A fórmula

Slide 74

Proposição 4.2. *Sejam $n \geq k \geq 0$. Então* $\left(\begin{array}{c} n \\ k \end{array} \right) = \frac{P(n,k)}{k!} = \frac{n!}{k!(n-k!)}$

Demonstração. Vamos fazer isso de uma maneira um pouco diferente. Fixe k letras distintas. Quantas palavras de comprimento k podemos escrever com elas? $k!$. Assim, para cada conjunto de k letras, temos $k!$ palavras distintas. Note que se tomamos dois conjuntos diferentes de k letras cada, formamos palavras distintas - e variando sobre todos os conjuntos de k letras, obtemos todas as palavras. Assim

$$k! \left(\begin{array}{c} n \\ k \end{array} \right) = P(n,k)$$

e portanto temos o resultado desejado. □

Finalizando a comissão

Slide 75

Assim, para a mesma escolha da comissão, agora não importando como as pessoas se organizam, temos $\left(\begin{array}{c} 50 \\ 4 \end{array} \right) = \frac{50!}{46!4!} = 230300$.

Simetria

Slide 76

Pela simetria da fórmula, pode-se notar que $\left(\begin{array}{c} n \\ k \end{array} \right) = \left(\begin{array}{c} n \\ n-k \end{array} \right)$. Mas também podemos notar essa igualdade de outra forma: o primeiro conta como escolher k, dentre n, o segundo, conta como escolher $n-k$, dentre n. Claramente, quando se escolhe k, se escolhe $n-k$ (os não escolhidos). Logo, essas duas quantidades deveriam ser mesmo iguais.

Subconjuntos

Slide 77

Proposição 4.3. *Considere o conjunto $A = \{a_1, ..., a_n\}$. Então existem* $\left(\begin{array}{c} n \\ k \end{array} \right)$ *subconjuntos A com k elementos.*

[20] todos eles irreais, mas fazer o quê?

[21] Lê-se "combinação de n k a k" ou "n escolhe k".

Demonstração. Basta notar que é o mesmo que montar palavras de comprimento k, sem repetição e não importando a ordem. □

Proposição 4.4. *Seja $n \geq 1$. Então $\sum_{i=1}^{n} \binom{n}{k} = 2^n - 1$.*

Demonstração. É só ver que o lado esquerdo contou quantos subconjuntos de um conjunto de n elementos existem, com exceção do vazio. □

Já vimos isso antes, não?

Um exemplo

Slide 78

Um famoso jogo de azar consiste em cada pessoa escolher 6 números distintos entre 1 e 60. Ao final, são sorteados 6 números (distintos) e quem acertar os 6 vence.

Vejamos qual a chance de alguém vencer. Quem jogar vai escolher uma palavra de comprimento 6 com todos os símbolos distintos e precisa que essa seja a palavra sorteada. Então a chance de acertar é uma entre todas as palavras de comprimento 6, sem repetição e sem importar a ordem. Ou seja, 1 em

$$\binom{60}{6} = \frac{60!}{54!6!} = 50.063.860$$

Bilhetes múltiplos

Slide 79

Pode-se fazer uma aposta com 10 números (e se vence se os 6 sorteados estiverem entre eles). Isso equivale a quantos bilhetes "simples"?

Para isso basta contarmos quantos bilhetes simples estão nesta jogada: cada grupo de 6 é uma. Ou seja, na verdade se está fazendo a seguinte quantidade de jogadas simples:

$$\binom{10}{6} = \frac{10!}{6!4!} = \frac{10 \cdot 9 \cdot 8 \cdot 7}{4 \cdot 3 \cdot 2} = 210$$

Se o valor de uma aposta simples for $R\$4,50$, então isso equivaleria a apostar $R\$945$.

Ganhando menos

Slide 80

Mas também se ganha (menos) se acertar 5 números. Qual a chance de se ganhar tal prêmio? (e não ganhar o prêmio total dos 6)

Suponha que alguém escolheu 6 números. Vejamos quantos sorteios possíveis existem de forma que exatamente 5 destes números apareçam. Para cada grupo de 5 números jogados, existem $60 - 6 = 54$ possíveis sorteios nessas condições (montamos o sorteio com 5 dos números jogados mais um dos não escolhidos).

Slide 81

Assim, a quantidade de sorteios possíveis é

$$\binom{6}{5} 54$$

Ou seja, comparando isso com todos os sorteios possíveis, obtemos que a chance de se vencer é 1 em:

$$\frac{\binom{60}{6}}{\binom{6}{5}54}$$

que é aproximadamente 154.518.

Ganhando menos ainda

Slide 82

Analogamente, se quisermos acertar apenas 4, obtemos uma em

$$\frac{\binom{60}{6}}{\binom{6}{4}\binom{54}{2}}$$

que é aproximadamente 2.332 (para justificar o denominador: para cada jogo de 4 entre 6, devemos "completar" o sorteio com 2 números entre os restantes).

Slide 83

Finalmente, jogando-se 10 números, qual a chance de se acertar exatamente 4?

Novamente, podemos fazer

$$\frac{\binom{60}{6}}{\binom{10}{4}\binom{50}{2}}$$

que dá aproximadamente 1 em 195.

Mas ganha mais coisas

Slide 84

Se são jogados 10 números e se acerta 5, ganha-se diversos prêmios de bilhetes de 5 números. Basicamente, para cada bilhete simples (6 números) possível entre os 10 jogados que contenha os 5 sorteados, ganha-se o correspondente valor.

Como são 5 números fixados, para completar o bilhete, falta só um, escolhido entre os cinco não sorteados. Ou seja, são 5 prêmios desse tipo.

Slide 85

Mas há prêmios para acertos de 4 números. Então, na mesma jogada que se jogam 10 números e se acertam 5, precisamos ver quantos bilhetes simples são possíveis de serem feitos com 4 sorteados e 2 não, dentre os 10.

Começamos escolhendo 4 entre os 5 sorteados e, para cada grupo desses, há $\binom{5}{2}$ formas de se completar o bilhete, pegando 2 dentre os não sorteados. Ou seja, temos

$$\binom{5}{4}\binom{4}{2} = 50$$

prêmios desse tipo.

Veja também

Slide 86

Aqui você pode encontrar diversos resultados sobre esse jogo (de forma oficial). Você consegue calcular todas as formas?

https://loterias.caixa.gov.br/Paginas/Mega-Sena.aspx

Slide 87

Aqui você tem uma história interessante sobre um jogo de loteria

https://www.bbc.com/portuguese/geral-62133938

Aula 5

Princípio da inclusão-exclusão

Slide 88

Considere um grupo X de indivíduos e suponha que tenhamos propriedades $P_1, ..., P_n$. Dado $S \subset \{P_1, ..., P_n\}$, denote por $N(S)$ a quantidade de indivíduos que satisfazem todas as P_i's em S. Note que[22] $N(\emptyset) = |X|$.

Um exemplo

Slide 89

Vejamos um exemplo para ver como esse tipo de situação pode ser abordada:

Num total de 63 alunos, temos que 47 fazem matemática pura, 51 são homens, 45 homens fazem matemática pura. Quantas mulheres não fazem matemática pura?

Neste caso, temos $|X| = 63$. Vamos chamar de P_1 ser homem, P_2 fazer matemática pura. Desta maneira, podemos notar que a quantidade de mulheres que não fazem matemática pura é dada por

Slide 90

- Adicionamos todos os indivíduos ($N(\emptyset)$);
- Tiramos os homens ($N(P_1)$);
- Tiramos quem faz matemática pura ($N(P_2)$);
- Note que nas subtrações acima, tiramos cada "homem que faz matemática pura" duas vezes, então precisamos acrescentar eles uma vez ($N(P_1, P_2)$).

$$N(\emptyset) - N(P_1) - N(P_2) + N(P_1, P_2)$$

Ou seja, $63 - 51 - 47 + 45 = 10$.

O teorema

Slide 91

Teorema 5.1 (Princípio da inclusão exclusão)**.** *A quantidade de indivíduos que não satisfazem nenhuma $P_1, ..., P_n$ é dada por*

$$\sum_{S \subset \{1,...,n\}} (-1)^{|S|} N(S).$$

Assim, a quantidade de elementos que satisfaz alguma das propriedades é dada por

$$N(\emptyset) - \sum_{S \subset \{1,...,n\}} (-1)^{|S|} N(S)$$

que, por sua vez, pode ser reduzida para

$$\sum_{S \subset \{1,...,n\}, S \neq \emptyset} (-1)^{|S|+1} N(S).$$

Exemplo de múltiplos

Slide 92

Quantos números entre 1 e 100 são múltiplos de 2, 3 ou 5?

Chame de P_i ser múltiplo de i. Assim, temos $N(P_2) = 50$, $N(P_3) = 33$, $N(P_5) = 20$. Também temos que $N(P_2, P_3) = N(P_6) = 16$, $N(P_2, P_5) = N(P_{10}) = 10$ e $N(P_3, P_5) = N(P_{15}) = 6$. Finalmente, $N(P_2, P_3, P_5) = N(P_{30}) = 3$.

Assim, a quantidade desejada é

$$50 + 33 + 20 - 16 - 10 - 6 + 3 = 74$$

Exemplo de almoço

Slide 93

Uma pessoa almoçou 34 vezes durante certo período[23]. Sabemos que essa pessoa tem 4 amigos e que, nestes almoços, ela almoçou com cada amigo 20 vezes, com cada dupla de amigos 11 vezes, com cada trio de amigos 5 vezes e com todos os 4 amigos uma única vez. Alguma vez a pessoa almoçou sozinha?

Slide 94

Vamos chamar os amigos de a, b, c, d. Daí, almoçar com o amigo x vamos denotar por P_x. Note que pelo enunciado, $N(\emptyset) = 34$, $N(P_a) = N(P_b) = N(P_c) = N(P_d) = 20$. Note também que $N(P_a, P_b) = N(P_a, P_c) = ... = 11$, $N(P_a, P_b, P_c) = N(P_a, P_b, P_d) = ... = 5$ e $N(P_a, P_b, P_c, P_d) = 1$. Assim

$$\begin{array}{rcl} \sum\limits_{S \subset \{a,b,c,d\}} (-1)^{|S|} N(S) & = & 34 - \binom{4}{1} 20 + \binom{4}{2} 11 - \binom{4}{3} 5 + \binom{4}{4} 1 \\ & = & 34 - 80 + 66 - 20 + 1 \\ & = & 1 \end{array}$$

Sobrejeções

Slide 95

Um avô tem 15 bilhetes de loteria (distintos) e quer distribuí-los entre seus 4 netos, cada um recebendo pelo menos um bilhete. De quantas maneira ele pode fazer isso?

Se chamamos de X o conjunto dos bilhetes e de Y o conjunto dos netos, podemos definir $f(x) = y$ como sendo "bilhete x vai para o neto y" e, desta maneira, as distribuições que estamos interessados são as sobrejetoras. Agora basta contá-las.

Considere P_i a[24]propriedade "i não pertence à imagem de f". Assim, só precisamos contar quantas funções não satisfazem nenhuma das P_i's.

Um resultado auxiliar

Slide 96

Lema 5.2. *Sejam $n \geq m > 0$. Considere P_i como acima, trabalhando com domínio das f's como $\{1, ..., n\}$ e contradomínio $\{1, ..., m\}$. Seja $S \subset \{P_1, ..., P_m\}$. Então*

$$N(S) = (m - |S|)^n.$$

Demonstração. Dada uma $f : \{1, ..., n\} \to \{1, ..., m\}$ satisfazendo toda $P_i \in S$, temos que ela é uma palavra de comprimento n num alfabeto com $m - |S|$ letras com repetição. Assim, $N(S) = (m - |S|)^n$. □

Quantidade de sobrejeções

Slide 97

Denote por $S(n,m)$ como sendo a quantidade de funções da forma $f : \{1,...,n\} \to \{1,...,m\}$ sobrejetoras. Temos

Teorema 5.3. $S(n,m) = \sum_{k=0}^{m}(-1)^k \left(\begin{array}{c} m \\ k \end{array} \right)(m-k)^n$.

Demonstração. Temos

$$\begin{array}{rcl} S(n,m) & = & \sum_{S\subset\{P_1,...,P_m\}}(-1)^{|S|}N(S) \\ & = & \sum_{S\subset\{P_1,...,P_m\}}(-1)^{|S|}(m-|S|)^n \\ & = & \sum_{k=0}^{m}(-1)^k \left(\begin{array}{c} m \\ k \end{array} \right)(m-k)^n \end{array}$$

□

Voltando ao avô

Slide 98

De curiosidade, aplicando esta fórmula, temos que o problema do avô tem como resposta $S(15,4) = 1.016.542.800$.

Amigo secreto

Slide 99

Vejamos agora o sorteio de um amigo secreto. Esse sorteio nada mais é que uma função $f : \{1,...,n\} \to \{1,...,n\}$ injetora (ou bijetora, é equivalente neste caso) e tal que $f(x) \neq x$ (ninguém sorteia a si mesmo).

Um resultado auxiliar

Slide 100

Considere P_i a propriedade de uma função $f : \{1,...,n\} \to \{1,...,n\}$ injetora ser tal que $f(i) = i$. Desta forma, temos:

Lema 5.4. *Seja $S \subset \{P_1,...,P_n\}$. Temos que*

$$N(S) = (n-|S|)!$$

Demonstração. Note que cada f nada mais é que uma palavra de comprimento n sem repetição e com essa restrição para a i-ésima casa. Assim, fixadas as posições que aparecem em S, temos que restam $(n-|S|)!$ possibilidades. □

Desarranjos

Slide 101

Uma função $f : \{1,...,n\} \to \{1,...,n\}$ injetora tal que $f(i) \neq i$ é chamada de um desarranjo. Denotamos por d_n a quantidade de desarranjos.

Teorema 5.5. $d_n = \sum_{k=0}^{n}(-1)^k \left(\begin{array}{c} n \\ k \end{array} \right)(n-k)!$

[22] Pense em cada P_i como uma restrição. Se você não dá alguma restrição, todos os indivíduos entram.

[23] Cuidado aqui, se a pessoa almoçou com um trio de amigos num certo dia, isso conta que ela almoçou uma vez para cada amigo do trio, cada dupla do trio e pelo trio completo.

[24] Cuidado com a dupla negação aqui: uma função vai ser sobrejetora se não satisfizer nenhuma das P_i's.

Demonstração. De fato

$$\begin{aligned} d_n &= \sum_{S\subset\{P_1,\ldots,P_n\}}(-1)^{|S|}N(S) \\ &= \sum_{S\subset\{P_1,\ldots,P_n\}}(-1)^{|S|}(n-|S|)! \\ &= \sum_{k=0}^{n}(-1)^k \binom{n}{k}(n-k)! \end{aligned}$$

□

Voltando ao amigo secreto

Slide 102

Note que, então a chance de um sorteio de amigo secreto dar certo é dada por $\frac{d_n}{n!}$. Temos:

Teorema 5.6. $\frac{d_n}{n!} = \sum_{k=0}^{n}(-1)^k\frac{1}{k!}$. *Que, no limite quando* $n \to +\infty$, *temos que vale* $\frac{1}{e}$.

Demonstração. Temos

$$\begin{aligned} \frac{d_n}{n!} &= \frac{\sum_{k=0}^{n}(-1)^k \binom{n}{k}(n-k)!}{n!} \\ &= \frac{\sum_{k=0}^{n}(-1)^k \frac{n!}{(n-k)!k!}(n-k)!}{n!} \\ &= \sum_{k=0}^{n}(-1)^k\frac{1}{k!} \end{aligned}$$

□

Exercícios da Aula 5

Exercício 5.1. De quantas maneiras é possível colocar 8 rainhas num tabuleiro de xadrez, sem colocar duas numa mesma coluna nem numa mesma linha e sem que nenhuma esteja na diagonal principal? (não descartar simetrias).

Aula 6

Listas Circulares

Slide 103

Exemplo 6.1. De quantas maneiras podemos acomodar 5 pessoas numa mesa de 5 lugares? (pensando que qualquer alteração de lugar é uma configuração diferente)

5!

Slide 104

Exemplo 6.2. De quantas maneiras podemos acomodar 5 pessoas numa mesa circular (de 5 cadeiras)? (Só importa a posição relativa entre elas).

Uma maneira de se pensar é a seguinte: fixe uma das pessoas. Distribua nos lugares restantes (no sentido horário). Assim, temos como resposta 4!.

Slide 105

Exemplo 6.3. Mesmo problema anterior, mas temos 8 pessoas e a mesa continua com 5 lugares.

Escolhidas as 5 pessoas que vão se sentar, já temos quantas posições possíveis. Assim, só falta ver quantos grupos de 5 vão se sentar:

$$\left(\begin{array}{c} 8 \\ 5 \end{array} \right) 4! = \frac{8!}{5!3!} 4! = 8 \cdot 7 \cdot 6 \cdot 4 = 1.344$$

Slide 106

Exemplo 6.4. Para sentar numa mesa circular com 10 lugares, temos 5 homens e 5 mulheres. De quantas de quantas maneiras podemos acomodá-los (posições relativas) de forma que se alternem entre homens e mulheres?

Fixamos, por exemplo, um homem. Daí para o seu lado temos 5 alternativas. Depois, 4 para os outros homens, depois 4 para as outras mulheres etc. Ou seja, temos

$$5 \cdot 4 \cdot 4 \cdot 3 \cdots 1 = 5!4!$$

Repetições

Slide 107

Vamos ver agora algumas contagens onde alguns elementos se repetem.

Exemplo 6.5. Temos n bolinhas brancas e 1 bolinha preta para colocar em fila. De quantas maneiras podemos fazer isso?

Basta notar que temos $n + 1$ lugares para a bolinha preta.

Slide 108

Exemplo 6.6. Temos n bolinhas brancas e 2 bolinhas pretas para colocar em fila. De quantas maneiras podemos fazer isso?

Podemos pensar que a primeira bolinha preta tem $n + 2$ posições possíveis, enquanto que a segunda tem $n + 1$. Mas note que não devemos contar como diferentes onde cada uma das bolinhas pretas parou. Assim, temos:

$$\frac{(n+2)(n+1)}{2}$$

Ainda mais bolinhas

Slide 109

Exemplo 6.7. Temos n bolinhas brancas e k bolinhas pretas. De quantas formas podemos colocá-las em fila?

Agora começa a ficar um pouco mais complicado, então vamos apelar para alguma regra mais geral. Podemos pensar que temos $n+k$ casas, uma para cada bolinha. Daí só precisamos selecionar k dessas casas para colocarmos bolinhas pretas. Mas isso é simplesmente contar quantos subconjuntos de tamanho k existem em $n+k$

$$\left(\begin{array}{c} n+k \\ k \end{array} \right) = \frac{(n+k)!}{n!k!}$$

Slide 110

Exemplo 6.8. Se o último exemplo está certo, deveríamos poder aplicá-lo no segundo exemplo:

$$\left(\begin{array}{c} n+2 \\ 2 \end{array} \right) = \frac{(n+2)!}{2!n!} = \frac{(n+2)(n+1)}{2}$$

Slide 111

Exemplo 6.9. Mesma situação anterior, mas agora com k bolinhas pretas e n bolinhas brancas, sendo que as brancas são numeradas de forma que elas fiquem distintas.

Podemos simplesmente contar as distribuições das pretas e depois, para cada uma desta, temos as distribuições das brancas:

$$\left(\begin{array}{c} n+k \\ k \end{array} \right) P(n,n)$$

Estrelas e barras

Slide 112

Vamos apresentar uma nova técnica de contagem na demonstração do seguinte resultado:

Proposição 6.10. *Sejam $k \leq n \in \mathbb{N}_{>0}$.* [25] *Então a quantidade de maneiras diferentes que podemos escrever $a_1 + \cdots + a_k = n$ com $a_i \in \mathbb{N}_{>0}$ é dada por $\left(\begin{array}{c} n-1 \\ k-1 \end{array} \right)$.*

Slide 113

Demonstração. Desenhe n $*$'s. Coloque $k-1$ |'s, cada uma entre dois $*$. Por exemplo, com $n=6$ e $k=3$, uma possível maneira é

$$*|***|**$$

Pense que a_1 indica a quantidade de $*$'s antes da primeira |, a_2 a quantidade entre a primeira e a segunda | etc.

Note que a quantidade de locais possíveis para as |'s é $n-1$ e precisamos escolher $k-1$ delas. Ou seja, existem $\left(\begin{array}{c} n-1 \\ k-1 \end{array} \right)$ maneiras de se fazer isso. □

Slide 114

Proposição 6.11. *Sejam $k, n \in \mathbb{N}_{>0}$. Então a quantidade de maneiras diferentes que podemos escrever $a_1 + \cdots + a_k = n$, com $a_i \in \mathbb{N}$ é dada por $\left(\begin{array}{c} n+k-1 \\ k-1 \end{array} \right) = \left(\begin{array}{c} n+k-1 \\ n \end{array} \right)$.*

[25] Estamos considerando que escrever $2+3$ e $3+2$ são formas diferentes.

Demonstração. Note que agora podemos colocar | em qualquer lugar, incluindo no começo, no fim ou mesmo colocar duas consecutivas (sem $*$ entre elas). Mas no total, entre $*$'s e |'s, temos espaço para $n+k-1$ símbolos. Se quisermos ver onde colocar as |'s, temos simplesmente $\begin{pmatrix} n+k-1 \\ k-1 \end{pmatrix}$ lugares. Se quisermos simplesmente contar onde colocar $*$, temos $\begin{pmatrix} n+k-1 \\ n \end{pmatrix}$. □

Aula 7

Pinos e elásticos

Slide 115

Considere $2n$ pinos numerados de 1 a $2n$, colocados em formato circular. Tendo j elásticos idênticos ($j \leq n$), de quantas formas podemos prender os elásticos nos pinos, sendo que um elástico prende dois pinos consecutivos e não queremos colocar 2 elásticos num mesmo pino?

Organizando

Slide 116

Podemos representar cada elástico preso com um $*$ e cada pino sem elástico como $|$. Desta forma, temos j $*$'s e $2n-2j$ $|$'s para dispor[26].

Slide 117

Ou seja, como fizemos antes, temos $\binom{2n-2j+j}{j} = \binom{2n-j}{j}$ maneiras de fazer isso. Mas note que isso só conta configurações que começam com um elástico ou com um pino solto. Faltam as que há um elástico entre o último pino e o primeiro. Para contar essas, temos $j-1$ $*$'s e as mesmas $2n-2j$ $|$'s. Assim, temos mais $\binom{2n-2j+j-1}{j-1} = \binom{2n-j-1}{j-1}$ configurações.

Fazendo as contas

Slide 118

Dá para simplificar essa fórmula:

$$\begin{aligned}
\binom{2n-j}{j} + \binom{2n-j-1}{j-1} &= \tfrac{(2n-j)!}{j!(2n-2j)!} + \tfrac{(2n-j-1)!}{(j-1)!(2n-2j)!} \\
&= \tfrac{(2n-j)!}{j!(2n-2j)!} + \tfrac{(2n-j-1)!j}{j!(2n-2j)!} \\
&= \tfrac{(2n-j)!+(2n-j-1)!j}{j!(2n-2j)!} \\
&= \tfrac{1}{(2n-j)} \tfrac{(2n-j)(2n-j)!+(2n-j)!j}{j!(2n-2j)!} \\
&= \tfrac{2n}{2n-j} \binom{2n-j}{j}
\end{aligned}$$

Mãos de poker

Slide 119

Vamos mostrar como calcular as chances de certas mãos saírem num jogo de poker. Um baralho consiste em 52 cartas, divididas em 4 naipes (♢, ♠, ♡, ♣), sendo que cada naipe tem 13 cartas listadas a seguir em ordem crescente:

2 3 4 5 6 7 8 9 10 J Q K A

Um sorteio no poker tipicamente é a escolha de 5 cartas, dentre as 52. Ou seja, temos $\binom{52}{5}$ possíveis sorteios (2.598.960). A seguir vamos calcular quantos sorteios são possíveis contendo cada um dos itens pontuáveis.

[26] Pense na contagem de elásticos com sendo os dois pinos presos como uma coisa só.

Dupla

Slide 120

Uma dupla consiste de duas cartas de mesmo valor (e, portanto, naipes diferentes). Cuidado que aqui queremos que o sorteio tenha apenas uma dupla (e não duas, nem um trio etc). Uma maneira de organizar o cálculo é a seguinte: contamos quantas são as duplas possíveis, vezes as distribuições dos naipes nesta dupla, como juntar mais 3 valores distintos ao sorteio (e diferentes da dupla) e, finalmente, como distribuir os naipes para os tais valores. Desta forma, a expressão fica

$$\binom{13}{1}\binom{4}{2}\binom{12}{3}\binom{4}{1}^3$$

dando um total de 1.098.240 possibilidades.

Duas duplas

Slide 121

Sorteio de duas duplas que não formem quatro cartas de mesmo valor (e que a última seja de valor distinto ao das duplas). Seguindo o raciocínio acima, temos:

$$\binom{13}{2}\binom{4}{2}^2\binom{11}{1}\binom{4}{1}$$

dando um total de 123.552 possibilidades.

Trio

Slide 122

Sorteio de 3 cartas de mesmo valor, com as duas últimas com valores distintos (entre si e do trio).

$$\binom{13}{1}\binom{4}{3}\binom{12}{2}\binom{4}{1}^2$$

dando um total de 54.912 possibilidades.

Quadra

Slide 123

Sorteio de 4 cartas de mesmo valor.

$$\binom{13}{1}\binom{12}{1}\binom{4}{1}$$

dando um total de 624 possibilidades.

Full house

Slide 124

Sorteio de um trio e uma dupla.

$$\binom{13}{1}\binom{4}{3}\binom{12}{1}\binom{4}{2}$$

dando um total de 3.744 possibilidades.

Straight

Slide 125

Todas as 5 cartas do sorteio são consecutivas entre si, mas não do mesmo naipe. Podemos escolher onde a sequência começa (cuidado que aqui a sequência pode ser $A2345$ ou $10JQKA$, mas não coisas do tipo $QKA23$), daí escolher qual o naipe de cada carta e descontar os casos em que todas são do mesmo naipe.

$$\binom{10}{1}\binom{4}{1}^5 - \binom{10}{1}\binom{4}{1}$$

dando um total de 10.200 possibilidades.

Flush

Slide 126

Todas as 5 cartas do mesmo naipe, mas não em sequência. Só precisamos fazer o sorteio dos valores e daí escolher um dos naipes, mas descontar as que estiverem em sequência.

$$(\binom{13}{5} - \binom{10}{1})\binom{4}{1}$$

dando um total de 5.108 possibilidades.

Straight flush

Slide 127

Todas as cartas consecutivas e do mesmo naipe. Mas exclui-se o caso em que termina em A.

$$\binom{9}{1}\binom{4}{1}$$

dando um total de 36 possibilidades.

Royal straight flush

Slide 128

Todas as cartas consecutivas, do mesmo naipe e terminando em A.

$$\binom{4}{1}$$

dando um total de 4 possibilidades.
Curiosidade: para sortear um royal straight flush, a chance é de 1 em 649.740. Compare com o que fizemos no sorteio de loteria.

Aula 8

Rudimentos de lógica

Slide 129

Primeiramente, vejamos a diferença entre provar e convencer. Quando damos um argumento do porque algo vale, em geral, estamos tentando convencer alguém de que o que dizemos é verdade. Mas há espaço para discussão. No momento em que provamos determinada coisa, tal espaço inexiste. Em geral, numa prova (demonstração), assumimos algo como verdade e depois deduzimos outras afirmações. A grande diferença entre convencer e provar é que enquanto no "convencer" muitos dos passos são passíveis de discussão, numa demonstração apenas o que assumimos como verdade é passível disso. Vejamos um exemplo (conhecido como **silogismo**)[27]:

Exemplo 8.1.
- Todo homem é mortal;
- Sócrates é um homem;
- Logo, Sócrates é mortal.

Slide 130

Examinemos um pouco mais de perto tal construção. As duas primeiras afirmações (que chamaremos de premissas ou hipóteses) é o que assumimos como verdade. A última é chamada de conclusão[28]. Podemos até discutir se as duas primeiras afirmações são verdadeiras ou não. Mas uma vez que supomos as duas como verdadeiras, não há outra opção para a conclusão a não ser que ela seja verdadeira também. Note também que nada precisamos assumir (ou saber) sobre os termos "homem", "mortal" ou mesmo "Sócrates". Isto é, seguindo essa estrutura, podemos criar outras tentativas de provas:

Exemplo 8.2.
- Nenhum cachorro voa;
- Snoopy é um cachorro;
- Logo, Snoopy não voa.

Slide 131

Exemplo 8.3.
- Todo pássaro é amarelo;
- Todo papagaio é um pássaro;
- Todo papagaio é amarelo.

Não exemplos

Slide 132

A conclusão do último silogismo é claramente falsa. Mas isso não é um problema do desenvolvimento do silogismo, mas sim do fato que a primeira hipótese também é falsa. O que se tenta criar com os silogismos é uma maneira em que o único jeito de se obter uma afirmação falsa seja assumindo como verdade uma outra afirmação falsa. Ou seja, nesse exemplo obtemos como conclusão uma afirmação falsa ("Todo papagaio é amarelo") porque uma das nossas hipóteses era falsa ("Todo pássaro é amarelo"). De qualquer forma, do ponto de vista de estrutura, tal silogismo está correto: duas hipóteses e uma conclusão que decorre delas. O caso é diferente nos próximos exemplos:

Exemplo 8.4.
- Alguns cachorros são pretos;

[27] Um silogismo basicamente é a obtenção de uma conclusão a partir de duas premissas.

[28] A ideia aqui é que o silogismo estar certo ou não, não depende de fatores externos a ele - por exemplo, não faz diferença se as premissas são verdadeiras ou não.

- Snoopy é um cachorro;
- Logo, Snoopy é preto.

Slide 133

Exemplo 8.5.
- Algumas flores são vermelhas;
- Sócrates é um homem;
- Logo, Snoopy é um cachorro.

O problema com o primeiro silogismo é que tentamos derivar a partir de que alguns cachorros são pretos que algum determinado é preto. Isso não é verdade. Se só sabemos que alguns são pretos, ao tomarmos um exemplo em particular, não podemos concluir que ele necessariamente é preto. Podem ser verdadeiras simultaneamente as frases "Alguns cachorros são pretos", "Snoopy é um cachorro" e "Snoopy não é preto". É diferente no caso do Exemplo 8.1, onde derivamos que a partir de "todos", um exemplo em particular tinha determinada propriedade.

O problema no segundo silogismo é que as hipóteses e a conclusão nada dizem uma sobre as outras. Ou seja, tais frases podem ser verdadeiras ou falsas em conjunto.

Imprecisão

Slide 134

Um dos problemas com silogismos é que eles são feitos em linguagem corriqueira (no nosso caso, em Português). Isso muitas vezes pode ocasionar problemas como no próximo exemplo:

Exemplo 8.6.
- Quanto mais queijo suíço, mais buracos há nele;
- Quanto mais buracos houver num pedaço de queijo, menos queijo há em tal pedaço;
- Logo, quanto mais queijo, menos queijo.

Slide 135

Exemplo 8.7.
- Todo cavalo raro é caro;
- Um cavalo barato é raro;
- Logo, um cavalo barato é caro.

Tais exemplos são exemplos de **sofismas**, que é algo em que aparentemente as regras lógica foram seguidas mas a conclusão é claramente falsa. O grande problema aqui é o uso da linguagem corriqueira. Se tentarmos dar um caráter mais formal (veremos mais adiante como fazer isso) aos conceitos de "mais", "menos", "caro", "barato" e "raro" que aparecem em tais exemplos, veremos que teremos problemas. Uma maneira de contornarmos tal problema é abandonar a linguagem corriqueira e usarmos uma linguagem própria, onde não sobre espaço para interpretações. Veremos como fazer isso nas próximas seções.

Paradoxo

Slide 136

Para finalizar, vamos mostrar como a linguagem coloquial não é adequada para desenvolver demonstrações. Considere a seguinte frase:

"Esta afirmação é falsa"

Note que não há como dizer que esta afirmação é verdadeira ou falsa, uma vez que se a considerarmos verdadeira, ela se diz falsa. E se a considerarmos falsa, teremos que ela é verdadeira. Tal problema ocorre porque tal frase faz uma **autorreferência**. Isso será algo a ser evitado quando formalizarmos nossa ideia de demonstração.

Slide 137

Um problema com autorreferência é que ela nem sempre é explícita. Por exemplo, considere N o conjunto de todos os números naturais em podem ser descritos com até 100 palavras em português. Por, exemplo, 1 pertence a esse conjunto (a palavra "um" atesta isso). E também 10^{1000} já que "10 elevado a mil" também atesta. Mas note que a quantidade de palavras é finita e que, portanto, as possiveis combinações destas finitas palavras em grupos de 100 também é finito. Ou seja, o conjunto N claramente é finito e, portanto, diferente de $\mathbb{N}$ - o conjunto de todos os naturais. Dessa forma, podemos tomar n como "o menor elemento que não está em N". O que, traduzindo, pode ser escrito como "o menor elemento que não pode ser descrito com menos de 100 palavras". Note que, desta forma, acabamos de descrever n com menos de 100 palavras e portanto ele está em N.

Proposições

Slide 138

Vamos começar a ver agora como representar afirmações usando uma simbologia mais apropriada. Começamos simplesmente trocando as afirmações por letras. Isso, entre outras vantagens, vai nos ajudar a ver quais coisas seguem da estrutura com que estamos mexendo, já que o que cada afirmação quer dizer fica de lado.

É preciso deixar claro que o que veremos aqui é um enfoque bastante simplificado. Para quem tiver curiosidade sobre o assunto, recomendamos [**?**] sobre esse assunto.

Vamos começar com o que vem a ser uma **proposição simples**. Intuitivamente, ela é uma afirmação qualquer que possui sentido por si só. O melhor é explicar por exemplos:

Exemplo 8.8. "Existe um cachorro branco" é uma proposição simples, assim como "$7 > 4$", "o Sol é uma estrela" ou mesmo "$5 > 10$". Note que não pedimos que uma proposição seja verdadeira.

Por outro lado, "camisa" não é uma proposição simples, já que ela não afirma nada sobre coisa alguma.

Slide 139

As proposições simples representaremos por letras, normalmente $p, q, r...$ De posse das proposições simples, vejamos o que é uma **proposição composta**. Esta nada mais é do que uma ou mais proposições (simples ou já compostas) utilizando-se pelo menos um **conectivo**. Os conectivos comumente usados são (mas outros podem ser utilizados também):

- $\neg$ (negação);
- $\wedge$ (e);
- $\vee$ (ou);
- $\rightarrow$ (implicação);
- $\leftrightarrow$ (bi-implicação).

Slide 140

Por exemplo, se p e q são proposições, então $p \vee q$ também é. Assim como $p \to q$ ou $\neg q$. No caso em que já temos proposições compostas, utiliza-se parênteses para evitar ambiguidades. Por exemplo, $(p \vee q) \wedge (\neg s)$. Mas qual a interpretação que devemos dar a esses conectivos? A negação serve para quando queremos o contrário de uma afirmação. Isto é, $\neg p$ é verdadeira se, e somente se, p é falsa. O conectivo $\wedge$ serve para indicar que ambas as proposições devem ser verdadeiras. Isto é, $p \wedge q$ é verdadeira se, e somente se, p e q são verdadeiras simultaneamente.

Tabela verdade

Slide 141

Um jeito fácil de definir um conectivo é por meio de uma **tabela verdade**. Vejamos os dois exemplos anteriores:

p	$\neg p$
V	F
F	V

Slide 142

p	q	$p \wedge q$
V	V	V
V	F	F
F	V	F
F	F	F

Ou

Slide 143

Nas primeiras colunas, estão indicados todos os possíveis valores de p e q, enquanto na última, indicamos os correspondentes valores com o conectivo. Note que, de fato, $p \wedge q$ só é verdadeira quando ambas p e q o são também. Vejamos o conectivo $\vee$. Queremos que $p \vee q$ só seja falso quando ambos p e q forem falsos, isto é, basta um deles ser verdadeiro para que $p \vee q$ seja verdadeiro (veja nos exercícios sobre outra intepretação de "ou", que chamaremos de "ou exclusivo"). Assim, a tabela fica

p	q	$p \vee q$
V	V	V
V	F	V
F	V	V
F	F	F

Slide 144

A tabela da bi-implicação também é simples, basta que os valores de p e q sejam idênticos para que a bi-implicação seja verdadeira:

p	q	$p \leftrightarrow q$
V	V	V
V	F	F
F	V	F
F	F	V

Slide 145

Já a implicação muitas vezes causa confusão. Quando que a implicação $p \to q$ é verdadeira? Neste caso, é mais fácil pensar quando ela é falsa. Ela só é falsa no caso em que p é verdadeiro e q é falso. De modo que todos os outros casos são verdadeiros. Assim, a tabela fica:

p	q	$p \to q$
V	V	V
V	F	F
F	V	V
F	F	V

Note que as duas últimas linhas da tabela podem causar estranhamento. Mas um argumento em favor delas é "se p é falsa, então não importa o que aconteça com q, ainda temos que $p \to q$".

Slide 146

Tabelas verdade não precisam conter apenas um conectivo, nem precisam ter apenas 3 colunas. Muitas vezes diversas colunas nos ajudam a encontrar quando uma certa proposição composta é verdadeira ou não. Por exemplo:

p	q	$\neg q$	$p \wedge (\neg q)$
V	V	F	F
V	F	V	V
F	V	F	F
F	F	V	F

Slide 147

Observe o seguinte exemplo:

p	q	$p \to q$	$(\neg q) \to (\neg p)$
V	V	V	V
V	F	F	F
F	V	V	V
F	F	V	V

Note que as duas últimas colunas são idênticas. Nesse caso, dizemos que $(p \to q)$ e $((\neg q) \to (\neg p))$ são **equivalentes**. Isto é, elas tem o mesmo comportamento, não importa quais os valores de p e q. Num certo sentido, escrever a primeira proposição é o mesmo que escrever a segunda.

Slide 148

Vejamos mais um exemplo de equivalência:

p	q	$p \to q$	$(\neg p) \vee q$
V	V	V	V
V	F	F	F
F	V	V	V
F	F	V	V

Slide 149

Terminamos com um outro tipo de proposição:

p	$\neg p$	$p \vee (\neg p)$
V	F	V
F	V	V

Note a última coluna. Não importa se p é verdade ou não, $p \vee (\neg p)$ é sempre verdade. Proposições que são sempre verdadeiras, independente de seus significados, são ditas **tautologias**.

Alongamentos da Aula 8

Alongamento 8.1. Para tentar resolver o problema do queijo, tente ver que um dos "mais" indica um sentido absoluto, enquanto o outro indica um sentido relativo (numa conotação de densidade). Tente deixar as frases mais específicas de forma a deixar clara a falha do silogismo.

Alongamento 8.2. Faça a tabela verdade do **ou exclusivo**, isto é, $p \dot{\vee} q$ é verdadeiro caso p ou q sejam verdadeiros mas não ambos ao mesmo tempo.

Alongamento 8.3. Construa uma tabela verdade para cada uma das proposições abaixo:

(a) $p \vee (p \wedge q)$;

(b) $p \to (\neg q)$;

(c) $\neg(p \to q)$;

(d) $p \vee (q \vee r)$;

(e) $p \to (q \to r)$.

Exercícios da Aula 8

Exercício 8.1. Numa ilha existem duas portas, cada uma vigiada por um guardião. Uma porta vai para o céu e a outra vai para o inferno. Sabe-se também que um dos guardiões sempre fala a verdade e que o outro sempre fala a mentira (mas não se sabe quem guarda qual porta). Supondo que você queira ir para o céu e que só tem direito a fazer uma pergunta aos guardiões (uma para ambos, não para cada), que pergunta fazer para descobrir qual a porta certa?

Exercício 8.2. Sejam a, b e c números reais. Vamos considerar as seguintes afirmações p, q, r, s, t e u:

- p: $a > b$
- q: $a < b$
- r: $a < c$
- s: $a > c$
- t: $b < c$
- u: $b > c$.

Use [29] conectivos para compor essas proposições de forma a obter uma que signifique:

(a) $a = b$;

(b) $a \neq b$;

(c) $a \geq b$;

(d) $a < b < c$;

(e) c está entre a e b e é diferente de ambos.

Exercício 8.3. Escreva uma proposição equivalente a $p \wedge q$ só usando os seguintes símbolos: $p, q, \neg, \vee$ e parênteses.

Exercício 8.4. Mostre que proposição $(p \to q) \leftrightarrow ((\neg p) \vee q)$ é uma tautologia.

Exercício 8.5. Um conectivo é dito binário se ele recebe duas proposições (por exemplo, $\wedge$ e $\vee$ são binários, enquanto $\neg$ é unário - pois só recebe uma proposição). Quantos conectivos binários não equivalentes entre si podem ser definidos?

[29] As proposições obtidas não vão seguir diretamente das afirmações aqui - para obter a interpretação correta, você pode usar coisas como "se x, y são reais, então $x \leq y$ ou $y \leq x$".

Aula 9

Quantificando

Slide 150

Com o que fizemos até agora, não trabalhamos com muita comodidade sobre frases do tipo "todos os cachorros são brancos" ou "existe pelo menos um pássaro amarelo". Nossa única escolha seria tratar tais frases como proposições simples. O problema aparece quando tentamos usar os conectivos. Vamos a um exemplo para mostrar um dos possíveis problemas. Suponha que numa fazenda só existam vacas pretas e vacas brancas. Suponha que temos duas proposições:

- p: "todas as vacas são pretas";
- q: "todas as vacas são brancas".

Como construir uma proposição que indique o que há na fazenda a partir destas duas?

Na linguagem coloquial, apareceu um "e". Mas se tentamos usar $p \wedge q$, obtemos uma proposição que diz que todas as vacas são pretas e brancas (malhadas?). Não é o que queremos. Se tentamos usar o $\vee$, temos ainda outro significado. $p \vee q$ quer dizer que todas as vacas são pretas ou que todas as vacas são brancas. Ou seja, isso só é verdade se todas as vacas forem pretas, ou se todas as vacas forem brancas (ou se todas forem brancas e pretas ao mesmo tempo). Novamente, não é isso que gostaríamos. Vamos mostrar aqui um método que faz com que os "quantificadores" (todos, algum, nenhum etc.) tenham um comportamento parecido com os conectivos, isto é, que possamos trabalhar com eles mesmo sem nos preocuparmos com seus significados.

Quantificadores

Slide 151

Os quantificadores com os quais trabalharemos são dois $\exists$ (existe) e $\forall$ (para todo). Para usar quantificadores, precisamos da noção de variável. Variável fará o papel do objeto em nossas proposições, podendo representar números, conjuntos, vacas etc. Usaremos letras para variáveis, por exemplo x, y, z, mas muitas vezes usaremos letras indexadas, como v_1, v_2 etc. Comecemos com um exemplo. Considere a frase "x é branco". Por enquanto, não temos ideia do que x possa ser, então não temos como dizer se tal frase é verdadeira ou não. Vejamos como fica depois do uso de um quantificador "$(\forall x\ x$ é branco)". Se combinarmos que nossas variáveis podem representar as vacas de nosso exemplo, esta frase é lida como "todas as vacas são brancas". O que, no nosso exemplo, é falso. Vamos usar uma notação um pouco mais simbólica. A frase "x é branco", indica uma propriedade sobre x (ainda que não saibamos o que x possa ser). E x é a única variável nessa frase. Assim, vamos indicar "x é branco" por $B(x)$. Desta forma, a frase acima fica $(\forall x\ B(x))$. Podemos indicar também a frase "x é preto" por $P(x)$. Desta forma, podemos tratar $B(x)$ e $P(x)$ como proposições e trabalhar como fizemos na seção anterior, isto é, utilizar os conectivos. Qual a ideia do sentido de $\forall x$? Ele significa que para qualquer x que tomarmos, a proposição que vem a seguir deve ser verdadeira. Assim, se x representa uma vaca, para que a frase original seja verdadeira devemos exigir que valha $B(x) \vee P(x)$ (note que não é $B(x) \wedge P(x)$ - nesse caso teríamos que cada x, isto é, que cada vaca, fosse branca e preta ao mesmo tempo). Assim, nossa frase em notação simbólica fica $(\forall x(B(x) \vee P(x)))$. Aproveitando o exemplo, para dizer que há pelo menos uma vaca branca, podemos escrever $(\exists x\ B(x))$.

Resumindo, temos:

- $(\forall x\ A(x))$ quer dizer que, para cada valor para x, a afirmação $A(x)$ é verdadeira;
- $(\exists x\ A(x))$ quer dizer que há pelo menos um valor para x de forma que $A(x)$ seja verdadeira.

Note que o $A(x)$ pode ser algo "composto" como $(B(x) \vee P(x))$.

Exemplo

Slide 152

Considere as seguintes propriedades sobre números reais:

- $P(x)$ dada por "$x \geq 0$";
- $N(x)$ dada por "$x \leq 0$".

Se queremos dizer que há um número real positivo (não estrito), podemos simplesmente escrever $(\exists x\ P(x))$. Se queremos dizer que todo número real é positivo ou negativo, podemos dizer $(\forall x\ (P(x) \vee N(x)))$. Se quisermos dizer que existe um que é positivo e negativo ao mesmo tempo (o 0 tem essa propriedade), podemos dizer $(\exists x(P(x) \wedge N(x)))$. Podemos também dizer que todo número que não for negativo é positivo: $(\forall x((\neg N(x)) \rightarrow P(x)))$.

Mais de um quantificador

Slide 153

É claro que podemos usar conectivos em fórmulas que já possuam quantificadores. Fazemos isso mantendo os mesmos valores de verdadeiro ou falso que apresentamos na seção anterior. Por exemplo: $(\forall x P(x)) \vee (\forall y B(y))$ só é verdade se for verdade que todos os valores de x satisfazem $P(x)$ ou que todos os valores de y satisfazem $B(y)$ ou ambas as coisas.

Podemos também quantificar sobre fórmulas já quantificadas. Para isso, precisaremos de propriedades sobre mais de uma variável. Façamos um exemplo. Considere a propriedade sobre x, y dada por $M(x, y)$ significando $x > y$. Se x, y vão simbolizar números reais, precisamos dizer quais exatamente: se algum, se todos etc. Começamos com a seguinte fórmula $(\exists x M(x, y))$. Com isso que queremos dizer que algum x é maior que y. Mas qual o valor de y? Resolvemos isso com o uso de outro quantificador.

Slide 154

Vejamos algumas possibilidades:

(a) $(\exists y(\exists x M(x, y)))$;

(b) $(\forall y(\forall x M(x, y)))$;

(c) $(\exists y(\forall x M(x, y)))$;

(d) $(\forall y(\exists x M(x, y)))$;

(e) $(\forall x(\exists y M(x, y)))$.

Vejamos o significado de cada uma das fórmulas acima. (a) simplesmente diz que há um y e um x de forma que $x > y$. E, de fato, tal frase é verdadeira (basta tomarmos $x = 1$ e $y = 0$). Já (b) diz que para qualquer y e qualquer x que tomarmos, teremos que $x > y$. Essa frase é falsa, pois para ser verdadeira deveria valer para qualquer valor de x e y que tomássemos (e ela é falsa se tomarmos $x = 0$ e $y = 1$). O item (c) significa que existe algum y que é menor que qualquer x (o que é falso), enquanto que o item (d) diz que para qualquer y que tomarmos, existe algum x que é maior que y (que é verdade). Note que a única diferença entre o item (e) e o item (c) é a ordem em que os quantificadores foram colocados. Mas isso apresenta diferença de significado. O item (e) diz que para todo x, existe um y que é menor que ele (o que é verdade, ao contrário do que diz o item (c)).

Negando quantificadores

Slide 155

A negação de quantificadores costuma causar um pouco de confusão. Considere a fórmula

$$(\forall x P(x)).$$

Estamos afirmando que todo x satisfaz a propriedade P. Então o que significa

$$\neg(\forall x P(x))?$$

Simplesmente ela quer dizer que não é verdade que todo x satisfaz a propriedade P. Isto é, que é verdade que

$$(\exists x(\neg P(x))).$$

O que é muito diferente de

$$(\forall x(\neg P(x)))$$

que simplesmente diz que todos os valores de x não satisfazem P.

Slide 156

Por outro lado, dizer que

$$\neg(\exists x P(x))$$

é o mesmo que afirmar que não é verdade que algum x satisfaz a propriedade P. Isto é, para qualquer valor de x, $P(x)$ não é satisfeito. Isto é, tal afirmação é equivalente a

$$(\forall x(\neg(P(x)))).$$

Ou seja, para negar um quantificador basta "trocar o mesmo e negar o que vem depois".

Exemplo

Slide 157

Comecemos com a negação a da seguinte fórmula[30]

$$(\forall x(\exists y(x < y))).$$

Vamos utilizar o método descrito acima, sem nos preocupar com o sinificado. Ou seja, começamos escrevendo a negação da fórmula:

$$\neg(\forall x(\exists y(x < y))).$$

Daí negamos o primeiro quantificador (o segundo fica "aguardando"):

$$(\exists x(\neg(\exists y(x < y)))).$$

Agora negamos o segundo:

$$(\exists x(\forall y\ \neg(x < y)))$$

. Ou seja, nossa primeira fórmula significava que "para todo x existe um y que é maior que ele". Negando isso, obtemos pelo método acima descrito uma fórmula que significa "existe um x que para qualquer y que tomamos, não é verdade que $x < y$". Note que, de fato, a última afirmação descreve exatamente o contraexemplo necessário para dizer que a afirmação original era falsa.

Demonstrações

Slide 158

Informalmente, uma demonstração é uma sequência de afirmações, sendo que cada uma é consequência das anteriores ou é algo sabidamente verdadeiro. Vamos examinar isso mais de perto. Como dizer que algo é consequência de outras coisas? Para não deixar dúvidas, deixaremos claro o que entendemos por isso. Diremos que B é consequência de afirmações anteriores se dentre as anteriores tivermos uma afirmação do tipo A e uma do tipo $A \to B$. Tal regra é comumente resumida da seguinte forma[31]:

Slide 159

$$\frac{\begin{array}{l}A \\ A \to B\end{array}}{B}$$

A interpretação disso é "se sabemos que A vale e que toda vez que A vale, B vale, então B vale"[32].

Exemplo 9.1. Vamos mostrar que $A \to B$ e $B \to C$ implicam que $A \to C$. O que queremos mostrar é que toda vez que ocorre A, ocorre C. Isso, quando vale tanto $A \to B$ como $B \to C$. Isto é, vamos assumir que valem A, $A \to B$ e $B \to C$ e ver se conseguimos mostrar que vale C. Do fato que A e $A \to B$ valem, temos que B vale. Do fato que B e $B \to C$ valem, temos que vale C. Ou seja, obtemos o que desejávamos.

Axiomas

Slide 160

Mas e a parte do "sabidamente verdadeiro"? O que algumas pessoas acham que é verdadeiro, outras podem achar que não é. Assim, teremos que ser bastante precisos com o que podemos supor verdadeiro ou não. Primeiramente, é claro que podemos supor verdadeiras tudo o que for logicamente verdadeiro, como as tautologias - lembre que elas são verdadeiras independentemente de qualquer coisa. Mas e o resto? O resto é o que vamos chamar de axiomas.

Um **axioma** é uma afirmação que vamos supor verdadeira. O uso disso em geral é o seguinte: queremos definir uma determinada coisa, dizemos quais os axiomas que isso satisfaz e daí deduzimos tudo o que podemos a partir de tais axiomas. Ou seja, tudo aquilo que satisfizer tais axiomas, vai satisfazer suas consequências também. Vamos dar a seguinte definição como exemplo:

Exemplo

Slide 161

Definição 9.2. Dizemos que uma relação $\preceq$ é uma **relação de ordem** sobre um conjunto A se são satisfeitas as seguintes condições[33]:

(a) $\forall a \in A \ (a \preceq a)$ (reflexiva);

(b) $\forall a \in A \ \forall b \in A \ (a \preceq b \wedge b \preceq a) \to a = b$ (antissimétrica);

(c) $\forall a \in A \ \forall b \in A \ \forall c \in A((a \preceq b \wedge b \preceq c) \to a \preceq c)$ (transitiva).

[30] Vamos escrever as propriedades necessárias já dentro das fórmulas, para facilitar a leitura. Se tiver dificuldades, escreva-as separadamente como vínhamos fazendo.

[31] Essa regra é conhecida como *modus ponens*. Veja o Exercício 9.3

[32] Formalmente, precisamos de mais regras que envolvem substituição de variáveis. Por exemplos, precisamos poder deduzir $\forall x \ P(x)$ a partir de $\forall y \ P(y)$ - mas não seremos tão formais neste texto.

[33] Vamos começar a usar quantificacores "restritos", isto é, em vez de dizer $\forall x$, diremos $\forall x \in X$. A leitura é simplesmente "para todo x que for elemento de X temos...". Uma maneira de formalizar isso seria toda vez escrever "$\forall x((x \in X) \to ...$", mas isso deixaria a leitura mais complicada. Deixaremos de lado também alguns parênteses quando isso não gerar dúvidas

Os itens (a), (b) e (c) são os axiomas de ordem. Para dizermos que uma determinada relação é uma ordem, ela tem que satisfazer tais axiomas. Por outro lado, tudo que provarmos para uma relação de ordem, vai valer para qualquer relação que satisfaça tais axiomas.

Quando queremos indicar que $a \leq b$ mas $a \neq b$, usamos $a < b$ - nesse caso, muitas vezes nos referenciamos a $<$ como "ordem estrita".

Slide 162

Um exemplo de uma ordem sobre um conjunto é a relação $\leq$ sobre os números reais. Verificamos isso simplesmente notando que para qualquer $x \in \mathbb{R}$, temos $x \leq x$; que para todo $x \in \mathbb{R}$ e todo $y \in \mathbb{R}$, se $x \leq y$ e $y \leq x$, então $x = y$; e, por fim, que para qualquer $x \in \mathbb{R}$, qualquer $y \in \mathbb{R}$ e qualquer $z \in \mathbb{R}$, temos que $x \leq y$ e $y \leq z$, então $x \leq z$.

Outro exemplo

Slide 163

Um outro exemplo de ordem, um tanto diferente, é o seguinte:
Exemplo 9.3. Considere a relação $|$ sobre os números naturais maiores que 0 dada por $m|n$ se "m divide n". Note que tal relação também é uma relação de ordem. De fato:

(a) $m|m$ para todo $m \in \{k \in \mathbb{N} : k > 0\}$, já que m divide m se $m \neq 0$;

(b) Se m divide n e n divide m, temos que, necessariamente, $m = n$;

(c) Se m divide n e n divide k, então m divide k.

Na verdade, voltaremos a este exemplo mais tarde e poderemos provar a última afirmação.

Como mostramos a Proposição **??** para qualquer ordem, obtemos o mesmo resultado em particular para $|$. Qual a interpretação do resultado neste caso?

Mínimo

Slide 164

Considere a seguinte definição:
Definição 9.4. Seja $\preceq$ uma ordem sobre A. Dizemos que $a \in A$ é um **mínimo** de A se vale $a \preceq b$ para todo $b \in A$.

Poderíamos nos perguntar se a existência de um mínimo é consequência dos axiomas de ordem. Isto é, se podemos provar a partir de tais axiomas a seguinte proposição:

$$\exists a \in A \ \forall b \in A \ a \preceq b.$$

Independência

Slide 165

A resposta para isso é que não. Não podemos provar tal proposição a partir de tais axiomas. Mas então alguém poderia dizer que se não podemos provar tal afirmação, deveríamos poder provar sua negação. Mas isso também não é verdade. Não podemos provar tal afirmação nem sua negação. E como provar isso? (que não podemos provar). Isso é simples. Suponha que pudéssemos provar tal afirmação. Então todas as relações que satisfaçam os axiomas de ordem devem satisfazer tal afirmação também. Por outro lado, se pudéssemos provar sua negação, então todas as relações que satisfaçam os axiomas de ordem deve satisfazer tal negação também. Ou seja, se mostrarmos uma relação de ordem que satisfaça

a existência de mínimo e uma outra que não satisfaça (isto é, que satisfaça sua negação) teremos que nem a existência nem sua negação podem ser consequências dos axiomas de ordem. Este é o caso em que dizemos que uma afirmação é **independente** de certa coleção de axiomas.
Exemplo 9.5. Note que 1 é um mínimo na ordem $|$ sobre $\{n \in \mathbb{N} : n > 0\}$ já que $1|b$ para todo $b \in \mathbb{N} \setminus \{0\}$. Ou seja, $|$ é uma ordem que admite mínimo. Por outro lado, $\leq$ é uma ordem sobre $\mathbb{R}$ que não admite mínimo. Basta notar que, para qualquer $x \in \mathbb{R}$, $\neg(x \leq (x-1))$.

Exercícios da Aula 9

Exercício 9.1. Considere as seguintes propriedades sobre cachorros:

- $B(x)$, "x é branco";
- $P(x)$, "x é preto";
- $R(x)$, "x é rápido";

Só utilizando as propriedades acima, quantificadores e conectivos, escreva fórmulas que afirmem:

(a) Há pelo menos um cachorro branco;

(b) Todo cachorro preto é rápido.

(c) Nenhum cachorro branco é rápido.

(d) Negue a fórmula obtida no item (a). O que ela quer dizer?

Exercício 9.2. Escreva a fórmula que diz que a função $f : \mathbb{R} \to \mathbb{R}$ é contínua no ponto x_0 só usando símbolos.

Exercício 9.3. Monte uma tabela verdade que justifique o *modus ponens*. Isto é, com entradas p e q, verifique que a única linha em que p e $p \to q$ tem valores verdadeiros é a linha em que q também é verdade.

Exercício 9.4. Considere $\preceq$ uma ordem sobre A. Seja $B \subset A$. Defina em B a seguinte relação, para qualquer $x, y \in B$, $x \preceq^* y$ se, e somente se, $x \preceq y$. Mostre que $\preceq^*$ é uma ordem sobre B. Esta é chamada de **restrição** de $\preceq$ a B (em geral, denotamos as duas ordens com o mesmo símbolo).

Exercício 9.5. Mostre que $\preceq$ dada por, para $(a, b), (c, d) \in \mathbb{R}^2$, $(a, b) \preceq (c, d)$ se, se somente se

$$(a < c) \vee (a = c \wedge b \leq d)$$

é uma ordem sobre $\mathbb{R}^2$. Esta ordem é chamada de **ordem lexicográfica**.

Exercício 9.6. Mostre que $\subseteq$ é uma relação de ordem sobre o conjunto de todos os subconjuntos de um conjunto X fixado.

Exercício 9.7. Mostre que a seguinte afirmação é independente dos axiomas de ordem:

$$\forall a \in A \; \forall b \in A \; (a \prec b \to (\exists c \in A \; a \prec c \wedge c \prec b))$$

Exercício 9.8. Aplique nosso método de negação de fórmulas para escrever a fórmula que diz "A não tem mínimo".

Exercício 9.9. Negue a fórmula que diz que uma função $f : \mathbb{R} \to \mathbb{R}$ não é contínua num ponto x_0. Dê um exemplo de uma função não contínua no ponto 1 e mostre que, de fato, ela não é contínua.

Exercício 9.10. Suponha que $\prec$ é uma ordem sobre A e que tal ordem tem um mínimo. Mostre que tal mínimo é único. Isto é, suponha a é um mínimo e suponha que b também seja. Mostre que $a = b$.

Aula 10

Números naturais

Slide 166

Vamos começar dando uma definição axiomática para os números naturais. Posteriormente, mostraremos como definir em tal conjunto as operações básicas, como a soma e a multiplicação.

Depois, mostraremos como usar os naturais para definir outros conjuntos importantes em matemática, como os inteiros e os racionais. Ou seja, de certa forma, vamos mostrar como fundamentar parte da matemática assumindo apenas algumas afirmações sobre números naturais.

Axiomas de Peano

Slide 167

Para escrever tais axiomas, usaremos, além dos símbolos usuais já descritos, os seguintes símbolos: 0 (zero) e s (sucessor)[34].

(a) $0 \in \mathbb{N}$;

(b) $\forall n \in \mathbb{N}\ s(n) \in \mathbb{N}$;

(c) $\forall n \in \mathbb{N}\ s(n) \neq 0$;

(d) $\forall n \in \mathbb{N}\ \forall m \in \mathbb{N}\ s(n) = s(m) \to n = m$;

(e) Seja $P(x)$ uma propriedade sobre elementos de $\mathbb{N}$. Se valem

(i) $P(0)$;

(ii) $\forall n \in \mathbb{N}\ P(n) \to P(s(n))$;

Então vale $P(n)$ para todo $n \in \mathbb{N}$.

O axioma (e) é conhecido como **princípio de indução**. O conjunto $\{0, 1, 2, ...\}$ satisfaz as propriedades acima se interpretamos o símbolo $s(n)$ como $n+1$. Para notar que vale o princípio de indução em tal conjunto, suponha que não vale[35]. Então existe n o menor tal que não vale $P(n)$. Note que tal n não pode ser o 0 já que temos que vale $P(0)$. Sabemos então que $n = m + 1$ para algum $m \in \{0, 1, 2, ...\}$. Como $m < n$, temos que vale $P(m)$. Logo, vale $P(s(m))$. Mas $P(s(m)) = P(m + 1) = P(n)$, contradição.

Consequências

Slide 168

Agora vamos começar a ver algumas consequências de tais axiomas. Ou seja, propriedades que os números naturais também tem e que decorrem do fato deles satisfazerem os axiomas de Peano.

O primeiro resultado basicamente diz que, ao tomarmos sucessores, nunca voltamos ao próprio elemento:

Proposição 10.1. *Temos que $s(n) \neq n$ para todo $n \in \mathbb{N}$.*

Demonstração. Vamos provar isso por indução. Ou seja, para concluirmos o que queremos, basta mostrarmos, utilizando o princípio de indução, que a fórmula $P(x)$ vale para todo $x \in \mathbb{N}$, onde $P(x)$ é "$s(x) \neq x$". Para mostrar isso por indução, precisamos mostrar que vale $P(0)$ e que se vale $P(n)$ vale $P(s(n))$. Note que $0 \neq s(0)$ já que $0 \in \mathbb{N}$ (por (a)) e, portanto, $s(0) \neq 0$ por (c).

[34] Basicamente estes axiomas dizem: 0 é um número natural; se algo é um número, seu sucessor também é; 0 não é sucessor de ninguém; se dois números tem o mesmo sucessor, eles são iguais e, finalmente, que vale a indução.

[35] Basicamente o que estamos fazendo aqui é provar que se todo conjunto não vazio admite mínimo, então vale indução.

Agora suponha que vale $P(n)$ para algum n. Ou seja, vale $n \neq s(n)$. Vamos mostrar que vale $P(s(n))$, isto é, $s(n) \neq s(s(n))$. Suponha que não, isto é, que vale $s(n) = s(s(n))$. Por (d), temos que $n = s(n)$, contrariando nossa hipótese. □

Slide 169

O próximo resultado diz que, com exceção do 0, todo natural é sucessor de outro natural:

Proposição 10.2. *Se $n \in \mathbb{N}$ e $n \neq 0$, então existe $m \in \mathbb{N}$ tal que $n = s(m)$.*

Demonstração. Novamente, vamos mostrar por indução. Ou seja, vamos mostrar que vale a fórmula $P(x)$ para todo $x \in \mathbb{N}$ onde $P(x)$ é a fórmula

$$x \neq 0 \to \exists m\ x = s(m).$$

Note que $0 \neq 0 \to \exists m\ 0 = s(m)$ simplesmente porque não vale $0 \neq 0$ (não importa que também não valha o lado direito da implicação).

Slide 170

Agora suponha que vale $P(n)$ para algum n. Isto é, para tal n vale:

$$n \neq 0 \to \exists m\ n = s(m).$$

Precisamos mostrar então que vale $P(s(n))$. Isto é, precisamos mostrar que, se vale $s(n) \neq 0$ (o que vale!), então vale que existe m tal que $s(n) = s(m)$. Considere $m = n$. Note que, então $s(n) = s(m)$ como queríamos. □

A soma nos naturais

Slide 171

Vejamos agora como definir a operação de soma $(+)$ sobre os naturais:
Definição 10.3. Chamamos de **soma** nos naturais (ou **adição**) uma função $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ tal que sejam satisfeitas:

(a) $\forall a \in \mathbb{N}\ f(a, 0) = a$;

(b) $\forall a \in \mathbb{N}\ \forall b \in \mathbb{N}\ f(a, s(b)) = s(f(a, b))$.

Consequências

Slide 172

Vamos ver que, na verdade, existe uma única função f que satisfaz os axiomas acima. Antes, vamos provar algumas propriedades que qualquer função que satisfaz tais axiomas vai satisfazer:
Lema 10.4. *Seja $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ uma soma sobre $\mathbb{N}$. Então, dado $a \in \mathbb{N}$, temos que $f(0, a) = a$.*

Demonstração. Vamos mostrar a afirmação $P(x)$ dada por

$$f(0, x) = x$$

por indução.

$P(0)$**:** Temos que $f(0, 0) = 0$ pelo axioma (a) de adição.

$P(n) \to P(s(n))$**:** Suponha que $f(0, n) = n$ e vamos provar que $f(0, s(n)) = s(n)$. Temos, por (b), que $f(0, s(n)) = s(f(0, n)) = s(n)$.

□

Slide 173

Lema 10.5. *Seja $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ uma soma sobre $\mathbb{N}$. Então, dados $a, b \in \mathbb{N}$, temos que $f(a, s(b)) = f(s(a), b)$*

Demonstração. Seja $a \in \mathbb{N}$. Considere a seguinte afirmação $P(x)$ para $x \in \mathbb{N}$:

$$f(a, s(x)) = f(s(a), x).$$

Note que se $P(x)$ for verdadeira para todo $x \in \mathbb{N}$, temos o resultado desejado (já que o a é qualquer). Vamos mostrar $P(x)$ por indução.

$P(0)$: Temos $f(a, s(0)) = s(f(a, 0)) = s(a)$. Por outro lado, $f(s(a), 0) = s(a)$. Logo, temos $P(0)$.

Slide 174

$P(n) \to P(s(n))$: Suponha que vale $f(a, s(n)) = f(s(a), n)$ e vamos mostrar $f(a, s(s(n))) = f(s(a), s(n))$. Temos

$$\begin{aligned} f(a, s(s(n))) &= s(f(a, s(n))) \\ &= s(f(s(a), n)) \\ &= f(s(a), s(n)) \end{aligned}$$

□

Slide 175

Finalmente, podemos provar que qualquer função que satisfaça os axiomas de soma precisa ser comutativa:

Proposição 10.6. *Seja $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ uma soma sobre $\mathbb{N}$. Então, dados $a, b \in \mathbb{N}$, temos que $f(a, b) = f(b, a)$.*

Demonstração. Seja $a \in \mathbb{N}$. Considere a seguinte afirmação sobre $x \in \mathbb{N}$:

$$f(x, a) = f(a, x).$$

Vamos chamar tal afirmação de $P(x)$. Note que se mostrarmos $P(x)$ para todos os $x \in \mathbb{N}$, teremos o resultado desejado (já que o a é qualquer). Assim, vamos mostrar $P(n)$ por indução sobre $n \in \mathbb{N}$.

Slide 176

$P(0)$: Temos que $f(x, 0) = x$, pelo axioma (a) da definição de soma. Por outro lado, temos que $f(0, x) = x$ também (pelo Lema 10.4).

$P(n) \to P(s(n))$: Suponha que vale $f(n, a) = f(a, n)$ e vamos mostrar que $f(s(n), a) = f(a, s(n))$. Temos:

$$\begin{aligned} f(s(n), a) &\overset{10.5}{=} f(n, s(a)) \\ &= s(f(n, a)) \\ &= s(f(a, n)) \\ &= f(a, s(n)) \end{aligned}$$

□

Unicidade

Slide 177

Note que só dissemos duas condições sobre f, mas essas duas condições são suficientes para descrevê-la completamente, como atesta o seguinte resultado:

Proposição 10.7. *Suponha que $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ e $g : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ sejam duas adições sobre $\mathbb{N}$. Então, para quaisquer $a, b \in \mathbb{N}$ temos que $f(a, b) = g(a, b)$.*

Demonstração. Seja $a \in \mathbb{N}$. Considere $P(x)$ a seguinte afirmação para $x \in \mathbb{N}$:

$$f(a, x) = g(a, x).$$

Vamos mostrar tal afirmação por indução (note que isso é suficiente para o que queremos).

Slide 178

$P(0)$: Pelo axioma (a) da soma, temos que $f(a,0) = a = g(a,0)$.

$P(n) \to P(s(n))$: Vamos supor que vale $f(a,n) = g(a,n)$ e mostrar que vale $f(a,s(n)) = g(a,s(n))$. Temos $f(a,s(n)) = s(f(a,n)) = s(g(a,n)) = g(a,s(n))$. □

Notação

Slide 179

Assim, não há outra função sobre os naturais que satisfaça as condições impostas, além da soma usual que conhecemos.

Para manter a coerência com a notação usual, a partir deste momento adotaremos a notação $a+b$ no lugar da $f(a,b)$.

Mais consequências

Slide 180

Vejamos mais algumas propriedades sobre a soma:

Proposição 10.8. *Valem as seguintes propriedades:*

*(a) Dados $a,b \in \mathbb{N}$, temos $a+b = b+a$; (***comutativa***)*

*(b) Dados $a,b,c \in \mathbb{N}$, temos que $(a+b)+c = a+(b+c)$; (***associativa***)*

Demonstração. Note que o item (a) é simplesmente o que foi provado na Proposição 10.6.

Slide 181

Para o item (b), sejam $a,b \in \mathbb{N}$. Considere a seguinte afirmação $P(x)$ para $x \in \mathbb{N}$:

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

Vamos mostrar $P(x)$ por indução (note que isso é suficiente).

$P(0)$: $(a+b)+0 = a+b$, pelo axioma (a) da soma. Por outro lado, $a+(b+0) = a+b$, pelo mesmo axioma.

$P(n) \to P(s(n))$: Vamos supor que vale $(a+b)+n = a+(b+n)$ e vamos mostrar que $(a+b)+s(n) = a+(b+s(n))$. Temos

$$\begin{aligned}(a+b)+s(n) &= s((a+b)+n)\\ &= s(a+(b+n))\\ &= a+s(b+n)\\ &= a+(b+s(n))\end{aligned}$$

□

Slide 182

Proposição 10.9 (Lei do Cancelamento). *Sejam*[36] *$a,b,c \in \mathbb{N}$. Se $a+b = a+c$, então $b = c$.*

Demonstração. Sejam $b,c \in \mathbb{N}$. Considere $P(x)$ a seguinte afirmação para $x \in \mathbb{N}$:

$$(x+b = x+c) \to b = c.$$

Vamos mostrá-la por indução (note que isso é suficiente).

$P(0)$: Suponha que $0+b = 0+c$. Note que $0+b = b$ e que $0+c = c$. Logo, temos que $b = c$ como queríamos.

Slide 183

$P(n) \to P(s(n))$: Suponha que vale $(n + b = n + c) \to b = c$. Suponha que vale $s(n) + b = s(n) + c$. Logo, temos $b + s(n) = c + s(n)$. Pela axioma (b) da adição, temos $s(b + n) = s(c + n)$. Pelo axioma (d) dos naturais, temos que $b + n = c + n$. Logo, $n + b = n + c$ e, portanto, $b = c$. □

Mais notações

Slide 184

Finalmente, podemos passar a usar algumas notações mais usuais:
Definição 10.10. Vamos chamar de 1 o elemento $s(0)$ de $\mathbb{N}$. Também usaremos a notação usual para $s(1) = 2$, $s(2) = 3$...

Mais algumas consequências

Slide 185

Proposição 10.11. *Seja $a \in \mathbb{N}$. Então $s(a) = a + 1$.*

Demonstração. Considere $P(x)$ a seguinte afirmação para $x \in \mathbb{N}$:

$$s(x) = x + 1.$$

Vamos mostrá-la por indução.
$P(0)$: Temos $s(0) = 1$ por definição. Por outro lado, $0 + 1 = 1 + 0 = 1$.

Slide 186

$P(n) \to P(s(n))$: Suponha que vale $s(n) = n+1$ e vamos mostrar que vale $s(s(n)) = s(n)+1$. Temos

$$\begin{aligned} s(s(n)) &= s(n+1) \\ &= s(1+n) \\ &= 1 + s(n) \\ &= s(n) + 1 \end{aligned}$$

□

Dado o último resultado, daqui em diante muitas vezes utilizaremos a notação $n + 1$ no lugar da $s(n)$.

Exercícios da Aula 10

Exercício 10.1. Considere o seguinte argumento para mostrar que todos os cavalos são de uma mesma cor: Vamos mostrar que todos os cavalos tem apenas uma cor por indução sobre a quantidade de cavalos. Ou seja, $P(n)$ é a afirmação: Dada uma coleção de n cavalos, todos eles tem a mesma cor. É claro que temos que $P(0)$ vale (se não valesse, teria que ter um conjunto com 0 cavalos, sendo dois com cores diferentes). Agora vamos supor que vale $P(n)$ e mostrar $P(n + 1)$. Sejam $n + 1$ cavalos. Vamos mostrar que eles são todos de uma cor só. Pegue um dos cavalos e separe. Vamos chama-lo de a. Note que sobraram n cavalos. Pela nossa hipótese, os n cavalos são todos da mesma cor. Devolva o cavalo original e separe um outro qualquer (vamos chama-lo de b). Novamente ficamos com apenas n cavalos e, por hipótese, todos são da mesma cor. Assim, o cavalo a tem a mesma cor que os demais (diferentes de b). Mas, pela primeira passagem, o cavalo b tem a mesma cor que os demais. Ou seja, a e b tem a mesma cor, que é a cor dos demais. Logo, todos tem a mesma cor.

Qual o erro cometido acima?

Exercício 10.2. Note que, se tirarmos o axioma $s(n) \neq 0$ para todo $n \in \mathbb{N}$, teríamos que o conjunto $N = \{0\}$ também iria satisfazer todos os axiomas listados (colocando N no lugar de $\mathbb{N}$).

[36] Dá muita vontade "somar $-a$ dos dois lados" - mas note que a gente ainda nem tem o que é subtração (ou números negativos).

Aula 11

O produto nos naturais

Slide 187

Vamos agora, de forma semelhante ao que fizemos com a soma, definir o produto de naturais.

Definição 11.1. Chamamos de **produto** (ou de **multiplicação**) uma função $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ que satisfaz:

(a) $\forall a \in \mathbb{N}\ f(a, 0) = 0$;

(b) $\forall a \in \mathbb{N}\ \forall b \in \mathbb{N}\ f(a, s(b)) = a + f(a, b)$.

Unicidade

Slide 188

Da mesma forma que com a soma, o produto também é único:

Proposição 11.2. *Sejam $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ e $g : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ dois produtos sobre $\mathbb{N}$. Então, dados $a, b \in \mathbb{N}$, temos que $f(a, b) = g(a, b)$.*

Demonstração. Seja $a \in \mathbb{N}$. Considere $P(x)$ sendo $f(a, x) = g(a, x)$. Vamos mostrar $P(x)$ para todo $x \in \mathbb{N}$ por indução.

$P(0)$**:** Temos, pelo axioma (a) que $f(a, 0) = 0 = g(a, 0)$.

$P(n) \to P(s(n))$**:** Suponha que vale $f(a, n) = g(a, n)$ e vamos mostrar que vale $f(a, s(n)) = g(a, s(n))$. Temos

$$\begin{aligned} f(a, s(n)) &= a + f(a, n) \\ &= a + g(a, n) \\ &= g(a, s(n)) \end{aligned}$$

□

Notação

Slide 189

Dada a unicidade, denotaremos o único produto sobre os naturais por $\cdot$. Isto é, em vez de usarmos $f(a, b)$ usaremos $a \cdot b$. Muitas vezes omitiremos o $\cdot$ e usaremos simplesmente ab.

Consequências

Slide 190

Lema 11.3. *Seja $a \in \mathbb{N}$. Então $0 \cdot a = 0$.*

Demonstração. Considere $P(x)$ sendo $0 \cdot x = 0$. Vamos mostrar por indução.

$P(0)$**:** $0 \cdot 0 = 0$, pelo axioma (a).

$P(n) \to P(s(n))$**:** Suponha $0 \cdot n = 0$. Temos

$$\begin{aligned} 0 \cdot s(n) &= 0 + (0 \cdot n) \\ &= 0 + 0 \\ &= 0 \end{aligned}$$

□

Slide 191

Lema 11.4. *Sejam $a, b \in \mathbb{N}$. Então vale $s(b) \cdot a = a + (b \cdot a)$.*

Demonstração. Seja $b \in \mathbb{N}$. Considere $P(x)$ sendo $s(b) \cdot x = x + (b \cdot x)$. Vamos mostrar por indução. Temos:

$P(0)$: $s(b) \cdot 0 = 0$. Por outro lado, $0 + (c \cdot 0) = 0 + 0 = 0$.

Slide 192

$P(n) \to P(s(n))$: Suponha que vale $s(b) \cdot n = n + (b \cdot n)$. Temos

$$\begin{array}{rcl} s(b) \cdot s(n) & = & s(b) + (s(b) \cdot n) \\ & = & s(b) + (n + (b \cdot n)) \\ & = & (s(b) + n) + (b \cdot n) \\ & = & (b + s(n)) + (b \cdot n) \\ & = & s(n) + (b + (b \cdot n)) \\ & = & s(n) + (b \cdot s(n)) \end{array}$$

□

Slide 193

Proposição 11.5. *Valem as seguintes propriedades:*

*(a) Dados $a, b \in \mathbb{N}$, $a \cdot b = b \cdot a$; (***comutativa***)*

*(b) Dados $a, b, c \in \mathbb{N}$, $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$; (***distributiva***).*

*(c) Dados $a, b, c \in \mathbb{N}$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$; (***associativa***)*

Slide 194

Demonstração. Seja $a \in \mathbb{N}$. Considere $P(x)$ sendo $a \cdot x = x \cdot a$. Vamos mostrar por indução.

$P(0)$: Temos que $a \cdot 0 = 0 = 0 \cdot a$ (pelo Lema 11.3).

$P(n) \to P(s(n))$: Suponha $a \cdot n = n \cdot a$. Temos

$$\begin{array}{rcl} a \cdot s(n) & = & a + (a \cdot n) \\ & = & a + (n \cdot a) \\ & \overset{11.4}{=} & s(n) \cdot a \end{array}$$

Slide 195

Considere $P(x)$ sendo $a \cdot (b + x) = (a \cdot b) + (a \cdot x)$. Vamos mostrar por indução.

$P(0)$: $a \cdot (b + 0) = a \cdot b$. Por outro lado, $a \cdot b + a \cdot 0 = a \cdot b + 0 = a \cdot b$.

$P(n) \to P(s(n))$: Suponha que vale $a \cdot (b + n) = (a \cdot b) + (a \cdot n)$. Vamos mostrar $a \cdot (b + s(n)) = (a \cdot b) + (a \cdot (s(n))$. Temos:

$$\begin{array}{rcl} a \cdot (b + s(n)) & = & a \cdot (s(b + n)) \\ & = & a + (a \cdot (b + n)) \\ & = & a + ((a \cdot b) + (a \cdot n)) \\ & = & (a \cdot b) + (a + (a \cdot n)) \\ & = & (a \cdot b) + (a \cdot s(n)) \end{array}$$

Slide 196

Sejam $a, b \in \mathbb{N}$. Considere $P(x)$ sendo $(a \cdot b) \cdot x = a \cdot (b \cdot x)$. Vamos mostrar por indução.

$P(0)$: Temos que $(a \cdot b) \cdot 0 = 0$. Por outro lado, $a \cdot (b \cdot 0) = a \cdot 0 = 0$.

$P(n) \to P(s(n))$: Suponha que vale $(a \cdot b) \cdot n = a \cdot (b \cdot n)$. Temos

$$\begin{array}{rcl} (a \cdot b) \cdot s(n) & = & (a \cdot b) + ((a \cdot b) \cdot n) \\ & = & (a \cdot b) + (a \cdot (b \cdot n)) \\ & \overset{(dist.)}{=} & a \cdot (b + (b \cdot n)) \\ & = & a \cdot (b \cdot s(n)) \quad \square \end{array}$$

Slide 197

Proposição 11.6. *Sejam $a, b \in \mathbb{N}$. Se $a \cdot b = 0$, então $a = 0$ ou $b = 0$.*

Demonstração. Suponha $a \cdot b = 0$. Temos que mostrar $a = 0 \vee b = 0$. Suponha que $b \neq 0$. Vamos mostrar que então $a = 0$ (note que isso é suficiente). Como $b \neq 0$, existe $m \in \mathbb{N}$ tal que $s(m) = b$. Assim, temos que $a \cdot s(m) = 0$. Por outro lado, temos que $a \cdot s(m) = a + (a \cdot m)$. Assim, temos que $a + (a \cdot m) = 0$. Logo, $a = 0$ e $a \cdot m = 0$[37]. Em particular, temos que $a = 0$ como queríamos. □

Slide 198

Proposição 11.7. *Seja $a \in \mathbb{N}$. Então $1 \cdot a = a$.*

Demonstração. Considere $P(x)$ sendo $1 \cdot x = x$. Vamos mostrar por indução.

$P(0)$**:** Como $1 \cdot 0 = 0$, temos o resultado.

$P(n) \to P(s(n))$**:** Suponha que vale $1 \cdot n = n$. Temos:

$$\begin{aligned} 1 \cdot s(n) &= 1 + (1 \cdot n) \\ &= 1 + n \\ &= s(n) \end{aligned}$$

□

Slide 199

Para evitar o uso excessivo de parênteses, vamos utilizar as convenções usuais. Por exemplo, em vez de escrevermos $(a+b)+c$, escreveremos $a+b+c$ (já que pela associativa, não importa como interpretamos a última notação). Também usaremos o "critério de prioridade" do produto sobre a soma. Por exemplo, $ab + c$ deverá ser interpretado como $(a \cdot b) + c$.

Slide 200

Vamos agora definir a ordem sobre os naturais.

Definição 11.8. Dados $a, b \in \mathbb{N}$, vamos denotar por $a \leq b$ se existe $m \in \mathbb{N}$ tal que $a + m = b$. Esta é a **ordem** usual sobre $\mathbb{N}$.

Slide 201

Proposição 11.9. *A relação $\leq$ definida acima é de fato uma ordem sobre $\mathbb{N}$.*

Demonstração. Precisamos mostrar que valem os axiomas de ordem.

Reflexiva: Seja $a \in \mathbb{N}$. Como $a + 0 = a$, temos que $a \leq a$.

Antissimétrica: Sejam $a, b \in \mathbb{N}$ tais que $a \leq b$ e $b \leq a$. Vamos mostrar que $a = b$. Temos então que existe $m \in \mathbb{N}$ tal que $a + m = b$ e que existe $k \in \mathbb{N}$ tal que $b + k = a$. Logo, de $a + m = b$ temos que $(b + k) + m = b$. Assim $b + (k + m) = b + 0$. Logo, $k + m = 0$. Temos[38] que $k = m = 0$. Assim, de $a + m = b$ temos que $a = b$ como queríamos.

Slide 202

Transitiva: Sejam $a, b, c \in \mathbb{N}$ tais que $a \leq b$ e $b \leq c$. Vamos mostrar que $a \leq c$. Sejam $m, k \in \mathbb{N}$ tais que $a + m = b$ e $b + k = c$. Note que tomando $t = m + k$, temos

$$\begin{aligned} a + t &= a + (m + k) \\ &= (a + m) + k \\ &= b + k \\ &= c \end{aligned}$$

Logo, $a \leq c$. □

[37] Exercício 11.3

[38] Pelo Exercício 11.3.

Consequências

Slide 203

Os axiomas de ordem não implicam que, dados dois elementos quaisquer, eles precisam ser comparáveis. Mas, no caso desta ordem específica que apresentamos, isso vale:
Definição 11.10. Dizemos que uma ordem $\preceq$ sobre X é uma **ordem total** sobre X se, dados $a, b \in X$, temos que $a \preceq b$ ou $b \preceq a$.

Slide 204

Lema 11.11. *Valem as seguintes afirmações:*

(a) Seja $a \in \mathbb{N}$. Então $a < a + 1$;

(b) Sejam $a, b \in \mathbb{N}$. Então $a < b \to a + 1 \leq b$.

Demonstração. (a) Note que $a \leq a + 1$, pois $a + 1 = a + 1$. Agora suponha que $a = a + 1$. Mas então $a = s(a)$, contradição.

(b) Temos que existe $m \in \mathbb{N}$ tal que $a + m = b$, com $m \neq 0$ (pois, se $m = 0$, teríamos $a = b$). Assim, $m = s(n)$. Logo, $a + s(n) = b$ e, portanto $(a + 1) + n = b$. Isto é, $a + 1 \leq b$.

□

Slide 205

Proposição 11.12. *A ordem $\leq$ definida acima é uma ordem total sobre $\mathbb{N}$.*

Demonstração. Seja $a \in \mathbb{N}$. Considere $C_a = \{m \in \mathbb{N} : m \leq a \vee a \leq m\}$ (leia como "o conjunto de todos os elementos comparáveis com a"). Vamos mostrar que $C_a = \mathbb{N}$. Como a é qualquer, note que isso implica o resultado (já que dado qualquer a, ele é comparável com todos os outros elementos de $\mathbb{N}$). Vamos mostrar isso por indução. Isto é, considere $P(x)$ a afirmação $C_x = \mathbb{N}$.

$P(0)$: Note que dado qualquer $m \in \mathbb{N}$, temos que $0 \leq m$ (pois $0 + m = m$). Assim, $C_0 = \mathbb{N}$.

Slide 206

$P(n) \to P(n + 1)$: Suponha que vale $C_n = \mathbb{N}$, vamos mostrar que $C_{n+1} = \mathbb{N}$. Seja $m \in \mathbb{N}$. Temos que mostrar que $m \in \mathbb{N}$. Temos que $m \in C_n$ (pela hipótese de indução). Assim, temos dois casos:

- Caso $m \leq n$: Como $m \leq n$ e $n < n + 1$, temos que $m \leq n + 1$ e, portanto, $m \in C_{n+1}$ como queríamos.
- Caso $n \leq m$: Vamos dividir esse caso em dois. Se $n < m$, então $n + 1 \leq m$ e, portanto, $m \in C_{n+1}$. Se $n = m$, então $m \leq n + 1$ e, portanto, $m \in C_{n+1}$.

□

Slide 207

Finalmente, com a ajuda da ordem, podemos provar a lei de cancelamento para o produto:

Proposição 11.13. *Sejam $a, b, c \in \mathbb{N}$ com $c \neq 0$. Se $ac = bc$, então $a = b$.*

Demonstração. Suponha que $a \leq b$ (note que o outro caso seria $b \leq a$, que seria análogo). Então existem $m \in \mathbb{N}$ tal que $a + m = b$. Assim, de $ac = bc$, temos que $ac = (a + m)c$. Ou seja, $ac = ac + mc$ e, portanto, $mc = 0$. Como $c \neq 0$, temos que $m = 0$ e, portanto, $a = b$ como queríamos. □

Curiosidade

Slide 208

Vamos fechar esta seção com uma curiosidade sobre a formulação apresentada aqui.

Dizemos que um número $n \in \mathbb{N}$ está escrito recursivamente na base b se n está escrito na base b, cada expoente também está escrito na base b, cada expoente de cada expoente também etc. Por exemplo, considere o número 521. Ele escrito na base 2 fica

$$521 = 2^9 + 2^3 + 2^0$$

Mas os expoentes 9 e 3 não estão escritos na base 2, assim, arrumamos:

$$521 = 2^{2^3+2^0} + 2^{2^1+2^0} + 2^0$$

Apareceu um novo 3, daí fazemos:

$$521 = 2^{2^{2^{2^0}+2^0}+2^0} + 2^{2^{2^0}+2^0} + 2^0$$

Agora o processo terminou.

Slide 209

Note podemos fazer isso em qualquer base fixada. Para cada possível base $b \in \mathbb{N}$, com $b \geq 2$, considere a função $p_b : \mathbb{N} \to \mathbb{N}$ que faz o seguinte processo:

- p_b recebe um número n;
- escreve o número n recursivamente na base b;
- substitui cada ocorrência da base b por $(b+1)$ e faz a conta;
- a função p_b retorna o valor obtido na conta acima.

Por exemplo, lembrando que já fizemos a expansão acima,

$$\begin{aligned} p_2(521) &= 3^{3^{3^1+3^0}+3^0} + 3^{3^1+3^0} + 3^0 \\ &= 1.330.279.464.729.113.309.844.748.891.857.449.678.491 \\ &\approx 13 \cdot 10^{38} \end{aligned}$$

Slide 210

Essa função pode ser definida formalmente por recursão. De posse de tal função (na verdade, de posse de cada p_b), podemos definir a seguinte sequência, dado $k \in \mathbb{N}$:

- $g_k(1) = k$;
- $g_k(n+1) = \begin{cases} p_{n+1}(g_k(n)) - 1 & \text{se } g_k(n) > 0; \\ 0 & \text{caso contrário} \end{cases}$

Chamamos $g_k(1), g_k(2), g_k(3), ...$ de **sequência de Goodstein** de k.

Exemplos

Slide 211

Vejamos alguns exemplos:

Exemplo 11.14. Adotando $k = 3$, temos

- $g_3(1) = 3$;
- $g_3(2) = 3$;
- $g_3(3) = 3$;

- $g_3(4) = 3$;
- $g_3(5) = 2$;
- $g_3(6) = 1$;
- $g_3(7) = 0$.

Note que uma vez que o valor 0 é atingido, a sequência fica constante.

Slide 212

Exemplo 11.15. Adotando $k = 4$, temos

- $g_4(1) = 4$;
- $g_4(2) = 4$;
- $g_4(3) = 26$;
- $g_4(4) = 41$;
- $g_4(5) = 60$;
- $g_4(6) = 83$;
- $g_4(7) = 109$;
- $g_4(24) = 1151$;
- $g_4(3 \cdot 2^{402\ 653\ 209}) = 3 \cdot 2^{402\ 653\ 210} - 1$
- $g_4(3 \cdot 2^{402\ 653\ 211}) = 0$ (essa é a primeira vez que tal função dá 0)

Slide 213

Na verdade, pode-se provar:

Teorema 11.16 (Goodstein)**.** *Dado $k \geq 1$, existe $n \in \mathbb{N}$ tal que $g_k(n) = 0$.*

Talvez o mais interessante aqui é que o teorema acima é impossível de ser provado só com o uso dos axiomas de Peano aqui apresentados - ou seja, sua afirmação é uma afirmação independente de tais axiomas (ver, por exemplo, Seção 10.2 de [**?**]).

Exercícios da Aula 11

Exercício 11.1. Mostre que, dados $a, b, c \in \mathbb{N}$, se $b + a = c + a$, então $b = c$.

Exercício 11.2. Seja $a \in \mathbb{N}$ tal que $n + a = n$ para todo $n \in \mathbb{N}$. Mostre que $a = 0$ (um elemento satisfazendo tal propriedade é dito um **elemento neutro** com relação à operação $+$. Assim, o que estamos mostrando com esse exercício é que o 0 é o único elemento neutro com relação à $+$).

Exercício 11.3. Sejam $a, b \in \mathbb{N}$ tais que $a + b = 0$.

(a) Mostre que $b = 0$.

(b) Conclua que $a = 0$ e $b = 0$.

Exercício 11.4. Mostre por indução que vale a seguinte identidade para todo $x \in \mathbb{N}$:

$$2 \cdot (0 + 1 + \cdots + x) = (x + 1)x$$

Exercício 11.5. Considere k retas num plano, sendo que nenhuma delas é paralela a outra e que, para cada ponto do plano, passe no máximo duas destas retas. Considere R sendo a quantidade de regiões em que o plano foi dividido por tais retas. Mostre que vale a seguinte identidade:

$$2R = kk + k + 2$$

Exercício 11.6. Considere $f : \mathbb{N} \to \mathbb{N}$ satisfazendo as seguintes propriedades:

(A) $f(0) = 1$;

(B) Para todo $a \in \mathbb{N}$, $f(s(a)) = f(a) \cdot s(a)$;

Mostre que, dados $a, b \in \mathbb{N}$, temos que vale uma, e somente uma, das seguintes afirmações:

(i) $a < b$

(ii) $b < a$

(iii) $a = b$

Exercício 11.7. Sejam $a, b, c \in \mathbb{N}$. Mostre que se $a \leq b$, então $a + c \leq b + c$.

Exercício 11.8. Sejam $a, b, c \in \mathbb{N}$. Mostre que se $a \leq b$, então $ac \leq bc$.

Exercício 11.9. Seja $a \in \mathbb{N}$. Mostre que não existe $b \in \mathbb{N}$ tal que $a < b$ e $b < a + 1$.

Exercício 11.10. Seja $P(x)$ uma afirmação sobre $x \in \mathbb{N}$. Seja $a \in \mathbb{N}$. Se

(a) vale $P(a)$;

(b) vale $P(n) \to P(n + 1)$ para todo $n \geq a$.

Mostre que então vale $P(x)$ para todo $x \in \mathbb{N}$ tal que $a \leq x$.

Exercício 11.11. Seja $a \in \mathbb{N}$ tal que $a \cdot n = n$ para todo $n \in \mathbb{N}$. Mostre que $a = 1$ (um elemento satisfazendo tal propriedade é dito um **elemento neutro** com relação à operação $\cdot$. Assim, o que estamos mostrando com esse exercício é que o 1 é o único elemento neutro com relação à $\cdot$).

Exercício 11.12. Considere uma pista circular onde se encontram k postos de combutível ($k \geq 1$). Sabe-se que somando a quantidade total de combustível dos postos, tem-se o suficiente para que um carro possa dar uma volta completa. Mostre que existe um local da pista em que um carro, mesmo sem combustível, possa começar e dar uma volta completa.

Exercício 11.13. Dizemos que $f : (\mathbb{N} \setminus \{0\}) \times \mathbb{N} \to \mathbb{N}$ é uma **exponenciação** se f satisfaz:

(A) Dado $a \in \mathbb{N}$, $a \neq 0$ temos $f(a, 0) = 1$;

(B) Dados $a, b \in \mathbb{N}$, com $a \neq 0$, temos $f(a, s(b)) = f(a, b)a$.

(a) Calcule, pela definição, $f(2, 1)$, $f(2, 2)$ e $f(2, 3)$.

(b) Mostre que a exponenciação é única. Assim, usaremos a notação a^b, em vez de $f(a, b)$. Reescreva os axiomas A e B com essa nova notação.

(c) Mostre que, dados $a, b, c \in \mathbb{N}$, com $a \neq 0$, temos $(a^b) \cdot (a^c) = a^{b+c}$.

(d) Mostre que, dados $a, b, c \in \mathbb{N}$, com $a \neq 0$, temos $(a^b)^c = a^{(bc)}$.

Aula 12

Números inteiros

Slide 214

Agora vamos usar o que temos sobre os naturais para conseguir definir o conjunto dos inteiros. Isto é, uma vez que se tenha os números naturais, apresentaremos um método que se obtém os inteiros. Podemos pensar os números inteiros como representantes de "diferenças" entre números naturais. Por exemplo, o 5 representa a diferença entre 7 e 2 (quanto falta para o 2 "chegar" no 7). Já o -3 representa a diferença entre 8 e 11. Ou seja, para definirmos os inteiros, podemos usar pares de naturais. Desta forma, poderíamos representar o 5 como $(7, 2)$ e o -3 por $(8, 11)$. Veremos no que se segue que fazer essa representação nos facilita muitos casos. Mas ela tem um incoveniente: por exemplo, os pares $(4, 1)$ e $(7, 4)$ representam ambos o número 3. Veremos em seguida uma maneira de lidar com essa repetição. Tal método nos será útil em muitas outras situações.

Relações de equivalência

Slide 215

Antes de definirmos os inteiros, precisaremos do conceito de relação de equivalência.

Definição 12.1. Seja X um conjunto. Dizemos que uma relação $\sim$ é uma **relação de equivalência** se são satisfeitas:

(a) Para todo $x \in X$, temos que $x \sim x$; (**reflexiva**)

(b) Para todos $x, y \in X$, temos que $x \sim y \to y \sim x$; (**simétrica**)

(c) Para todos $x, y, z \in X$, temos que $(x \sim y \wedge y \sim z) \to x \sim z$. (**transitiva**)

Exemplos

Slide 216

Primeiramente, note que a igualdade é uma relação de equivalência:

Exemplo 12.2. A igualdade é uma relação de equivalência sobre um conjunto X, já que, para todo $x \in X$ temos que $x = x$. Também temos que se $x = y$ então $y = x$ para quaisquer $x, y \in X$. E, por último, temos que se $x = y$ e $y = z$, então $x = z$ para todo $x, y, z \in X$.

Slide 217

Exemplo 12.3. Dados $a, b \in \mathbb{N}$, dizemos que $a \sim b$ se o conjunto dos divisores primos de a e de b são iguais. Por exemplo, temos que $6 \sim 12$ já que os divisores primos de ambos são $\{2, 3\}$. Note que tal relação é uma relação de equivalência (exercício).

Slide 218

Proposição 12.4. *Seja* [39] $f : X \to Y$ *uma função. Então a relação* $\sim$ *dada por* $a \sim b$ *se, e somente se,* $f(a) = f(b)$ *para todo* $a, b \in X$ *é uma relação de equivalência sobre* X*.*

Demonstração. Vamos mostrar os axiomas de relação de equivalência:

(a) Seja $a \in X$. Note que $f(a) = f(a)$, logo $a \sim a$.

[39] Uma ideia aqui é pensar Y como um conjunto de cores. Assim, $f(x)$ é a cor de x e a classe de x são os elementos com a mesma cor de x.

(b) Sejam $a, b \in X$. Note que, se $a \sim b$, então $f(a) = f(b)$ e, portanto $b \sim a$ (pois $f(b) = f(a)$).

(c) Sejam $a, b, c \in X$. Suponha $a \sim b$ e $b \sim c$. Então $f(a) = f(b)$ e $f(b) = f(c)$. Assim $f(a) = f(c)$ e, portanto, $a \sim c$ como queríamos.

□

Classe de equivalência

Slide 219

Uma relação de equivalência serve para agrupar elementos "similares":
Definição 12.5. Seja X um conjunto e $\sim$ uma relação de equivalência sobre X. Dado $x \in X$, denotamos por $[x]$ (ou $\overline{x}$) o conjunto $\{y \in X : y \sim x\}$ (**classe de equivalência** de x). Denotamos por $X/\sim$ o conjunto de todas as classes de equivalência, isto é, $X/\sim = \{[x] : x \in X\}$.

Consequências

Slide 220

O seguinte lema nos vai ser útil em diversos resultados:
Lema 12.6. *Seja $\sim$ uma relação de equivalência sobre X. Sejam $a, b \in X$. Se existe $x \in [a] \cap [b]$, então $[a] = [b]$.*

Demonstração. Temos que mostrar que $[a] \subset [b]$ e que $[b] \subset [a]$. Seja $y \in [a]$. Então $y \sim a$. Como $x \sim a$ (pois $x \in [a]$), temos que $y \sim x$. Como $x \sim b$, temos que $y \sim b$. Logo, $y \in [b]$. Assim mostramos que $[a] \subset [b]$. Analogamente, mostramos que $[b] \subset [a]$ (exercício). □

Slide 221

Esse agrupamento muitas vezes é útil:

Proposição 12.7. *Seja $f : X \to Y$ uma função. Considere $\sim$ a relação de equivalência sobre X dada por, para $a, b \in X$, $a \sim b$ se, e somente se, $f(a) = f(b)$. Então a função $\tilde{f} : X/\sim \to Y$ dada por $\tilde{f}([a]) = f(a)$ é injetora.*

Demonstração. Primeiramente, vamos mostrar que $\tilde{f}$ está bem definida. Isto porque usamos um "representante" da classe $[a]$ para para definir quanto é $\tilde{f}([a])$. Poderia ser que alguém tomasse $b \in [a]$ e tivesse um resultado diferente. Vamos mostrar que isso não ocorre. Seja $b \in [a]$. Então $b \sim a$. Logo, $f(b) = f(a)$. Assim, dado qualquer representante b da classe $[a]$, $\tilde{f}([a]) = f(a) = f(b)$.

Slide 222

Vamos agora mostrar que tal função é, de fato, injetora. Sejam $[a], [b] \in X/\sim$. Suponha que $\tilde{f}([a]) = \tilde{f}([b])$. Vamos mostrar que $[a] = [b]$. Note que temos $f(a) = f(b)$. Logo, $a \sim b$ e, portanto, $b \in [a]$. Pelo Lema 12.6, temos que $[a] = [b]$. □

Partições

Slide 223

Definição 12.8. Seja X um conjunto. Chamamos uma família $\mathcal{F}$ de subconjuntos de X de uma **partição** de X se são satisfeitas:

(a) $\bigcup_{F \in \mathcal{F}} F = X$;

(b) Se $A, B \in \mathcal{F}$ são distintos, então $A \cap B = \emptyset$.

Slide 224

Proposição 12.9. *Seja* [40]$\mathcal{F}$ *uma partição sobre um conjunto* X*. Então* $\sim$ *definido por* $a \sim b$ *(para* $a, b \in X$*) se, e somente se, existe* $F \in \mathcal{F}$ *tal que* $a, b \in F$ *é uma relação de equivalência sobre* X*. Esta é chamada de* **relação de equivalência induzida** *por* $\mathcal{F}$*.*

Demonstração. Vamos mostrar os axiomas de relação de equivalência para $\sim$:

- Seja $x \in X$. Como $\bigcup_{F \in \mathcal{F}} F = X$, existe $F \in \mathcal{F}$ tal que $x \in F$. Logo, $x \sim x$ (pois $x \in F$).
- Sejam $x, y \in X$ tais que $x \sim y$. Então existe $F \in \mathcal{F}$ tal que $x, y \in F$. Logo, $y \sim x$.

Slide 225

- Sejam $x, y, z \in X$ tais que $x \sim y$ e $y \sim z$. Então existe $F \in \mathcal{F}$ tal que $x, y \in F$ e existe $G \in \mathcal{F}$ tal que $y, z \in G$. Note que $y \in F \cap G$. Pelo axioma (b) de partição, se F e G fossem distintos, teríamos $F \cap G = \emptyset$. Logo, $F = G$. Assim, $x, y, z \in F$ e, portanto, $x \sim z$.

□

Números inteiros

Slide 226

Vamos agora ver a relação de equivalência que vai nos permitir definir os inteiros.

Proposição 12.10. *Considere a relação* $\sim$ *sobre* $\mathbb{N}^2$ *dada por*

$$(a, b) \sim (c, d) \text{ se, e somente se } a + d = c + b$$

onde $(a, b), (c, d) \in \mathbb{N}^2$*. Então* $\sim$ *é uma relação de equivalência*[41] *sobre* $\mathbb{N}^2$*.*

Demonstração. Vamos mostrar os axiomas de relação de equivalência:

- Seja $(a, b) \in \mathbb{N}^2$. Temos que $a + b = a + b$, logo $(a, b) \sim (a, b)$.
- Sejam $(a, b), (c, d) \in \mathbb{N}^2$ tais que $(a, b) \sim (c, d)$. Temos que $c + b = a + d$, logo $(c, d) \sim (a, b)$.

Slide 227

- Sejam $(a, b), (c, d), (e, f) \in \mathbb{N}^2$ tais que $(a, b) \sim (c, d)$ e $(c, d) \sim (e, f)$. Temos $a + d = c + b$. Logo $a + d + f = c + b + f$. Também temos que $c + f = e + d$. Logo, temos $c + f + b = e + d + b$. Desta forma obtemos $a + d + f = e + d + b$ e, portanto, $a + f = e + b$. Isto é, $(a, b) \sim (e, f)$.

□

Slide 228

Definição 12.11. Chamamos de $\mathbb{Z}$ o conjunto $\mathbb{N}^2/\sim$ onde $\sim$ é a relação de equivalência definida no item anterior. Cada elemento de $\mathbb{Z}$ é chamado de **número inteiro**.

Somando

Slide 229

Definição 12.12. Sejam $[(a, b)], [(c, d)] \in \mathbb{Z}$. Definimos[42] $[(a, b)] + [(c, d)] = [(a + c, b + d)]$ (**soma nos inteiros**).

Slide 230

Proposição 12.13. *A operação de soma está bem definida.*

Demonstração. Precisamos mostrar que tal definição independe dos representantes de classe tomados. Ou seja, precisamos mostrar que se $(a,b) \sim (x,y)$ e $(c,d) \sim (w,z)$ então $(a+c, b+d) \sim (x+w, y+z)$. Temos que $a+y = b+x$ e que $c+z = d+w$. Assim

$$\begin{aligned}(a+c)+(y+z) &= (a+y)+(c+z)\\ &= (b+x)+(d+w)\\ &= (b+d)+(x+w)\end{aligned}$$

□

Slide 231

Proposição 12.14. *Temos que a soma satisfaz as seguintes propriedades:*

(a) Comutativa;

(b) Associativa;

Demonstração. Vamos mostrar que ela é comutativa e vamos deixar a associativa como exercício. Sejam $[(a,b)], [(c,d)] \in \mathbb{Z}$. Vamos mostrar que $[(a,b)] + [(c,d)] = [(c,d)] + [(a,b)]$. Temos

$$\begin{aligned}[(a,b)] + [(c,d)] &= [(a+c, b+d)]\\ &= [(c+a, d+b)]\\ &= [(c,d)] + [(a,b)]\end{aligned}$$

□

Slide 232

Proposição 12.15. *Para qualquer* $[(a,b)] \in \mathbb{Z}$*, temos que* $[(a,b)] + [(0,0)] = [(a,b)]$

Demonstração. Basta notar que $(a+0, b+0) \sim (a,b)$, já que $a+0+b = b+0+a$. □

Slide 233

Proposição 12.16 (Lei do Cancelamento). *Sejam* $[(a,b)], [(c,d)], [(x,y)] \in \mathbb{Z}$*. Se* $[(a,b)] + [(x,y)] = [(c,d)] + [(x,y)]$*, então* $[(a,b)] = [(c,d)]$*.*

Demonstração. Temos que $[(a+x, b+y)] = [(c+x, d+y]]$. Assim, $a+x+d+y = b+y+c+x$. Assim, cancelando $x+y$, temos $a+d = b+c$, isto é, $(a,b) \sim (c,d)$. □

Multiplicando

Slide 234

Definição 12.17. Sejam $[(a,b)]$, $[(c,d)] \in \mathbb{Z}$. Definimos[43] $[(a,b)] \cdot [(c,d)] = [(ac+bd, ad+bc)]$. Este é o **produto nos inteiros**. Assim como fizemos com $\mathbb{N}$, omitiremos o sinal $\cdot$ normalmente.

Slide 235

Proposição 12.18. *A operação de produto está bem definida.*

Demonstração. Ver os exercícios. □

[40] Veja o exercício 12.2 para o processo contrário.

[41] A inspiração desta relação de equivalência vem do seguinte. Queremos que $a-b = c-d$. Ou seja, queremos que $a+d = c+b$.

[42] A inspiração para essa definição vem do seguinte: queremos definir $(a-b)+(c-d)$ e isso é igual a $(a+c)-(b+d)$.

[43] A inspiração para essa definição é: queremos definir $(a-b)\cdot(c-d)$ e isso é igual a $(ac+db)-(ad-bc)$.

Propriedades básicas

Slide 236

Proposição 12.19. *Valem as seguintes propriedades para o produto.*

(a) Associativa;

(b) Comutativa;

Demonstração. Ver Exercício 12.9 □

Slide 237

Proposição 12.20. *Vale a propriedade distributiva entre a soma e o produto em* $\mathbb{Z}$*. Isto é, dados* $[(a,b)], [(c,d)], [(x,y)] \in \mathbb{Z}$*, temos que*

$$[(x,y)]([(a,b)+(c,d)]) = ([(x,y)][(a,b)]) + ([(x,y)][(c,d)])$$

Demonstração. Temos

$$\begin{aligned}
[(x,y)]([(a,b)+(c,d)]) &= [(x,y)][(a+c,b+d)] \\
&= [(x(a+c)+y(b+d), x(b+d)+y(a+c))] \\
&= [(xa+xc+yb+yd, xb+xd+ya+yc)] \\
&= [(xa+yb, xb+ya)] + [(xc+yd, xd+yc)] \\
&= ([(x,y)][(a,b)]) + ([(x,y)][(c,d)])
\end{aligned}$$

□

Slide 238

Proposição 12.21. *Seja* $[(a,b)] \in \mathbb{Z}$*. Então* $[(1,0)][(a,b)] = [(a,b)]$.

Demonstração. Temos $[(a,b)][(1,0)] = [(a1+b0, a0+b1)] = [(a,b)]$. □

Alongamentos da Aula 12

Alongamento 12.1. Considere a igualdade como uma relação de equivalência sobre um conjunto X. Dado $x \in X$, quem é o conjunto $[x]$?

Alongamento 12.2. Mostre que se na Proposição 12.7 supormos também que f é sobrejetora, então $\tilde{f}$ é bijetora.

Alongamento 12.3. Seja $f : X \to Y$ uma função. Seja $\sim$ uma relação de equivalência sobre Y. Mostre $\simeq$ dada por $a \simeq b$ se $f(a) \simeq f(b)$ é uma relação de equivalência sobre X. Prove a Proposição 12.4 usando esse alongamento.

Exercícios da Aula 12

Exercício 12.1. Considere as mesmas hipóteses da Proposição 12.9.

(a) Mostre que, para todo $x \in X$, existe um único $F_x \in \mathcal{F}$ tal que $x \in F_x$;

(b) Na notação do item anterior, mostre que $F_x = [x]$, considerando a relação de equivalência induzida por $\mathcal{F}$.

Exercício 12.2. A ideia deste exercício é complementar a Proposição 12.9. Seja $\sim$ uma relação de equivalência sobre X.

(a) Seja $x \in X$. Mostre que existe $y \in X$ tal que $x \in [y]$.

(b) Sejam $x, y \in X$. Mostre que se $[x], [y]$ forem distintos (como conjuntos), então $[x] \cap [y] = \emptyset$.

(c) Mostre $\{[x] : x \in X\}$ é uma partição sobre X. Esta é chamada de **partição induzida** pela relação de equivalência $\sim$.

Exercício 12.3. Considere $f : X \to Y$ sobrejetora e $g : Y \to Z$ injetora. Considere $\sim$ relação de equivalência sobre X dada por $a \sim b$ se $g(f(a)) = g(f(b))$[44] Mostre que existe uma função bijetora entre $X/\sim$ e Y

Exercício 12.4. Sejam $a, b \in \mathbb{N}$.

(a) Dê um exemplo de forma que $[(a, b)] = [(x, y)]$, mas $a \neq x$ e $b \neq y$.

(b) Mostre que se $[(x, b)] = [(a, b)]$, então $x = a$.

(c) Enuncie e prove o análo ao exercício anterior, fixando a primeria coordenada.

Exercício 12.5. Mostre que vale a propriedade associativa para a soma em $\mathbb{Z}$.

Exercício 12.6. Mostre que o elemento neutro da soma é único, isto é, dado $[(a, b)] \in \mathbb{Z}$ tal que para todo $[(x, y)] \in \mathbb{Z}$ temos que $[(x, y)] + [(a, b)] = [(x, y)]$, então $[(a, b)] = [(0, 0)]$.

Exercício 12.7. Mostre que $[(a, b)] \in \mathbb{Z}$ é tal que $[(a, b)] = [(0, 0)]$ se, e somente se, $a = b$.

Exercício 12.8. Mostre que o produto dos inteiros está bem definido.

Exercício 12.9. Mostre as propriedades associativa e comutativa para o produto em $\mathbb{Z}$.

Exercício 12.10. Mostre que o elemento neutro do produto é único.

Exercício 12.11. Sejam $[(a, b)], [(c, d)] \in \mathbb{Z}$.

(a) Mostre que $[(a, b)][(0, 1)] = [(b, a)]$;

(b) Mostre que $[(a, b)] + [(b, a)] = [(0, 0)]$;

(c) Mostre que se $[(a, b)] + [(c, d)] = [(0, 0)]$, então $[(a, b)] = [(d, c)]$.

[44] Note que isso é de fato uma relação de equivalência pela Proposição 12.4.

Aula 13

Forma canônica

Slide 239

Proposição 13.1. *Seja* $[(a,b)] \in \mathbb{Z}$. *Então existe* $x \in \mathbb{N}$ *tal que* $[(a,b)] = [(x,0)]$ *ou* $[(a,b)] = [(0,x)]$.

Demonstração. Vamos separar em 3 casos:

$a = b$**:** Neste caso, tomamos $x = 0$ e $[(a,b)] = [(0,0)]$ (ver Exercício 12.7).

$a < b$**:** Seja $m \in \mathbb{N}$ tal que $a+m = b$. Vamos mostrar que $(a,b) \sim (0,m)$. De fato, temos que $a+m = b+0$.

$b < a$**:** Seja $m \in \mathbb{N}$ tal que $b+m = 0$. Vamos mostrar que $(a,b) \sim (m,0)$. De fato, temos que $a+0 = b+m$.

□

Slide 240

Definição 13.2. Dizemos que um elemento de $\mathbb{Z}$ está escrito na **forma canônica** se ele está escrito na forma $[(x,0)]$ ou $[(0,x)]$. Pelo resultado anterior, temos que todo elemento pode ser escrito na forma canônica. Note que tal representação é única (ver Exercício 13.1) .

Aplicando

Slide 241

Escrever os elementos na forma canônica muitas vezes facilita demonstrações:
Proposição 13.3. *Sejam* $[(a,b)], [(c,d)] \in \mathbb{Z}$ *tais que* $[(a,b)][(c,d)] = [(0,0)]$. *Então* $[(a,b)] = [(0,0)]$ *ou* $[(c,d)] = [(0,0)]$.

Demonstração. Seja $x \in \mathbb{N}$ tal que $[(a,b)] = [(x,0)]$ ou $[(a,b)] = [(0,x)]$ e seja $y \in \mathbb{N}$ tal que $[(c,d)] = [(y,0)]$ ou $[(c,d)] = [(0,y)]$. Temos 4 casos. Vamos mostrar 2, deixando os outros dois como exercício:

- Pela definição do produto, temos $[(x,0)][(y,0)] = [(xy,0)]$. De $[(xy,0)] = [(0,0)]$, temos que $xy = 0$ (pelo Exercício 12.4) . Logo, $x = 0$ ou $y = 0$ e, portanto, $[(a,b)] = [(0,0)]$ ou $[(c,d)] = [(0,0)]$.

Slide 242

- Pela definição do produto, temos que $[(x,0)][(0,y)] = [(0,xy)]$. Como no caso anterior, temos que $xy = 0$ e, portanto, $x = 0$ ou $y = 0$. Assim $[(a,b)] = [(0,0)]$ ou $[(c,d)] = [(0,0)]$.

□

Ordem

Slide 243

Definição 13.4. Sejam $[(a,b)], [(c,d)] \in \mathbb{Z}$. Seja $x \in \mathbb{N}$ tal que $[(a,b)] = [(x,0)]$ ou $[(a,b)] = [(0,x)]$ e seja $y \in \mathbb{N}$ tal que $[(c,d)] = [(y,0)]$ ou $[(c,d)] = [(0,y)]$. Dizemos que $[(a,b)] \leq [(c,d)]$ se, e somente se, ocorre um dos seguintes casos[45]:

[45] A ideia escondida aqui é que o primeiro caso os dois são positivos, no segundo um é e o outro não e no terceiro caso ambos são negativos.

- $[(a,b)] = [(x,0)]$, $[(c,d)] = [(y,0)]$ e $x \leq y$;
- $[(a,b)] = [(0,x)]$, $[(c,d)] = [(y,0)]$;
- $[(a,b)] = [(0,x)]$, $[(c,d)] = [(0,y)]$ e $y \leq x$.

Esta é a **ordem usual sobre os inteiros**[46].

É total

Slide 244

Proposição 13.5. *A ordem sobre os inteiros é total.*

Demonstração. Sejam $[(a,b)], [(c,d)] \in \mathbb{Z}$. Temos que mostrar que $[(a,b)] \leq [(c,d)]$ ou $[(c,d)] \leq [(a,b)]$. Sejam $x, y \in \mathbb{N}$ tais que $[(a,b)] = [(x,0)]$ ou $[(a,b)] = [(0,x)]$ e $[(c,d)] = [(y,0)]$ ou $[(c,d)] = [(0,y)]$. Vamos analisar os casos:

- Se $[(a,b)] = [(x,0)]$ e $[(c,d)] = [(y,0)]$. Se $x \leq y$, temos que $[(x,0)] \leq [(y,0)]$. Caso contrário, temos que $y \leq x$ e, portanto, $[(y,0)] \leq [(x,0)]$.
- Se $[(a,b)] = [(x,0)]$ e $[(c,d)] = [(0,y)]$, então $[(0,y)] \leq [(x,0)]$.

Os outros casos são análogos. □

Notações

Slide 245

Definição 13.6. Denotamos por x o elemento $[(x,0)]$. Denotamos por $-x$ o elemento $[(0,x)]$. Assim, denotamos por $x + (-y)$ o elemento $[(x,0)] + [(0,y)]$. Muitas vezes, omitimos o $+$, ficando apenas $x - y$. Chamamos de **positivo** um elemento da forma $[(x,0)]$ e de **negativo** um da forma $[(0,y)]$.

Regras de sinal

Slide 246

Proposição 13.7. *(a) O produto de dois positivos é positivo;*

(b) O produto de dois negativos é positivo;

(c) O produto de um positivo com um negativo é negativo;

Demonstração. Sejam $a, b \in \mathbb{N}$.

(a) Temos que $[(a,0)][(b,0)] = [(ab,0)]$;

(b) Temos que $[(0,a)][(0,b)] = [(ab,0)]$;

(c) Temos que $[(a,0)][(0,b)] = [(0,ab)]$.

□

Notação

Slide 247

Definição 13.8. Dado $[(a,b)] \in \mathbb{Z}$, denotamos por $-[(a,b)]$ o elemento $[(b,a)]$.

Propriedades básicas

Slide 248

Proposição 13.9. *Sejam $a, b \in \mathbb{Z}$. Temos:*

(a) $-(-a) = a$;

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

Demonstração. (a) Seja $[(x,y)] = a$. Então $-(-[(x,y)]) = -[(y,x)] = [(x,y)]$.

(b) Sejam $[(x,y)] = a$ e $[(w,z)] = b$. Temos

$$\begin{aligned} a(-b) &= [(x,y)](-([w,z])) \\ &= [(x,y)][(z,w)] \\ &= [(xz+yw, xw+yz)] \\ &= -[(xw+yz, xz+yw)] \\ &= -([(x,y)][(w,z)]) \end{aligned}$$

□

Slide 249

Proposição 13.10. *Dado um elemento $z \in \mathbb{Z}$, temos que z é positivo se, e somente se, $-z$ é negativo.*

Demonstração. Suponha z positivo. Então existe $a \in \mathbb{N}$ tal que $z = [(a,0)]$. Assim, $-z = -[(a,0)] = [(0,a)]$ e, portanto, é negativo.

Por outro lado, se $-z$ é negativo, existe $a \in \mathbb{N}$ tal que $-z = [(0,a)]$. Logo, $z = -(-z) = -[(0,a)] = [(a,0)]$ é positivo. □

Notação

Slide 250

Vamos identificar $\mathbb{N} = \{z \in \mathbb{Z} : z \geq 0\}$ da maneira usual.

Slide 251

Definição 13.11. Dados $a, b \in \mathbb{Z}$, dizemos que a **divide** b (e denotamos por $a|b$) se existe $m \in \mathbb{Z}$ tal que $am = b$.

Propriedades básicas

Slide 252

Proposição 13.12. *Sejam $a, b, c \in \mathbb{Z}$. Temos:*

(a) $1|a$;

(b) $a|0$;

[46] veja o Exercício 13.2

(c) $a|a$*;*

(d) Se $a|b$ *e* $b|c$*, então* $a|c$*.*

Demonstração. (a) Basta notar que $1a = a$.

(b) Basta notar que $a0 = 0$.

(c) Basta notar que $a1 = a$.

(d) Seja $m \in \mathbb{Z}$ tal que $am = b$. Seja $n \in \mathbb{Z}$ tal que $bn = c$. Vamos provar que $a(mn) = c$. De fato, $a(mn) = (am)n = bn = c$.

□

Slide 253

Proposição 13.13. *Sejam* $a, b \in \mathbb{Z}$*. Então* $ab = (-a)(-b)$*.*

Demonstração. Temos $(-a)(-b) = (-1a)(-1b) = (-1)(-1)(a)(b) = ab$[47]. □

Diferenças entre casos

Slide 254

Nos naturais, temos uma única possibilidade para que um produto dê 1:

Lema 13.14. *Se* $a, b \in \mathbb{N}$ *são tais que* $ab = 1$*, então* $a = b = 1$*.*

Demonstração. Note que $b \neq 0$ (pois $a0 = 0 \neq 1$). Assim, existe $m \in \mathbb{N}$ tal que $b = m + 1$. Substituindo, temos $ab = a(m + 1) = am + a$. Isto é, $a + am = 1$. Assim, temos que $a \leq 1$. Como $a \in \mathbb{N}$, temos $a = 0$ ou $a = 1$. Como $a \neq 0$ (pois $0b = 0 \neq 1$), temos que $a = 1$. Como $1b = 1 \cdot 1$, temos, pela lei do cancelamento, que $b = 1$. □

Slide 255

Já nos inteiros, temos duas possibilidades para um produto dar 1:

Lema 13.15. *Se* $a, b \in \mathbb{Z}$ *são tais que* $ab = 1$*, então* $a = b = 1$ *ou* $a = b = -1$*.*

Demonstração. Temos 3 casos: a, b são positivos, a, b são negativos e o terceiro caso é o que um é positivo e o outro é negativo (neste último caso, podemos supor sem problemas que a é positivo e b é negativo). Note também que, claramente, a, $b \neq 0$.

- $a, b > 0$. Neste caso, pelo lema anterior, temos que $a, b = 1$.

Slide 256

- $a, b < 0$. Note que

$$\begin{aligned} 1 &= ab \\ &= (-a)(-b) \end{aligned}$$

  Como $(-a), (-b)$ são positivos, temos que $-a, -b = 1$ e, portanto, $a, b = -1$.

- $a > 0$ e $b < 0$. Note que, neste caso, $ab < 0$ e, portanto, não pode ser 1 (ou seja, esse caso era impossível de ocorrer).

□

Slide 257

Proposição 13.16. *Sejam $a, b \in \mathbb{Z}$. Se $a|b$ e $b|a$, então $a = b$ ou $a = -b$.*

Demonstração. Primeiramente, note que se $b = 0$, como $b|a$, temos que $a = 0$ e, portanto, o resultado vale. Logo, podemos supor agora que $b \neq 0$.

De $a|b$, temos que existe $m \in \mathbb{Z}$ tal que $am = b$. De $b|a$, temos que existe n tal que $bn = a$. Assim, de $am = b$, temos que $(bn)m = b$. Como $b \neq 0$, pela lei do cancelamento, temos que $nm = 1$. Pelo lema anterior, $n = m = 1$ ou $n = m = -1$ e temos o resultado. □

Menor elemento

Slide 258

Teorema 13.17 (Princípio do menor elemento)**.** *Seja $S \subset \mathbb{N}$. Se $S \neq \emptyset$, então existe $m \in S$ mínimo de S (isto é, $m \leq s$ para todo $s \in S$).*

Demonstração. Considere o conjunto

$$M = \{x \in \mathbb{N} : \text{para todo } s \in S,\ x \leq s\}.$$

Note que $0 \in M$. Como $S \neq \emptyset$, temos que existe $s \in S$. Note que $s + 1 \notin M$. Logo, $M \neq \mathbb{N}$. Considere a propriedade $P(x)$ como

$$x \in M.$$

Slide 259

Note que temos $P(0)$. Logo, como tal propriedade não pode valer para todo $x \in \mathbb{N}$, temos que existe $n \in \mathbb{N}$ tal que $P(n) \not\to P(n + 1)$ (pois a indução não pode valer). Isto é, existe $n \in \mathbb{N}$ tal que $P(n)$ e $\neg P(n + 1)$. Vamos mostrar que tal n é o mínimo de S. Como vale $P(n)$, temos que $n \leq s$ para todo $s \in S$. Resta mostrar que $n \in S$. Suponha que não. Então vale que, para qualquer $s \in S$, $n < s$. Logo, $n + 1 \leq s$ (pelo Lema 11.11) para qualquer $s \in S$. Assim, $n + 1 \in M$ e, portanto, $P(n + 1)$, contradição. □

Divisão

Slide 260

Teorema 13.18 (Algoritmo da divisão de Euclides)**.** *Sejam*[48] *$a, b \in \mathbb{Z}$ tais que $a \geq 0$ e $b > 0$. Então existem inteiros q e r tais que $a = bq + r$ com $0 \leq r < b$.*

Demonstração. Considere o conjunto

$$S = \{a - bx : x \in \mathbb{Z} \text{ e } a - bx \geq 0\}.$$

Note que $S \neq \emptyset$, pois tomando $x = 0$, temos que $a - bx = a \geq 0$. Seja r o menor elemento de S. Assim, para algum $q \in \mathbb{Z}$, temos que $r = a - bq$. Logo, $r + bq = a$. Note que, como $r \in S$, $r \geq 0$.

Slide 261

Se mostrarmos que $r < b$ terminamos. Suponha que não. Temos

$$\begin{array}{rcl} 0 & \leq & r - b \\ & = & (a - bq) - b \\ & = & a - b(q + 1) \end{array}$$

Note então que $a - b(q + 1) \in S$. E note que $a - b(q + 1) = a - bq - b < a - bq = r$, já que $b > 0$. Mas isso contradiz a minimalidade de r. □

[47] A útima igualdade segue de um alongamento da seção anterior.

[48] Veja o caso geral no Exercício 13.11.

Valor absoluto

Slide 262

Definição 13.19. Dado $z \in \mathbb{Z}$, definimos o valor absoluto de z (denotado por $|z|$) da seguinte maneira:

$$|z| = \begin{cases} z & \text{se } z \geq 0 \\ -z & \text{se } z < 0 \end{cases}$$

Propriedades básicas

Slide 263

Proposição 13.20. *Sejam $a, b \in \mathbb{Z}$. Temos que valem as seguintes afirmações:*

(a) $|a| \geq 0$*;*

(b) $|a| = 0 \to a = 0$*;*

(c) $a \leq |a|$*;*

Demonstração. (a) Se $a \geq 0$, temos que $|a| = a \geq 0$. Se $a < 0$, temos que $|a| = -a > 0$.

(b) Suponha que $a \neq 0$. Se $a > 0$, temos que $|a| = a > 0$ e, portanto $|a| \neq 0$. Se $a < 0$, temos que $|a| = -a > 0$ e novamente temos que $|a| \neq 0$.

(c) se $a \geq 0$, temos que $|a| = a$ e, portanto, $a \leq |a|$. Se $a < 0$, temos que $a < |a|$ pelo item (a).

□

Alongamentos da Aula 13

Alongamento 13.1. Mostre que $(-1)(-1) = 1$.

Alongamento 13.2. Seja $a \in \mathbb{Z}$. Mostre que $-a = (-1)a$.

Exercícios da Aula 13

Exercício 13.1. Mostre que cada elemento de $\mathbb{Z}$ tem apenas uma única representação na forma canônica.

Exercício 13.2. Mostre que a relação apresentada de fato é uma ordem sobre $\mathbb{Z}$.

Exercício 13.3. Mostre a **Lei do Cancelamento** do produto em $\mathbb{Z}$: Dados $[(a, b)], [(c, d)], [(x, y)] \in \mathbb{Z}$ tais que $[(a, b)][(x, y)] = [(c, d)][(x, y)]$ e $[(x, y)] \neq [(0, 0)]$, então $[(a, b)] = [(c, d)]$.

Exercício 13.4. Sejam $a, b \in \mathbb{Z}$ mostre que $a \leq b$ se, e somente se, existe $m \in \mathbb{Z}$ positivo tal que $a + m = b$.

Exercício 13.5. Mostre que $z \in \mathbb{Z}$ é positivo se, e somente se, $z \geq 0$ $(0 = [(0, 0)])$.

Exercício 13.6. Sejam $a, b, c \in \mathbb{Z}$.

(a) Mostre que se $a \leq b$, então $a + c \leq b + c$;

(b) Mostre que se $a \leq b$ e $c \geq 0$, então $ac \leq bc$;

(c) Mostre que se $a \leq b$ e $c \leq 0$, então $bc \leq ac$.

Exercício 13.7. Mostre que $|$ é uma ordem sobre $\mathbb{N}$. Ela é uma ordem sobre $\mathbb{Z}$?

Exercício 13.8. Mostre que dado $a \in \mathbb{Z}$, temos que $-|a| \leq a$.

Exercício 13.9. Sejam $a, b \in \mathbb{Z}$.

(a) Mostre que $a + b \leq |a| + |b|$;

(b) Mostre que $-(|a| + |b|) \leq a + b$;

(c) Mostre que $|a + b| \leq |a| + |b|$.

Exercício 13.10. Sejam $a, b \in \mathbb{Z}$. Mostre que $|ab| = |a||b|$.

Exercício 13.11. Sejam $a, b \in \mathbb{Z}$.

(a) Se $a < 0$ e $b > 0$, mostre que existem $q, r \in \mathbb{Z}$ tais que $a = bq + r$ com $0 \leq r < b$.

(b) Se $b < 0$, mostre que existem $q, r \in \mathbb{Z}$ tais que $a = bq + r$ com $0 \leq r < |b|$.

(c) Conclua o caso geral do **Algoritmo da divisão de Euclides**: Dados $a, b \in \mathbb{Z}$ tais que $b \neq 0$, existem $q, r \in \mathbb{Z}$ tais que $a = bq + r$ com $0 \leq r < |b|$.

Exercício 13.12. Considere uma fila de pessoas em que a primeira pessoa é uma mulher e a última é um homem. Mostre que há pelo menos um homem que está imediatamente atrás de uma mulher.

Aula 14

Números primos

Slide 264

Um conceito bastante útil é o de número primo:

Definição 14.1. Dado[49] um $p \in \mathbb{N}$, dizemos que p é **primo** se $p > 1$ e se $a \in \mathbb{N}$ é tal que $a|p$, então $a = p$ ou $a = 1$.

Slide 265

O próximo resultado vai facilitar algumas demonstrações por indução ou por argumentos de minimalidade:

Proposição 14.2. *Sejam $a, b \in \mathbb{N}$ tais que $a, b > 1$. Se $a|b$, então $a \leq b$.*

Demonstração. Como $a|b$, existe $n \in \mathbb{N}$ tal que $an = b$. Note que $n \neq 0$ pois $b \neq 0$. Assim, existe $m \in \mathbb{N}$ tal que $n = m + 1$. Temos

$$\begin{aligned} b &= an \\ &= a(m+1) \\ &= am + a \end{aligned}$$

Logo, $a \leq b$. □

Slide 266

Já temos material suficiente para provar que todo número maior que 1 é divisível por algum primo:

Proposição 14.3. *Dado $a \in \mathbb{N}$, com $a > 1$, existe p primo tal que $p|a$.*

Demonstração. Seja $D = \{n \in \mathbb{N} : n > 1 \text{ e } n|a\}$. Note que $D \neq \emptyset$ já que $a \in D$. Seja p o mínimo de D. Vamos mostrar que p é primo. Suponha que não. Então existe d tal que $d > 1$, $d \neq p$ e $d|p$. Pela Proposição 14.2, temos que $d < p$. Note que, como $d|p$ e $p|a$, temos que $d|a$. Logo, $d \in D$ contrariando a minimalidade de p. □

Decomposição

Slide 267

Com o resultado anterior, podemos decompor cada $a > 1$ em fatores primos:

Proposição 14.4. *Dado $a \in \mathbb{N}$, com $a > 1$. Então existem $p_1, ..., p_n$ primos tais que $a = p_1 \cdots p_n$.*

Demonstração. Considere $A = \{a \in \mathbb{N} : a > 1 \text{ e existem } p_1, ..., p_n \text{ primos tais que } a = p_1 \cdots p_n\}$. Temos que mostrar que $A = \{a \in \mathbb{N} : a > 1\}$. Suponha que não. Então $\{a \in \mathbb{N} : a > 1\} \setminus A$ é não vazio. Seja m o mínimo de tal conjunto. Note que $m > 1$. Pela Proposição 14.3, existe p primo tal que $p|m$. Pela Proposição 14.2, temos dois casos $p = m$ ou $p < m$. Se $p = m$, temos uma contradição com a definição de m (pois $m \notin A$).

Slide 268

Se $p < m$, note que existe k tal que $pk = m$ e tal que $k > 1$ (se $k = 0$, teríamos $m = 0$ e se $k = 1$, teríamos $m = p$). Assim, pela minimalidade m, temos que existem $p_1, ..., p_n$ tais que $k = p_1 \cdots p_n$. Logo, $m = (p_1 \cdot \cdots \cdot p_n)p$, contrariando a definição de m. □

mdc

Slide 269

Definição 14.5. Sejam[50] $a, b \in \mathbb{Z}$. Dizemos que d é um **máximo divisor comum** de a e b se

(a) $d \geq 0$;

(b) $d|a$ e $d|b$;

(c) Se e satisfaz (a) e (b), então $e|d$.

Slide 270

Proposição 14.6. *Se d e e são máximos divisores comuns de a e b, então $d = e$.*

Demonstração. Basta notar que $d|e$ e $e|d$. Logo, como ambos são positivos, temos que $d = e$. □

Slide 271

Proposição 14.7. *Sejam $a, b \in \mathbb{Z}$ com $a, b \neq 0$. Então[51] o mínimo do conjunto $\{ax + by : ax + by > 0$ e $x, y \in \mathbb{Z}\}$ é o máximo divisor comum de a e b.*

Demonstração. Vamos chamar o conjunto do enunciado de A. Note que $A \neq \emptyset$ (exercício). Assim, seja d o mínimo de A. Note que $d > 0$. Sejam $x, y \in \mathbb{Z}$ tais que $d = ax + by$. Vamos mostrar que $d|a$. Suponha que não. Aplique o algoritmo da divisão de Euclides e tome $a = dq + r$ com $0 < r < d$. Note que

$$\begin{aligned} r &= a - dq \\ &= a - (ax + by)q \\ &= a(1 - xq) - b(yq) \end{aligned}$$

Slide 272

Logo $r \in A$, contrariando a minimalidade de d. Podemos provar de maneira análoga que $d|b$. Assim, só nos resta mostrar que dado $e \geq 0$ tal que $e|a$ e $e|b$ temos que $e|d$. Como $e|a$, existe m tal que $em = a$. Como $e|b$, existe n tal que $en = b$. Assim, temos

$$\begin{aligned} d &= ax + by \\ &= emx + eny \\ &= e(mx + ny) \end{aligned}$$

Logo, $d|e$ como queríamos. □

Forma usual

Slide 273

Definição 14.8. Dados $a, b \in \mathbb{Z}_{\neq 0}$, chamamos de $mdc(a, b)$ o máximo divisor comum de a e b.

Slide 274

Finalmente, podemos também definir o máximo divisor comum entre a e b de forma mais "próxima" de seu nome:

Proposição 14.9. *Sejam $a, b \in \mathbb{Z}_{\neq 0}$. Então M é o máximo divisor comum entre a e b se, e somente se, $M|a$, $M|b$ e, dado qualquer n tal que $n|a$ e $n|b$, temos que $n \leq M$.*

[49] Veja o Alongamento 14.1.

[50] Essa definição não se parece muito com o que o nome indica - mas veremos depois que ela chega no mesmo lugar - mas ela é mais prática neste contexto.

[51] Note que se $a = 0$, pode ser que o máximo divisor comum entre a e b não exista. Por exemplo, não existe máximo divisor comum entre 0 e 3, pois o único divisor de 0 é o próprio 0 e 0 não é divisor de 3.

Demonstração. Suponha que M é o máximo divisor comum entre a, b. Pela definição, já temos que $M|a$ e $M|b$. Assim, dado n tal que $n|a$ e $n|b$, resta mostrar que $n \leq M$. Temos dois casos:

- Se $n < 0$, então $n < M$, já que $M \geq 0$.
- Se $n \geq 0$, então pela definição de máximo divisor comum entre a e b, temos que $n|M$. Logo, como $M, n \in \mathbb{N}$, pela Proposição 14.2, temos que $n \leq M$ como queríamos.

Slide 275

Agora suponha M como no enunciado. Primeiramente, note que $M \geq 0$. Pois, caso contrário, teríamos que $-M$ também seria um divisor de a e b e $M < -M$, contrariando a definição de M. Assim, M satisfaz as condições (a) e (b) da definição de máximo divisor comum. Seja $d = mdc(a, b)$. Pela definição de d, temos que $M|d$. Ou seja, $M \leq d$. Por outro lado, temos que $d \leq M$ pela definição de M. Logo, $M = d$. □

Relacionando com primos

Slide 276

Proposição 14.10. *Se p é primo e $p \not| a$ para $a \in \mathbb{Z}$, então $mdc(p, a) = 1$.*

Demonstração. Seja $d \geq 0$ tal que $d|a$ e $d|p$. Note que, como p é primo, temos que $d = p$ ou $d = 1$. Como $p \not| a$, temos que $d = 1$. □

Slide 277

Proposição 14.11. *Sejam p primo e $a, b \in \mathbb{Z}$ tais que $p|ab$. Então $p|a$ ou $p|b$.*

Demonstração. Suponha que $p \not| a$. Então $mdc(a, p) = 1$. Sejam $x, y \in \mathbb{Z}$ tais que $ax + py = 1$. Assim, temos que $b = abx + pby$. Seja k tal que $pk = ab$. Temos que $b = pkx + pby = p(kx + by)$. Logo, $p|b$. □

Slide 278

Corolário 14.12. *Se p é um primo e $p|a_1 \cdots a_n$, então existe j tal que $p|a_j$.*

Demonstração. Vamos provar por indução sobre n. Note que o caso $n = 2$ é o que foi feito anteriormente. Agora suponha que vale o caso n e vamos provar o caso $n + 1$. Suponha $p|a_1 \cdots a_{n+1}$. Se $p|a_{n+1}$, terminamos. Caso contrário, $p|a_1 \cdots a_n$ (pela proposição anterior). Assim, por hipótese de indução, temos que $p|a_j$ para algum $j = 1, ..., n$. □

Unicidade da decomposição

Slide 279

Teorema 14.13. *A decomposição feita na Proposição 14.4 é única a menos da ordem dos fatores.*

Demonstração. Seja $a \in \mathbb{Z}$ com $a > 1$. Sejam $p_1, ..., p_n, q_1, ..., q_m$ primos tais que[52] $a = p_1 \cdots p_n = q_1 \cdots q_m$. Vamos mostrar que $p_1 = q_1$. Suponha que $p_1 \leq q_1$ (o outro caso é análogo). Note que $p_1|a$, então $p_1|q_1 \cdots q_m$. Assim, p_1 divide algum dos q_j's e, portanto, é igual a algum deles. Como q_1 é o menor dos q_j's, temos que $q_1 \leq p_1$ - como a gente já tinha suposto $p_1 \leq q_1$, temos a igualdade.

Slide 280

Agora, aplicando a lei do cancelamento, temos que

$$p_2 \cdots p_n = q_2 \cdots q_m.$$

Com argumento análogo ao anterior, obtemos que $p_2 = q_2$. Repetimos o processo até "acabar" com os primos de um lado (sobrando 1 do outro lado). Note que teríamos um produto de primos resultando em 1 - ou seja, a única possibilidade é se os primos do outro lado também acabarem. Em outras palavras, $n = m$. □

Congruência

Slide 281

Definição 14.14. Seja $m \in \mathbb{N}$, com $m \neq 0$. Considere a seguinte relação sobre $\mathbb{Z}$: $a \equiv_m b$ se, e somente se, $m|a - b$ (para $a, b \in \mathbb{Z}$). A notação mais usual para isso é $a \equiv b \mod m$.

Slide 282

Proposição 14.15. *A relação $\equiv_m$ definida acima é uma relação de equivalência sobre $\mathbb{Z}$.*

Demonstração. Sejam $a, b, c \in \mathbb{Z}$. Temos:

(a) $a \equiv_m a$: Temos que $m|a - a$ pois $a - a = 0$;

(b) Se $a \equiv_m b$, então $b \equiv_m a$: De fato, se $m|a - b$, então existe $n \in \mathbb{Z}$ tal que $mn = a - b$. Logo, $-nm = b - a$ e, portanto, $m|b - a$;

(c) Se $a \equiv_m b$ e $b \equiv_m c$, então $a \equiv_m c$: Seja $p \in \mathbb{Z}$ tal que $pm = a - b$ e seja $q \in \mathbb{Z}$ tal que $qm = b - c$. Temos que $pm + qm = a - b + b - c$, isto é, $(p + q)m = a - c$. Logo, $m|a - c$ com queríamos.

□

Slide 283

Proposição 14.16. *Sejam $a, b, c, d \in \mathbb{Z}$ e $m \in \mathbb{Z}$ com $m \neq 0$. Temos:*

- *Se $a \equiv_m b$, então $-a \equiv_m -b$;*
- *Se $a \equiv_m b$, então $a + c \equiv_m b + c$;*
- *Se $a \equiv_m b$, então $ac \equiv_m bc$;*
- *Se $a \equiv_m b$ e $c \equiv_m d$, então $a + c \equiv_m b + d$;*
- *Se $a \equiv_m b$ e $c \equiv_m d$, então $ac \equiv_m bc$;*
- *Se $r \in \mathbb{N}$ e $a \equiv_m b$, então $a^r \equiv_m b^r$.*

Demonstração.

- Temos que $m|a - b$. Note que $m|b - a$.
- Temos que $m|a - b$. Note que $(a + c) - (b + c) = a - b$. Logo, $m|(a + c) - (b + c)$;
- Temos que $m|a - b$. Note que $m|c(a - b)$.

Slide 284

- Temos que $m|a-b$ e $m|c-d$. Assim, existem $x, y \in \mathbb{Z}$ tais que $mx = a-b$ e $my = c-d$. Logo, $(a+c)-(b+d) = (a-b)+(c-d) = mx+my = m(x+y)$. Logo, $m|(a+c)-(b+d)$.
- Temos que $m|a-b$ e $m|c-d$. Assim, existem $x, y \in \mathbb{Z}$ tais que $mx = a-b$ e $my = c-d$. Logo, $ac-bd = ac-bc+bc-bd = c(a-b)+b(c-d) = cmx+bmy = m(cx+by)$. Assim, $m|ac-bd$.
- Vamos mostrar por indução sobre r. Note que vale para $r = 0$, pois $1 \equiv_m 1$. Suponha que vale para $r = n$ e vamos mostrar para $r = n+1$. Temos que $a \equiv_m b$, logo, pela hipótese de indução, temos que $a^n \equiv_m b^n$. Assim, pelo item (e), temos que $a^n a \equiv_m b^n b$. Isto é, $a^{n+1} \equiv_m b^{n+1}$.

□

Slide 285

Proposição 14.17. *Sejam $a, b \in \mathbb{Z}$ e $m \in \mathbb{N}$ com $m \neq 0$. Sejam r_1, r_2 dados pelo algoritmo da divisão de Euclides de a e b por m, isto é, $a = mq_1 + r_1$ e $b = mq_2 + r_2$ com $0 \leq r_1, r_2 < m$. Então $a \equiv_m b$ se, e somente se, $r_1 = r_2$.*

Demonstração. Suponha que $a \equiv_m b$. Queremos mostrar que $r_1 = r_2$. Seja $n \in \mathbb{Z}$ tal que $mn = a-b$. Vamos fazer o caso $r_1 \geq r_2$ (o outro é análogo). Temos

$$\begin{aligned} r_1 - r_2 &= (a - mq_1) - (b - mq_2) \\ &= (a-b) + (mq_2 - mq_1) \\ &= mn - m(q_2 - q_1) \\ &= m(n - q_2 + q_1) \end{aligned}$$

Slide 286

Logo, $m|r_1 - r_2$. Note que $r_1 < m$, logo, $r_1 - r_2 < m$. Assim, a única possibilidade para que $m|r_1 - r_2$ é se $r_1 - r_2 = 0$, isto é, $r_1 = r_2$ como queríamos.

Agora suponha que $r_1 = r_2$. Temos que $a-b = mq_1 - r_1 - (mq_2 - r_2) = m(q_1 - q_2)$. Isto é, $m|a-b$. □

Exemplos

Slide 287

Exemplo 14.18. Como fazer para descobrir em que dia da semana cai uma data que vai ocorrer daqui a 40 dias? E 500?

Vamos dar um número de 0 a 6, para cada dia da semana, começando no domingo. Vamos supor que o dia 0 cai num domingo. Logo o dia 1, cai numa segunda. E o dia 8? Bom, temos que $8 = 7 + 1$. Note que esse 7 representa uma "volta" completa na semana. Então é "domingo" mais um dia. Isto é, segunda. Se fosse o dia 20, teríamos $20 = 2 \cdot 7 + 6$. Note que os múltiplos de 7 marcam as "voltas" completas na semana, assim, temos que tal dia é "domingo" mais 6 dias. Isto é, sábado. Vamos calcular em que dia semana será uma data daqui a 90 dias. No nosso exemplo, vamos supor que hoja é sexta. Logo, o dia associado é 5.

Assim, daqui a 90 dias, será o resto de 95 dividido por 7. Como $95 = 13 \cdot 7 + 4$, teremos que o dia da semana será o correspondente a 4, isto é, quinta.

Slide 288

Exemplo 14.19. Qual é o o último dígito de 27^{500}? Primeiramente, note que o último digito de um número é o resto da divisão de tal número por 10. Ou seja, queremos achar a entre 0 e 9 de forma que $a \equiv_{10} 27^{500}$. A primeira coisa que podemos notar é que $27 \equiv_{10} 7$. Logo, $a \equiv_{10} 7^{500}$. Note também que $7^2 = 49$. Logo $7^2 \equiv_{10} 49 \equiv_{10} 9 \equiv_{10} -1$. Assim, $7^{500} = (7^2)^{250} \equiv_{10} (-1)^{250} \equiv_{10} 1$. Logo, o último dígito de 27^{500} é 1.

Exemplo 14.20. Maneira alternativa de resolver o problema anterior: Partimos do ponto em que temos que $27^{500} \equiv 7^{500}$. Vejamos como se comportam as potências de 7 módulo 10. Temos $7^0 \equiv 1$, $7^1 \equiv_{10} 7$, $7^2 \equiv_{10} 9$, $7^3 \equiv_{10} 3$, $7^4 \equiv_{10} 1$, ou seja, elas formam um ciclo de comprimento 4. Assim, temos que $7^{500} \equiv_{10} 7^0 \equiv_{10} 1$, pois 500 tem resto 0 na divisão por 4.

Alongamentos da Aula 14

Alongamento 14.1. Seja $p > 1$. Mostre que p é primo se, e somente se, p é minimal com relação a ordem $|$ (divide) restrita a $\{a \in \mathbb{N} : a > 1\}$.

Exercícios da Aula 14

Exercício 14.1. Sejam $a, b \in \mathbb{Z}$. Mostre que se $a|b$, então $mdc(a, b) = |a|$.

Exercício 14.2. Sejam $a, b \in \mathbb{Z}$. Dizemos que $x \in \mathbb{Z}$ é um múltiplo de a se existe $y \in \mathbb{Z}$ tal que $ay = x$. Defina o **mínimo múltiplo comum** (denotado por $mmc(a, b)$) como sendo o mínimo do conjunto $M = \{m \in \mathbb{N} : (\exists p \in \mathbb{Z}\ ap = m) \wedge (\exists q \in \mathbb{Z}\ bq = m)\}$. Mostre que M necessariamente é não vazio (assim garantimos a existência do mínimo).

Exercício 14.3. Sejam $a, b \in \mathbb{N}$, tais que $a, b > 0$.

(a) Mostre que existe k tal que $b = mdc(a, b)k$;

(b) Mostre que ak é múltiplo de b;

(c) Note que $mmc(a, b) \leq ak$;

(d) Mostre que $mmc(a, b)mdc(a, b) \leq ab$.

Exercício 14.4. Mostre que um número $n \in \mathbb{N}$ é múltiplo de 4 se, e somente se, o número formado pelos seus dois últimos dígitos é múltiplo de 4.

Exercício 14.5. Seja $n \in \mathbb{N}$ ímpar. Mostre que $2^n + 1$ é divisível por 3.

Exercício 14.6. Prove que todo ano (incluindo bissextos) tem pelo menos uma sexta-feira 13.

Exercício 14.7. Sejam $a, b \in \mathbb{N}$ com $b > 0$. Sejam $q_1, q_2, r_1, r_2 \in \mathbb{N}$ tais que $a = bq_1 + r_1 = bq_2 + r_2$ com $0 \leq r_1, r_2 < b$. Mostre que $q_1 = q_2$ e $r_1 = r_2$ (isto é, mostre que a resposta do algoritmo de Euclide é única).

Exercício 14.8. Dizemos que um número $n \in \mathbb{N}$ é **par** se $2|n$. Dizemos que n é **ímpar** caso contrário.

(a) Mostre que todo número par pode ser escrito na forma $2k$, onde $k \in \mathbb{N}$;

(b) Mostre que todo número ímpar pode ser escrito na forma $2k + 1$, onde $k \in \mathbb{N}$;

(c) Mostre que todo número da forma $2k$ é par (para $k \in \mathbb{N}$);

(d) Mostre que todo número da forma $2k + 1$ é ímpar (para $k \in \mathbb{N}$);

(e) Seja $n \in \mathbb{N}$. Mostre que n^2 é par se, e somente se, n é par.

Exercício 14.9. Sejam $p_1, ..., p_n$ primos. Mostre que p_i não divide $p_1 \cdot \cdots \cdot p_n + 1$ para qualquer $i = 1, ..., n$.

Exercício 14.10. Mostre que existem infinitos primos.

[52] Só escrevemos os primos em ordem crescente

Aula 15

Inteiros mod n

Slide 290

Definição 15.1. Dado $n \in \mathbb{N}_{>1}$, vamos chamar de **inteiros mod n**[53] o conjunto $\mathbb{Z}/\equiv_n$ com as operações usuais. Por comodidade, vamos denotar os elementos de tal conjunto por $0, ..., n-1$. Vamos denotar tal conjunto por MOD_n.

Slide 291

Vamos adotar o seguinte abuso: dados $a, b \in MOD_n$, podemos nos referir a eles como $a = b$ (pensando neles como as clases) ou $a \equiv_n b$ (pensando neles com representantes das classes). Note que isso não dá problema pois existe um único representante entre $0, ..., n-1$.

Propriedades básicas

Slide 292

Proposição 15.2. *Seja p primo. Sejam $a, b \in MOD_p$. Se $ab \equiv_p 0$, então $a \equiv_p 0$ ou $b \equiv_p 0$.*

Demonstração. Note que se $ab \equiv_p 0$, então $p|ab$. Como p é primo, temos que $p|a$ ou $p|b$. O primeiro caso implica que $a \equiv_p 0$ e o segundo implica que $b \equiv_p 0$. □

Slide 293

Proposição 15.3. *Seja p primo e sejam a, x, y inteiros módulo p, com $a \not\equiv_p 0$. Se $ax \equiv_p ay$, então $x \equiv_p y$.*

Demonstração. Como $ax \equiv_p ay$, temos que $ax - ay \equiv_p 0$. Isto é,

$$a(x-y) \equiv_p 0$$

Pelo resultado anterior, temos que $a \equiv_p 0$ ou $(x-y) \equiv_p 0$. Como $a \not\equiv_p 0$, temos que $x \equiv_p y$ como queríamos. □

Slide 294

Lema 15.4. *Seja p primo. Seja a um inteiro mod p tal que $a \not\equiv_p 0$. Temos que $\pi_a : MOD_p \to MOD_p$ dada por $\pi_a(x) = ax$ é injetora.*

Demonstração. Suponha $x, y \in MOD_p$. Note que $\pi_a(x) = \pi_a(y)$ quer dizer $ax \equiv_p ay$. Pelo resultado anterior, temos que $x = y$. □

Slide 295

Corolário 15.5. *Seja p primo. Seja a um inteiro mod p tal que $a \not\equiv_p 0$. Temos que $\pi_a : MOD_p \to MOD_p$ dada por $\pi_a(x) = ax$ é bijetora.*

Demonstração. Note [54]que, como a função é injetora, ela tem p elementos na imagem. Como o contradomínio também tem p elementos, temos que a função é sobrejetora. □

Slide 296

Proposição 15.6. *Seja p primo. Seja $a \in MOD_p$ com $a \neq 0$. Então existe um único $b \in MOD_p$ tal que $ab = 1$. Muitas vezes vamos denotar tal elemento por a^{-1}.*

Demonstração. Considere a função π_a acima. Como ela é sobrejetora, existe $b \in MOD_p$ tal que $\pi_a(b) = 1$. Isto é, $ab = 1$.

Vejamos agora que ele é único. Sejam $b, c \in MOD_p$ tais que $ab = 1$ e $ac = 1$. Então, pela Proposição 15.3, temos de $ab = ac$ que $b = c$. □

Corpo

Slide 297

Definição 15.7. Dizemos que $(F, \oplus, \odot)$ é[55]um **corpo** se $\oplus$ e $\odot$ são associativas, comutativas e ainda valem, para todo $a, b, c \in F$:

(i) $a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$;

(ii) Existe $0 \in F$ tal que $0 \oplus x = x$ para todo $x \in F$;

(iii) Existe $1 \in F$ tal que $1 \odot x = x$ para todo $x \in F$;

(iv) Existe $x \in F$ tal que $a \oplus x = 0$;

(v) Se $a \neq 0$, existe $x \in F$ tal que $x \odot a = 1$.

Exemplos

Slide 298

Tanto os racionais como os reais satisfazem a definição de corpo com as operações usuais.

MOD_p é corpo

Slide 299

Proposição 15.8. *Seja p primo. Então MOD_p é um corpo com as operações usuais.*

Demonstração. Note que as operações serem associativas, comutativas e a regra de distributividade seguem diretamente das mesmas propriedades sobre $\mathbb{Z}$. Note que 0 e 1 também fazem os papeis de elementos neutros em MOD_p. Dado $a \in MOD_p$, note que $a + (p - a) = p \equiv_p 0$. Já a última propriedade é simplesmente a Proposição 15.6. □

Propriedades de corpos

Slide 300

Vamos ver algumas propriedades simples sobre corpos:

Lema 15.9. *Seja F um corpo. Dado $x \in F$, temos que $0x = 0$.*

[53] O nome não é bem esse, mas todo mundo usa na hora de falar.

[54] Note que esse argumento não vale para conjuntos infinitos.

[55] Normalmente vamos denotar $\oplus$ por $+$ e $\odot$ por $\cdot$ (ou mesmo omitir o símbolo, como usualmente).

Demonstração. Seja $y \in F$ tal que $0x + y = 0$. Temos

$$0x = (0 + 0)x = 0x + 0x$$

Somando y dos dois lados, obtemos

$$0 = 0x + y = 0x + 0x + y = 0x$$

como queríamos. □

Slide 301

Proposição 15.10. *Seja F um corpo*[56]*. Sejam $a, b \in F$ tais que $ab = 0$. Então $a = 0$ ou $b = 0$.*

Demonstração. Suponha que $a \neq 0$. Vamos provar que $b = 0$ (note que isso é suficiente para o que queremos). Então existe $x \in F$ tal que $ax = 1$. Assim, de $0 = ab$, temos $0x = xab$. Como $0x = 0$ pelo lema anterior, temos que $0 = b$. □

Quando MOD_m não é corpo

Slide 302

No caso em que $m \in \mathbb{Z}_{>1}$ mas não é primo, temos que MOD_m não é corpo.

Proposição 15.11. *Seja $m \in \mathbb{Z}_{>1}$ não primo. Então MOD_m não é corpo.*

Demonstração. Note que, pelo resultado anterior, basta mostrarmos que existem $a, b \in MOD_n$ não nulos tais que $ab = 0$. Como m não é primo, existe a tal que $a|m$ e $a \neq 1$ e $a \neq m$. Seja b tal que $ab = m$. Note que $b \neq 1$ e $b \neq m$. Note também que $a, b \neq 0$. Mas temos

$$ab = m \equiv_m 0.$$

□

Primos entre si

Slide 303

Definição 15.12. Dizemos que $a, b \in \mathbb{Z}_{>1}$ são **primos entre si** se $mdc(a, b) = 1$.

Algumas propriedades básicas

Slide 304

Lema 15.13. *Sejam a, b primos entre si. Seja $z \in \mathbb{Z}$. Se $a|z$ e $b|z$, então $ab|z$.*

Demonstração. Como $a|z$, existe m tal que $am = z$. Como $b|z$, existe n tal que $bn = z$. Sejam $x, y \in \mathbb{Z}$ tais que $ax + by = 1$. Multiplicando tal equação por z dos dois lados, temos

$$\begin{aligned} z &= z(ax + by) \\ &= zax + zby \\ &= bnax + amby \\ &= ab(nx + my) \end{aligned}$$

Ou seja, $ab|z$. □

Slide 305

Lema 15.14. *Sejam $a, b, c \in \mathbb{N}$ primos entre si. Então ab e c são primos entre si.*

Demonstração. Seja x divisor comum entre ab e c. Suponha que $x \neq 1$. Então existe p primo tal que $p|x$. Logo, $p|ab$ e $p|c$. Como $p|ab$, temos que $p|a$ ou $p|b$. Logo, a e c não são primos entre si, ou b e c não são primos entre si. □

Slide 306

Corolário 15.15. *Sejam $a_1, ..., a_n, b \in \mathbb{N}_{>1}$ primos entre si. Então $a_1 \cdots a_n$ e b são primos entre si.*

Demonstração. Por indução sobre n. Se $n = 2$, é exatamente o lema anterior. Note que, por hipótese de indução, temos que $a_1 \cdots a_n$, a_{n+1} e b são primos entre si. Então, novamente pelo lema, temos que $a_1 \cdots a_{n+1}$ e b são primos entre si. □

Slide 307

Proposição 15.16. *Sejam a, b primos entre si. Sejam r e s inteiros. Então o sistema*

$$\begin{cases} x \equiv_a r \\ x \equiv_b s \end{cases}$$

admite alguma solução c e é equivalente a

$$x \equiv_{ab} c$$

Demonstração. Como a e b são primos entre si, existem $\alpha, \beta \in \mathbb{Z}$ tais que

$$\alpha a + \beta b = 1.$$

Slide 308

Considere

$$c = s\alpha a + r\beta b.$$

Vamos mostrar que tal c satisfaz as condições do enunciado. Suponha que x seja uma solução para $x \equiv_{ab} c$. Ou seja, existe $k \in \mathbb{Z}$ tal que

$$x = c + kab = s\alpha a + r\beta b + kab.$$

Vejamos que tal x é, de fato, uma solução para o sistema.

Slide 309

Primeiramente, temos que

$$\begin{aligned} x - r &= s\alpha a + r\beta b + kab - r \\ &= s\alpha a + r(\beta b - 1) + kab \\ &= s\alpha a - \alpha a r + kab \\ &= a(s\alpha - r\alpha + kb) \end{aligned}$$

Ou seja, temos que

$$x \equiv_a r.$$

De forma análoga, podemos mostrar que $x \equiv_b s$.

Slide 310

Agora suponha x uma solução para o sistema. Note que, pelo que vimos acima, c é uma solução para o sistema. Logo:

$$x \equiv_a c$$

$$x \equiv_b c$$

Ou seja, $a|(x-c)$ e $b|(x-c)$. Como a, b são primos entre si, pelo Lema 15.13, temos que $ab|(x-c)$. Ou seja, $x \equiv_{ab} c$. □

Teorema chinês do resto

Slide 311

Corolário 15.17 (Teorema chinês do resto)**.** *Sejam $a_1, ..., a_n$ primos entre si e sejam $r_1, ..., r_n \in \mathbb{Z}$. Então o sistema*

$$\begin{cases} x & \equiv_{a_1} & r_1 \\ & \vdots & \\ x & \equiv_{a_n} & r_n \end{cases}$$

admite solução b e é equivalente à equação $x \equiv_A b$, onde $A = a_1 \cdots a_n$.

Demonstração. Vamos provar por indução sobre n. O caso 2 é o resultado anterior. Suponha então que temos $n+1$ equações como no enuciado. Por hipótese de indução, existe b' tal que o sistema formado pelas primeiras n equações é equivalente a $x \equiv_{A'} b'$, onde $A' = a_1 \cdots a_n$.

Slide 312

Pelo Corolário 15.15, temos que a_{n+1} e A' são primos entre si. Assim, novamente pelo resultado anterior, temos que existe b tal que o sistema

$$\begin{cases} x & \equiv_{A'} & b' \\ x & \equiv_{a_{n+1}} & r_{n+1} \end{cases}$$

é equivalente a

$$x \equiv_A b$$

onde $A = A'a_{n+1} = a_1 \cdots a_{n+1}$. Ou seja, a última equação é equivalente ao sistema do enunciado. □

Exemplo

Slide 313

Qual o menor natural k tal que k dividido por 3 tem resto 2, dividido por 5 tem resto 3 e dividido por 7 tem resto 2?

Primeiramente, note que a pergunta é equivalente a perguntar qual a menor solução positiva para

$$\begin{cases} x & \equiv_3 & 2 \\ x & \equiv_5 & 3 \\ x & \equiv_7 & 2 \end{cases}$$

Slide 314

Já sabemos que tal sistema é equivalente a uma equação da forma

$$x \equiv_{105} a$$

[56] Espaços que satisfazem isso são chamados de **domínios de integridade**.

para algum a. Podemos simplesmente repetir o processo da demonstração do resultado para calcular o a, mas há um modo mais fácil. A terceira equação é equivalente a encontrar b tal que $x = 7b + 2$. Substituindo na segunda equação, obtemos $7b + 2 \equiv_5 3$. Ou seja $2b \equiv_5 1$. Lembrando que 3 é o inverso de 2 em MOD_5, multiplicando ambos os lados por 3, temos

$$b \equiv_5 3.$$

Slide 315

Ou seja, existe c tal que $b = 5c + 3$. Substituindo o b, temos $x = 7b + 2 = 7(5c + 3) + 2 = 35c + 23$. Substituindo na primeira equação $35c + 23 \equiv_3 2$ Ou seja

$$2c \equiv_3 0.$$

Assim,

$$c \equiv_3 0.$$

Slide 316

Logo, existe d tal que $c = 3d$. Voltando na equação com x:

$$x = 35c + 21 = 35(3d) + 23 = 105d + 23.$$

Para termos o menor k possível, fazemos $d = 0$ e, portanto, $k = 23$.

Exercícios da Aula 15

Exercício 15.1. Considere $\mathbb{R}^2$ com as seguintes operações:

$$(a, b) \oplus (x, y) = (a + x, b + y)$$

$$(a, b) \odot (x, y) = (ax, by)$$

Com essas operações, $\mathbb{R}^2$ é um corpo?

Exercício 15.2. Os seguintes sistemas admitem soluções?[57]

(a) $\begin{cases} x \equiv_2 1 \\ x \equiv_6 3 \end{cases}$

(b) $\begin{cases} x \equiv_2 1 \\ x \equiv_6 4 \end{cases}$

Exercício 15.3. Considere uma pista circular. O carro A demora 5 minutos para dar uma volta completa. Já o carro B, demora 3 minutos para dar uma volta completa e larga 17 minutos depois do carro A. Finalmente, o carro C demora 4 minutos para dar uma volta e larga 8 minutos depois do carro B. Supondo que esses carros fiquem dando voltas com velocidades constantes, é verdade que eles passarão pela chegada ao mesmo tempo em algum momento? Se sim, quantos minutos depois da largada do carro A será o primeiro momento em que isso ocorre?

[57] Compare com o enunciado do Teorema chinês do resto.

Aula 16

Racionais

Slide 317

Definição 16.1. Considere o conjunto[58] $A = \{(a, b) \in \mathbb{Z} : b \neq 0\}$ e considere $\sim$ a seguinte relação sobre A: dados $(a, b), (x, y) \in A$, definimos $(a, b) \sim (x, y)$ se, e somente se, $ay = bx$.

Slide 318

Proposição 16.2. *A relação $\sim$ definida acima é uma relação de equivalência sobre A.*

Demonstração. Note que $(a, b) \sim (a, b)$. Também temos que $(a, b) \sim (x, y)$ implica que $(x, y) \sim (a, b)$. Agora vejamos a transitiva. Sejam $(a, b), (x, y), (\alpha, \beta) \in A$ tais que $(a, b) \sim (x, y)$ e $(x, y) \sim (\alpha, \beta)$. Temos que mostrar que $(a, b) \sim (\alpha, \beta)$. Isto é, $a\beta = b\alpha$. Temos

$$ay = bx$$

$$x\beta = y\alpha.$$

Assim, multiplicando por β a primeira equação, temos $ay\beta = bx\beta$. Logo, $ay\beta = by\alpha$. Como $y \neq 0$, temos $a\beta = b\alpha$ como queríamos. □

Slide 319

Definição 16.3. Denotamos por $\mathbb{Q}$ o conjunto $A/\sim$. Chamamos tal conjunto de conjunto dos **números racionais**.

A soma

Slide 320

Definição 16.4. Definimos[59] a operação de **soma** sobre os racionais da seguinte maneira: dados $[(a, b)], [(x, y)] \in \mathbb{Q}$, definimos $[(a, b)] + [(x, y)] = [(ay + xb, by)]$.

Slide 321

Proposição 16.5. *A operação de soma está bem definida.*

Demonstração. Primeiramente, note que, de fato, $(ay + xb, by) \in A$, já que $by \neq 0$ (pois tanto b como y são diferentes de 0). Agora vamos mostrar que ela independe dos representantes. Sejam $(a, b), (c, d), (x, y), (w, z) \in A$ tais que $(a, b) \sim (x, y)$ e $(c, d) \sim (w, z)$. Vamos mostrar que $(ad + cb, db) \sim (xz + wy, yz)$ isto é, $(ad + cb)yz = (xz + wy)db$. Temos $ay = bx$ e $cz = dw$. Logo

$$\begin{aligned} (ad + cb)yz &= adyz + cbyz \\ &= aydz + czby \\ &= bxdz + dwby \\ &= (xz + wy)db \end{aligned}$$

□

O produto

Slide 322

Definição 16.6. Definimos[60] a operação de **produto** sobre os racionais da seguinte maneira: dados $[(a,b)], [(x,y)] \in \mathbb{Q}$, definimos $[(a,b)] \cdot [(x,y)] = [(ax, by)]$.

Slide 323

Proposição 16.7. *A operação de produto está bem definida.*

Demonstração. Veja o Exercício 16.2. □

Forma canônica

Slide 324

Definição 16.8. Dizemos que um elemento $[(a,b)] \in \mathbb{Q}$ está na **forma canônica** se $b > 0$.

Slide 325

Proposição 16.9. *Todo número $q \in \mathbb{Q}$ admite uma representação na forma canônica.*

Demonstração. Seja $[(a,b)] = q$. Se $b > 0$, nada temos a fazer. Se $b < 0$, observe que $[(-a,-b)] = [(a,b)]$ (pois $-ab = -ba$) e $[(-a,-b)]$ está na forma canônica. □

Ordem

Slide 326

Definição 16.10. Sejam $q, r \in \mathbb{Q}$. Dizemos que $q \leq r$ se $ay \leq xb$ se $q = [(a,b)]$, $r = [(x,y)]$ e $[(a,b)]$ e $[(x,y)]$ estão na forma canônica.

Slide 327

Proposição 16.11. *A relação $\leq$ definida acima está bem definida.*

Demonstração. Precisamos mostrar que se valem

$$[(a_1,b_1)] = [(a_2,b_2)]$$
$$[(x_1,y_1)] = [(x_2,y_2)]$$
$$[(a_1,b_1)] \leq [(x_1,y_1)]$$

então vale $[(a_2,b_2)] \leq [(x_2,y_2)]$.

Slide 328

Note que as duas primeiras equações se traduzem para $a_1b_2 = b_1a_2$ e $x_1y_2 = y_1x_2$. Assim, de $a_1y_1 \leq b_1x_1$, multiplicando ambos os lados por b_2y_2 (que é maior que 0), temos

$$a_1y_1b_2y_2 \leq b_1x_1b_2y_2.$$

Substituindo a_1b_2 por b_1a_2 do lado esquerdo e x_1y_2 por x_2y_1 do lado direito, obtemos:

$$b_1a_2y_1y_2 \leq b_2y_1x_2b_1.$$

Cancelando b_1y_1 (que é diferente de 0), temos $a_2y_2 \leq b_2x_2$, isto é, $[(a_2,b_2)] \leq [(x_2,y_2)]$ como queríamos. □

[58] Intuitivamente, estamos querendo que (a,b) represente $\frac{a}{b}$. Então, para $\frac{a}{b} = \frac{x}{y}$, temos a condição apresentada.

[59] Aqui é só pensar que estamos fazendo a soma usual, mas sem simplificar.

[60] Novamente, isso é apenas a operação usual, sem simplificações.

Slide 329

Proposição 16.12. *A relação $\leq$ definida acima é uma ordem total sobre $\mathbb{Q}$.*

Demonstração. Ver o exercício 16.4 □

Notação

Slide 330

Definição 16.13. Seja $[(a, b)] \in \mathbb{Q}$ escrito na forma canônica. Denotamos $[(a, b)]$ por $\frac{a}{b}$. No caso em que $b = 1$, utilizamos simplesmente a.

Note que tal notação fica coerente com o que tínhamos antes. Isto é, $\frac{a}{1} + \frac{b}{1} = \frac{a+b}{1} = a + b$, onde a última soma é entre inteiros. Note que temos a mesma coisa para o produto.

Assim, como fizemos antes no caso de $\mathbb{N}$ para $\mathbb{Z}$, vamos considerar que $\mathbb{Z} \subset \mathbb{Q}$ como usualmente.

É corpo

Slide 331

Veja nos exercícios que, com as operações aqui apresentadas, $\mathbb{Q}$ é corpo.

Exercícios da Aula 16

Exercício 16.1. Qual o problema com a relação $\sim$ se deixarmos A conter pontos da forma $(x, 0)$?

Exercício 16.2. Mostre que o produto dos racionais está bem definido. Atenção, mostre também que o resultado de tal operação pertence a $\mathbb{Q}$ (veja o começo da demonstração da Proposição 16.5).

Exercício 16.3. Mostre que a soma e o produto são associativas, comutativas e que vale a distributiva.

Exercício 16.4. Mostre que a relação $\leq$ definida acima é uma ordem total sobre $\mathbb{Q}$.

Exercício 16.5. Encontre um elemento neutro para a soma. Mostre que ele é único.

Exercício 16.6. Encontre um elemento neutro para o produto. Mostre que ele é único.

Exercício 16.7. Mostre que se $q \in \mathbb{Q}$ e $q \neq 0$, então existe $r \in \mathbb{Q}$ tal que $qr = 1$. Neste caso dizemos que r é o **inverso** de q e o denotamos por q^{-1}. Mostre que tal inverso é único.

Exercício 16.8. Definimos a **divisão** em $\mathbb{Q}$ como sendo, dados $a, b \in \mathbb{Q}$, com $b \neq 0$, $\frac{a}{b} = ab^{-1}$. Mostre que isso é coerente com a notação que já tínhamos, isto é, se $a, b \in \mathbb{Z}$ com $b \neq 0$, então $[(a, b)] = \frac{a}{b} = ab^{-1}$.

Aula 17

Números reais

Slide 332

Vamos ver agora como definir o conjunto dos números reais, supondo já conhecido o conjunto dos racionais. Veremos duas maneiras[61] de se fazer isso. A primeira, usa mais a ideia de ordem. A segunda, trabalha mais com a noção de convergência de sequências.

Começamos estendendo a noção de intervalo apresentada anteriormente. Antes, definimos intervalo apenas para $\mathbb{R}$. Mas podemos fazer o mesmo para qualquer conjunto totalmente ordenado:

Definição 17.1. Seja X um conjunto totalmente ordenado. Um subconjunto $A \subset X$ é um intervalo se, dados $a, b \in A$ tais que $a < b$, se $c \in X$ é tal que $a < c < b$, então[62] $c \in A$.

Exemplos

Slide 333

Note que, nesse contexto, algo ser um intervalo ou não depende de "onde" ele é subconjunto.

O conjunto $\{n \in \mathbb{N} : 3 < n \text{ e } n < 20\}$ é um intervalo nos naturais. O conjunto $\{q \in \mathbb{Q} : 3 < q \text{ e } q < 20\}$ também é um intervalo em $\mathbb{Q}$. Mas o conjunto $\{n \in \mathbb{Q} : 3 < n, n < 20 \text{ e } n \in \mathbb{N}\}$ não é um intervalo em $\mathbb{Q}$.

Corte de Dedekind

Slide 334

Definição 17.2. Chamamos [63]de um **corte de Dedekind** um par (I, J) onde $I, J \subset \mathbb{Q}$ são intervalos não vazios tais que

- $I \cup J = \mathbb{Q}$;
- se $i \in I$, existe $k \in I$ tal que $i < k$;
- dados $i \in I$ e $j \in J$ temos que $i < j$.

Exemplo

Slide 335

Exemplo 17.3. (I, J) é um corte de Dedekind, onde $I = \{q \in \mathbb{Q} : q < 0\}$ e $J = \{q \in \mathbb{Q} : q \geq 0\}$ (exercício).

Slide 336

O truque com os cortes para se construir os reais é mais ou menos o seguinte: cada corte vai representar um real e a ideia desse real é ser o elemento que fica entre I e J. No exemplo acima, o real representado é o 0. Note que ele é o mínimo de J (isso acontece com qualquer outro racional). A situação fica mais interessante quando o corte representa um irracional, como vamos ver no próximo exemplo (não vamos usar isso no exemplo, mas tenha em mente que o corte representa o número $\sqrt{2}$).

Slide 337

(I, J) é um corte de Dedekind onde $I = \{q \in \mathbb{Q} : qq < 2 \vee q < 0\}$ e $J = \{q \in \mathbb{Q} : 2 < qq \wedge q > 0\}$[64]. Primeiramente, precisamos provar que I e J são intervalos. Vamos provar que J é um intervalo (I fica como exercício). Sejam $a, b \in J$ com $a < b$. Seja $q \in \mathbb{Q}$ tal que $a < q < b$. Como $0 < a$, temos que $0 < q$. Assim, só falta mostrar que $2 < qq$. De fato, como $a < q$, temos $aa < qa$ e $aq < qq$. Logo, $aa < qq$ e, portanto, $2 < qq$.

Vejamos que $I \cup J = \mathbb{Q}$. Note que é suficiente mostrarmos que $\mathbb{Q} \subset I \cup J$. Seja $q \in \mathbb{Q}$. Se $q < 0$, $q \in I$. Se $q \geq 0$, temos dois casos. Se $qq < 2$, então $q \in I$. Se $qq > 2$, temos que $qq \in J$[65].

Slide 338

Se $i \in I$, precisamos mostrar que existe $k \in I$ tal que $i < k$. Se $i < 0$, basta tomarmos $k = \frac{i}{2}$. Se $i > 0$ e $ii < 2$, considere

$$k = \frac{2i + 2}{i + 2}.$$

Primeiramente, note que $k > i$ pois

$$\begin{array}{rcl} i & = & \frac{i(i+2)}{i+2} \\ & = & \frac{ii+2i}{i+2} \\ & < & \frac{2+2i}{i+2} \\ & = & k \end{array}$$

Slide 339

Note também que $kk < 2$, pois

$$\begin{array}{rcl} 2 - kk & = & 2 - \frac{2i+2}{i+2}\frac{2i+2}{i+2} \\ & = & 2 - \frac{4i^2+8i+4}{i^2+4i+4} \\ & = & \frac{2i^2+8i+8-(4i^2+8i+4)}{i^2+4i+4} \end{array}$$

Slide 340

Note que, como o denominador é positivo, só precisamos analisar o sinal do numerador. Assim

$$\begin{array}{rcl} 2i^2 + 8i + 8 - 4i^2 - 8i - 4 & = & 4 - 2i^2 \\ & > & 4 - 2 \cdot 2 \\ & = & 0 \end{array}$$

Ou seja, tal diferença é positiva, como queríamos.

Finalmente, só precisamos mostrar que, dados $i \in I$ e $j \in J$, temos que $i < j$ - vamos deixar isso como exercício.

Resultados básicos

Slide 341

Vamos agora provar alguns resultados básicos sobre os cortes.

Lema 17.4. *Seja (I, J) um corte de Dedekind. Se $a \in I$ e $b < a$, então $b \in I$.*

Demonstração. Suponha que não. Então $b \in J$. Mas isso contraria a última propriedade da definição de corte. □

Slide 342

[61] Mas essas duas formas são equivalentes.

[62] Note que a única diferença para a definição em $\mathbb{R}$ é que trocamos $\mathbb{R}$ por X.

[63] A ideia aqui é que o corte divide o racionais em duas "metades", uma para esquerda (no sentido de menor) e uma para direita.

[64] Faça um desenho de I e J!

[65] Note que o caso $qq = 2$ é impossível.

Note que se tomarmos $q \in \mathbb{Q}$, existe um corte natural associado a ele:

$$I_q = \{r \in \mathbb{Q} : r < q\}$$
$$J_q = \{r \in \mathbb{Q} : r \geq q\}$$

Repare que é o análogo com o que fizemos com o 0 no primeiro exemplo. Por outro lado, note que não podemos fazer o análogo com $J = \{r \in \mathbb{Q} : r > q\}$, pois neste caso $q \in I$ e, portanto, I teria máximo, o que contraria a definição de corte.

Slide 343

Note que num corte, como $I \cup J = \mathbb{Q}$ e $I \cap J = \emptyset$, o próprio I serve para determinar o corte (basta definirmos $J = \mathbb{Q} \setminus I$).

Proposição 17.5. *Dados (A, B) e (X, Y) dois cortes de Dedekind, dizemos que $(A, B) \leq (X, Y)$ se $A \subset X$. Tal relação é uma ordem total sobre o conjunto dos cortes.*

Demonstração. Que é uma relação de ordem, não há nada a provar, já que a inclusão é uma relação de ordem. Resta mostrar que tal relação é total. Sejam (A, B) e (X, Y) dois cortes. Suponha que $(A, B) \not\leq (X, Y)$, isto é, $A \not\subset X$. Vamos provar que $X \subset A$. Seja $x \in X$. Como $A \not\subset X$, existe $a \in A \setminus X$. Note que $a \in Y$. Assim, para todo $z \in X$, temos que $z < a$. Em particular, temos $x < a$. Assim, $x \in A$ pelo lema. □

Relacionando as ordens

Slide 344

A ordem aqui apresentada é compatível com a que vem de $\mathbb{Q}$:
Proposição 17.6. *Sejam $q, r \in \mathbb{Q}$. Então $q < r$ se, e somente se, $(I_q, J_q) < (I_r, J_r)$.*

Demonstração. Basta notar que, pela definição de I_q, $I_q \subset I_r$ se, e somente se, $q \leq r$. □

Majorantes

Slide 345

Definição 17.7. Seja $(X, \leq)$ conjunto totalmente ordenado e seja $A \subset X$ um conjunto não vazio. Dizemos $m \in X$ é um **majorante** para A se $a \leq m$ para todo $a \in A$. Dizemos que $A \subset X$ é **limitado superiormente** se A admite um majorante.

Exemplo

Slide 346

1 e 3 são majorantes para o conjunto $[0, 1]$ em $\mathbb{Q}$.

Supremo

Slide 347

Definição 17.8. Seja $(X, \leq)$ um conjunto totalmente ordenado. Seja $A \subset X$ um conjunto limitado superiormente. Dizemos que $a \in X$ é um **supremo** de A (notação $\sup A$), se $a = \min\{m : m$ é majorante de $A\}$.

Um caso simples

Slide 348

Proposição 17.9. *Sejam X totalmente ordenado e $A \subset X$. Se $a = \max A$, então $a = \sup A$.*

Demonstração. Seja $m \in X$ majorante para A. Em particular, $m \geq a$. Assim, $\sup A \geq a$. Por outro lado, note que o próprio a é um majorante para A. Então $\sup A \leq a$. □

Exemplo

Slide 349

Um supremo pode não existir:

Exemplo 17.10. Em $\mathbb{Q}$, não existe $\sup A$, onde $A = \{q \in \mathbb{Q} : q > 0 \wedge q^2 < 2\}$.

Unicidade

Slide 350

Mas, se o supremo existe, ele é único:

Proposição 17.11. *Seja $(X, \leq)$ conjunto totalmente ordenado e seja $A \subset X$ conjunto limitado superiormente. Sejam a, b supremos de A. Então $a = b$.*

Demonstração. Como a é o menor dos majorantes de A e como b é um majorante de A, temos que $a \leq b$. A outra desigualdade é análoga. □

Completude

Slide 351

Definição 17.12. Seja $(X, \leq)$ conjunto totalmente ordenado. Dizemos que $\leq$ é uma **ordem completa** se, para todo $A \subset X$ limitado, existe $a = \sup A$.

Slide 352

Proposição 17.13. *A ordem definida acima para o conjunto de todos os cortes de Dedekind é completa.*

Demonstração. Seja $\mathcal{A}$ um conjunto de cortes que seja limitado. Isto é, existe (I, J) tal que, para todo $(A, B) \in \mathcal{A}$, temos que $A \subset I$. Vamos provar que existe um supremo para $\mathcal{A}$. Considere (X, Y) onde

$$X = \bigcup_{(A,B)\in\mathcal{A}} A$$

$$Y = \mathbb{Q} \setminus X$$

Slide 353

Vamos provar que $(X, Y) = \sup \mathcal{A}$. Primeiramente, note que $X \neq \emptyset$, pois qualquer A tal que $(A, B) \in \mathcal{A}$ é tal que $A \neq \emptyset$ e $A \subset X$. Note também que existe $j \in J$ e que, portanto, $j \notin A$ para qualquer $(A, B) \in \mathcal{A}$. Assim, $j \in Y$ e, portanto, Y é não vazio.

Vamos provar que X é um intervalo. De fato, sejam $a, b \in X$ e $c \in \mathbb{Q}$ tais que $a < c < b$. Seja A tal que $(A, B) \in \mathcal{A}$ e tal que $b \in A$ (existe pela definição de X). Pelo Lema 17.4, temos que $c \in A$ e, portanto, $c \in X$ como queríamos. Vamos deixar o restante da prova de que (X, Y) é um corte como exercício.

Slide 354

Note que, pela definição de (X, Y), temos automaticamente que $A \subset X$ para todo $(A, B) \in \mathcal{A}$. Isto é, (X, Y) é um majorante para $\mathcal{A}$. Resta mostrar que é o menor. Para isso, basta mostrar que $X \subset I$. De fato, dado $x \in X$, temos que $x \in A$ para algum $(A, B) \in \mathcal{A}$. Como (I, J) é majorante, temos que $A \subset I$. Logo, $x \in I$ como queríamos. □

Os reais

Slide 355

Finalmente, conseguimos nossa primeira definição do conjunto $\mathbb{R}$:

Definição 17.14. Chamamos de $\mathbb{R}$ o conjunto de todos os cortes de Dedekind com a ordem apresentada acima.

Slide 356

As operações sobre $\mathbb{R}$ podem ser definidas de maneira natural a partir das operações definidas sobre $\mathbb{Q}$. Por exemplo, $(A, B) + (X, Y) = (A \oplus X, B \oplus Y)$, onde $I \oplus J = \{i + j : i \in I, j \in j\}$.

Exercícios da Aula 17

Exercício 17.1. Seja (I, J) um corte de Dedekind. Prove as seguintes afirmações:

(a) Se $q \notin I$, então $q \in J$.

(b) $I \cap J = \emptyset$.

(c) Se $q \in \mathbb{Q}$ é tal que existe $j \in J$ tal que $j < q$, então $q \in J$.

Exercício 17.2. Seja $(X, \leq)$ conjunto ordenado completo. Sejam A, B não vazios tais que B é limitado superiormente e $A \subset B$.

(a) Mostre que A é limitado superiormente.

(b) Mostre que $\sup A \leq \sup B$.

(c) Dê um exemplo nessas condições em que $A \neq B$ mas $\sup A = \sup B$.

(d) Dê um exemplo nessas condições em que $\sup A < \sup B$.

Exercício 17.3. Vamos mostrar que tentar repetir o processo não acrescenta novos números.

(a) Refaça a definição de corte, mas desta vez supondo I, J intervalos em $\mathbb{R}$ e de forma que $I \cup J = \mathbb{R}$.

(b) Note que para cada $x \in \mathbb{R}$, (I_x, J_x) é um corte (veja a definição análoga no caso de $\mathbb{Q}$).

(c) Mostre que, dado um corte (I, J), J admite mínimo (ou seja, $(I, J) = (I_x, J_x)$ para algum $x \in \mathbb{R}$ como acima).

Aula 18

Sequência convergente

Slide 357

Nesta[66] seção vamos apresentar uma segunda maneira de definir números reais.

Começamos com a ideia do que é uma sequência ser convergente para um ponto:

Definição 18.1. Seja $(q_n)_{n\in\mathbb{N}}$ uma sequência de racionais. Dizemos que tal sequência **converge para** q se, para todo $\varepsilon \in \mathbb{Q}_{>0}$, existe $n_0 \in \mathbb{N}$ tal que, para todo $m \geq n_0$, temos que $|q_m - q| < \varepsilon$.

Exemplos

Slide 358

Exemplo 18.2. Considere $(q_n)_{n\in\mathbb{N}}$ dada por $q_n = q$ para todo $n \in \mathbb{N}$. Vamos provar que $(q_n)_{n\in\mathbb{N}}$ converge para q. De fato, dado $\varepsilon \in \mathbb{Q}_{>0}$, temos

$$|q_n - q| = 0 < \varepsilon.$$

Ou seja, podemos tomar $n_0 = 0$.

Slide 359

Exemplo 18.3. A sequência $(\frac{1}{n+1})_{n\in\mathbb{N}}$ **converge** para 0. De fato, dado $\varepsilon \in \mathbb{Q}_{>0}$, note que $\varepsilon = \frac{a}{b}$ com $a, b > 0$. Seja $n_0 = b$. Note que

$$\frac{1}{b} < \frac{a}{b}$$

Assim, dado $m \geq n_0$, temos

$$\left|\frac{1}{m+1} - 0\right| = \frac{1}{m+1} < \frac{1}{m} \leq \frac{1}{n_0} = \frac{1}{b} < \frac{a}{b} = \varepsilon$$

Sequência de Cauchy

Slide 360

Intuitivamente, uma sequência convergente tem seus pontos ficando arbitrariamente próximos de um ponto fixado (para onde a sequência converge). Podemos mudar um pouco o conceito e pedir que os pontos da sequência fiquem próximos uns dos outros - mas não necessariamente próximos de um ponto fixado:

Definição 18.4. Seja $(q_n)_{n\in\mathbb{N}}$ uma sequência de racionais. Dizemos que $(q_n)_{n\in\mathbb{N}}$ é uma **sequência de Cauchy** se, para todo $\varepsilon \in \mathbb{Q}_{>0}$, existe $n_0 \in \mathbb{N}$ tal que, para todo $m, n \geq n_0$ temos $|q_n - q_m| < \varepsilon$.

Relacionando

Slide 361

Se os pontos da sequência ficam próximos de um ponto fixado, eles ficam próximos entre si:

Proposição 18.5. *Se $(q_n)_{n\in\mathbb{N}}$ é uma sequência convergente, então $(q_n)_{n\in\mathbb{N}}$ é uma sequência de Cauchy.*

[66] Uma das vantagens deste segundo método é que ele envolve conceitos que são bastante úteis em outros contextos - por exemplo, completamento de espaços métricos.

Demonstração. Seja q tal que $(q_n)_{n\in\mathbb{N}}$ converge para q. Seja $\varepsilon \in \mathbb{Q}_{>0}$. Como $(q_n)_{n\in\mathbb{N}}$ converge para q, existe n_0 tal que, para todo $k \geq n_0$, temos[67]

$$|q_k - q| < \frac{\varepsilon}{2}.$$

Slide 362

Sejam $n, m \geq n_0$. Temos

$$\begin{array}{rcl} |q_n - q_m| & = & |q_n - q + q - q_m| \\ & \leq & |q_n - q| + |q - q_m| \\ & < & \frac{\varepsilon}{2} + \frac{\varepsilon}{2} \\ & = & \varepsilon \end{array}$$

□

Slide 363

Algumas sequências de Cauchy não convergem - por exemplo, tome uma aproximação racional para $\sqrt{2}$. A ideia aqui será representar cada real por uma sequência de Cauchy - lembrando que as sequências de Cauchy neste contexto são formadas por números racionais. Um problema que aparece aqui é a falta de unicidade. Para cada real existem diversas sequências de Cauchy que convergem para ele. Por isso, teremos que trabalhar com classes de equivalências e considerar como iguais as sequências que convergem para o mesmo lugar. Mas como ainda não temos para onde essas sequências convergem (afinal, ainda estamos definindo os reais), precisamos usar um truque parecido com a definição de sequência de Cauchy.

Uma relação de equivalência

Slide 364

Definição 18.6. Sejam $(x_n)_{n\in\mathbb{N}}$ e $(y_n)_{n\in\mathbb{N}}$ sequências de Cauchy. Dizemos que $(x_n)_{n\in\mathbb{N}} \cong (y_n)_{n\in\mathbb{N}}$ se $(x_n - y_n)_{n\in\mathbb{N}}$ converge[68] para 0.

Slide 365

Proposição 18.7. *A relação $\cong$ definida acima é uma relação de equivalência.*

Demonstração. É claro que $(x_n)_{n\in\mathbb{N}} \cong (x_n)_{n\in\mathbb{N}}$ pois $(x_n - x_n)_{n\in\mathbb{N}}$ é a sequência constante igual a 0.

Se $(x_n)_{n\in\mathbb{N}} \cong (y_n)_{n\in\mathbb{N}}$, precisamos mostrar que $(x_n)_{n\in\mathbb{N}} \cong (y_n)_{n\in\mathbb{N}}$. Como $(x_n)_{n\in\mathbb{N}} \cong (y_n)_{n\in\mathbb{N}}$, então a sequência $(x_n - y_n)_{n\in\mathbb{N}}$ converge para 0. Ou seja, dado $\varepsilon \in \mathbb{Q}_{>0}$, existe n_0 tal que, para todo $k \geq n_0$, temos que $|x_k - y_k| < \varepsilon$. Como $|x_k - y_k| = |y_k - x_k|$, temos o resultado.

Slide 366

Finalmente, se $(x_n)_{n\in\mathbb{N}} \cong (y_n)_{n\in\mathbb{N}}$ e $(y_n)_{n\in\mathbb{N}} \cong (z_n)_{n\in\mathbb{N}}$, precisamos mostrar que $(x_n)_{n\in\mathbb{N}} \cong (z_n)_{n\in\mathbb{N}}$. Seja $\varepsilon \in \mathbb{Q}_{>0}$. Como $(x_n)_{n\in\mathbb{N}} \cong (y_n)_{n\in\mathbb{N}}$, existe n_1 tal que, para todo $k \geq n_1$ temos

$$|x_k - y_k| < \frac{\varepsilon}{2}.$$

Analogamente, existe n_2 tal que, para todo $k \geq n_2$, temos

$$|y_k - z_k| < \frac{\varepsilon}{2}.$$

Assim, considere $n_0 = \max\{n_1, n_2\}$. Dado $k \geq n_0$[69], temos:

[67] Em vez de usar ε na definição de que converge, usamos $\frac{\varepsilon}{2}$ - como era para qualquer ε, podemos fazer isso.
[68] Note que essa condição é equivalente a para todo $\varepsilon \in \mathbb{Q}_{>0}$ existe n_0 tal que para todo $n \geq n_0$ $|x_n - y_n| < \varepsilon$.
[69] Note que, assim, $k \geq n_1$ e $k \geq n_2$.

$$\begin{aligned} |x_k - z_k| &= |x_k - y_k + y_k - z_k| \\ &\leq |x_k - y_k| + |y_k - z_k| \\ &< \tfrac{\varepsilon}{2} + \tfrac{\varepsilon}{2} \\ &= \varepsilon \end{aligned}$$

□

Slide 367

Proposição 18.8. *Se $(x_n)_{n\in\mathbb{N}}$ e $(y_n)_{n\in\mathbb{N}}$ convergem para x e y respectivamente, então $(x_n)_{n\in\mathbb{N}} \cong (y_n)_{n\in\mathbb{N}}$ se, e somente se, $x = y$.*

Demonstração. Suponha $(x_n)_{n\in\mathbb{N}} \cong (y_n)_{n\in\mathbb{N}}$. Suponha que $x \neq y$. Então $\varepsilon = |x - y| > 0$. Como $(x_n)_{n\in\mathbb{N}} \cong (y_n)_{n\in\mathbb{N}}$, existe n_1 tal que, para todo $k \geq n_1$,

$$|x_k - y_k| < \frac{\varepsilon}{3}.$$

Como $(x_n)_{n\in\mathbb{N}}$ converge para x, existe n_2 tal que, para todo $k \geq n_2$,

$$|x - x_k| < \frac{\varepsilon}{3}.$$

Slide 368

Analogamente, existe n_3 tal que, para todo $k \geq n_3$,

$$|y - y_k| < \frac{\varepsilon}{3}.$$

Assim, seja $k = \max\{n_1, n_2, n_3\}$. Temos

$$\begin{aligned} |x - y| &= |x - x_k + x_k - y_k + y_k - y| \\ &\leq |x - x_k| + |x_k - y_k| + |y_k - y| \\ &< \tfrac{\varepsilon}{3} + \tfrac{\varepsilon}{3} + \tfrac{\varepsilon}{3} \\ &= \varepsilon \end{aligned}$$

contrariando a definição de ε.

Slide 369

Agora suponha $x = y$. Seja $\varepsilon > 0$. Seja n_1 tal que, para todo $k \geq n_1$,

$$|x - x_k| < \frac{\varepsilon}{2}.$$

Seja n_2 tal que, para todo $k \geq n_2$,

$$|y - y_k| < \frac{\varepsilon}{2}.$$

Considere $n_0 = \max\{n_1, n_2\}$. Assim, dado $k \geq n_0$, temos

$$\begin{aligned} |x_k - y_k| &= |x_k - x + x - y_k| \\ &\leq |x_k - x| + |x - y_k| \\ &= |x_k - x| + |y - y_k| \\ &< \varepsilon \end{aligned}$$

□

Definindo $\mathbb{R}$

Slide 370

Definição 18.9. Podemos definir $\mathbb{R}$ como sendo o conjunto de todas as classes de equivalência de sequências de Cauchy de racionais pela relação acima.

Soma

Slide 371

Como exemplo, vamos fazer a soma. Dadas duas sequências $(x_n)_{n\in\mathbb{N}}$ e $(y_n)_{n\in\mathbb{N}}$, definimos $[(x_n)_{n\in\mathbb{N}}]+[(y_n)_{n\in\mathbb{N}}]$ como $[(x_n+y_n)_{n\in\mathbb{N}}]$[70].

Vejamos que isso está bem definido. Vamos começar provando que x_n+y_n é de Cauchy. Seja $\varepsilon>0$. Sejam n_x, n_y tais que, se $n,m>n_x$,

$$|x_n-x_m|<\frac{\varepsilon}{2}$$

e que, se $n,m>n_y$,

$$|y_n-y_m|<\frac{\varepsilon}{2}.$$

Slide 372

Seja $n_0>n_x,n_y$. Temos então que, dados $n,m>n_0$,

$$\begin{array}{rcl}|(x_n+y_n)-(x_m-y_m)| & \leq & |x_n-x_m|+|y_n-y_m| \\ & < & \frac{\varepsilon}{2}+\frac{\varepsilon}{2} \\ & = & \varepsilon\end{array}$$

Slide 373

Para terminar que está bem definida, resta mostrar que, se $(x_n)_{n\in\mathbb{N}}\cong(a_n)_{n\in\mathbb{N}}$ e $(y_n)_{n\in\mathbb{N}}\cong(b_n)_{n\in\mathbb{N}}$, então $(x_n+y_n)_{n\in\mathbb{N}}\cong(a_n+b_n)_{n\in\mathbb{N}}$. De fato, fixe $\varepsilon>0$. Sejam n_x,n_y tais que, se $n>n_x$,

$$|x_n-a_n|<\frac{\varepsilon}{2}$$

e, se $n>n_y$,

$$y_n-b_n<\frac{\varepsilon}{2}.$$

Slide 374

Fixe $n_0>n_x,n_y$. Assim, dado $n>n_0$, temos

$$\begin{array}{rcl}|(x_n+y_n)-(a_n-b_n) & \leq & |x_n-a_n|+|y_n-b_n| \\ & < & \frac{\varepsilon}{2}+\frac{\varepsilon}{2} \\ & = & \varepsilon\end{array}$$

Exercícios da Aula 18

Exercício 18.1. Mostre que a sequência $(q_n)_{n\in\mathbb{N}}$ dada por $q_n=0$ se n é par e $q_n=1$ se n é ímpar não converge.

Exercício 18.2. Suponha que $(x_n)_{n\in\mathbb{N}}$ converge para a e para b. Mostre que $a=b$.

Exercício 18.3. Sejam $q,a\in\mathbb{Q}$. Suponha que $(q_n)_{n\in\mathbb{N}}$ converge para q. Mostre que a sequência $(q_n+a)_{n\in\mathbb{N}}$ converge para $q+a$.

[70] onde $[\cdot]$ indica a classe de equivalência.

Aula 19

Cardinalidade

Slide 375

Definição 19.1. Sejam A e B dois conjuntos. Dizemos que A e B tem a mesma **cardinalidade** se existe $f : A \to B$ bijetora. Notação: $|A| = |B|$.

Exemplos

Slide 376

Proposição 19.2. $|\mathbb{N}| = |\mathbb{N} \setminus \{0\}|$

Demonstração. Basta considerar $f : \mathbb{N} \to \mathbb{N} \setminus \{0\}$ dada por $f(n) = n + 1$. □

Slide 377

Proposição 19.3. *Considere* $P = \{n \in \mathbb{N} : n \text{ é par}\}$. *Então* $|P| = |\mathbb{N}|$.

Demonstração. Basta notar que a função $f : \mathbb{N} \to P$ dada por $f(n) = 2n$ é uma bijeção (exercício). □

Transitividade

Slide 378

Proposição 19.4. *Sejam* A, B, C *conjuntos. Se* $|A| = |B|$ *e* $|B| = |C|$, *então* $|A| = |C|$.

Demonstração. Sejam $f : A \to B$ e $g : B \to C$ funções bijetoras. Note que $g \circ f : A \to C$ é bijetora (exercício). □

Mais exemplos

Slide 379

Proposição 19.5. *Considere* $I = \{n \in \mathbb{N} : n \text{ é ímpar}\}$. *Então* $|I| = |\mathbb{N}|$.

Demonstração. Basta notar que $f : \mathbb{N} \to I$ dada por $f(n) = 2n + 1$ é bijetora (exercício). □

Slide 380

Corolário 19.6. $|P| = |I|$.

Slide 381

Proposição 19.7. $|\mathbb{Z}| = |\mathbb{N}|$.

Demonstração. Considere $f : \mathbb{N} \to \mathbb{Z}$ dada por

$$f(n) = \begin{cases} \frac{n}{2} & \text{se } n \text{ é par} \\ -\frac{(n+1)}{2} & \text{se } n \text{ é ímpar} \end{cases}$$

Note que f é injetora (exercício). Vamos mostrar que ela é sobrejetora. Seja $z \in \mathbb{Z}$. Se $z \geq 0$, tome $n = 2z$. Note que $f(n) = \frac{2z}{2} = z$. Se $z < 0$, tome $n = -2z - 1$. Note que $f(n) = -\frac{-2z-1+1}{2} = z$. □

Dificuldades

Slide 382

Nem sempre é fácil verificar a existência de funções injetoras. Por exemplo, pode-se provar que $|\mathbb{N}| = |\mathbb{N} \times \mathbb{N}|$. Uma maneira é você perceber que a função $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ dada por

$$f(a, b) = \frac{1}{2}(a + b)(a + b + 1) + b$$

é bijetora.

Não é tarefa simples encontrar uma função como acima, nem mostrar que ela de fato é bijetora (vale tentar um pouco).

Cantor-Bernstein-Schroeder

Slide 383

Para contornar esse tipo de problema, o seguinte resultado ajuda bastante:

Teorema 19.8 (Cantor-Bernstein-Schroeder)**.** *Sejam A, B conjuntos e sejam $f : A \to B$ e $g : B \to A$ funções injetoras. Então $|A| = |B|$.*

Demonstração. Vamos provar o resultado supondo que $A \cap B = \emptyset$. Para ver como obter o caso geral a partir desse, veja o Exercício 19.2. Seja $x \in A \cup B$. Defina

- $s_0^x = x$
- $s_{n+1}^x = \begin{cases} f(s_n^x) & \text{se } s_n^x \in A \\ g(s_n^x) & \text{se } s_n^x \in B. \end{cases}$
- $s_{-(n+1)}^x = \begin{cases} f^{-1}(s_{-n}^x) & \text{se } s_{-n}^x \text{ está definido e pertence a } Im(f) \\ g^{-1}(s_{-n}^x) & \text{se } s_{-n}^x \text{ está definido e pertence a } Im(g) \end{cases}$

Note que s_z^x pode não estar definido para todo $z \in \mathbb{Z}$. Considere

$$S^x = \{s_z^x \in A \cup B : z \in \mathbb{Z} \text{ e } s_z^x \text{ está definido}\}$$

Note que $(S^x)_{x \in A \cup B}$ forma uma partição sobre $A \cup B$ (cuidado, pode acontecer que $S^x = S^y$ mesmo com $x \neq y$). De fato, sejam $s_z^y = s_k^x$. Note que, então $s_{z+m}^y = s_{k+m}^x$ para qualquer $m \in \mathbb{Z}$. Logo, $S^y = S^x$.

Com isso, se mostrarmos que $|S^x \cap A| = |S^x \cap B|$, terminamos[71]. Temos alguns casos:

- Se s_z^x está definido para todo z, f induz uma bijeção, pois é sobrejetora.
- Se z é o menor tal que s_z^x está definido e $s_z^x \in A$, então f induz uma bijeção (já que é sobrejetora).
- Se z é o menor tal que s_z^x está definido e $s_z^x \in B$, então g induz uma bijeção (já que é sobrejetora).

□

Aplicando

Slide 384

Assim, fica mais fácil mostrar o resultado que comentamos:

Proposição 19.9. $|\mathbb{N}| = |\mathbb{N} \times \mathbb{N}|$.

Demonstração. Considere $f : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ dada por $f(n) = (n, n)$ e $g : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ dada por $g(a, b) = 2^a 3^b$. Note que as duas funções são injetoras facilmente. □

Slide 385

Também podemos provar o seguinte:

Proposição 19.10. $|\mathbb{Q}| = |\mathbb{N}|$.

Demonstração. Como podemos ver $\mathbb{N} \subset \mathbb{Q}$, já temos a função $f : \mathbb{N} \to \mathbb{Q}$ injetora. Por outro lado, podemos tomar a função $g : \mathbb{Q} \to \mathbb{Z} \times \mathbb{Z}$ dada por $f(\frac{a}{b}) = (a, b)$, onde $\frac{a}{b}$ está na forma simplificada. Note que tal função é injetora. Como $|\mathbb{N}| = |\mathbb{Z}|$, temos que $|\mathbb{N} \times \mathbb{N}| = |\mathbb{Z} \times \mathbb{Z}|$ (veja os alongamentos) e como $|\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$, temos que $|\mathbb{Z} \times \mathbb{Z}| = |\mathbb{N}|$. Assim, existe $h : \mathbb{Q} \to \mathbb{N}$ injetora. □

Partes aumenta de cardinalidade

Slide 386

Um dos resultados que vamos mostrar nesta seção é que o conjunto dos reais tem cardinalidade maior que a dos naturais. Faremos isso de uma maneira indireta, mas os resultados intermediários também são úteis em outras situações.

Proposição 19.11. $|\mathbb{N}| \neq |\wp(\mathbb{N})|$.

Demonstração. Suponha que exista $f : \mathbb{N} \to \wp(\mathbb{N})$ bijeção. Considere o conjunto $A = \{a \in \mathbb{N} : a \notin f(a)\}$. Como f é uma bijeção e $A \in \wp(\mathbb{N})$, temos que existe $b \in \mathbb{N}$ tal que $f(b) = A$. Vamos ver que isso dá uma contradição. Note que se $b \in A$, então $b \in f(b)$ e, portanto, $b \notin A$. Por outro lado, se $b \notin A$, então $b \notin f(b)$ e, portanto, $b \in A$. □

$\mathbb{R}$ e $\wp(\mathbb{N})$

Slide 387

Note que, claramente, existe uma função injetora de $\mathbb{N}$ em $\wp(\mathbb{N})$. Por exemplo, podemos tomar $f(n) = \{n\}$. Assim, o que o resultado anterior nos diz é que não existe uma função injetora de $\wp(\mathbb{N})$ em $\mathbb{N}$ (ou, equivalentemente, que não existe uma função sobrejetora de $\mathbb{N}$ em $\wp(\mathbb{N})$.

Proposição 19.12. *Existe*[72] *uma função injetora de* $\mathbb{R}$ *em* $\wp(\mathbb{N})$.

Demonstração. Note que basta provarmos que existe uma função injetora de $\mathbb{R}$ em $\wp(\mathbb{Q})$. Para cada $r \in \mathbb{R}$, existe $(q_n^r)_{n\in\mathbb{N}}$ sequência de racionais que converge para r. Podemos tomar tal sequência de forma que $x_n^r \neq x_m^r$ se $n \neq m$ (pense um pouco para se convencer disso). Vamos provar que a função $f : \mathbb{R} \to \wp(\mathbb{Q})$ dada por

$$f(r) = \{x_n^r : n \in \mathbb{N}\}$$

é injetora.

Slide 388

Sejam $r \neq s \in \mathbb{R}$. Considere $\varepsilon = |r - s|$. Como $(x_n^r)_{n\in\mathbb{N}}$ converge para r, existe n_r tal que, se $n \geq n_r$, temos

$$|x_n^r - r| < \frac{\varepsilon}{2}.$$

Analogamente, existe n_s tal que, se $n \geq n_s$, temos

$$|x_n^s - s| < \frac{\varepsilon}{2}.$$

Vamos mostrar que $f(x_r) \cap f(x_s)$ é finito - note que isso prova que $f(x_r) \neq f(x_s)$ já que eles são infinitos.

Slide 389

Suponha que não, então existe $a \in f(x_r) \cap f(x_s)$ tal que $a = x_n^r$ e $a = x_k^s$ com $n > n_r$ e $k > n_s$. Assim,

$$\begin{aligned} |r-s| &= |r-a+a-s| \\ &\leq |r-a| + |a-s| \\ &= |r-x_n^r| + |x_k^s - s| \\ &< \varepsilon \end{aligned}$$

contradição. □

Função característica

Slide 390

Já temos "metade" da igualdade $|\mathbb{R}| = |\wp(\mathbb{N})|$. Vamos agora à outra metade.

Definição 19.13. Dados conjuntos $A \subset B$, denotamos por $\chi_A^B : B \to \{0,1\}$ a função dada por

$$\chi_A^B(x) = \begin{cases} 1 & \text{se } x \in A \\ 0 & \text{se } x \notin A \end{cases}$$

Chamamos tal função de **função característica** de A em B. Normalmente, quando B está claro no contexto, o omitimos.

Mesma cardinalidade

Slide 391

Proposição 19.14. $|\mathcal{F}| = |\wp(\mathbb{N})|$ *onde* $\mathcal{F} = \{\chi_A^{\mathbb{N}} : A \subset \mathbb{N}\}$.

Demonstração. Basta notar que a função $\varphi : \mathcal{F} \to \wp(\mathbb{N})$ dada por $\varphi(\chi_A) = A$ é bijetora[73]. □

Existe uma injetora

Slide 392

Proposição 19.15. *Existe uma função injetora de* $\wp(\mathbb{N})$ *em* $\mathbb{R}$.

Demonstração. Note que é suficiente mostrarmos que existe uma função injetora de $\mathcal{F}$ em $\mathbb{R}$. Considere $\varphi : \mathcal{F} \to \mathbb{R}$ dada por[74]

$$\varphi(\chi_A) = 0, \chi_A(0)\chi_A(1)\cdots\chi_A(n)\cdots$$

□

Juntando tudo

Slide 393

Corolário 19.16. $|\mathbb{R}| = |\wp(\mathbb{N})|$

[71] Pois cada um dos pedaços terá uma bijeção e depois é só juntar todas

[72] Para uma demonstração alternativa, veja o Exercício 19.5

[73] Cuidado aqui - temos uma função onde cada elemento de seu domínimo é uma função e cada elemento de sua imagem é um conjunto.

[74] Você pode escrever essa função em termos de uma somatória se preferir.

Demonstração. Note que temos o seguinte diagrama (cada "flecha" indica uma função injetora):

$$\wp(\mathbb{N}) \leftrightarrow \mathcal{F} \to \mathbb{R}$$

$$\wp(\mathbb{N}) \leftrightarrow \wp(\mathbb{Q}) \leftarrow \mathbb{R}$$

□

Consequência

Slide 394

Corolário 19.17. *Não existe $f : \mathbb{R} \to \mathbb{N}$ injetora.*

Alongamentos da Aula 19

Alongamento 19.1. Sejam A, B, X, Y conjuntos tais que $|A| = |X|$ e $|B| = |Y|$. Mostre que $|A \times B| = |X \times Y|$.

Alongamento 19.2. Mostre que se existe $f : A \to B$ sobrejetora, então existe $g : B \to A$ injetora.

Alongamento 19.3. Mostre que se existe $f : A \to B$ injetora, então existe $g : B \to A$ sobrejetora.

Alongamento 19.4. Determine $\wp(X)$ onde:

(a) $X = \{a, b, c, d\}$;

(b) $X = \{\emptyset\}$;

(c) $X = \emptyset$;

(d) $X = \wp(\{1, 2\})$.

Alongamento 19.5. Mostre que se $|A| = |B|$, então $|\wp(A)| = |\wp(B)|$.

Exercícios da Aula 19

Exercício 19.1. Mostre que $|\mathbb{N}^n| = |\mathbb{N}|$ para todo $n \in \mathbb{N}_{>0}$.

Exercício 19.2. Este é um um roteiro para mostrar que, se vale o Teorema de Cantor-Bernstein-Schoroeder para conjuntos disjuntos, então vale para o caso geral. Sejam $f : A \to B$ e $g : B \to A$ injetoras.

(a) Considere os conjuntos $A' = \{(a, 0) : a \in A\}$ e $B' = \{(b, 1) : b \in B\}$. Note que tais conjuntos são disjuntos.

(b) Mostre que $|A| = |A'|$ e $|B| = |B'|$.

(c) Conclua o resultado.

Exercício 19.3. Enuncie e prove uma segunda versão do Teorema de Cantor-Bernstein-Schoroeder, onde as funções f e g do enunciado original são sobrejetoras em vez de injetoras.

Exercício 19.4. Mostre que, dado X um conjunto, então $|X| \neq |\wp(X)|$.

Exercício 19.5. Lembre-se que cada $r \in \mathbb{R}$ pode ser visto como um par (I_r, J_r) que é um corte de Dedekind. Mostre que a função $f : \mathbb{R} \to \wp(\mathbb{Q})$ dada por $f(r) = I_r$ é injetora. Use isso para uma demonstração alternativa da Proposição 19.12

Aula 20

Vamos discutir o conceito de enumerabilidade na forma de exercícios:

Definição 20.1. Dizemos que um conjunto X é **enumerável**[75] se $|X| = |\mathbb{N}|$.

Exercício 20.1. Sejam A e B conjuntos enumeráveis. Mostre que $A \cup B$ é enumerável (para facilitar, mostre o caso em que eles são disjuntos).

Exercício 20.2. Mostre que, se para cada $n \in \mathbb{N}$, X_n é enumerável, então $\bigcup_{n\in\mathbb{N}} X_n$ é enumerável (novamente, faça o caso em que eles são todos dois a dois disjuntos).

Exercício 20.3. Se A é enumerável, mostre que $A \times \mathbb{N}$ é enumerável.

Exercício 20.4. Mostre que $\mathbb{N}^n$ é enumerável.

Exercício 20.5. Seja X um conjunto enumerável. Para cada $n \in \mathbb{N}_{>0}$, considere $X_n = \{A \subset X : A$ tem n elementos$\}$.

(a) Mostre que X^n é enumerável.

(b) Mostre que, como X é enumerável, existe uma ordem total sobre X.

(c) Construa $f : X_n \to X^n$ injetora.

(d) Mostre que então existe $g : X_n \to \mathbb{N}$ injetora.

(e) Mostre que existe $h : \mathbb{N} \to X_n$ injetora.

(f) Conclua que X_n é enumerável.

Definição 20.2. Dizemos que um conjunto A é **finito** se A tem n elementos para algum $n \in \mathbb{N}$.

(g) Mostre que $\mathcal{F}$ é enumerável, onde $\mathcal{F} = \{F \subset X : F$ é finito$\}$.

Exercício 20.6. Mostre que $Y = \{A \subset \mathbb{N} : A$ é infinito$\}$ é não enumerável.

Vamos terminar essa seção apresentando um resultado interessante sobre os números reais:

Definição 20.3. Dizemos que $r \in \mathbb{R}$ é um **número algébrico** se existe um polinômio p não nulo com coeficientes racionais tal que $p(r) = 0$.

Exemplo 20.4. Qualquer $q \in \mathbb{Q}$ é algébrico, já que $x - q$ é um polinômico como acima. $\sqrt{2}$ também é algébrico, já que $x^2 - 2$ também é como acima.

Proposição 20.5. *O conjunto dos números algébricos é enumerável.*

Demonstração. Seja P' o conjunto de todos os polinômios de coeficientes racionais. Note que, para qualquer $n \in \mathbb{N}_{>0}$, $\mathbb{Q}^n$ é enumerável. Assim, $Q = \bigcup_{n\in\mathbb{N}_{>0}} \mathbb{Q}^n$ é enumerável. Note que existe uma bijeção $\varphi : Q \to P$ dada por

$$\varphi(q_0, ..., q_n) = q_0 + q_1 x + \cdots + q_n x^n$$

Assim, se considerarmos P o conjunto dos polinômios não nulos de coeficientes racionais, temos que P também é enumerável. Seja $f : \mathbb{N} \to P$ bijeção. Dado $n \in \mathbb{N}$, considere

$$Z_n = \{r \in \mathbb{R} : p(r) = 0, \text{onde } p = f(n)\}$$

Note que cada Z_n é finito (isso foge do escopo desse texto, mas não é tão ruim de provar). Note também que $\bigcup_{n\in\mathbb{N}} Z_n$ é o conjunto de todos os números algébricos. Assim, como tal união é enumerável, temos os resultados. □

[75] Em geral, um conjunto finito também é dito enumerável, mas vamos supor nestes exercícios que todos os conjuntos são infinitos para facilitar.

Aula 21

Axiomas para conjuntos

Slide 395

Qual a ideia intuitiva que temos de conjuntos? Normalmente pensamos que um conjunto é qualquer coleção de coisas. Seguindo esse raciocínio, poderíamos fazer:

$$T = \{X : X \text{ é um conjunto}\}.$$

Este seria o conjunto de todos os conjuntos. Como o próprio T é um conjunto, temos que $T \in T$. Isso é estranho, mas ainda assim não parece ser uma contradição.

Slide 396

Como isso é estranho, poderíamos então criar o conjunto dos conjuntos não estranhos:

$$R = \{X \in T : X \notin X\}$$

Teríamos, por exemplo, que $T \notin R$. Por outro lado, $\mathbb{N} \in R$. Mas e R? Note que não temos opção para R: se $R \in R$, pela definição de R, temos que $R \notin R$. Por outro lado, se $R \notin R$, novamente pela definição de R, temos que $R \in R$. Ou seja, a existência de R implica numa contradição. Este é conhecido como o **paradoxo de Russel**. Quem quiser saber mais sobre a história deste problema, recomendamos [**?**].

Slide 397

Para evitar problemas como o Paradoxo de Russel, apresentamos uma lista do que podemos fazer com conjuntos. Esta lista é conhecida como ZFC (Zermelo, Fraenkel e Axioma da Escolha). Vamos apresentar a lista aqui, com alguns comentários.

Quem quiser saber mais sobre o assunto, recomendamos [**?**].

Existência

Slide 398

Existe um conjunto que não possui elementos. Em símbolos, $\exists x\ \forall y\ y \notin x$. Denotamos tal conjunto por $\emptyset$.

Extensão

Slide 399

Dois conjuntos são iguais se possuem os mesmos elementos. Em símbolos: $\forall x\ \forall y(\forall z\ (z \in x \to z \in y) \wedge (z \in y \to z \in x)) \to x = y$.

Slide 400

Quando ocorre $\forall z\ z \in y \to z \in x$, usamos a seguinte notação: $y \subset x$. Desta forma, podemos denotar o último axioma como $\forall x\ \forall y(x \subset y \wedge y \subset x) \to x = y$.

Separação

Slide 401

Se P é uma propriedade e x é um conjunto, existe o subconjunto y que contém exatamente os elementos de x que satisfazem a propriedade P. Em símbolos $\forall x\ \exists y((\forall z \in x\ P(z) \to z \in y) \wedge (\forall z \in y \to (z \in x \wedge P(z))))$. A notação usual para isso é $y = \{z \in x : P(z)\}$.

Par

Slide 402

Se x e y são conjuntos, então existe um conjunto z que contém os dois como elementos. Em símbolos: $\forall x\ \forall y\ \exists z\ x \in z \wedge y \in z$. Note que tal axioma não garante que os únicos elementos de z sejam x e y mas, para isso, podemos usar o axioma da Separação. No caso em que os únicos elementos de z sejam x e y a notação fica $z = \{x, y\}$. Se, além disso, se $x = y$, usamos a notação $z = \{x\}$.

União

Slide 403

Para todo conjunto x, existe um conjunto y que contém todos os elementos dos elementos de x. Em símbolos: $\forall x\ \exists y\ \forall a\ \exists z \in x\ a \in z \to a \in y$. Novamente, tal axioma não garante que os únicos elementos de y sejam esses, mas isso pode ser feito utilizando-se o axioma da Separação. No caso em que o conjunto y contém exatamente tais elementos, a notação usual é $y = \bigcup_{z \in x} z$. Agora podemos provar que dados conjuntos A e B, existe o conjunto $A \cup B$. Primeiramente mostramos que existe o conjunto $\{A, B\}$ (exercício). Depois, mostramos que existe $y = \bigcup_{z \in \{A,B\}} z$ (note que este é o conjunto desejado).

Partes

Slide 404

Dado x um conjunto, existe um conjunto y que contém todos os subconjuntos de x. Em símbolos: $\forall x\ \exists y\ \forall z\ z \subset x \to z \in y$. Novamente, não temos garantido que os únicos elementos de y sejam os subconjuntos de x, mas podemos contornar isso com o axioma da separação. Se for o caso em que os elementos de y forem os subconjuntos de x, usamos a notação $y = \wp(x)$.

Infinito

Slide 405

Dado um conjunto x, denotamos por $S(x)$ o conjunto $x \cup \{x\}$ (podemos fazer isso pelo axioma do par (veja o Exercício 21.3 e da união). O axioma do infinito diz que existe um conjunto A tal que $\emptyset \in A$ e tal que para todo $x \in A$, $S(x) \in A$. Em símbolos: $\exists A\ \emptyset \in A \wedge (\forall x \in A\ S(x) \in A)$.

Uma outra interpretação

Slide 406

Há mais alguns axiomas, mas os faremos após uma pequena digressão.

Uma característica do método axiomático é que podemos ter diferentes interpretações para o que os axiomas descrevem[76]. Isso ocorre também com os axiomas aqui apresentados. Por exemplo, considere a relação $\ll$ definida sobre $\mathbb{N}$ da seguinte forma:

$a \ll b$ se, e somente se, o a-ésimo termo da expansão binária de b é 1

Exemplo

Slide 407

Por exemplo, $b = 25$ em binário dá 11001_2 então $0 \ll 25$, $1 \not\ll 25$, $4 \ll 25$.

Essa relação satisfaz todos os axiomas apresentados acima, com exceção ao do infinito (interpretando $\ll$ como $\in$). Por exemplo, o número 0 faz papel de $\emptyset$ uma vez que não existe a tal que $a \ll 0$. Se a e b são números distintos, o número $k = 2^a + 2^b$ é tal que $a \ll k$ e $b \ll k$.

[76] Isso é um dos objetos de estudo de uma área conhecida como teoria dos modelos.

Fórmulas tipo função

Slide 408

Começamos com a ideia principal de uma função: associar a cada elemento de um lado, um único elemento do outro. Com isso em mente, podemos definir uma fórmula do "tipo função". Basicamente é uma fórmula P, que a cada $a_1, ..., a_n$ conjuntos, associa um único conjunto b tal que $P(b, a_1, ..., a_n)$ seja satisfeita. Muitas vezes usamos uma notação mais parecida com função $b = f(a_1, ..., a_n)$.

Exemplos

Slide 409

Exemplo 21.1. Considere $P(x, y)$ sendo $y \in x \wedge (\forall z \in x\ z = y)$. Note que a cada a que tomarmos, só existe um conjunto b satisfazendo $P(b, a)$ (a saber, $b = \{a\}$).

Slide 410

Exemplo 21.2. Se omitirmos a parte "$\forall z \in x\ z = y$" na propriedade P anterior, não temos mais que P é do tipo função. Pois tanto $b_1 = \{a, \emptyset\}$ como $b_2 = \{a\}$ (suponha $a \neq \emptyset$) são distintos e $P(b_1, a)$ e $P(b_2, a)$ são satisfeitas.

Par ordenado

Slide 411

Podemos formalizar a ideia do que é uma função usando o que já temos até aqui. Comecemos com a ideia do par ordenado:
Definição 21.3. Sejam x, y dois conjuntos. Definimos o **par ordenado** como o conjunto $\{\{x\}, \{x, y\}\}$. Notação (x, y). Neste caso, dizemos que x é a primeira coordenada do par e que y é a segunda.

Algumas propriedades

Slide 412

- Existe uma fórmula P tal que $P(x)$ é verdadeira se, e somente se, x é um par ordenado;
- Existe uma fórmula P_1 tal que $P_1(a, x)$ é verdadeira se, e somente se x é um par ordenado e a é a primeira coordenada de x;
- Existe uma fórmula P_2 tal que $P_2(a, x)$ é verdadeira se, e somente se x é um par ordenado e a é a segunda coordenada de x;

Slide 413

Proposição 21.4. *Sejam (x, y) e (a, b) dois pares ordenados. Então $(x, y) = (a, b)$ se, e somente se, $x = a$ e $y = b$.*

Conjunto dos pares ordenados

Slide 414

Definição 21.5. Se X e Y são conjuntos, denotamos por $X \times Y$ o conjunto de todos os pares ordenados (x, y) tais que $x \in X$ e $y \in Y$.

Observação

Slide 415

Na verdade, é necessário provar que se X e Y são conjuntos, então $X \times Y$ é de fato um conjunto. Isso é possível usando o fato que $X \cup Y$ é um conjunto e, portanto, $\wp(\wp(X \cup Y))$ é conjunto. Finalmente, usamos o axioma da separação para tomarmos apenas os pares ordenados desejados.

Função

Slide 416

Definição 21.6. Chamamos de uma função f de X em Y um subconjunto de $X \times Y$ tal que, para todo $x \in X$, existe $y \in Y$ tal que $(x, y) \in f$ e que se $(x, y_1), (x, y_2) \in f$, então $y_1 = y_2$. Neste caso, denotamos $(x, y) \in f$ como $f(x) = y$.

Substituição

Slide 417

Agora podemos continuar com a lista dos axiomas de ZFC:

Considere P uma fórmula do tipo função. Se x é um conjunto, então existe o conjunto y de todos os elementos associados ao aplicar-se P aos elementos de x. Em símbolos: $\forall x \ \ (\forall a_1, ..., a_n \in x \exists! z \ P(z, a_1, ..., a_n)) \rightarrow (\exists y \forall z \ \forall a_1, ..., a_n \in x P(z, a_1, ..., a_n) \rightarrow z \in y)$.

O $\exists! z$ quer dizer "existe um único z satisfazendo o que vem a seguir". No caso em que y contém exatamente tais elementos, denotamos $y = \{z : P(z, a_1, ..., a_n), a_1, ..., a_n \in x\}$. Ou, usando a notação de função, $y = \{f(a_1, ..., a_n) : a_1, ..., a_n\}$.

Fundação

Slide 418

Todo conjunto x não vazio possui um elemento que é disjunto de x. Em símbolos $\forall x \ x \neq \emptyset \rightarrow (\exists y \in x \ y \cap x = \emptyset)$. Este é o axioma de ZFC que é menos usado em matemática em geral. Apesar disso, serve, por exemplo, para impedir que existam conjuntos x tais que $x \in x$ (veja o Exercício 21.10). Também o usaremos para mostrar a propriedade fundamental do par ordenado.

Escolha

Slide 419

Se x é um conjunto de conjuntos não vazios, então existe uma função $f : x \rightarrow \bigcup_{a \in x} a$ tal que $f(y) \in y$ para todo $y \in x$. Ou seja, se temos uma família de conjuntos não vazios, podemos "escolher" um elemento de cada conjunto.

Exercícios da Aula 21

Exercício 21.1. Mostre que o conjunto vazio é único. Isto é, que só existe um conjunto sem elementos.

Exercício 21.2. Mostre que existem os seguintes conjuntos:

(a) $\{\emptyset\}$;

(b) $\{\{\emptyset\}\}$;

(c) $\{\emptyset, \{\emptyset\}\}$.

Exercício 21.3. Se x é um conjunto, mostre que $\{x\}$ também é um conjunto.

Exercício 21.4. Mostre que se $\{x\}$ é um conjunto, então x também é.

Exercício 21.5. A ideia deste exercício é formalizar o conceito de intersecção. Seja A um conjunto não vazio. Seja $b \in A$. Defina $\bigcap_{a \in A} a = \{x \in b : \forall a \in A \; x \in a\}$.

(a) Justifique a existência de tal conjunto.

(b) Mostre que tal definição independe da escolha do b. Isto é, seja $c \in A$. Mostre que $\{x \in b : \forall a \in A \; x \in a\} = \{x \in c : \forall a \in A \; x \in a\}$;

(c) Se A e B são conjuntos, defina $A \cap B$ com o que foi feito acima.

Exercício 21.6. Mostre que podemos omitir o axioma da existência. Isto é, que a existência do conjunto vazio pode ser obtida a partir dos outros axiomas.

Exercício 21.7. Mostre que não existe o conjunto de todos os conjuntos.

Exercício 21.8. Mostre que se a, b, c são conjuntos, então existe o conjunto $\{a, b, c\}$.

Exercício 21.9. (a) Escreva numa fórmula "x tem exatamente um elemento" (um conjunto desta forma é dito **unitário**);

(b) Escreva numa fórmula "x tem exatamente dois elementos".

Exercício 21.10. Mostre que não existe x tal que $x \in x$.

Exercício 21.11. Mostre que não existem conjuntos a, b tais que $a \in b \in a$.

Exercício 21.12. Seja X um conjunto. Mostre que existe o conjunto A formado por todos os unitários de elementos de X. (Isto é, $A = \{\{x\} : x \in X\}$).

Aula 22

Novamente, faremos essa parte na forma de exercícios.

Definição 22.1. Vamos chamar de um conjunto indutivo um conjunto X satisfazendo:

$$\emptyset \in X \wedge (\forall y \; y \in X \to S(y) \in X)$$

Exercício 22.1. Algum dos axiomas implica a existência de um conjunto indutivo?

Exercício 22.2. Sejam A e B conjuntos indutivos. É verdade que $A \cap B$ é indutivo?

Exercício 22.3. Fixe X um conjunto indutivo. Considere $I = \{A \subset X : A \text{ é indutivo}\}$.

(a) $I \neq \emptyset$?

(b) Seja $N = \bigcap_{A \in I} A$. É verdade que $\emptyset \in N$?

(c) É verdade que $\{\emptyset\} \in N$?

(d) Se $n \in N$, é verdade que $S(n) \in N$?

(e) Mostre que N é indutivo.

(f) Suponha que $B \subset N$ é indutivo. Mostre que $N \subset B$. Conclua que $N = B$.

(g) Olhe os axiomas de Peano. Veja se há alguma semelhança entre N e S e o que está lá.

Exercício 22.4. Quantos elementos tem $S(\emptyset)$? E $S(S(\emptyset))$? E $S(S(S(\emptyset)))$? Se aplicarmos S n vezes a $\emptyset$, quantos elementos teremos no final?