Fundamentos de Matemática

Leandro F. Aurichi [1]

5 de junho de 2017

[1]Instituto de Ciências Matemáticas e de Computação - Universidade de São Paulo, São Carlos, SP

Capítulo 1

Basicão

1.1 Um primeiro problema

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

1 A geladeira só possa ser aberta quando houver pelo menos a metade do moradores na casa;

2 Qualquer grupo de moradores que tenha pelo menos a metade dos moradores, precisa conseguir abrir a geladeira.

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

Antes de atacarmos o problema propriamente dito, tente resolver os seguintes casos mais fáceis:

Exercício 1.1.1. Quantos cadeados e quantas chaves (no mínimo) precisaríamos ter se quiséssemos que qualquer morador da república pudesse abrir a geladeira?

Exercício 1.1.2. Quantos cadeados e quantas chaves (no mínimo) precisaríamos ter se quiséssemos que a geladeira só fosse aberta quando todos os moradores estivessem presentes?

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 nos vai poupar tempo no futuro.

Funções

Primeiramente, considere um grupo com 5 pessoas. Note que 6 pessoas é o menor grupo com mais da metade do total de moradores, 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 possa abrir. Assim, para cada grupo de 5 pessoas, precisa existir pelo menos um cadeado que esse grupo não abra.

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

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 deixa-la clara. Uma associação, em matemática, nada mais é que uma função, que denotamos da seguinte maneira:

$$f : A \longrightarrow B$$

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 $f(a)$). 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 é, são todos os elementos de B que são da forma $f(a)$ para algum elemento a de A.

No nosso problema, vamos considerar uma função

$$c : G \longrightarrow C$$

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.

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

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.

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 um propriedade bastante importante sobre funções e que nos será bastante útil neste problema. Dizemos que uma função $f : A \longrightarrow B$ é **injetora** se, dados $a \neq b$, temos que $f(a) \neq f(b)$.

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. 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 $c(g_1)$ 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.

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.

Com isso, já temos uma importante informação sobre o conjunto imagem da função c ($\mathrm{Im}(c)$): 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.

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 você esteja sozinho nela. Agora suponha que chegou um grupo g de 5 moradores. Sabemos que o grupo não consegue abrir o cadeado $c(g)$. Mas tambem sabemos que g junto com você forma um grupo de 6 pessoas. Logo, vocês conseguem abrir a geladeira. 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 morador precisa carregar é, pelo menos, a quantidade de grupos de 5 outras pessoas da república.

Juntando tudo para resolver o problema

Já sabemos que para resolver o problema, vamos precisar de pelo menos um cadeado para cada grupo de 5 moradores. Também sabemos que cada mora-

dor vai ter que carregar uma chave para cada grupo de outros 5 moradores (excluindo ele).

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.

Vamos mostrar que não. Ou seja, vamos mostrar que existe uma solução com tais quantidades. Portanto, essa seria a melhor solução possível.

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.

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

Falta ver quais são as quantidades exatas. Essas fórmulas serão apresentadas formalmente no Capítulo **??**. Vamos só aplicá-las aqui sem maiores discussões.

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

$$C_5^{11} = \frac{11!}{5!6!} = \frac{11 \cdot 10 \cdot 9 \cdot 8 \cdot 7}{5 \cdot 4 \cdot 3 \cdot 2} = 462$$

Já para as chaves, para cada morador são necessárias a quantidade de combinações de 10 5 a 5:

$$C_5^{10} = \frac{10!}{5!5!} = \frac{10 \cdot 9 \cdot 8 \cdot 7 \cdot 6}{5 \cdot 4 \cdot 3 \cdot 2} = 252$$

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

Exercícios

Exercício 1.1.3. Na solução apresentada, é verdade que cada uma das chaves que uma pessoa fixada carrega são todas diferentes? (note que se tivesse alguma repetida, poderíamos diminuir o total de chaves)

Exercício 1.1.4. Na solução apresentada, quantas cópias de cada chave existem? Quantas chaves diferentes existem?

1.2 Conjuntos

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. Se temos um conjunto A e um elemento a deste conjunto, denotamos esta relação por

Para ter algo mais rigoroso, dá um certo trabalho e foge do escopo deste texto. Mas se você estiver curioso, dê uma olhada em [1].

$$a \in A$$

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

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. No nosso 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 são as seguintes:

Proposição 1.2.1. *Sejam A, B, C conjuntos. Valem as seguintes propriedades:*

Essas propriedades podem parecer bem bobinhas. Mas serão bastante úteis no futuro. Principalmente a propriedade (c).

(a) $A \subset A$;

(b) Se $A \subset B$ *e* $B \subset C$, *então* $A \subset C$;

(c) Se $A \subset B$ *e* $B \subset A$, *então* $A = B$.

A maior dificuldade dessa demonstração é que tudo parece óbvio demais. Mas vamos com um pouco de calma.

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

(b) 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.

(c) O grande truque aqui é: dois conjuntos são o mesmo conjunto se eles tem os mesmos elementos. Daí agora ficou fácil: $A \subset B$ 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 $B \subset A$).

□

Quando temos um conjunto A, podemos querer tomar um subconjunto B dele, formado só com os elementos que satisfaçam uma determinada propriedade P. Seguimos 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 e intersecção

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 $\mathbb{N} = P \cup I$

Basicamente porque todo número natural é par ou ímpar.

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, $P \cap I = \emptyset$.

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

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

Vamos apresentar uma igualdade bastante útil (há várias parecidas no Alongamento 1.2.6).

Proposição 1.2.2. *Sejam A, B e C conjuntos. Então vale a seguinte igualdade:*

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

Demonstração. Essa demonstração 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.

$\subset$: Seja $x \in (A \cup B) \cap (A \cup C)$. 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.

$\supset$: 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.

□

Conjunto de subconjuntos

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

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

Sim, 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.

Observe que, não importa quem seja o conjunto A, sempre teremos que $\emptyset \in \wp(A)$ (veja o comentário na seção anterior) e que $A \in \wp(A)$ (veja a Proposição 1.2.1).

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 é muito fácil 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

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.

Essa notação também serve para finitos conjuntos. Por exemplo, se A_1, A_2 e A_3 são conjuntos, 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.

Mais ou menos como fazemos com somatórias.

Proposição 1.2.3. *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. □

Exemplo 1.2.4. Para cada $n \in \mathbb{N}$, considere $A_n = \{n\}$. 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 $A_n = \{n\}$). Assim, $n \in \bigcup_{n\in\mathbb{N}} A_n$.

Diferença entre conjuntos

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:

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

Lê-se A menos B

Uma coisa "estranha" aqui é que B não precisa estar contido em A (veja o Alongamento 1.2.7).

Intervalos

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:

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

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

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

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, $c \in [1, +\infty[$.

Sim, nem usamos o b aqui.

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.

Observe que a união de dois dois intervalos não necessariamente é um intervalo (ver o Alongamento 1.2.8). Por outro lado, com a intersecção a resposta é sempre um intervalo:

Proposição 1.2.5. *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, $c \in I \cap J$. □

Na verdade, de forma análoga, se prova que a intersecção qualquer de intervalos (não só de dois) é sempre um intervalo (veja o Exercício 1.2.11)

Problemas com conjuntos

Comentamos no início da seção que chamar de conjunto qualquer coleção gera problemas. Vamos aqui ilustrar isso.

Se qualquer coleção é um conjunto, temos que o seguinte é um conjunto:

$$T = \{X : X \text{ é um conjunto}\}$$

Ou seja, a coleção de todos os conjuntos seria um conjunto. Note que isso já é um pouco estranho, uma vez que $T \in T$, já que T também é um conjunto. Assim, é natural tentarmos ver a coleção dos conjuntos mais "normais":

$$N = \{X \in T : X \notin X\}$$

Diretamente das definições, temos que $T \notin N$. Mas e o próprio N?

Se $N \in N$, pela definição de N, temos que $N \notin N$. Por outro lado, se $N \notin N$, novamente pela definição de N, temos que $N \in N$.

Essa contradição segue de termos aceito como conjunto qualquer coleção.

Alongamentos

Alongamento 1.2.6. Verifique as seguintes afirmações para conjuntos A, B e C dados:

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

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

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

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

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

Alongamento 1.2.7. Sejam A, B conjuntos. Mostre que $A \smallsetminus B = A \smallsetminus (A \cap B)$.

Alongamento 1.2.8. 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) $I \smallsetminus J$ não é um intervalo;

(d) $I \smallsetminus J$ é um intervalo;

Exercícios

Exercício 1.2.9. Seja A um conjunto. Determine $\bigcup_{B\in\wp(A)} B$.

Exercício 1.2.10. Determine:

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

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

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

Exercício 1.2.11. Mostre que se cada I_a para $a \in A$ é um intervalo, então $\bigcap_{a\in A} I_a$ é um intervalo.

Exercício 1.2.12. Mostre que, dados dois intervalos I, J, se $I \cap J \neq \emptyset$, então $I \cup J$ é um intervalo.

1.3 Máximos, mínimos e coisas parecidas

Máximo e mínimo

Dado $A \subset \mathbb{R}$, chamamos de **máximo** de A um elemento $a \in A$ tal que $a \geq x$ para todo $x \in A$. Denotamos tal elemento por $\max A$. Note que tal elemento pode não existir (veja os exemplos).

Exemplo 1.3.1. Considere o conjunto $A = \{1, 2, 3\}$. Note que $3 = \max A$, já que $3 \in A$ e $3 \geq 1, 2, 3$.

Exemplo 1.3.2. Note que $\max[0, 1] = 1$.

Exemplo 1.3.3. Note que $\max[0, 1[$ não existe. Isso é fácil de se notar. Suponha que $a = \max[0, 1[$. A primeira coisa a se notar é que $a \in [0, 1[$, logo $0 \leq a < 1$. Note que $\frac{1+a}{2} \in [0, 1[$ e note também que $a < \frac{1+a}{2}$. Logo, a não pode ser o máximo de $[0, 1[$.

Pegamos o que faltava para chegar no 1 e paramos no meio do caminho. Faça um desenho que ajuda.

O máximo de um conjunto pode até não existir. Mas se existir, só tem um:

Proposição 1.3.4. *Seja $A \subset \mathbb{R}$. Se a e b são máximos de A, então $a = b$.*

Demonstração. Basta notar que $a \leq b$ e que $b \leq a$ (o primeiro fato por b ser máximo, o segundo, por a ser máximo). □

Analogamente ao que fizemos com o máximo, também podemos definir o mínimo. Dado $A \subset \mathbb{R}$, chamamos de **mínimo** de A (denotado por $\min A$) um elemento $a \in A$ tal que $a \leq x$ para todo $x \in A$. Como no caso do máximo, o mínimo pode não existir. E, como no caso do máximo, se o mínimo se existir, é único (veja o Alongamento 1.3.22).

Exemplo 1.3.5. $\min[0, 1] = 0$.

Exemplo 1.3.6. O mínimo de $\{\frac{1}{n} : n \in \mathbb{N}_{>0}\}$ não existe.[1]

Algumas relações entre máximo e operações entre conjuntos são bem fáceis de descrever:

Proposição 1.3.7. *Sejam $A, B \subset \mathbb{R}$ conjuntos que admitam máximos. Valem as seguintes afirmações:*

(a) Se $A \subset B$, então $\max A \leq \max B$

(b) $\max(A \cup B) = \max\{\max A, \max B\}$

Demonstração. (a) Sejam $a = \max A$ e $b = \max B$. Como $a \in A$ e, portanto, $a \in B$, temos que $a \leq b$ como queríamos.

(b) Seja $c = \max\{\max A, \max B\}$. Vamos fazer o caso em que $c = \max A$ (o caso $c = \max B$ é análogo). Note que, assim, $\max A \geq \max B$. Primeiramente, note que $c \in A \cup B$ já que $c \in A$. Seja $x \in A \cup B$. Se $x \in A$, já temos que $c \geq x$, pois $c = \max A$. Se $x \in B$, então $x \leq \max B$ e, como $c \geq \max B$, temos que $c \geq x$.

□

O mínimo tem comportamento parecido (veja o Exercício 1.3.24).

Majorante e minorante

Seja $A \subset \mathbb{R}$. Dizemos que $a \in \mathbb{R}$ é um **majorante** para A se $a \geq x$ para todo $x \in A$. Note que a principal diferença para a definição de máximo é que não estamos exigindo que $a \in A$.

Ou **limitante superior**

Exemplo 1.3.8. 1 é um majorante para $[0, 1[$. Mas note que 2 também é.

Assim como π, π^2, 7 e outros.

O exemplo anterior já nos diz que outra propriedade que diferencia o majorante do máximo é que o majorante não necessariamente é único.

Na verdade, ou o conjunto não tem majorantes ou tem infinitos. Veja o Exercício 1.3.26

De forma análoga, podemos definir o minorante.

Diretamente das definições, temos o seguinte:

Proposição 1.3.9. *Máximo é um majorante. Mínimo é um minorante.*

Definição 1.3.10. Um conjunto $A \subset \mathbb{R}$ é dito **limitado superiormente** se ele admite majorante. É dito **limitado inferiormente** se ele admite minorante. É dito simplesmente **limitado** se é limitado superiormente e inferiormente.

Veja o Exercício 1.3.27

Proposição 1.3.11. *Seja $A \subset \mathbb{R}$. Então A é limitado se, e somente se, existem $x, y \in \mathbb{R}$ tais que $A \subset [x, y]$.*

Demonstração. Suponha A limitado. Seja x um minorante para A e seja y um minorante para A. Vamos provar que $A \subset [x, y]$. De fato, dado $a \in A$, temos que $x \leq a \leq y$ e, portanto, $a \in [x, y]$.

Agora suponha que $A \subset [x, y]$. Note então que x é um minorante para A e y é um majorante. □

Supremo e ínfimo

Como vimos, um majorante dá uma informação sobre o conjunto e pode existir muitos deles - mas nos reais, podemos tomar um majorante especial, que num certo sentido é o que mais dá informações sobre o cojunto:

Definição 1.3.12. Seja A um conjunto limitado superiormente. Dizemos que a é **supremo** de A ($\sup A$) se $a = \min M$, onde $M = \{x \in \mathbb{R} : x$ é majorante de $A\}$. Notação $a = \sup A$.

Exemplo 1.3.13. $\sup[0, 1[= 1$.

De fato, note que 1 é um majorante para o conjunto. Mais que isso, dado qualquer $a < 1$, a não é um majorante do conjunto. Logo, 1 é o menor dos majorantes e, portanto, é o supremo do conjunto.

Proposição 1.3.14. *Seja $A \subset \mathbb{R}$. Se a é o máximo de A, então a é supremo de A.*

[1] Veja o Alongamento 1.3.23

Demonstração. Suponha que $a = \max A$. Note que a é um majorante para A. Por outro lado, seja b um majorante de A. Como $a \in A$, temos que $a \leq b$. Ou seja, a é o menor dos majorantes. □

Proposição 1.3.15. *Um conjunto $A \subset \mathbb{R}$ admite, no máximo, um supremo.*

Demonstração. Sejam a, b supremos de A. Como b é majorante e a é supremo (e, portanto, o menor dos majorantes), temos que $a \leq b$. De maneira análoga, temos que $b \leq a$. Logo, $a = b$. □

Exemplo 1.3.16. O conjunto $[0, +\infty[$ não admite supremo (já que nem admite majorantes).

Fato 1.3.17. *Todo subconjunto de $\mathbb{R}$ não vazio e limitado superiormente admite supremo.*

Na verdade, isso é uma propriedade bastante particular dos reais. Para se prova-la é preciso entrar em detalhes de como os reais são definidos (na verdade, dependendo de como é a definição, esse fato é suposto como um axioma da definição dos reais).

De forma análoga, podemos definir o ínfimo:

Definição 1.3.18. Seja A um conjunto limitado inferiormente. Dizemos que a é **ínfimo** de A ($\inf A$) se $a = \max M$, onde $M = \{x \in \mathbb{R} : x \text{ é minorante de } A\}$. Notação $a = \inf A$.

Todos os resultados que apresentamos sobre supremos funcionam de forma análoga para os ínfimos.

O fato da existência de supremos e ínfimos como acima implica um outro resultado, também bastante particular dos reais:

Proposição 1.3.19. *Sejam $(a_n)_{n\in\mathbb{N}}$ e $(b_n)_{n\in\mathbb{N}}$ sequências de números reais de forma que $[a_{n+1}, b_{n+1}] \subset [a_n, b_n]$ para todo $n \in \mathbb{N}$. Então $\bigcap_{n\in\mathbb{N}}[a_n, b_n] \neq \emptyset$.*

Uma sequência de intervalos $(I_n)_{n\in\mathbb{N}}$ tal que $I_{n+1} \subset I_n$ é chamada de encaixante.

Demonstração. Pela condição sobre a_n's e b_n's acima, temos que valem as seguintes desigualdades:

$$a_0 \leq a_1 \leq \cdots a_n \leq \cdots \leq b_n \leq \cdots \leq b_1 \leq b_0$$

Note que, assim, temos que os a_n's são minorantes para o conjunto $\{b_n : n \in \mathbb{N}\}$ e que os b_n's são majorantes para $\{a_n : n \in \mathbb{N}\}$. Em particular, o conjunto $\{a_n : n \in \mathbb{N}\}$ é limitado superiormente. Portanto, admite supremo.

Vamos chamar tal supremo de a. Como cada b_n é majorante deste conjunto, temos que $a \leq b_n$ para cada n. Além disso, como o próprio a é majorante, temos que cada $a_n \leq a$. Ou seja, $a \in [a_n, b_n]$ para todo $n \in \mathbb{N}$. □

Os exemplos a seguir ilustram como as hipótese do resultado anterior são necessárias:

Exemplo 1.3.20. $\bigcap_{n\in\mathbb{N}}[n, +\infty[= \emptyset$.

Exemplo 1.3.21. $\bigcap_{n\in\mathbb{N}}]0, \frac{1}{n+1}[= \emptyset$

Vamos tentar ver porque isso é algo particular dos reais. Todas as definições que fizemos antes (máximos, majorantes, supremos etc.) poderiam ser feitas sobre qualquer conjunto com uma ordem. Isso inclui a definição de intervalo apresentada aqui. Por exemplo, poderíamos fazer essa definições no conjunto $\mathbb{N}$. Nele, os intervalos são coisas "estranhas". Por exemplo

Estamos pensando todas as definições só se considerando os números naturais.

$$[0, 5[= \{0, 1, 2, 3, 4\}$$

Ou, pior ainda,

$$]0, 1[= \emptyset$$

Mas $\mathbb{N}$ é um conjunto bastante diferente de $\mathbb{R}$. Um conjunto mais próximo é o conjunto $\mathbb{Q}$ (se você sabe o que é um corpo, temos que os dois são corpos, ao contrário de $\mathbb{N}$).

Mas em $\mathbb{Q}$, nem todo subconjunto limitado superiormente admite supremo:

$$\{x \in \mathbb{Q} : x^2 < 2\}$$

Intuitivamente, o supremo desse conjunto deveria ser $\sqrt{2}$, mas tal elemento não pertence a $\mathbb{Q}$ (certo?).

Alongamentos

Alongamento 1.3.22. Mostre que se a, b são mínimos para A, então $a = b$.

Alongamento 1.3.23. Mostre que não existe mínimo de $\{\frac{1}{n} : n \in \mathbb{N}_{>0}\}$.

Exercícios

Exercício 1.3.24. Sejam $A, B \subset \mathbb{R}$ conjuntos que admitam mínimos.

(a) Mostre que se $A \subset B$, então $\min A \geq \min B$.

(b) Mostre que, se existe o mínimos de $A \cup B$, então $\min(A \cup B) = \min\{\min A, \min B\}$.

Exercício 1.3.25. Sejam $A, B \subset \mathbb{R}$ conjuntos que admitam mínimos. Mostre que, mesmo que existam os mínimos de A e de B, pode não existir o mínimo de $A \cap B$.

Exercício 1.3.26. Seja $A \subset \mathbb{R}$ tal que A admite majorante a. Mostre que todo elemento de $[a, +\infty[$ é um majorante.

Exercício 1.3.27. Seja $A \subset \mathbb{R}$. Mostre que A é limitado se, e somente se, existe $L \in \mathbb{R}_{>0}$ tal que $A \subset [-L, L]$.

Capítulo 2

Funções

2.1 Polinômios

Dizemos que $p : \mathbb{R} \longrightarrow \mathbb{R}$ é um **polinômio** (ou uma **função polinomial**) se existem $a_0, ..., a_n \in \mathbb{R}$ tais que $p(x) = a_0 + a_1x + \cdots + a_nx^n$ para todo $x \in \mathbb{R}$. Se $a_n \neq 0$, então dizemos que o **grau** de p é n.

Tem gente que faz uma diferença formal entre os dois conceitos. Não vamos gastar tempo com isso aqui.

Nesta seção, vamos nos concentrar apenas em polinômios reais. Mas você pode notar que (quase) tudo o que fazemos aqui pode ser repetido em qualquer lugar onde haja produtos e somas (por exemplo, em $\mathbb{C}$ ou em matrizes $n \times n$).

Proposição 2.1.1. *Polinômios são fechados para a soma e produto.*

Isso quer dizer que soma de dois polinômios é um polinômio e o mesmo para o produto de polinômios.

Demonstração. Sejam p e q polinômios. Então existem $a_0, ..., a_n$ e $b_0, ..., b_m \in \mathbb{R}$ tais que $p(x) = a_0 + a_1x + \cdots + a_nx^n$ e $q(x) = b_0 + b_1x + \cdots + b_mx^m$. Para facilitar as contas, considere $k = \max\{n, m\}$ e re-escreva

$$p(x) = a_0 + a_1x + \cdots + a_kx^k$$
$$q(x) = b_0 + b_1x + \cdots + b_kx^k$$

fazendo $a_j, b_i = 0$ quando necessário.

Desta forma, temos que

$$\begin{aligned} p(x) + q(x) &= (a_0 + a_1x + \cdots + a_kx^k) + (b_0 + b_1x + \cdots + b_kx^k) \\ &= (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_k + b_k)x^k \end{aligned}$$

Para o produto é a mesma coisa, apenas um pouco mais chato de fazer a conta. □

É só desenvolver o lado esquerdo.

Vamos usar o seguinte truque:

$$(x-\alpha)(x^{n-1}+x^{n-2}\alpha+\cdots x\alpha^{n-2}+\alpha^{n-1})=(x^n-\alpha^n)$$

se $\alpha \in \mathbb{R}$ e $n>1$

Com esse truque, já é imediato provar o seguinte resultado:

Lema 2.1.2. *Sejam $\alpha \in \mathbb{R}$ e $n>1$. Então existe q polinômio tal que*

$$(x^n-\alpha^n)=(x-\alpha)q(x)$$

onde o grau de q é menor que n.

Basta tomar como q o polinômio que aparece no truque.

Proposição 2.1.3. *Seja p um polinômio de grau maior que 1. Seja $\alpha \in \mathbb{R}$. Temos então que existe q polinômio tal que $p(x)-p(\alpha)=(x-\alpha)q(x)$. Além disso, o grau de q é menor que o grau de p.*

Demonstração. Sejam $a_0,...,a_n \in \mathbb{R}$ tais que $p(x)=a_0+a_1x+\cdots+a_nx^n$. Note que

$$p(x)-p(\alpha)=a_1(x-\alpha)+a_2(x^2-\alpha^2)+\cdots+a_n(x^n-\alpha^n)$$

Note que podemos usar o lema em (quase) cada termo do lado direito. Assim, existem $q_2,...,q_n$ polinômios tais que

$$\begin{aligned} p(x)-p(\alpha) &= a_1(x-\alpha)+a_2(x-\alpha)q_2(x)+\cdots+a_n(x-\alpha)q_n(x) \\ &= (x-\alpha)(a_1+a_2q_2(x)+\cdots a_nq_n(x)) \end{aligned}$$

Note que $q(x)=a_1+a_2q_2(x)+\cdots+a_nq_n(x)$ é um polinômio, assim só resta estimarmos o grau de r. Note que o grau de cada q_j é menor que j (pelo lema). Assim, pelos Exercício 2.1.14, temos que o grau de r é menor que n como queríamos. □

Com esse resultado, podemos provar diversos resultados folclóricos de maneira simples:

Definição 2.1.4. Dizemos que $\alpha \in \mathbb{R}$ é uma **raiz** de um polinômio p se $p(\alpha)=0$.

Teorema 2.1.5. *Sejam p um polinômio e $\alpha \in \mathbb{R}$. Então α é raiz de p se, e somente se, $p(x) = (x - \alpha)q(x)$ para algum polinômio q.*

Demonstração. Suponha que α é uma raiz de p. Se o grau de p é menor ou igual a 1, o resultado é imediato. Caso contrário, pela proposição anterior, sabemos que existe q tal que

$$p(x) - p(\alpha) = (x - \alpha)q(x)$$

Lembrando ue $p(\alpha) = 0$, temos o que queríamos.

Por outro lado, se $p(x) = (x - \alpha)q(x)$, temos que

$$p(\alpha) = (\alpha - \alpha)q(\alpha) = 0$$

□

Teorema 2.1.6. *Se p tem grau $n \in \mathbb{N}_{\geq 1}$, então p tem no máximo n raizes.*

Demonstração. Se $n = 1$, então p tem uma única raiz. Por outro lado, se $n > 1$ e p tem pelo menos uma raiz α, então existe um polinômio q de grau menor que n tal que $p(x) = (x - \alpha)q(x)$. Se q tiver grau maior que 1 e uma raiz β, podemos aplicar o mesmo processo e obter r de grau menor que o de q de forma que $q(x) = (x - \beta)r(x)$. Desta forma

$$p(x) = (x - \alpha)(x - \beta)r(x)$$

Podemos aplicar esse processo enquanto os polinômios tiverem raízes e seus graus forem maiores que 1. Ou seja, nesse processo aparecem no máximo n raízes. □

Se você souber indução, essa demonstração fica bem mais fácil. Vamos ver indução mais para frente e refazer isso.

Um corolário estranho desse resultado é o seguinte:

Corolário 2.1.7. *O único polinômio com infinitas raizes é o identicamente nulo.*

Demonstração. Simplesmente porque, se p não é o polinômio nulo, seu grau é algum $n > 0$. □

Proposição 2.1.8. *Dois polinômios são iguais se, e somente se, seus coeficientes são iguais.*

Demonstração. É claro que se os coeficientes são iguais, os polinômios são iguais. Por outro lado, suponha que existam $a_0, ..., a_n, b_0, ..., b_m \in \mathbb{R}$ de forma que $a_0 + \cdots a_n x^n = b_0 + \cdots + b_m x^m$ para todo $x \in \mathbb{R}$. Da mesma forma que fizemos antes, podemos supor que $m, n = k$. Ou seja, temos que

$$a_0 + \cdots a_k x^k = b_0 + \cdots + b_k x^k$$

para todo $x \in \mathbb{R}$. Assim

$$(a_0 - b_0) + \cdots + (a_k - b_k)x^k = 0$$

para todo $x \in \mathbb{R}$. Em outras palavras, tal polinômio tem infinitas raízes. Logo, ele obrigatoriamente é o polinômio nulo. Assim, $a_0 = b_0$, ..., $a_k = b_k$ como queríamos. □

Definição 2.1.9. Seja $f : \mathbb{R} \to \mathbb{R}$ uma função. Chamamos de **gráfico** de f o conjunto $\{(x, y) \in \mathbb{R}^2 : y = f(x)\}$.

Teorema 2.1.10. *Dados $n+1$ pontos do plano (com os x's distintos), existe um, e apenas um, polinômio de grau no máximo n cujo gráfico contém todos esses pontos.*

Demonstração. Unicidade: Suponha que p e q sejam polinômios como no enunciado. Note que, então $r(x) = p(x) - q(x)$ tem grau no máximo n e $n + 1$ raízes (os x's dos pontos do enunciado). Ou seja, r necessariamente é o polinômio nulo e, portanto, $p = q$.

Existência: podemos usar a seguinte fórmula: sejam $(x_0, y_0), ..., (y_n, x_n)$ os $n + 1$ pontos. Note que o seguinte polinômio satisfaz o enunciado:

$$p(x) = \sum_{i=0}^{n} y_i \prod_{j \neq i} \frac{1}{x_i - x_j}(x - x_j)$$

□

Uma aplicação interessante do último resultado é a seguinte:

Corolário 2.1.11. *Não existem 3 pontos colineares numa parábola.*

Demonstração. A menos de rotação, podemos supor que a parábola é o gráfico de algum $p(x)$ de grau 2. Suponha que existam (x_0, y_0), (x_1, y_1), (x_2, y_2) no gráfico de p colineares. Como p é função, temos que x_0, x_1 e x_2 são todos distintos. Se uma reta r contivesse tais pontos, ela teria que ser o gráfico de algum q de grau 1. Mas isso é impossível pelo teorema anterior. □

Exercícios

Exercício 2.1.12. Seja $A \subset \mathbb{R}^2$. Escreva uma condição necessária e suficiente para existir $f : \mathbb{R} \to \mathbb{R}$ função tal que A seja o gráfico de f.

Exercício 2.1.13. Suponha que $A \subset \mathbb{R}^2$ seja um gráfico de alguma função f.

(a) Se para todo $b \in \mathbb{R}$ temos que o conjunto $\{a \in \mathbb{R} : (a, b) \in A\}$ é não vazio, o que podemos dizer sobre f?

(b) Se para todo $b \in \mathbb{R}$ temos que o conjunto $\{a \in \mathbb{R} : (a, b) \in A\}$ tem no máximo um ponto, o que podemos dizer sobre f?

Exercício 2.1.14. Sejam p e q polinômios de grau n e m respectivamente. Mostre que:

(a) Grau de $p + q$ é menor ou igual a $\max\{n, m\}$.

(b) Grau de pq é igual a $n + m$.

Exercício 2.1.15. Dê um exemplo de polinômios p e q de forma que o grau de $p + q$ seja estritamente menor que os graus de p e q.

2.2 Indução

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:

Vamos que certa propriedade vale para 0. Depois, provamos que se a tal propriedade vale para algum $n \in \mathbb{N}$, ela precisa vale para $n + 1$. Com essas duas verificações, provamos que ela vale para todos os naturais.

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:

Fato 2.2.1. *Todo subconjunto não vazio de* $\mathbb{N}$ *admite mínimo.*

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

Vamos ver como isso funciona na prática:

Proposição 2.2.2. *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 $2^0 = 1 = 2^{0+1} - 1$.

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:

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

O HI acima indica onde usamos a hipótese de indução. □

Note que pelo argumento acima indica, 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, isso vale para qualquer k_0 que seja o primeiro que a gente prova que vale.

Isso é útil em alguns casos, como por exemplo:

Proposição 2.2.3. *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

$$4(n + 1) = 4n + 4 < 2^n + 2 \cdot 2 < 2^n + 2^n = 2^{n+1}$$

□

Nem sempre as afirmações envolvem só naturais:

Proposição 2.2.4. *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.

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 tem 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. □

Vamos provar novamente o teorema da seção passada, agora usando indução:

Teorema 2.2.5. *Se p é um polinômio de grau $n \geq 1$, então p tem, no máximo, n raízes.*

Demonstração. Se $n = 1$, temos que p tem uma única raiz e, portanto, o resultado vale. Agora suponha que vale o resultado para n e vamos provar para $n + 1$. Seja p de grau $n + 1$. Se p não tem raiz, terminamos. Se p tem alguma raiz α, sabemos que existe q de grau menor que $n + 1$ tal que

$$p(x) = (x - \alpha)q(x)$$

Como q tem grau menor que $n + 1$, vale a hipótese de indução para ele (veja comentário abaixo). Assim, q tem, no máximo, n raízes. Como as raízes de p são as raízes de q mais a raiz α, temos o resultado. □

Note que usamos em vez que vale para n, vale para $n+1$, usamos que se vale para todos menores iguais a n, vale para $n+1$. Note que esse é um outro jeito de fazer indução, que também funciona pelo argumento apresentado no início da seção.

Exercícios

Exercício 2.2.6. Mostre que para todo $n \geq 1$, temos que $3^{n+1} > 2n$.

Exercício 2.2.7. Mostre que $n^3 - n$ é múltiplo de 3 para todo $n \in \mathbb{N}$.

Exercício 2.2.8. Mostre que $n^2 - 1$ é múltiplo de 8 para todo n ímpar.

2.3 Inversas

Se A estiver claro no contexto, em geral o omitimos e denotamos simplesmente Id.

Dado um conjunto A, vamos denotar por $Id_A : A \to A$ a **função identidade**, isto é, $Id(a) = a$ para todo $a \in A$.

Definição 2.3.1. Sejam A e B conjuntos e $f : A \to B$ uma função. Dizemos que $g : B \to A$ é uma **inversa à esquerda** de f se $g \circ f = Id_A$. Dizemos que g é uma **inversa à direita** se $f \circ g = Id_B$.

Proposição 2.3.2. *Sejam A e B conjuntos e $f : A \to B$ uma função. Então f é injetora se, e somente se, admite uma inversa à esquerda.*

Demonstração. Suponha que f é injetora. Fixe $a_0 \in A$ qualquer. Dado $b \in \text{Im}(f)$ existe um único $a_b \in A$ tal que

$$f(a_b) = b$$

Defina $g : B \to A$ por

$$g(b) = \begin{cases} a_b & \text{se } b \in Im(f) \\ a_0 & \text{caso contrário} \end{cases}$$

Vejamos que g é uma inversa à esquerda de f. Seja $a \in A$. Note que, então, $f(a) \in \text{Im}(f)$ e que, pelo fato de f ser injetora, $a_{f(a)} = a$. Assim

$$g(f(a)) = a_{f(a)} = a$$

Agora suponha que $g : B \to A$ é uma inversa à esquerda de f. Sejam $x, y \in A$ tais que $f(x) = f(y)$. Aplicando g de ambos os lados obtemos

$$g(f(x)) = g(f(y))$$

Como g é inversa à esquerda, obtemos $x = y$. □

Note que na construção da g no resultado anterior, não fez muita diferença quem foi o a_0 escolhido. Ou seja, é bem simples construir uma f que admita diferentes g's como inversas à esquerda (veja o Exercício 2.4.1).

Proposição 2.3.3. *Sejam A e B conjuntos e $f : A \to B$ uma função. Então f é sobrejetora se, e somente se, admite uma inversa à direita.*

Demonstração. Suponha f sobrejetora. Para cada $b \in B$, existe $a_b \in A$ tal que $f(a_b) = b$. Defina $g : B \to A$ por $g(b) = a_b$. Então

$$f(g(b)) = f(a_b) = b$$

Podem existir vários a's com essa propriedade. Simplesmente escolhemos um.

Por outro lado, suponha que $g : B \to A$ seja uma inversa à direita de f. Vamos mostrar que f é sobrejetora. Seja $b \in B$. Temos que $b = f(g(b))$. Logo, $b \in \mathrm{Im}(f)$. □

Proposição 2.3.4. *Se g é uma inversa à esquerda de f e h é uma inversa à direita de f, então $g = h$.*

Neste caso, como f tem as duas inversas, f tem que ser bijetora.

Demonstração. Seja $b \in B$. Temos que $g(b) = g(f(h(b))) = h(b)$. □

Dada a unicidade do resultado acima, quando f é bijetora de denotamos por f^{-1} sua inversa à direita (ou à esquerda) e a chamamos simplesmente de **inversa** de f.

2.4 Exercícios

Exercício 2.4.1. Dê um exemplo de $f : A \to B$ que admita duas inversas à esquerda distintas.

Exercício 2.4.2. Mostre que se f é bijetora, então f admite uma única inversa à esquerda (analogamente, uma única inversa à direita).

Exercício 2.4.3. Sejam $f : X \to X$ e $g : X \to X$ bijetoras. Suponha que $f \circ g = g \circ f$. É verdade que f é a inversa de g?

2.5 Funções Racionais

Uma função racional é uma função f tal que existem p, q polinômios de forma que $f(x) = \frac{p(x)}{q(x)}$.

Observação 2.5.1. Note que o domínio de f é restrito aos pontos $x \in \mathbb{R}$ onde $q(x) \neq 0$.

Para os pontos x que não são raízes do polinômio q, muitas vezes podemos simplificar a conta:

Exemplo 2.5.2. Considere $f(x) = \frac{x^3+x^2-x-1}{x-1}$.

Note que 1 é raiz de $x^3 + x^2 - x - 1$. Logo, pelo que vimos anteriormente, temos que $x^3 + x^2 - x - 1 = p(x)(x - 1)$ para algum p. Fazemos a conta de forma parecida com a que fazemos com números:

$$\begin{array}{rcrcrcr|l}
x^3 & + & x^2 & - & x & - & 1 & x - 1 \\
\cline{8-8}
x^3 & - & x^2 & & & & & x^2 + 2x + 1 \\
\cline{1-3}
 & & 2x^2 & - & x & - & 1 & \\
 & & 2x^2 & - & 2x & & & \\
\cline{3-5}
 & & & & x & - & 1 & \\
 & & & & & & 0 &
\end{array}$$

Assim, temos

$$\begin{array}{rcl}
\frac{x^3+x^2-x-1}{x-1} & = & \frac{(x-1)(x^2+2x+1)}{x-1} \\
 & = & x^2 + 2x + 1
\end{array}$$

Para todo $x \neq 1$.

Exemplo 2.5.3. Considere $f(x) = \frac{x^3-3x^2+5x-15}{x^2-9}$. Novamente, temos que $(x - 3)$ divide ambas as partes. Fatorando

$$\begin{array}{rcrcrcr|l}
x^3 & - & 3x^2 & + & 5x & - & 15 & x - 3 \\
\cline{8-8}
x^3 & - & 3x^2 & & & & & x^2 + 5 \\
\cline{1-3}
 & & & & 5x & - & 15 & \\
 & & & & 5x & - & 15 & \\
\cline{5-7}
 & & & & & & 0 &
\end{array}$$

E $(x^2 - 9) = (x - 3)(x + 3)$. Assim

$$\begin{array}{rcl}
\frac{x^3-3x^2+5x-15}{x^2-9} & = & \frac{(x-3)(x^2+5)}{(x-3)(x+3)} \\
 & = & \frac{x^2+5}{x+3}
\end{array}$$

para todo $x \neq 3$.

Exemplo 2.5.4. Considere $f(x) = \frac{x^3-x^2-21x+45}{x^2-6x+9}$. Note que 3 é raiz de ambos. Assim:

$$\begin{array}{rcrcrcr|l}
x^3 & - & x^2 & - & 21x & + & 45 & x - 3 \\
\cline{8-8}
x^3 & - & 3x^2 & & & & & x^2 + 2x - 15 \\
\cline{1-5}
 & & 2x^2 & - & 21x & + & 45 & \\
 & & 2x^2 & - & 6x & & & \\
\cline{3-5}
 & & & - & 15x & + & 45 & \\
 & & & - & 15x & + & 45 & \\
\cline{3-5}
 & & & & & & 0 &
\end{array}$$

E

$$\begin{array}{rcrcrcr|l}
x^2 & - & 6x & + & 9 & & & x - 3 \\
\cline{7-7}
x^2 & - & 3x & & & & & x - 3 \\
\cline{1-5}
 & - & 3x & + & 9 & & & \\
 & - & 3x & + & 9 & & & \\
\cline{2-5}
 & & & & 0 & & &
\end{array}$$

Assim, para $x \neq 3$, temos que $\frac{x^3-x^2-21x+45}{x^2-6x+9} = \frac{(x-3)(x^2+2x-15)}{(x-3)(x-3)} = \frac{x^2+2x-15}{x-3}$. Note que 3 ainda é raiz de ambas as parte. Assim

$$\begin{array}{rcrcrcr|l}
x^2 & + & 2x & - & 15 & & & x - 3 \\
\cline{7-7}
x^2 & - & 3x & & & & & x + 5 \\
\cline{1-5}
 & & 5x & - & 15 & & & \\
 & & 5x & - & 15 & & & \\
\cline{3-5}
 & & & & 0 & & &
\end{array}$$

Ou seja, para $x \neq 3$, $f(x) = x + 5$.

Note que, assim, na verdade observamos que o denominador dividia o numerador. Então podíamos ter feito a conta inteira de uma vez. Vejamos:

$$\begin{array}{rcrcrcr|l}
x^3 & - & x^2 & - & 21x & + & 45 & x^2 - 6x + 9 \\
\cline{8-8}
x^3 & - & 6x^2 & + & 9x & & & x + 5 \\
\cline{1-5}
 & & 5x^2 & - & 30x & + & 45 & \\
 & & 5x^2 & - & 30x & + & 45 & \\
\cline{3-5}
 & & & & & & 0 &
\end{array}$$

Proposição 2.5.5. *Se f e g são funções racionais, então $f+g$ e fg também são.*

Aqui só precisamos tomar cuidado com os domínios das funções. Note que não podemos fazer as contas aqui se $q(x) = 0$ ou $s(x) = 0$.

Demonstração. Seja p, q, r, s polinômios tais que

$$f(x) = \frac{p(x)}{q(x)} \; g(x) = \frac{r(x)}{s(x)}$$

onde, a primeira igualdade vale para todo x tal que $g(x) \neq 0$ e a segunda vale para todo x tal que $s(x) \neq 0$.

Então

$$(f+g)(x) = \frac{p(x)s(x) + r(x)q(x)}{q(x)s(x)}$$

$$(fg)(x) = \frac{p(x)r(x)}{q(x)s(x)}$$

Como soma e produto de polinômios é polinômio, temos o resultado. □

Se uma função é racional, para provarmos isso basta exibirmos os polinômios correspondentes. Mas e quando uma função não é racional? Daí temos uma tarefa mais "complicada": temos que provar é impossível encontrar os tais polinômios. No próximo exemplo, vamos mostrar uma maneira de se fazer isso:

Exemplo 2.5.6. A função $\text{sen} : \mathbb{R} \to \mathbb{R}$ não é uma função racional.

De fato, suponha que existam p e q polinômios tais que

$$\text{sen}(x) = \frac{p(x)}{q(x)}$$

Como $\text{sen}(x)$ está definida para todo $x \in \mathbb{R}$, temos que $q(x) \neq 0$ para todo $x \in \mathbb{R}$. Note que, se $\alpha \in \mathbb{R}$ é tal que $\text{sen}(\alpha) = 0$, então necessariamente $p(\alpha) = 0$. Assim, como sen tem infinitas raízes, p também tem - o que é impossível.

Uma outra maneira pode ser por meio de limites, como no curso de Cálculo.

2.6 Exponencial

Nesta seção, vamos trabalhar com a função exponencial. Começamos a trabalhar com ela sobre $\mathbb{N}$ e depois veremos uma maneira de como estender tal

conceito para $\mathbb{Z}$, $\mathbb{Q}$ e, finalmente, $\mathbb{R}$. Vamos começar da seguinte maneira: fixe $a \in \mathbb{R}_{>0}$. Considere a seguinte função $f_a : \mathbb{N}_{>0} \longrightarrow \mathbb{R}$ dada por

Com o uso de Cálculo, é mais fácil definir primeiro o logaritmo de uma maneira bastante simples e, depois, definir a exponencial como sua inversa. Para quem tiver curiosidade de ver como isso pode ser feito, sugerimos [].

$$f_a(n) = \underbrace{a \cdots a}_{a \text{ } n \text{ vezes}}$$

Você já viu isso antes, costumamos denotar isso por a^n.

Em provas por indução, uma propriedade muito útil desta função é a seguinte. Dado qualquer $n \in \mathbb{N}_{>1}$

$$f_a(n+1) = f_a(n)a$$

Colocando na notação mais comum, temos

$$a^{n+1} = a^n a$$

Vejamos algumas propriedades que essa função tem.

Proposição 2.6.1. *Seja $a \in \mathbb{R}$ e sejam $p, q \in \mathbb{N}_{>0}$. Então $a^p a^q = a^{p+q}$.*

Sim, poderíamos simplesmente contar quantos a's aparecem do lado direito e do lado esquerdo da equação. Mas daí qual seria a graça?

Demonstração. Vamos fazer por indução sobre q começando com $q = 1$. De fato, temos

$$a^p a^1 = a^{p+1}$$

como queríamos.

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

$$a^p a^{q+1} = a^p(a^q a) = (a^p a^q)a = a^{p+q}a = a^{p+(q+1)}$$

□

Proposição 2.6.2. *Seja $a \in \mathbb{R}$ e sejam $p, q \in \mathbb{N}_{>0}$. Então $(a^p)^q = a^{pq}$*

Demonstração. Novamente, vamos fazer por indução. Começando com $q = 1$, temos

$$(a^p)^1 = a^p = a^{p1}$$

Agora suponha o resultado válido para q e vamos provar para $q+1$. Temos

$$(a^p)^{q+1} = (a^p)^q a^p = a^{pq}a^p = a^{pq+p} = a^{p(q+1)}$$

□

Basta multiplicar os dois lados por a^n

Note que, como $a > 0$, então $a^k > 0$ para todo k. Daí, temos dois casos. Se $a > 1$, temos que $a^{n+1} > a^n$ para todo n. Por outro lado, se $1 < a$, então $a^n < a^{n+1}$. Claramente, se $a = 1$, então $a^n = 1$.

Então a função f_a é **estritamente crescente** se $a > 1$ e **estritamente decrescente** se $a < 1$ (sempre tomando-se $a > 0$).

Vamos analisar o conjunto das potências de a:

$$\{a^k : k \in \mathbb{N}_{>0}\}$$

Pelo que observamos antes, temos que para $a \in]0, 1[$, tal conjunto é limitado por 0 e por a. Isto é, dado qualquer $k \in \mathbb{N}_{>0}$, temos

$$0 < a^k < a$$

Mas e se $a > 1$? Cuidado aqui, não podemos simplesmente dizer que tal conjunto não é limitado superiormente simplesmente pelo motivo da sequência $(a^k)_{k>0}$ ser crescente - lembre por exemplo, de sequências como $(1 - \frac{1}{n})_{n>0}$. Mas, ainda assim, podemos provar que tal conjunto é, de fato, ilimitado superiormente. Para isso, vamos usar o seguinte resultado auxiliar:

Proposição 2.6.3 (Desigualdade de Bernoulli)**.** *Sejam $x \in \mathbb{R}_{\geq 0}$ e $k \in \mathbb{N}_{\geq 1}$. Então*

$$(1 + x)^k \geq 1 + kx$$

Demonstração. Vamos mostrar por indução em k. Caso $k = 1$, temos que vale trivialmente. Agora suponha o caso k e vamos provar para $k + 1$.

$$\begin{aligned}(1 + x)^{k+1} &= (1 + x)^k(1 + x) \\ &\geq (1 + kx)(1 + x) \\ &= 1 + x + kx + kx^2 \\ &\geq 1 + x + kx \\ &= 1 + (k + 1)x\end{aligned}$$

□

Com essa desigualdade, conseguimos provar o seguinte resultado:

Proposição 2.6.4. *Seja $a \in \mathbb{R}_{>1}$. Então o conjunto $\{a^n : n \in \mathbb{N}_{\geq 1}\}$ não é limitado superiormente.*

Demonstração. Suponha que $L \in \mathbb{R}$ seja um limitante superior para o conjunto. Seja Δ tal que $a = 1 + \Delta$. Note que $\Delta > 0$. Seja k tal que $1 + k\Delta > L$ (existe pois $\Delta > 0$). Assim, temos

$$a^k = (1 + \Delta)^k \geq 1 + k\Delta > L$$

Logo, L não pode ser um majorante das potências de a. □

Proposição 2.6.5. *Sejam $a, b \in \mathbb{R}$ e $p \in \mathbb{N}_{>0}$. Então $(ab)^p = a^p b^p$.*

Demonstração. Por indução sobre p. Com $p = 1$, temos o resultado imediatamente. Agora suponha o caso p e vamos provar o caso $p + 1$. Temos

$$(ab)^{p+1} = (ab)^p(ab) = a^p b^p ab = a^p a b^p b = a^{p+1} b^{p+1}$$

□

Corolário 2.6.6. *Sejam $b \in \mathbb{R}_{\neq 0}$ e $p \in \mathbb{N}_{>0}$. Então $(\frac{1}{b})^p = \frac{1}{b^p}$.*

Demonstração. Como $1 = b\frac{1}{b}$, temos que $1^p = (b\frac{1}{b})^p$. Logo, $b^p(\frac{1}{b})^p = 1$. Ou seja

$$(\frac{1}{b})^p = \frac{1}{b^p}$$

□

Corolário 2.6.7. *Sejam $a, b \in \mathbb{R}$ com $b \neq 0$. Seja $p \in \mathbb{N}_{>0}$. Então $(\frac{a}{b})^p = \frac{a^p}{b^p}$.*

Estendendo a função para $\mathbb{Z}$

Numa tentativa de deixar mais claro o que vamos fazer, vamos novamente adotar a notação funcional $f_a(n) = a^n$. Vamos tentar estender a ideia de f_a, mas agora para todos os inteiros. Gostaríamos que essa extensão fosse tal que os resultados da última seção valessem. Especialmente, gostaríamos que a igualdade

$$f_a(k)f_a(m) = f_a(k + m) \tag{2.1}$$

continuasse valendo.

Comecemos por tentar definir o que seria $f_a(0)$. Se quisermos manter a igualdade 2.1, vemos que, fazendo $m = 0$, obtemos

$$f_a(k)f_a(0) = f(k) = f(k + 0) = f(k)$$

O único jeito de obtermos isso é definindo $f_a(0) = 1$.

De maneira análoga, dado $-k$, para $k > 0$, temos que para manter a igualdade

$$f_a(-k)f_a(k) = f_a(0) = 1$$

só temos como opção para $f_a(-k) = \frac{1}{f_a(k)}$.

Note que agora já não podemos mais fazer isso para qualquer a - temos que pedir que $a \neq 0$, para garantir que $f_a(k) \neq 0$.

Desta maneira, dado $a \neq 0$, podemos definir $f_a : \mathbb{Z} \to \mathbb{R}$. Colocando em notação mais comum, temos que $a^0 = 1$ e $a^{-k} = \frac{1}{a^k}$ e, de fato, as duas igualdades anteriores continuam valendo. Para isso, vamos usar alguns resultados auxiliares:

Lema 2.6.8. *Sejam $p \in \mathbb{Z}$ e $a \in \mathbb{R}_{\neq 0}$. Então $a^{p-1} = a^p a^{-1}$.*

Demonstração. Vamos dividir em alguns casos. Se $p - 1 = 0$, temos que $1 = a^1 \frac{1}{a^{-1}}$. Se $p - 1 > 0$, então $p - 1 = b > 0$. Sabemos que

$$a^{b+1} = a^b a$$

Multiplicando por $a^{-1} = \frac{1}{a}$ de ambos os lados, obtemos

$$a^{b+1}a^{-1} = a^b$$

Substituindo de volta o valor de p:

$$a^p a^{-1} = a^{p-1}$$

Agora, se $p - 1 < 0$, então $p - 1 = -k$ para algum $k > 0$. Assim

$$a^{p-1} = a^{-k} = \frac{1}{a^k} = \frac{1}{a^{k-1}a} = \frac{1}{a^{k-1}}\frac{1}{a} = a^{k+1}a^{-1} = a^p a^{-1}$$

□

Lema 2.6.9. *Sejam $p \in \mathbb{Z}$, $k \in \mathbb{N}$ e $a \in \mathbb{R}_{\neq 0}$. Então $a^{p-k} = \frac{a^p}{a^k}$.*

Demonstração. Por indução sobre k. Com $k = 0$, o resultado é imediato. Agora suponha que vale para k e vamos provar para $k + 1$. Temos

$$a^{p-(k+1)} = a^{p-k-1} = a^{p-k}a^{-1} = \frac{a^p}{a^k}\frac{1}{a} = \frac{a^p}{a^{k+1}}$$

□

Lema 2.6.10. *Seja $a \in \mathbb{R}_{\neq 0}$. Se $p \in \mathbb{Z}$ e $k \in \mathbb{N}$, então $(a^p)^k = a^{pk}$.*

Demonstração. Note que, se $p \in \mathbb{N}$, o resultado segue pelos resultados anteriores. Resta só o caso em que $p = -r$ para algum $r \in \mathbb{N}$. Neste caso, temos

$$(a^p)^k = (a^{-r})^k = (\frac{1}{a^r})^k = \frac{1^k}{(a^r)^k} = \frac{1}{a^{rk}} = a^{-rk} = a^{pk}$$

□

Proposição 2.6.11. *Seja $a \in \mathbb{R}_{\neq 0}$. Dados $p, q, \in \mathbb{Z}$, temos que:*

(a) $a^p a^q = a^{p+q}$

(b) $(a^p)^q = a^{pq}$

Demonstração. Note que se $p, q > 0$, já temos o resultado. Vejamos alguns dos outros casos. Primeiramente, suponha $p \in \mathbb{Z}$ e $q = 0$. Então

$$a^p a^q = a^p = a^{p+q}$$

$$(a^p)^q = 1 = a^{pq}$$

Agora suponha que $p \in \mathbb{Z}$ e $q = -k$ para algum $k \in \mathbb{N}$. Então

$$a^p a^q = a^p a^{-k} = a^p \frac{1}{a^k} = \frac{a^p}{a^k} = a^{p-k}$$

$$(a^p)^q = (a^p)^{-k} = \frac{1}{(a^p)^k} = \frac{1}{a^{pk}} = a^{-pk} = a^{pq}$$

□

Estendendo para $\mathbb{Q}$

Será que dá para estender f_a para todo $\mathbb{Q}$? Seja $\frac{p}{q} \in \mathbb{Q}$. Tentando manter a igualdade da seção anterior

$$(a^m)^k = a^{mk} \tag{2.2}$$

Deveríamos ter que

$$(a^{\frac{p}{q}})^q = a^p$$

Ou seja, $a^{\frac{p}{q}}$ precisa ser o número que, elevado a q, dá a^p. Normalmente denotamos isso por $\sqrt[q]{a^p}$. E aqui já caímos com problemas novamente: tome por exemplo $a < 0$, $p = 3$ e $q = 2$. Temos que $a^3 < 0$. Por outro lado, a igualdade acima pediria que $(a^{\frac{3}{2}})^2 = a^3$. Ou seja, $a^{\frac{3}{2}}$ precisaria ser um número real cujo quadrado é negativo. Desta forma, para que essa função tenha chance de ficar bem definida nos reais, precisamos agora evitar $a < 0$. Ou seja, daqui para frente, sempre teremos $a \in \mathbb{R}_{>0}$.

Para se fazer a extensão para os reais, precisamos usa Cálculo (definimos como uma extensão contínua da função construída até aqui).

2.7 Logaritmo

O objetivo desta seção é definir a função logaritmo (em alguma base) que, nada mais é que a inversa da exponencial. Antes, vejamos que, de fato, a função exponencial possui uma inversa e vejamos algumas propriedades.

Proposição 2.7.1. *Seja $A, B \subset \mathbb{R}$. Se uma função $f : A \longrightarrow B$ é estritamente crescente, então f é injetora. Além disso, se f tiver inversa, f^{-1} é estritamente crescente também.*

Demonstração. Sejam $x \neq y \in A$. Se $x < y$, então $f(x) < f(y)$ (o outro caso é análogo) e, portanto, $f(x) \neq f(y)$.

Agora sejam $x < y \in B$. Suponha que $f^{-1}(y) \leq f^{-1}(x)$. Então, $f(f^{-1}(y)) \leq f(f^{-1}(x))$. Logo, $y \leq x$, contradição. □

Da mesma maneira, podemos provar o resultado análogo para funções estritamente decrescentes.

Vamos usar que a função exponencial com base $a > 0$ tem as seguintes propriedades:

$$a^{b+c} = a^b a^c$$

$$a^b > 0$$

$$a^b < 1 \text{ se } a < 1$$

$$a^b > 1 \text{ se } a > 1$$

Com isso, é fácil mostrar o seguinte resultado:

Note que em ambos os casos a função é injetora

Proposição 2.7.2. *Se $a \in]0, 1[$, a função a^x é estritamente decrescente. Já se $a \in]1, +\infty[$, a^x é estritamente crescente.*

Demonstração. Suponha $a \in]0,1[$. Sejam $x < y \in \mathbb{R}$. Denote por $h = y - x$. Então, como $a < 1$, temos

$$a^h < 1$$

Multiplicando por a^x de ambos os lados, obtemos

$$a^y < a^x$$

e, portanto, a^x é estritamente decrescente.

O caso em que $a > 1$ é análogo. □

Corolário 2.7.3. *Seja $a \in \mathbb{R}_{>0}$, com $a \neq 1$. Então a função $f_a : \mathbb{R} \longrightarrow \mathbb{R}_{>0}$ é bijetora ($f_a(x) = a^x$).*

Na verdade, no último resultado precisamos que f_a é sobrejetora em $\mathbb{R}_{>0}$ (o que pode ser visto em Cálculo).

Definição 2.7.4. Dado $a \in \mathbb{R}_{>0}$ com $a \neq 1$, definimos $\log_a = f_a^{-1}$.

Ou seja, segue diretamente da definição de $\log_a$ que

faça a substituição usando f_a e f_a^{-1} que fica fácil

$$log_a a^x = x$$

$$a^{\log_a x} = x$$

Ou seja, $y = \log_a x$ se, e somente se, $a^y = x$.

Corolário 2.7.5. *Seja $a \in \mathbb{R}_{>0}$. Então valem:*

(a) $\log_a : \mathbb{R}_{>0} \longrightarrow \mathbb{R}$ *é bijetora.*

(b) se $a > 1$, $\log_a$ *é estritamente crescente.*

(c) se $a < 1$, $\log_a$ *é estritamente decrescente.*

Proposição 2.7.6. *Seja $a \in \mathbb{R}_{>0}$, então, para todo $x, y \in \mathbb{R}_{>0}$ temos*

(a) $\log_a(x) + \log_a(y) = \log_a(xy)$.

(b) $k \log_a(x) = \log_a(x^k)$ *para* $k \in \mathbb{R}$.

Demonstração. (i) Sejam $v, w \in \mathbb{R}$ tais que $v = \log_a x$ e $w = \log_a x$. Assim, $a^v = x$ e $a^w = y$. Calculando

$$xy = a^v a^w = a^{v+w}$$

Tomando-se log de ambos os lados, temos

$$\log_a(xy) = \log_a a^{v+w} = v + w = \log_a x + \log_a y$$

(ii) Seja $v = \log_a(x)$. Então $a^v = x$. Temos

$$x^k = (a^v)^k = a^{vk}$$

Tomando-se o log dos dois lados

$$\log_a(x^k) = \log_a a^{vk} = vk = k \log_a(x)$$

□

Proposição 2.7.7. *Sejam $a, b \in \mathbb{R}_{>0}$. Então, para todo $x \in \mathbb{R}_{>0}$ temos*

$$\log_a x = \log_a b \log_b x$$

Demonstração. Sejam u, v, w tais que $u = \log_a x$, $v = \log_a b$ e $w = \log_b x$. Então $a^u = x$, $a^v = b$ e $b^w = x$. Assim, temos

$$a^u = x = b^w = (a^v)^w = a^{vw}$$

Como a função exponencia é injetora, temos $u = vw$. Isto é,

$$\log_a x = \log_a b \log_b x$$

□

2.8 Funções trigonométricas

Você vai ver isso em Cálculo

se você andou 2π, você voltou para o mesmo lugar.

Considere uma circunferência de raio 1 e centrada na origem do $\mathbb{R}^2$. Sabemos que o comprimento da circunferência é 2π. Suponha que você comece no ponto $(1, 0)$ e ande sobre a circunferência em sentido antihorário. Suponha que você tenha andado t e parado num ponto (x, y). São dois pontos da circunferência, mas quais? Esses dois pontos chamaremos de $x = \cos t$ e

$y = \text{sen}t$. Se o seu t era negativo, ande distância relativa ao valor absoluto de t, mas no sentido horário.

Ou seja, cos : $\mathbb{R} \longrightarrow \mathbb{R}$ e sen : $\mathbb{R} \longrightarrow \mathbb{R}$. Alguns valores conseguimos calcular facilmente: $\text{sen}(\pi) = -1$, $\text{sen}(\frac{\pi}{2}) = 0$ etc.

Com essa definição, já conseguimos provar alguns fatos elementares:

Proposição 2.8.1. *Seja $t \in \mathbb{R}$. Temos:* Faça um desenho

(a) $sen^2(t) + \cos^2(t) = 1$

(b) $-1 \leq \cos(t), sen(t) \leq 1$

(c) $\cos(-t) = \cos(t)$

(d) $sen(-t) = -sen(t)$

Como a cada volta que damos na circunferência faz com que os valores se repitam, conseguimos provar o seguinte também:

Proposição 2.8.2. *Sejam $t \in \mathbb{R}$ e $k \in \mathbb{Z}$. Temos:*

(a) $\cos(t + 2k\pi) = \cos(t)$

(b) $sen(t + 2k\pi) = sen(t)$

Proposição 2.8.3 (Lei dos cossenos)**.** *Dado um triângulo de lados de comprimento a, b, c e cujo ângulo θ é oposto ao lado de comprimento c, temos que $c^2 = a^2 + b^2 - 2ab\cos\theta$.*

Demonstração. Chame de C o vértice oposto ao lado de comprimento c (analogamente, nomeie os vértices A e B). Fixamos a origem em C (ou seja, $C = (0, 0)$). Colocamos o vértice B no eixo x. Assim, $B = (a, 0)$. Note que, desta forma, as coordenadas de A são $(b\cos\theta, b\text{sen}\theta)$. Por definição, a distância entre os vértices A e B é c. Por outro lado, podemos calcular a distância usando as coordenadas

$$\sqrt{(a - b\cos\theta)^2 + b^2\text{sen}^2\theta}$$

Juntando as duas informações:

$$\begin{aligned} c^2 &= (a - b\cos\theta)^2 + b^2\text{sen}^2\theta \\ &= a^2 - 2ab\cos\theta + b^2\cos\theta + b^2\text{sen}^2\theta \\ &= a^2 + b^2 - 2ab\cos\theta \end{aligned}$$

□

Você vai ver (ou viu) em geometria analítica (ou álgebra linear) que para "rotacionar" um ponto (x, y) em torno da origem com ângulo α, basta usar notação matricial:

$$\begin{pmatrix} \cos\alpha & -\text{sen}\alpha \\ \text{sen}\alpha & \cos\alpha \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix}$$

Também vai ver (ou viu) que para compor duas rotações, basta multiplicar as matrizes. Assim, fazer uma rotação por $\alpha+\beta$, pode ser escrita como uma rotação de β e depois de α. Assim:

$$\begin{array}{rcl} \begin{pmatrix} \cos(\alpha+\beta) & -\text{sen}(\alpha+\beta) \\ \text{sen}(\alpha+\beta) & \cos(\alpha+\beta) \end{pmatrix} & = & \begin{pmatrix} \cos\alpha & -\text{sen}\alpha \\ \text{sen}\alpha & \cos\alpha \end{pmatrix}\begin{pmatrix} \cos\beta & -\text{sen}\beta \\ \text{sen}\beta & \cos\beta \end{pmatrix} \\ & = & \begin{pmatrix} \cos\alpha\cos\beta - \text{sen}\alpha\text{sen}\beta & -(\cos\alpha\text{sen}\beta + \text{sen}\alpha\cos\beta) \\ \text{sen}\alpha\cos\beta + \cos\alpha\text{sen}\beta & \cos\alpha\cos\beta - \text{sen}\alpha\text{sen}\beta \end{pmatrix} \end{array}$$

2.9 Módulo

Vamos agora apresentar o conceito de módulo de um número real. Tal conceito vai nos ajudar mais tarde a trabalhar com a noção de "distância" entre dois reais (a saber, a "distância" entre a e b será dada por $|a-b|$).

Definição 2.9.1. Definimos a função **módulo**, denotada por $|\cdot|$ da seguinte maneira:

$$|x| = \begin{cases} x & \text{se } x \geq 0 \\ -x & \text{se } x < 0 \end{cases}$$

para todo $x \in \mathbb{R}$.

Proposição 2.9.2. *São verdadeiras as seguintes afirmações para quaisquer $x, y \in \mathbb{R}$:*

(a) $|x| \geq 0$;

(b) $|x| = |-x|$;

(c) $x \leq |x|$;

(d) $-|x| \leq x$;

(e) $|xy| = |x||y|$.

Na maior parte dos problemas com módulos, é mais fácil separar em casos. Em geral, dois casos: o "maior ou igual a 0" e o "menor que 0". Algumas vezes, é até mais fácil separar em três casos: "maior que 0", "menor que 0" e "igual a 0".

Demonstração. (a) Se $x \geq 0$, então $|x| = x \geq 0$. Se $x < 0$, então $|x| = -x > 0$, já que $x < 0$.

(b) Se $x \geq 0$, então $|x| = x$. Por outro lado, $|-x| = -(-x) = x$. Se $x < 0$, então $|x| = -x$. Por outro lado, $|-x| = -x$.

(c) Se $x \geq 0$, então $x = |x|$. Se $x < 0$, então $x < |x|$ pois $|x| \geq 0$ pelo item (a).

(d) Se $x \geq 0$, então $-|x| \leq x$ pois $-|x| \leq 0$ (item (a)). Se $x < 0$, então $-|x| = -(-x) = x$.

(e) Vamos aqui separar em mais casos. Caso $x > 0$ e $y > 0$, então $|xy| = xy = |x||y|$. Se $x < 0$ e $y > 0$, então $|xy| = -(xy) = (-x)y = |x||y|$ (a primeira igualdade segue do fato que $xy < 0$. A última igualdade é fácil de ver se você ler da direita para esquerda). O caso em que $x > 0$ e $y < 0$ é análogo ao anterior. Se $x < 0$ e $y < 0$, então $|xy| = xy = (-x)(-y) = |x||y|$. Finalmente, se x ou y forem 0, então $|xy| = 0 = |x||y|$.

□

O seguinte resultado muitas vezes facilita trabalhar com desigualdades envolvendo módulos.

Proposição 2.9.3. *Dados $a, x \in \mathbb{R}$, temos que*

$$|x| \leq a \text{ se, e somente se, } -a \leq x \leq a$$

Demonstração. Suponha $|x| \leq a$. Temos, por (c), que $x \leq |x| \leq a$, ou seja, que $x \leq a$. Por outro lado, temos, por (b) que $|x| = |-x|$. Logo, novamente por (c), temos que $-x \leq |-x| = |x| \leq a$. Isto é, $-x \leq a$. Note que isso implica $-a \leq x$. Assim, temos $-a \leq x \leq a$.

Agora suponha que $-a \leq x \leq a$. Vamos estimar $|x|$. Temos duas opções $x \geq 0$ e $x < 0$. Se $x \geq 0$, temos que $|x| = x \leq a$. Se $x < 0$, temos que $|x| = -x$. Note que, de $-a \leq x$, temos que $-x \leq a$. Logo, $|x| = -x \leq a$. Assim, $|x| \leq a$. □

Proposição 2.9.4 (**desigualdade triangular**). *Dados $a, b \in \mathbb{R}$, temos que $|a + b| \leq |a| + |b|$.*

Demonstração. Temos

$$-|a| \leq a \leq |a|$$

$$-|b| \leq b \leq |b|$$

Somando essas inequações, temos:

$$-(|a| + |b|) \leq a + b \leq |a| + |b|$$

Assim, obtemos $|a + b| \leq |a| + |b|$. □

Proposição 2.9.5. *Dados $a, b \in \mathbb{R}$, temos que $|a| - |b| \leq |a - b|$.*

Demonstração. Temos $|a| = |a - b + b| \leq |a - b| + |b|$. Logo, $|a| - |b| \leq |a - b|$. □

Exemplo 2.9.6. Considere a desigualdade $|x-7| < 3$. Para quais valores de x ela é verdadeira? Vamos apresentar dois métodos aqui. Um, simplesmente aplicando a Proposição 2.9.3. Isto é, a desigualdade vale se, e somente se, $-3 < x - 7 < 3$. Ou seja, a desigualdade vale se, e somente se, $4 < x < 10$. Na representação como intervalo, ela vale se, e somente se, $x \in]4, 10[$.

Vamos agora ao segundo método. Vamos olhar para $|x - 7|$ e separar nos casos possíveis. Se $x - 7 \geq 0$, temos que $|x - 7| = x - 7$. Ou seja, para os $x \geq 7$, a desigualdade vale se, e somente se, $x \geq 3 + 7 = 10$. No caso em que $x - 7 < 0$ (isto é, $x < 7$) temos que $|x - 7| = -(x - 7) = 7 - x$. Assim, para $x < 7$, a desigualdade vale se, e somente se, $-x < 3 - 7 = -4$. Isto é, $x > -4$. Juntando os dois casos, obtemos que a desigualdade vale se, e somente se, $-4 < x < 10$ (ou seja, o mesmo resultado obtido anteriormente).

Exemplo 2.9.7. Decida para quais valores de x vale a desigualdade:

$$|2x + 1| + |x - 1| < 3$$

Vamos dividir em casos. Note que o comportamento do que está dentro dos módulos muda em $x = -\frac{1}{2}$ e $x = 1$.

$x < -\frac{1}{2}$: a desigualdade fica equivalente a $-2x - 1 + (-x + 1) < 3$. Simplificando, $-3x < 3$, isto é, $x > -1$. Assim, para esse caso, vale qualquer $x \in]-1, -\frac{1}{2}[$.

$-\frac{1}{2} \leq x < 1$: a desigualdade fica equivalente a $2x+1+(-x+1) < 3$. Simplificando. $x < 1$. Assim, neste caso vale para qualquer $x \in [\frac{1}{2}, 1[$.

$x \geq 1$: a desigualdade fica equivalente a $2x + 1 + x - 1 < 3$. Simplificando, $3x < 3$, ou seja, $x < 1$. Como estamos no caso em que $x \geq 1$, não temos solução para esse caso.

Juntando todas as soluções, temos que a desigualdade vale para $x \in]-1, 1[$.

Exemplo 2.9.8. Decida para quais valores de x vale a desigualdade

$$|x-2| < |x+5|$$

Vamos analisar como o que está dentro dos módulos se comporta. Note que o comportamento muda em $x-2=0$ e $x+5=0$. Ou seja, em $x=2$ e $x=-5$. Assim, podemos dividir em 3 casos:

$x < -5$: Neste caso temos que $x-2<0$ e $x+5<0$, assim, a desigualdade é equivalente a

$$2-x < -x-5$$

Ou seja, $0<-7$, que é falso (não importa o valor de x). Assim, não existem soluções para esse caso.

$-5 \leq x < 2$: Neste caso, a desigualdade é equivalente a

$$2-x < x+5$$

Ou seja, $-2x<3$. Isto é, $x > -\frac{3}{2}$. Ou seja, neste caso temos que a solução é $x \in]-\frac{3}{2}, 2[$ (note que temos que deixar o intervalo dentro do caso sendo estudado

$x \geq 2$: Neste caso, a desigualdade é equivalente a

$$x-2 < x+5$$

Ou seja, $0<3$, que é verdadeira (não importando o valor de x). Ou seja, qualquer valor deste caso serve: $x \in [2, +\infty[$.

Analisando todos os casos, temos que a desigualdade é satisfeita se $x \in]-\frac{3}{2}, \infty[$.

Exemplo 2.9.9. Decida para quais valores de x vale a desigualdade

$$\frac{|1-x|}{|2x+2|} < 5$$

Primeiramente, note que tal desigualdade é equivalente a

$$\frac{|x-1|}{|2x+2|} < 5$$

(deixamos x sem o "$-$" na frente). Assim, os casos vão ser dados por $x=1$ e $x=-1$.

$x < -1$: Temos $\frac{1-x}{-2x-2} < 5$. Ou seja, $1 - x < -10x - 10$. Simplificando, $9x < -11$. Assim, $x < -\frac{11}{9}$. Desta forma, vale para $x \in]-\infty, -\frac{11}{9}[$.

$-1 \leq x < 1$: Temos $\frac{1-x}{2x+2} < 5$. Ou seja, $1-x < 10x+10$. Simplificando, $-11x < 9$. Assim, $x > -\frac{9}{11}$. Desta forma, vale para $x \in]-\frac{9}{11}, 1[$.

$x \geq 1$: Temos $\frac{x-1}{2x+2} < 5$. Ou seja, $x-1 < 10x+10$. Simplificando, $-9x < 11$. Assim, $x > -\frac{11}{9}$. Desta forma, vale para $x \in [1, +\infty[$.

Juntando os casos, temos que a desigualdade vale para $x \in]-\infty, -\frac{11}{9}[\cup]-\frac{9}{11}, +\infty[$.

Exercícios

Exercício 2.9.10. Sejam $x, y \in \mathbb{R}$. Mostre as seguintes afirmações:

(a) $||x|| = |x|$;

(b) $|x^2| = x^2$;

(c) $|x - y| = |y - x|$.

Exercício 2.9.11. Determine para quais valores de x valem as seguintes afirmações:

(a) $\frac{|x-2|}{|x+5|} < 10$;

(b) $\frac{|x+1|}{x-3} \leq 0$;

(c) $|x + 1| + |2x + 4| \geq 0$;

(d) $|4 - 2x| - |x + 1| \leq 2$.

Capítulo 3

Combinatória

3.1 Permutações

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 $A = \{1, 2, 3, 4\}$, temos que 113 e 345 são duas palavras de 3 letras de A. Note também que a ordem *importa*: $212 \neq 122$.

Denotaremos usualmente uma palavra p como

$$p = a_1 \cdots a_n$$

onde cada $a_1 \in A$ é a i-ésima letra de p.

Contar palavras possíveis com um alfabeto fixado é fácil. 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.

Exemplo 3.1.1. 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. 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

Ou seja, vão sobrar dois livros

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. Podemos tentar exibir todas:

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

Mas note que já deu uma quantidade razoável.

O exemplo acima 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

Proposição 3.1.2. *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 $P(n,q+1) = \frac{n!}{(n-q-1)!}$. Mas vejamos. 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 fim. 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. Ou seja:

$$\begin{aligned} P(n,q+1) &= P(n,q)(n-q) \\ &= \tfrac{n!}{(n-q)!}(n-q) \\ &= n\cdot(n-1)\cdots(n-q-1)(n-q) \\ &= \tfrac{n!}{(n-q-1)!} \end{aligned}$$

□

Se $k > n$, $P(n,k) = 0$.

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

Exemplo 3.1.3. Numa sala com 50 pessoas, qual a chance de duas fazerem aniversário no mesmo dia?

todos eles irreais, mas fazer o quê?

Vamos ter que supor vários fatos aqui: 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 interassados 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 $0,97$.

3.2 Combinações

Imagine que temos que montar um grupo de 4 alunos para uma comissão de forma que um seja o presidente, um seja o vice, um seja o tesoureiro e o último seja o estagiário. Se temos 50 alunos para dividir nestes 4 cargos, de quantas maneiras podemos fazer isso?

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

Mas e quisermos simplesmente montar uma chapa com 4 alunos, depois eles que decidam quem faz o que? Podemos pensar nisso como sendo uma palavra de 4 letras (cada letra um aluno diferente) mas que não importa qual a posição de cada letra (por exemplo, a palavra $ABCD = DBCA$). Vamos denotar tal quantidade da seguinte maneira: $C(n, k)$.

Lê-se combinação de n k a k

Proposição 3.2.1. *Sejam $n \geq k \geq 0$. Então* $C(n, k) = \begin{pmatrix} n \\ k \end{pmatrix} = \frac{P(n,k)}{k!} = \frac{n}{k!(n-k!)}$

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 que $k!$ palavras distintas. Ou seja,

$$k!C(n, k) = P(n, k)$$

e portanto temos o resultado desejado. □

Assim, para a mesma escolha da comissão, agora não importando como os alunos se organizam, temos $C(50,4) = \frac{50!}{46!4!} = 230300$.

Pela simetria da fórmula acima, 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 qantidades deveriam ser mesmo iguais.

Proposição 3.2.2. *Considere o conjunto $A = \{a_1, ..., a_n\}$. Então existem $\left(\begin{array}{c} n \\ k \end{array} \right)$ subconjuntos A com k elementos.*

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

Proposição 3.2.3. *Seja $n \geq 1$. Então $\sum_{i=1}^{n} \left(\begin{array}{c} n \\ k \end{array} \right) = 2^n - 1$.*

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

Exemplo 3.2.4. Um famoso jogo de azar consiste em cada jogagor escolher 6 números distintos entre 1 e 60. Ao final, são sorteados 6 números (distintos) e o jogador que acertar os 6 vence.

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

$$C(60,6) = \frac{60!}{54!6!} = 50.063.860$$

O jogador pode fazer uma aposta com 10 números (e ele 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, o jogador na verdade está fazendo a seguinte quantidade de jogadas simples:

$$C(10,6) = \frac{10!}{6!4!} = \frac{10 \cdot 9 \cdot 8 \cdot 7}{4 \cdot 3 \cdot 2} = 210$$

Se o valor de uma aposta simples fosse $R\$3,50$, então isso equivaleria a apostar $R\$735$.

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

Considere os 6 números escolhidos pelo jogador. Note que isso representa $C(6,5)$ grupos de 5 números. Para cada um destes grupos, existem outros 54 números que podem ser sorteados juntos para formar um sorteio vencedor de 5 mas não 6 números. Assim, temos que a chance do jogador ganhar é 1 em

$$\frac{C(60,6)}{C(6,5)54}$$

que é aproximadamente 154.518.

Analogamente, se quizermos acertar apenas 4, obtemos uma em

$$\frac{C(60,6)}{C(6,4)C(54,2)}$$

que é aproximadamente 2.332.

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

$$\frac{C(10,4)}{C(6,4)C(50,2)}$$

que dá aproximadamente 1 em 195

3.3 Princípio da inclusão-exclusão

Considere um grupo de X 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 $N(\emptyset) = |X|$.

Pense em cada Pi como uma restrição. Se você não dá alguma restrição, todos os indivíduos entram.

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

Exemplo 3.3.1. 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 matemática pura. Desta maneira, podemos notar que a quantidade de mulheres que não fazem matemática pura por:

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

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

Teorema 3.3.2 (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 propriedade 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 3.3.3. 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 $N(P_2, P_3) = N(P_6) = 16$, $N(P_2, P_5) = N(P_{10}) = 10$ 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

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

Sobrejeções

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, 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 propriedade "i não pertence a imagem de f". Assim, só precisamos contar quantas função não satisfazem nenhuma das P_i's.

Lema 3.3.4. *Sejam $n > m > 0$. 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 $f : \{1, ..., n\} \longrightarrow \{1, ..., m\}$ satisfazendo toda $P_i \in S$, temos que ela é uma palavra de comprimento n num alfabeto com $m - |S|$ letras com repetição. Assim, $N(S) = (m - |S|)^n$. □

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

Teorema 3.3.5. $S(n, m) = \sum_{k=0}^{m} (-1)^k C(m, k)(m - k)^n$.

Demonstração. Temos

$$\begin{aligned} S(n, m) &= \sum_{S \subset \{P_1, ..., P_m\}} (-1)^{|S|} N(S) \\ &= \sum_{S \subset \{P_1, ..., P_m\}} (-1)^{|S|} (m - |S|)^n \\ &= \sum_{k=0}^{m} (-1)^k C(m, k)(m - k)^n \end{aligned}$$

□

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

Vejamos agora o sorteio de um amigo secreto. Esse sorteio nada mais é que uma função $f : \{1, ..., n\} \longrightarrow \{1, ..., n\}$ injetora (ou bijetora, é equivalente neste caso) e tal que $f(x) \neq x$ (ninguém sorteia a si mesmo). Assim, considere P_i a propriedade de uma função $f : \{1, ..., n\} \longrightarrow \{1, ..., n\}$ injetora ser tal que $f(i) = i$. Desta forma, temos:

Lema 3.3.6. *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. □

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

Teorema 3.3.7. $d_n = \sum_{k=0}^{n}(-1)^k C(n,k)(n-k)!$

Demonstração. De fato

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

□

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

Teorema 3.3.8. $\frac{d_n}{n!} = \sum_{k=0}^{n}(-1)^k \frac{1}{k!}$. *Que, no limite quando* $n \longrightarrow +\infty$, *temos que vale* $\frac{1}{e}$.

Demonstração. Temos

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

□

De quantas maneiras é possível colocar 8 rainhas num tabuleiro de xadrez, sem colocar duas numa mesma coluna nem mesma linha e sem que nenhuma esteja na diagonal? (não descartar simetrias). Chame de linha-i uma linha em que tem uma única rainha na coluna i. Note que só precisamos "embaralhar" as linhas, de maneira que a linha-i não seja a i-ésima linha (daí teria uma rainha na diagonal). Ou seja, a resposta é d_8.

3.4 Circulares

Exemplo 3.4.1. De quantas maneiras podemos acomodar 5 pessoas numa mesa?

5!

Exemplo 3.4.2. 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!.

Exemplo 3.4.3. Mesmo problema anterior, mas temos 8 pessoas e a mesa continua com 5 lugares.

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

$$C(8,5)4! = \frac{8!}{5!3!}4!$$

Exemplo 3.4.4. 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

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

3.5 Repetições

Exemplo 3.5.1. 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.

Exemplo 3.5.2. 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, logo, temos:

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

Exemplo 3.5.3. Temos n bolinhas brancas e k bolinhas pretas. De quantas formas podemos colacá-as em fila?

Note que podemos simplesmente contar quantos subconjuntos de tamanho k existem em $n+k$ (daí esses marcamos de preto)

$$C(n+k,k) = \frac{(n+k)!}{n!k!}$$

Exemplo 3.5.4. Se o último exemplo está certo, deveríamos poder aplicá-lo no segundo exemplo:

$$C(n+2,2) = \frac{(n+2)!}{2!n!} = \frac{(n+2)(n+1)}{2}$$

Exemplo 3.5.5. 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:

$$C(n+k,k)P(n,n)$$

Dicas de alguns exercícios

1.2.12 Considere $a, b \in I \cup J$ e $x \in I \cup J$. Considere também $y \in I \cap J$. Analise as possibilidades entre as ordens de a, b, x, y.

Resolução de alguns exercícios

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

1.1.2 11 cadeados e 11 chaves (uma chave para cada cadeado, dando uma para cada morador).

Referências Bibliográficas

[1] P. R. Halmos. *Naive set theory*. The University Series in Undergraduate Mathematics. D. Van Nostrand Co., Princeton, N.J.-Toronto-London-New York, 1960.