Summary last week

- enumeration of set A is bijection from (initial segment of) $\mathbb{N}$ to A; A countable
- if initial segment, then A finite, otherwise countably infinite
- numbering inverse of enumeration

Summary last week

- enumeration of set A is bijection from (initial segment of) $\mathbb{N}$ to A; A countable
- if initial segment, then A finite, otherwise countably infinite
- numbering inverse of enumeration
- double counting: $\sum_{e_1 \in A} \mathrm{Deg}(e_1) = \sum_{e_2 \in B} \mathrm{Deg}(e_2)$, bipartite graph, partitions A,B
- pigeon hole principle: $\max(R) \geq \frac{\sum R}{\#(I)}$ for $R = (r_i)_{i \in I}$ collection of numbers
- in/exclusion principle: $\#(\bigcup_{i \in I} A_i) = \sum_{\substack{J \subseteq I \\ J \neq \emptyset}} (-1)^{\#(J)-1} \#(\bigcap_{j \in J} A_j)$

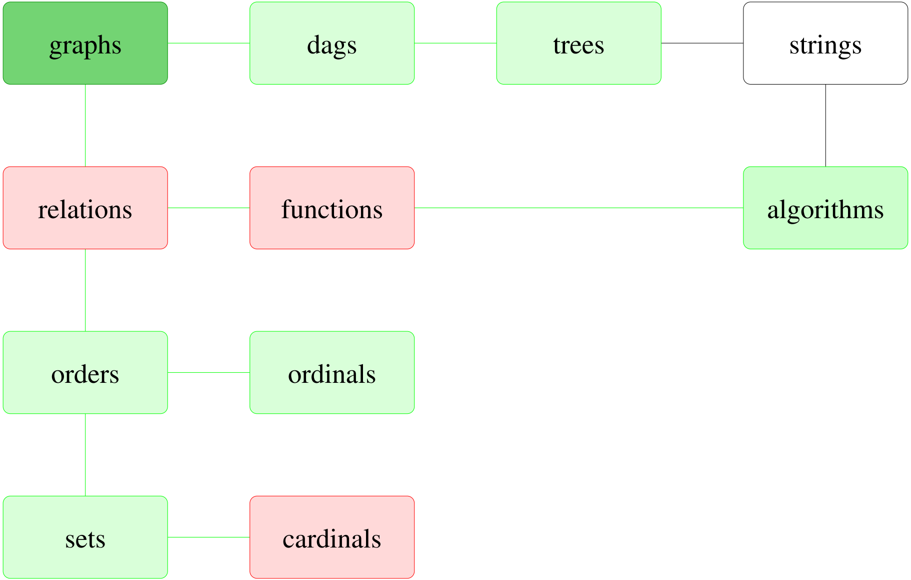
Summary last week

- enumeration of set A is bijection from (initial segment of) $\mathbb{N}$ to A; A countable
- if initial segment, then A finite, otherwise countably infinite
- numbering inverse of enumeration
- double counting: $\sum_{e_1 \in A} \mathrm{Deg}(e_1) = \sum_{e_2 \in B} \mathrm{Deg}(e_2)$, bipartite graph, partitions A,B
- pigeon hole principle: $\max(R) \geq \frac{\sum R}{\#(I)}$ for $R = (r_i)_{i \in I}$ collection of numbers
- in/exclusion principle: $\#(\bigcup_{i \in I} A_i) = \sum_{\substack{J \subseteq I \\ J \neq \varnothing}} (-1)^{\#(J)-1} \#(\bigcap_{j \in J} A_j)$
- $\#(A \times B) = \#(A) \cdot \#(B)$, if $A \cap B = \emptyset$ then $\#(A \cup B) = \#(A) + \#(B)$
- $\#(A - B) = \#(A) - \#(A \cap B)$, $\#(A^B) = \#(A)^{\#(B)}$ functions $B \to A$
- $(\#A)_{\#B}$ injective functions $B \to A$; falling factorial
- if $\#A = \#B$, then $\#A!$ bijective functions $B \to A$; if $B = A$, then permutations
- subsets of B, $\#(\mathcal{P}(B)) = 2^{\#B} = \#(\{0,1\}^B)$, characteristic functions $B \to \{0,1\}$
- $\#(\mathcal{P}_k(B)) = \binom{\#B}{k}$ subsets of size k; binomial coefficent $\binom{n}{k} = \frac{n!}{k!(n-k)!}$

Course themes

- directed and undirected graphs
- relations and functions
- orders and induction
- trees and dags
- finite and infinite counting
- elementary number theory
- Turing machines, algorithms, and complexity
- decidable and undecidable problem

Discrete structures



Infinite counting

Definition

A set A is countably infinite, if there is a bijection

$$e\colon \mathbb{N} \to A \,,\; i \mapsto a_i \,,$$

between the set of natural numbers $\mathbb{N}$ and A. A may than be written as

$$A = \{a_0, a_1, a_2, \ldots\} \,,$$

e is called an enumeration of A, and e^{-1} a numbering of A.

Infinite counting

Definition

A set A is countably infinite, if there is a bijection

$$e\colon \mathbb{N} \to A\,,\; i \mapsto a_i\,,$$

between the set of natural numbers $\mathbb{N}$ and A. A may than be written as

$$A = \{a_0, a_1, a_2, \ldots\}\,,$$

e is called an enumeration of A, and e^{-1} a numbering of A.

Example

- The set $\mathbb{N}$ of natural numbers is countably infinite
- And so is the set $\mathbb{Z}$ of integers

Theorem

The set $\mathbb{N} \times \mathbb{N}$ *is countably infinite.*

Theorem

The set $\mathbb{N} \times \mathbb{N}$ is countably infinite.

Proof.

We lay-out the pairs (m, n) two-dimensionally

$$\begin{matrix} (0,0) & (1,0) & (2,0) & (3,0) & \dots \\ (0,1) & (1,1) & (2,1) & (3,1) & \dots \\ (0,2) & (1,2) & (2,2) & (3,2) & \dots \\ (0,3) & (1,3) & (2,3) & (3,3) & \dots \\ \vdots \end{matrix}$$

Instead of an enumeration $e \colon \mathbb{N} \to \mathbb{N} \times \mathbb{N}$, we give a numbering $\nu \colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$. We number by dove tailing: $(0,0) \mapsto 0$, $(0,1) \mapsto 1$, $(1,0) \mapsto 2$, $(0,2) \mapsto 3$, $(1,1) \mapsto 4$, $(2,0) \mapsto 5$, $(0,3) \mapsto$?

Theorem

The set $\mathbb{N} \times \mathbb{N}$ is countably infinite.

Proof.

We lay-out the pairs (m, n) two-dimensionally

$$\begin{array}{ccccc} (0,0) & (1,0) & (2,0) & (3,0) & \dots \\ (0,1) & (1,1) & (2,1) & (3,1) & \dots \\ (0,2) & (1,2) & (2,2) & (3,2) & \dots \\ (0,3) & (1,3) & (2,3) & (3,3) & \dots \\ \vdots & & & & \end{array}$$

Instead of an enumeration $e\colon \mathbb{N} \to \mathbb{N} \times \mathbb{N}$, we give a numbering $\nu\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$. We number by dove tailing: $(0,0) \mapsto 0$, $(0,1) \mapsto 1$, $(1,0) \mapsto 2$, $(0,2) \mapsto 3$, $(1,1) \mapsto 4$, $(2,0) \mapsto 5$, $(0,3) \mapsto \frac{3 \cdot (3+1)}{2} = 6, \dots$

$(m, n) \mapsto$?

Theorem

The set $\mathbb{N} \times \mathbb{N}$ *is countably infinite.*

Proof.

We lay-out the pairs (m, n) two-dimensionally

$$\begin{array}{ccccc} (0,0) & (1,0) & (2,0) & (3,0) & \dots \\ (0,1) & (1,1) & (2,1) & (3,1) & \dots \\ (0,2) & (1,2) & (2,2) & (3,2) & \dots \\ (0,3) & (1,3) & (2,3) & (3,3) & \dots \\ \vdots & & & & \end{array}$$

Instead of an enumeration $e\colon \mathbb{N} \to \mathbb{N} \times \mathbb{N}$, we give a numbering $\nu\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$. We number by dove tailing: $(0,0) \mapsto 0$, $(0,1) \mapsto 1$, $(1,0) \mapsto 2$, $(0,2) \mapsto 3$, $(1,1) \mapsto 4$, $(2,0) \mapsto 5$, $(0,3) \mapsto \frac{3\cdot(3+1)}{2} = 6, \dots$

$(m,n) \mapsto \frac{(m+n)(m+n+1)}{2} + m$; is bijective ∎

Definition

A set is countable, if it is finite or countably infinite.

Definition

A set is countable, if it is finite or countably infinite.

Theorem

1. *Every subset of a countable set is countable.*
2. *The image of a countable set if countable.*
3. *The union of a sequence of countable sets is countable*
4. *The cartesian product of finitely many countable sets, is countable*

■

Definition

A set is countable, if it is finite or countably infinite.

Theorem

1. *Every subset of a countable set is countable.*
2. *The image of a countable set if countable.*
3. *The union of a sequence of countable sets is countable*
4. *The cartesian product of finitely many countable sets, is countable*

■

Example

The monoid of words Σ^* is countable, if Σ is a finite alphabet

$$\Sigma^* := \bigcup_{n \geqslant 0} \Sigma^n = \Sigma^0 \cup \Sigma^1 \cup \Sigma^2 \cup \cdots$$

Beyond countable?

Question

From the previous slides we know that being countable is preserved by various operations (product, subset, image, sequence).

1. Contrast this to that the product of two sets having, say, 4 elements has more than 4 elements (namely $4 \cdot 4 = 16$).
2. Can you find any operation on sets, such that applying it to countable sets yields a set having more than countably many elements?

Theorem (Cantor diagonalisation)

Let Σ be an alphabet containing at least two letters, say a and b, and let $s_0, s_1, s_2, \ldots$ be an infinite *sequence of* infinite *sequences in Σ:*

$$\begin{aligned} s_0 &= s_{00}s_{01}s_{02}\ldots \\ s_1 &= s_{10}s_{11}s_{12}\ldots \\ s_2 &= s_{20}s_{21}s_{22}\ldots \\ &\vdots \end{aligned}$$

Theorem (Cantor diagonalisation)

Let Σ be an alphabet containing at least two letters, say a and b, and let $s_0, s_1, s_2, \ldots$ be an infinite sequence of infinite sequences in Σ:

$$\begin{aligned} s_0 &= \overline{s_{00}} s_{01} s_{02} \ldots \\ s_1 &= s_{10} \overline{s_{11}} s_{12} \ldots \\ s_2 &= s_{20} s_{21} \overline{s_{22}} \ldots \\ &\vdots \end{aligned}$$

Then the sequence

$$d_n := \overline{s_{nn}} := \begin{cases} b & \text{if } s_{nn} = a \\ a & \text{if } s_{nn} \neq a \end{cases}$$

a new sequence, i.e. different from the given ones

Theorem (Cantor diagonalisation)

Let Σ be an alphabet containing at least two letters, say a and b, and let $s_0, s_1, s_2, \ldots$ be an infinite sequence of infinite sequences in Σ:

$$\begin{array}{rcl} s_0 & = & s_{00}s_{01}s_{02}\ldots \\ s_1 & = & s_{10}s_{11}s_{12}\ldots \\ s_2 & = & s_{20}s_{21}s_{22}\ldots \\ & \vdots & \end{array}$$

Then the sequence

$$d_n := \overline{s_{nn}} := \begin{cases} b & \text{if } s_{nn} = a \\ a & \text{if } s_{nn} \neq a \end{cases}$$

a new sequence, i.e. different from the given ones

Proof.

If d were not a new sequence, then there would be an index n such that $d = s_n$, and in particular $d_n = s_{nn}$, contradicting the construction of d as distinct at the diagonal. [8] ∎

Diagonalisation consequences

Corollary

none of the following are countable

1. *the set of infinite sequences over* $\{a, b\}$
2. *functions* $2^{\mathbb{N}}$*; as infinite sequence is function* $\mathbb{N} \to 2 = \{a, b\}$
3. *subsets* $\mathcal{P}(\mathbb{N})$*; by characteristic function* $2^{\mathbb{N}}$
4. *reals* $\mathbb{R}$*; by sequence obtained by decimal expansion*

Diagonalisation consequences

Corollary

none of the following are countable

1. *the set of infinite sequences over* $\{a, b\}$
2. *functions* $2^{\mathbb{N}}$*; as infinite sequence is function* $\mathbb{N} \to 2 = \{a, b\}$
3. *subsets* $\mathcal{P}(\mathbb{N})$*; by characteristic function* $2^{\mathbb{N}}$
4. *reals* $\mathbb{R}$*; by sequence obtained by decimal expansion*

Question

Can we still compare such sets in size/cardinality?

Diagonalisation consequences

Corollary

none of the following are countable

1. *the set of infinite sequences over* $\{a, b\}$
2. *functions* $2^{\mathbb{N}}$*; as infinite sequence is function* $\mathbb{N} \to 2 = \{a, b\}$
3. *subsets* $\mathcal{P}(\mathbb{N})$*; by characteristic function* $2^{\mathbb{N}}$
4. *reals* $\mathbb{R}$*; by sequence obtained by decimal expansion*

Question

Can we still compare such sets in size/cardinality?

Answer

Via injective functions.

Comparing set sizes

Definition

For sets A and B, we write $|A| \leq |B|$, if there is an injective function $f\colon A \to B$.

Comparing set sizes

Definition

For sets A and B, we write $|A| \leq |B|$, if there is an injective function $f: A \to B$.

Lemma

1. $|A| \leq |A|$
2. *if* $|A| \leq |B|$ *and* $|B| \leq |C|$, *then* $|A| \leq |C|$
3. $|A| \leq |B|$ *and* $|B| \leq |A|$, *does not imply* $A = B$

Proof.

1) by the identity function (is injective). 2) by composing the injective functions (is injective). 3) take e.g. $A = \mathbb{N}$ and $B = \mathbb{Z}$. ∎

Comparing set sizes

Definition

For sets A and B, we write $|A| \leq |B|$, if there is an injective function $f\colon A \to B$.

Lemma

1. $|A| \leq |A|$
2. *if* $|A| \leq |B|$ *and* $|B| \leq |C|$, *then* $|A| \leq |C|$
3. $|A| \leq |B|$ *and* $|B| \leq |A|$, *does not imply* $A = B$

Proof.

1) by the identity function (is injective). 2) by composing the injective functions (is injective). 3) take e.g. $A = \mathbb{N}$ and $B = \mathbb{Z}$. ∎

Suspicion for 3rd item

there is a bijection between A and B

Theorem (Schröder–Bernstein)

Let $f\colon A \to B$ and $g\colon B \to A$ be injective functions. Then there is a bijection $f' : A \to B$

Theorem (Schröder–Bernstein)

Let $f\colon A \to B$ and $g\colon B \to A$ be injective functions. Then there is a bijection $f'\colon A \to B$

Example (Picture on the board/animation next slide)

Let $A = \mathbb{N}$, $B = \{a\}^*$, and $f\colon A \to B$, $g\colon B \to A$ be defined by:

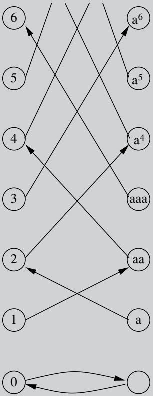
$$f(n) := a^{2n}$$
$$g(a^n) := 2n$$

f and g are injective; a bijection $f'\colon A \to B$ can be constructed from f,g by:

$$f'(n) := \begin{cases} \epsilon & \text{if } n = 0 \\ g^{-1}(n) = a^{\frac{n}{2}} & n \text{ has odd number of 2-factors} \\ f(n) = a^{2n} & \text{otherwise} \end{cases}$$

Animation of construction of bijection f' from injections f, g

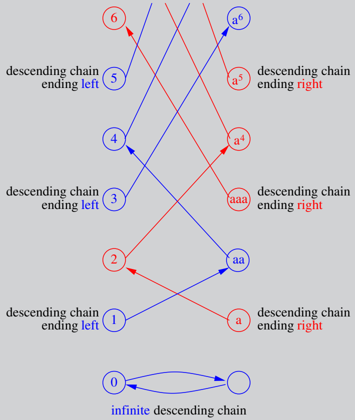
Example (Continued)



graph of f union g

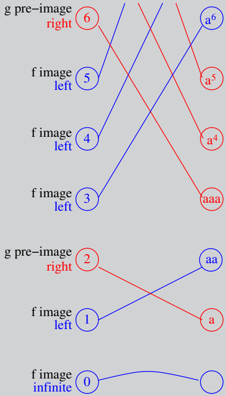
Animation of construction of bijection f' from injections f, g

Example (Continued)



Animation of construction of bijection f' from injections f, g

Example (Continued)



bijection f' by choosing g pre−image for nodes on chains ending right and f image for other nodes

Proof of Schröder–Bernstein theorem

Proof.

We construct $f' : A \to B$ and $g' : B \to A$ inverse to each other, as in animation.

- let $R = f \cup g$; viewed as relation on $A \uplus B$ (disjoint union)

Proof of Schröder–Bernstein theorem

Proof.

We construct $f' : A \to B$ and $g' : B \to A$ inverse to each other, as in animation.

- let $R = f \cup g$; viewed as relation on $A \uplus B$ (disjoint union)
- for $c \in A \cup B$ consider descending c-chain $\ldots c'' \; R \; c' \; R \; c$; unique by f,g injective. colour c red if c-chain ends in B (on the right), blue otherwise (ends on left or ∞).

Proof of Schröder–Bernstein theorem

Proof.

We construct $f' : A \to B$ and $g' : B \to A$ inverse to each other, as in animation.

- let $R = f \cup g$; viewed as relation on $A \uplus B$ (disjoint union)
- for $c \in A \cup B$ consider descending c-chain $\ldots c'' \; R \; c' \; R \; c$; unique by f,g injective. colour c red if c-chain ends in B (on the right), blue otherwise (ends on left or ∞).
- define $f'(a)$ for $a \in A$ by cases on the colour of a:

  a) $f'(a) := g^{-1}(a)$ (g pre-image if a is red; pre-image exists as a-chain ends on right)

  a) $f'(a) := f(a)$ (otherwise f image)

Proof of Schröder–Bernstein theorem

Proof.

We construct $f' : A \to B$ and $g' : B \to A$ inverse to each other, as in animation.

- let $R = f \cup g$; viewed as relation on $A \uplus B$ (disjoint union)
- for $c \in A \cup B$ consider descending c-chain $\ldots c'' \; R \; c' \; R \; c$; unique by f,g injective.
  colour c red if c-chain ends in B (on the right), blue otherwise (ends on left or ∞).
- define $f'(a)$ for $a \in A$ by cases on the colour of a:
  a) $f'(a) := g^{-1}(a)$ (g pre-image if a is red; pre-image exists as a-chain ends on right)
  a) $f'(a) := f(a)$ (otherwise f image)
- define $g'(b)$ for $b \in B$ by cases on the colour of b:
  b) $g'(b) := f^{-1}(b)$ (f pre-image if b is blue; exists as b-chain ends on left or ∞)
  b) $g'(b) := g(b)$ (otherwise g image)

Proof of Schröder–Bernstein theorem

Proof.

We construct $f' : A \to B$ and $g' : B \to A$ inverse to each other, as in animation.

- let $R = f \cup g$; viewed as relation on $A \uplus B$ (disjoint union)
- for $c \in A \cup B$ consider descending c-chain $\ldots c''\ R\ c'\ R\ c$; unique by f,g injective. colour c red if c-chain ends in B (on the right), blue otherwise (ends on left or ∞).
- define $f'(a)$ for $a \in A$ by cases on the colour of a:
  - **a)** $f'(a) := g^{-1}(a)$ (g pre-image if a is red; pre-image exists as a-chain ends on right)
  - **a)** $f'(a) := f(a)$ (otherwise f image)
- define $g'(b)$ for $b \in B$ by cases on the colour of b:
  - **b)** $g'(b) := f^{-1}(b)$ (f pre-image if b is blue; exists as b-chain ends on left or ∞)
  - **b)** $g'(b) := g(b)$ (otherwise g image)
- verify f', g' inverse to each other. $f' ; g'$ ($g' ; f'$ analogous) by cases on colour $a \in A$:
  - **a)** $g'(f'(a)) = g'(g^{-1}(a)) = g(g^{-1}(a)) = a$, as $g^{-1}(a)$ is red if a is, being on same chain.
  - **a)** $g'(f'(a)) = g'(f(a)) = f^{-1}(f(a)) = a$, as $f(a)$ is blue if a is, being on same chain. ∎

Partially ordering sets up to equinumerosity

Definition

$|M| := \{N \mid N \text{ equinumerous to } M\}$

Partially ordering sets up to equinumerosity

Definition

$|M| := \{N \mid N \text{ equinumerous to } M\}$

Lemma

if $A, A' \in |M|$ and $B, B' \in |N|$, and injection $f : A \to B$, then exists injection $f' : A' \to B'$.

Proof.

for bijections $g : A' \to A$ and $g' : B \to B'$, composition $g \,;\, f \,;\, g' : A' \to B'$ is injection. ∎

Partially ordering sets up to equinumerosity

Definition

$|M| := \{N \mid N \text{ equinumerous to } M\}$

Lemma

if $A, A' \in |M|$ and $B, B' \in |N|$, and injection $f : A \to B$, then exists injection $f' : A' \to B'$.

Proof.

for bijections $g : A' \to A$ and $g' : B \to B'$, composition $g \,;\, f \,;\, g' : A' \to B'$ is injection. ∎

Corollary

$\leq$ is a partial order on the collections $|M|$

Partially ordering sets up to equinumerosity

Definition

$|M| := \{N \mid N \text{ equinumerous to } M\}$

Lemma

if $A, A' \in |M|$ and $B, B' \in |N|$, and injection $f : A \to B$, then exists injection $f' : A' \to B'$.

Proof.

for bijections $g : A' \to A$ and $g' : B \to B'$, composition $g \,;\, f \,;\, g' : A' \to B'$ is injection. ∎

Corollary

$\leq$ is a partial order on the collections $|M|$

Corollary

$|\mathbb{N}| < |\mathbb{R}|$

Equivalence relations

Definition

An equivalence relation $\sim$ is a reflexive, symmetric, transitive relation

Equivalence relations

Definition

An equivalence relation $\sim$ is a reflexive, symmetric, transitive relation

Definition

- x and y are equivalent, if $(x, y) \in \sim$ that is, if $x \sim y$.

Equivalence relations

Definition

An equivalence relation $\sim$ is a reflexive, symmetric, transitive relation

Definition

- x and y are equivalent, if $(x, y) \in \sim$ that is, if $x \sim y$.
- The equivalence class of x is $[x] := \{y \in M \mid x \sim y\}$

Equivalence relations

Definition

An equivalence relation $\sim$ is a reflexive, symmetric, transitive relation

Definition

- x and y are equivalent, if $(x, y) \in \sim$ that is, if $x \sim y$.
- The equivalence class of x is $[x] := \{y \in M \mid x \sim y\}$
- The elements of an equivalence class K are the representatives of K

Equivalence relations

Definition

An equivalence relation $\sim$ is a reflexive, symmetric, transitive relation

Definition

- x and y are equivalent, if $(x, y) \in \sim$ that is, if $x \sim y$.
- The equivalence class of x is $[x] := \{y \in M \mid x \sim y\}$
- The elements of an equivalence class K are the representatives of K
- A system of representatives of $\sim$ is a set that contains a unique representative of each equivalence class of $\sim$.

Equivalence relations

Definition

An equivalence relation $\sim$ is a reflexive, symmetric, transitive relation

Definition

- x and y are equivalent, if $(x, y) \in \sim$ that is, if $x \sim y$.
- The equivalence class of x is $[x] := \{y \in M \mid x \sim y\}$
- The elements of an equivalence class K are the representatives of K
- A system of representatives of $\sim$ is a set that contains a unique representative of each equivalence class of $\sim$.

Remark

An equivalence class contains all objects having the same property

Example

- Relating equinumerous sets is an equivalence (same $\#$)
- Relating n to m if $n \pmod{k} = m \pmod{k}$ is an equivalence
- Relating $\frac{n}{m}$ and $\frac{n'}{m'}$ if $n \cdot m' = m \cdot n'$ is an equivalence (same normalised fraction)

Example

- Relating equinumerous sets is an equivalence (same $\#$)
- Relating n to m if $n \pmod{k} = m \pmod{k}$ is an equivalence
- Relating $\frac{n}{m}$ and $\frac{n'}{m'}$ if $n \cdot m' = m \cdot n'$ is an equivalence (same normalised fraction)

Example

Triples in $\mathbb{B}^3$ are equivalent, if obtained by reordering components

Example

- Relating equinumerous sets is an equivalence (same $\#$)
- Relating n to m if $n \pmod{k} = m \pmod{k}$ is an equivalence
- Relating $\frac{n}{m}$ and $\frac{n'}{m'}$ if $n \cdot m' = m \cdot n'$ is an equivalence (same normalised fraction)

Example

Triples in $\mathbb{B}^3$ are equivalent, if obtained by reordering components

$$\begin{aligned}\sim = \{&(000, 000), (001, 001), (001, 010), (001, 100), (010, 001),\\ &(010, 010), (010, 100), (100, 001), (100, 010), (100, 100),\\ &(011, 011), (011, 101), (011, 110), (101, 011), (101, 101),\\ &(101, 110), (110, 011), (110, 101), (110, 110), (111, 111)\}\end{aligned}$$

That is, 000

Example

- Relating equinumerous sets is an equivalence (same $\#$)
- Relating n to m if $n \pmod{k} = m \pmod{k}$ is an equivalence
- Relating $\frac{n}{m}$ and $\frac{n'}{m'}$ if $n \cdot m' = m \cdot n'$ is an equivalence (same normalised fraction)

Example

Triples in $\mathbb{B}^3$ are equivalent, if obtained by reordering components

$$\begin{aligned}\sim = \{&(000, 000), (001, 001), (001, 010), (001, 100), (010, 001),\\ &(010, 010), (010, 100), (100, 001), (100, 010), (100, 100),\\ &(011, 011), (011, 101), (011, 110), (101, 011), (101, 101),\\ &(101, 110), (110, 011), (110, 101), (110, 110), (111, 111)\}\end{aligned}$$

That is, 000, $001 \sim 010 \sim 100$

Example

- Relating equinumerous sets is an equivalence (same $\#$)
- Relating n to m if $n \pmod{k} = m \pmod{k}$ is an equivalence
- Relating $\frac{n}{m}$ and $\frac{n'}{m'}$ if $n \cdot m' = m \cdot n'$ is an equivalence (same normalised fraction)

Example

Triples in $\mathbb{B}^3$ are equivalent, if obtained by reordering components

$$\begin{aligned}\sim = \{&(000, 000), (001, 001), (001, 010), (001, 100), (010, 001),\\ &(010, 010), (010, 100), (100, 001), (100, 010), (100, 100),\\ &(011, 011), (011, 101), (011, 110), (101, 011), (101, 101),\\ &(101, 110), (110, 011), (110, 101), (110, 110), (111, 111)\}\end{aligned}$$

That is, 000, $001 \sim 010 \sim 100$, $011 \sim 101 \sim 110$

Example

- Relating equinumerous sets is an equivalence (same $\#$)
- Relating n to m if $n \pmod{k} = m \pmod{k}$ is an equivalence
- Relating $\frac{n}{m}$ and $\frac{n'}{m'}$ if $n \cdot m' = m \cdot n'$ is an equivalence (same normalised fraction)

Example

Triples in $\mathbb{B}^3$ are equivalent, if obtained by reordering components

$$\begin{aligned}\sim = \{&(000, 000), (001, 001), (001, 010), (001, 100), (010, 001),\\ &(010, 010), (010, 100), (100, 001), (100, 010), (100, 100),\\ &(011, 011), (011, 101), (011, 110), (101, 011), (101, 101),\\ &(101, 110), (110, 011), (110, 101), (110, 110), (111, 111)\}\end{aligned}$$

That is, 000, $001 \sim 010 \sim 100$, $011 \sim 101 \sim 110$, 111

Example

- Relating equinumerous sets is an equivalence (same $\#$)
- Relating n to m if $n \pmod{k} = m \pmod{k}$ is an equivalence
- Relating $\frac{n}{m}$ and $\frac{n'}{m'}$ if $n \cdot m' = m \cdot n'$ is an equivalence (same normalised fraction)

Example

Triples in $\mathbb{B}^3$ are equivalent, if obtained by reordering components

$$\begin{aligned}\sim = \{&(000, 000), (001, 001), (001, 010), (001, 100), (010, 001),\\ &(010, 010), (010, 100), (100, 001), (100, 010), (100, 100),\\ &(011, 011), (011, 101), (011, 110), (101, 011), (101, 101),\\ &(101, 110), (110, 011), (110, 101), (110, 110), (111, 111)\}\end{aligned}$$

That is, 000, 001 $\sim$ 010 $\sim$ 100, 011 $\sim$ 101 $\sim$ 110, 111
Equivalence classes: $\{000\}, \{001, 010, 100\}, \{011, 101, 110\}, \{111\}$ (prop: same $\#$ of 1s)

Example

- Relating equinumerous sets is an equivalence (same $\#$)
- Relating n to m if $n \pmod{k} = m \pmod{k}$ is an equivalence
- Relating $\frac{n}{m}$ and $\frac{n'}{m'}$ if $n \cdot m' = m \cdot n'$ is an equivalence (same normalised fraction)

Example

Triples in $\mathbb{B}^3$ are equivalent, if obtained by reordering components

$$\begin{aligned}\sim = \{&(000, 000), (001, 001), (001, 010), (001, 100), (010, 001),\\ &(010, 010), (010, 100), (100, 001), (100, 010), (100, 100),\\ &(011, 011), (011, 101), (011, 110), (101, 011), (101, 101),\\ &(101, 110), (110, 011), (110, 101), (110, 110), (111, 111)\}\end{aligned}$$

That is, 000, 001 $\sim$ 010 $\sim$ 100, 011 $\sim$ 101 $\sim$ 110, 111
Equivalence classes: $\{000\}, \{001, 010, 100\}, \{011, 101, 110\}, \{111\}$ (prop: same $\#$ of 1s)
System of representatives: $\{000, 001, 011, 111\}$, $\{000, 010, 011, 111\}$, . . .

Theorem

$x \sim z \Leftrightarrow [x] = [z]$ *for equivalence relation* $\sim$

Theorem

$x \sim z \Leftrightarrow [x] = [z]$ *for equivalence relation* $\sim$

Proof.

- $\Rightarrow$ (we show $[x] \subseteq [z]$; the other inclusion is analogous)

∎

Theorem

$x \sim z \Leftrightarrow [x] = [z]$ *for equivalence relation* $\sim$

Proof.

- $\Rightarrow$ (we show $[x] \subseteq [z]$; the other inclusion is analogous)
  $x \sim z$ and $y \in [x]$

■

Theorem

$x \sim z \Leftrightarrow [x] = [z]$ *for equivalence relation* $\sim$

Proof.

- $\Rightarrow$ (we show $[x] \subseteq [z]$; the other inclusion is analogous)
  $x \sim z$ and $y \in [x] \Rightarrow z \sim x$ (symmetry)

∎

Theorem

$x \sim z \Leftrightarrow [x] = [z]$ *for equivalence relation* $\sim$

Proof.

- $\Rightarrow$ (we show $[x] \subseteq [z]$; the other inclusion is analogous)
  $x \sim z$ and $y \in [x] \Rightarrow z \sim x$ (symmetry) $\Rightarrow x \sim y$ (Def. equivalence class)

∎

Theorem

$x \sim z \Leftrightarrow [x] = [z]$ *for equivalence relation* $\sim$

Proof.

- $\Rightarrow$ (we show $[x] \subseteq [z]$; the other inclusion is analogous)
  $x \sim z$ and $y \in [x] \Rightarrow z \sim x$ (symmetry) $\Rightarrow x \sim y$ (Def. equivalence class) $\Rightarrow z \sim y$ (transitivity)

∎

Theorem

$x \sim z \Leftrightarrow [x] = [z]$ *for equivalence relation* $\sim$

Proof.

- $\Rightarrow$ (we show $[x] \subseteq [z]$; the other inclusion is analogous)
  $x \sim z$ and $y \in [x] \Rightarrow z \sim x$ (symmetry) $\Rightarrow x \sim y$ (Def. equivalence class) $\Rightarrow z \sim y$ (transitivity) $\Rightarrow y \in [z]$ (Def. equivalence class)

∎

Theorem

$x \sim z \Leftrightarrow [x] = [z]$ *for equivalence relation* $\sim$

Proof.

- $\Rightarrow$ (we show $[x] \subseteq [z]$; the other inclusion is analogous)
  $x \sim z$ and $y \in [x] \Rightarrow z \sim x$ (symmetry) $\Rightarrow x \sim y$ (Def. equivalence class) $\Rightarrow z \sim y$ (transitivity) $\Rightarrow y \in [z]$ (Def. equivalence class)
- $\Leftarrow [x] = [z]$

∎

Theorem

$x \sim z \Leftrightarrow [x] = [z]$ *for equivalence relation* $\sim$

Proof.

- $\Rightarrow$ (we show $[x] \subseteq [z]$; the other inclusion is analogous)
  $x \sim z$ and $y \in [x] \Rightarrow z \sim x$ (symmetry) $\Rightarrow x \sim y$ (Def. equivalence class) $\Rightarrow z \sim y$ (transitivity) $\Rightarrow y \in [z]$ (Def. equivalence class)
- $\Leftarrow [x] = [z] \Rightarrow \{y \mid x \sim y\} = \{y \mid z \sim y\}$

∎

Theorem

$x \sim z \Leftrightarrow [x] = [z]$ *for equivalence relation* $\sim$

Proof.

- $\Rightarrow$ (we show $[x] \subseteq [z]$; the other inclusion is analogous)
  $x \sim z$ and $y \in [x] \Rightarrow z \sim x$ (symmetry) $\Rightarrow x \sim y$ (Def. equivalence class) $\Rightarrow z \sim y$ (transitivity) $\Rightarrow y \in [z]$ (Def. equivalence class)
- $\Leftarrow [x] = [z] \Rightarrow \{y \mid x \sim y\} = \{y \mid z \sim y\} \Rightarrow x \sim z$

∎

Theorem

$x \sim z \Leftrightarrow [x] = [z]$ *for equivalence relation* $\sim$

Proof.

- $\Rightarrow$ (we show $[x] \subseteq [z]$; the other inclusion is analogous)
  $x \sim z$ and $y \in [x] \Rightarrow z \sim x$ (symmetry) $\Rightarrow x \sim y$ (Def. equivalence class) $\Rightarrow z \sim y$ (transitivity) $\Rightarrow y \in [z]$ (Def. equivalence class)
- $\Leftarrow [x] = [z] \Rightarrow \{y \mid x \sim y\} = \{y \mid z \sim y\} \Rightarrow x \sim z$

■

Lemma

Let $f : M \to N$ *be a function. Then*

$$x \sim z \;:\Leftrightarrow f(x) = f(z)$$

defines an equivalence relation. The equivalence classes are the inverse images $f^{-1}(y) = \{x \in M \mid f(x) = y\}$ *for* $y \in f(M)$.

Definition

$\{B_1, \ldots, B_n\}$ is a partition of M, if $B_1 \uplus \ldots \uplus B_n = M$ ($\uplus$ denotes unions disjoint)

Definition

$\{B_1, \dots, B_n\}$ is a partition of M, if $B_1 \uplus \dots \uplus B_n = M$ ($\uplus$ denotes unions disjoint)
B_i are blocks

Definition

$\{B_1, \ldots, B_n\}$ is a partition of M, if $B_1 \uplus \ldots \uplus B_n = M$ ($\uplus$ denotes unions disjoint)
B_i are blocks

Example

$\{\{000\}, \{001, 010, 100\}, \{011, 101, 110\}, \{111\}\}$ is a partition of $\mathbb{B}^3$

Definition

$\{B_1, \ldots, B_n\}$ is a partition of M, if $B_1 \uplus \ldots \uplus B_n = M$ ($\uplus$ denotes unions disjoint)
B_i are blocks

Example

$\{\{000\}, \{001, 010, 100\}, \{011, 101, 110\}, \{111\}\}$ is a partition of $\mathbb{B}^3$

Theorem

(1) *Let P be a partition of M. Then is $\sim$ is an equivalence relation on M, such that*

$$x \sim y :\Leftrightarrow x \text{ and } y \text{ are in the same block of } P$$

Definition

$\{B_1, \ldots, B_n\}$ is a partition of M, if $B_1 \uplus \ldots \uplus B_n = M$ ($\uplus$ denotes unions disjoint)
B_i are blocks

Example

$\{\{000\}, \{001, 010, 100\}, \{011, 101, 110\}, \{111\}\}$ is a partition of $\mathbb{B}^3$

Theorem

(1) *Let P be a partition of M. Then is $\sim$ is an equivalence relation on M, such that*

$$x \sim y :\Leftrightarrow x \text{ and } y \text{ are in the same block of } P$$

(2) *Let $\sim$ be an equivalence relation on M. The set P of all equivalence classes w.r.t. $\sim$ is then a partition of M.*

Definition

$\{B_1, \ldots, B_n\}$ is a partition of M, if $B_1 \uplus \ldots \uplus B_n = M$ ($\uplus$ denotes unions disjoint)
B_i are blocks

Example

$\{\{000\}, \{001, 010, 100\}, \{011, 101, 110\}, \{111\}\}$ is a partition of $\mathbb{B}^3$

Theorem

(1) *Let P be a partition of M. Then is $\sim$ is an equivalence relation on M, such that*

$$x \sim y :\Leftrightarrow x \text{ and } y \text{ are in the same block of } P$$

(2) *Let $\sim$ be an equivalence relation on M. The set P of all equivalence classes w.r.t. $\sim$ is then a partition of M.*

(3) *The functions $P \mapsto \sim$ in (1) and $\sim \mapsto P$ in (2) are inverse to each other*

From orders to equivalence relations

Lemma

if $\leq$ is a reflexive, transitive, then $\leq \cap \geq$ is induced equivalence relation.

Proof.

reflexivity, transitivity of $\leq \cap \geq$ hold by the same for $\leq$; symmetry by definition. ∎

From orders to equivalence relations

Lemma

if $\leq$ is a reflexive, transitive, then $\leq \cap \geq$ is induced equivalence relation.

Proof.

reflexivity, transitivity of $\leq \cap \geq$ hold by the same for $\leq$; symmetry by definition. ∎

Example

1. $\frac{n}{m} \leq \frac{n'}{m'}$ if $n \cdot m' \leq m \cdot n'$ induces the equivalence on (positive) fractions above
2. relating sets by injections induces equinumerosity
3. $\leq$ on natural numbers induces equality $=$

Elementary number theory: Euclid

Definition

- $d \in \mathbb{Z}$ is a divisor of $a \in \mathbb{Z}$, if there exists a $c \in \mathbb{Z}$ such that $a = c \cdot d$
- „d divides a“, „a is a multiple of d“ $d \mid a$
- the divisor $\pm 1, \pm a$ are called trivial divisors of a

Elementary number theory: Euclid

Definition

- $d \in \mathbb{Z}$ is a divisor of $a \in \mathbb{Z}$, if there exists a $c \in \mathbb{Z}$ such that $a = c \cdot d$
- „d divides a“, „a is a multiple of d“ $d \mid a$
- the divisor $\pm 1, \pm a$ are called trivial divisors of a

Definition

Let $a, b \in \mathbb{Z}$, $a, b \neq 0$

- The greatest common divisor $\gcd(a, b)$ of a and b divides a and b, and for all c such that $c \mid a$ and $c \mid b$, c divides $\gcd(a, b)$
- The least common multiple $\mathrm{lcm}(a, b)$ of a and b is a multiple of both a and b, and for all c such that $a \mid c$ and $b \mid c$, c is a multiple of $\mathrm{lcm}(a, b)$

Theorem

Let $a, b, c \in \mathbb{Z}$ *with* $a \neq 0$*,* $b \neq 0$ *and* $a \neq c \cdot b$*; then*

$$\gcd(a, b) = \gcd(|a|, |b|) \quad \textit{and} \quad \gcd(a, b) = \gcd(a - c \cdot b, b)$$

Theorem

Let $a, b, c \in \mathbb{Z}$ *with* $a \neq 0$, $b \neq 0$ *and* $a \neq c \cdot b$; *then*

$$\gcd(a, b) = \gcd(|a|, |b|) \quad \textit{and} \quad \gcd(a, b) = \gcd(a - c \cdot b, b)$$

Proof.

- If $dc = a$, then $d(-c) = -a$, hence a and $|a|$ have the same divisors

Theorem

Let $a, b, c \in \mathbb{Z}$ *with* $a \neq 0$*,* $b \neq 0$ *and* $a \neq c \cdot b$*; then*

$$\gcd(a, b) = \gcd(|a|, |b|) \quad \textit{and} \quad \gcd(a, b) = \gcd(a - c \cdot b, b)$$

Proof.

- If $dc = a$, then $d(-c) = -a$, hence a and $|a|$ have the same divisors
- If an integer d divides a and b, then it also divides $a - c \cdot b$. Vice versa, if d divides $a - c \cdot b$ and b, then it also divides a.

Theorem

Let $a, b, c \in \mathbb{Z}$ *with* $a \neq 0$*,* $b \neq 0$ *and* $a \neq c \cdot b$*; then*

$$\gcd(a, b) = \gcd(|a|, |b|) \quad \textit{and} \quad \gcd(a, b) = \gcd(a - c \cdot b, b)$$

Proof.

- If $dc = a$, then $d(-c) = -a$, hence a and $|a|$ have the same divisors
- If an integer d divides a and b, then it also divides $a - c \cdot b$. Vice versa, if d divides $a - c \cdot b$ and b, then it also divides a.
- the common divisors of a and b are the common divisors of $a - c \cdot b$ and b, and therefore they have the same greatest common divisors as well

∎

Theorem (Euclidean algorithm for integers)

The greatest common divisor of non-zero integers can be computed as follows:

> *Replace the integers by their absolute values.*
>
> *While the integers are distinct, repeat:*
>
>   *Replace the larger of the two by the difference of the larger and the smaller.*
>
> *The resulting integer is the greatest common divisor.*

Theorem (Euclidean algorithm for integers)

The greatest common divisor of non-zero integers can be computed as follows:

> *Replace the integers by their absolute values.*
>
> *While the integers are distinct, repeat:*
>
> > *Replace the larger of the two by the difference of the larger and the smaller.*
>
> *The resulting integer is the greatest common divisor.*

If repeated subtraction is replaced by repeated integer division (with remainder), the following, typically faster, algorithm is obtained. ■

Theorem (Euclidean algorithm for integers)

The greatest common divisor of non-zero integers can be computed as follows:

> *Replace the integers by their absolute values.*
>
> *While the integers are distinct, repeat:*
>
> > *Replace the larger of the two by the difference of the larger and the smaller.*
>
> *The resulting integer is the greatest common divisor.*

If repeated subtraction is replaced by repeated integer division (with remainder), the following, typically faster, algorithm is obtained. ■

Theorem (Variant)

Replace the integers by their absolute values.

While neither integer is a multiple of the other, repeat:

Replace the larger of the two by its remainder after dividing by the other

The resulting divisor is the greatest common divisor.

Theorem (Variant)

Replace the integers by their absolute values.

While neither integer is a multiple of the other, repeat:

Replace the larger of the two by its remainder after dividing by the other

The resulting divisor is the greatest common divisor.

Proof.

- By the previous theorem, the greatest common divisors remain unchanged in each step of the algorithm, from which correctness follows

Theorem (Variant)

Replace the integers by their absolute values.

While neither integer is a multiple of the other, repeat:

    Replace the larger of the two by its remainder after dividing by the other

The resulting divisor is the greatest common divisor.

Proof.

- By the previous theorem, the greatest common divisors remain unchanged in each step of the algorithm, from which correctness follows
- Since the numbers remain positive in every iteration of the loop, and their maximum decreases by at least 1, the algorithm must terminate after finitely many steps ■

Theorem (Variant)

Replace the integers by their absolute values.

While neither integer is a multiple of the other, repeat:

Replace the larger of the two by its remainder after dividing by the other

The resulting divisor is the greatest common divisor.

Proof.

- By the previous theorem, the greatest common divisors remain unchanged in each step of the algorithm, from which correctness follows
- Since the numbers remain positive in every iteration of the loop, and their maximum decreases by at least 1, the algorithm must terminate after finitely many steps ∎

Example

We have $\gcd(138, -48) = 6$, according to the first method:

$$\begin{aligned}\gcd(138, -48) &= \gcd(138, 48) = \gcd(90, 48) = \gcd(42, 48)\\ &= \gcd(42, 6) = \gcd(36, 6) = \gcd(30, 6)\\ &= \gcd(24, 6) = \gcd(18, 6) = \gcd(12, 6)\\ &= \gcd(6, 6) = 6\end{aligned}$$

Example

We have $\gcd(138, -48) = 6$, according to the first method:

$$\begin{aligned}\gcd(138, -48) &= \gcd(138, 48) = \gcd(90, 48) = \gcd(42, 48)\\ &= \gcd(42, 6) = \gcd(36, 6) = \gcd(30, 6)\\ &= \gcd(24, 6) = \gcd(18, 6) = \gcd(12, 6)\\ &= \gcd(6, 6) = 6\end{aligned}$$

The second method yields

$$\gcd(138, -48) = \gcd(138, 48) = \gcd(42, 48) = \gcd(42, 6) = 6\,.$$

Theorem (Bézout's lemma)

Let a and b be non-zero integers. Then there exist natural numbers u and v with

$$u \cdot a + v \cdot b = \gcd(a, b)$$

which can be computed by the following algorithm

Set $A = (|a|, 1, 0)$ *and* $B = (|b|, 0, 1)$.

While B_1 *does not divide* A_1, *do:*

- *Compute the integer quotient of* A_1 *and* B_1.
- *Set* $C = B$.
- *Set* $B = A - q \cdot C$ *(componentwise)*
- *Set* $A = C$.

Set $u = sgn(a) \cdot B_2$ *and* $v = sgn(b) \cdot B_3$.

Proof.

- Let $T = (T_1, T_2, T_3)$ be a triple of integers and $(*)$ the property

$$T_1 = |a| \cdot T_2 + |b| \cdot T_3 \tag{$*$}$$

Proof.

- Let $T = (T_1, T_2, T_3)$ be a triple of integers and $(*)$ the property

$$T_1 = |a| \cdot T_2 + |b| \cdot T_3 \qquad (*)$$

- If the triples A and B have the property $(*)$, then so do all triples $A - q \cdot B$ and $q \in \mathbb{Z}$.

Proof.

- Let $T = (T_1, T_2, T_3)$ be a triple of integers and $(*)$ the property

$$T_1 = |a| \cdot T_2 + |b| \cdot T_3 \tag{$*$}$$

- If the triples A and B have the property $(*)$, then so do all triples $A - q \cdot B$ and $q \in \mathbb{Z}$.
- The first two triples in the algorithm have this property, hence all the subsequent triples have it as well. Restricting to the first components of triples the Euclidean algorithm is obtained. Therefore, we have for the final triples B

$$\gcd(a,b) = B_1 = |a| \cdot B_2 + |b| \cdot B_3 = \underbrace{\left(\operatorname{sgn}(a) \cdot B_2\right)}_{u} \cdot a + \underbrace{\left(\operatorname{sgn}(b) \cdot B_3\right)}_{v} \cdot b$$

Proof.

- Let $T = (T_1, T_2, T_3)$ be a triple of integers and $(*)$ the property

$$T_1 = |a| \cdot T_2 + |b| \cdot T_3 \tag{$*$}$$

- If the triples A and B have the property $(*)$, then so do all triples $A - q \cdot B$ and $q \in \mathbb{Z}$.
- The first two triples in the algorithm have this property, hence all the subsequent triples have it as well. Restricting to the first components of triples the Euclidean algorithm is obtained. Therefore, we have for the final triples B

$$\gcd(a, b) = B_1 = |a| \cdot B_2 + |b| \cdot B_3 = \underbrace{(\operatorname{sgn}(a) \cdot B_2)}_{u} \cdot a + \underbrace{(\operatorname{sgn}(b) \cdot B_3)}_{v} \cdot b$$

■

Example

Bézout's lemma for $a = 138$ and $b = -48$, yields $u = -1$, $v = -3$ and $\gcd(138, -48) = 6$

Example

Bézout's lemma for $a = 138$ and $b = -48$, yields $u = -1$, $v = -3$ and $\gcd(138, -48) = 6$

A	B	q
$(138, 1, 0)$	$(48, 0, 1)$	2
$(48, 0, 1)$	$(42, 1, -2)$	1
$(42, 1, -2)$	$(6, -1, 3)$	

Theorem (Computing the least common multiple)

Let a and b be non-zero integers. Then

$$\operatorname{lcm}(a, b) = \frac{|a| \cdot |b|}{\gcd(a, b)}\,.$$

Theorem (Computing the least common multiple)

Let a and b be non-zero integers. Then

$$\operatorname{lcm}(a,b) = \frac{|a| \cdot |b|}{\gcd(a,b)}\,.$$

Proof.

Obviously,

$$m := \frac{|b|}{\gcd(a,b)} \cdot |a| = \frac{|a|}{\gcd(a,b)} \cdot |b|$$

is a multiple both of a and b, hence a common multiple. We show that m is the least common multiple of a and b. To that end, let z be an arbitrary positive common multiple of a and b. Then there are integers c, d with

$$z = c \cdot a \quad \text{and} \quad z = d \cdot b$$