Proofs with ∃-introduction and ∃-elimination are unnecessarily long and cumbersome…

There are alternatives!

Proving an existential quantification

To prove

$\exists x[x \in \mathbb{Z} : x^3 - 2x - 8 \geq 0]$

Proof

It suffices to find a witness, i.e., an $x \in \mathbb{Z}$ satisfying

$$x^3 - 2x - 8 \geq 0.$$

$x = 3$ is a witness, since $3 \in \mathbb{Z}$ and $3^3 - 2 \cdot 3 - 8 = 13 \geq 0$

Conclusion: $\exists x[x \in \mathbb{Z} : x^3 - 2x - 8 \geq 0]$.

also x = 5 is a witness…

Alternative ∃ introduction

How do we prove an existential quantification?

by finding
a witness

∃∗-introduction

...

(k) P(a)

...

(l) Q(a)

...

{∃∗-intro on (k) and (l)}

(m) ∃x [P(x) : Q(x)]

(k < m, l < m)

strategy: wait until a witness object appears

does not always work

Using an existential quantification

We know $\exists x[x \in \mathbb{R} : a - x < 0 < b - x]$

We can declare an $x \in \mathbb{Z}$ (a witness) such that

$$a - x < 0 < b - x$$

and use it further in the proof. For example:

From $a - x < 0$, we get $a < x$.
From $b - x > 0$, we get $x < b$.
Hence, $a < b$.

Alternative ∃ elimination

How do we use an existential quantification in a proof?

we pick a witness

∃∗-elimination

|| ||

(k) ∃x [P(x) : Q(x)]

|| ||

{∃∗-elim on (k)}

(m) Pick x with P(x) and Q(x)

x must be new!

(k < m)

time for an example!

Back to
Naive Set Theory
Relations

Product of multiple sets

Direct product (Kartesisches Produkt)

$$A \times B = \{(x,y) \mid x \in A \text{ and } y \in B\}$$

ordered pairs

$(A \times B) \times C \neq A \times (B \times C)$

Therefore, we define

$A \times B \times C =$ … and $y \in B$ and $z \in C\}$

if $A_i = A$ for all i, then the product is denoted A^n

In general, for sets $A_1, A_2, \ldots, A_n$ with $n \geq 1$,

$$A_1 \times A_2 \times \ldots \times A_n = \prod_{1 \leq i \leq n} A_i = \{(x_1, x_2, \ldots, x_n) \mid x_i \in A_i \text{ for } 1 \leq i \leq n\}$$

sequence of length n

Relations

Def. If A and B are sets, then any subset $R \subseteq A \times B$ is a (binary) relation between A and B

similarly, unary relation (subset), n-ary relation...

Def. R is a relation on A if $R \subseteq A \times A$

some relations are special

Special relations

A relation $R \subseteq A \times A$ is:

reflexive	iff	for all $a \in A$, $(a,a) \in R$
symmetric	iff	for all $a,b \in A$, if $(a,b) \in R$, then $(b,a) \in R$
transitive	iff	for all $a,b,c \in A$, if $(a,b) \in R$ and $(b,c) \in R$, then $(a,c) \in R$
irreflexive	iff	for all $a \in A$, $(a,a) \notin R$
antisymmetric	iff	for all $a,b \in A$, if $(a,b) \in R$ and $(b,a) \in R$ then $a = b$
asymmetric	iff	for all $a,b \in A$, if $(a,b) \in R$, then $(b,a) \notin R$
total	iff	for all $a,b \in A$, $(a,b) \in R$ or $(b,a) \in R$

(infix) notation aRb for $(a,b) \in R$

Special relations

A relation R on A, i.e., $R \subseteq A \times A$ is:

equivalence	iff	R is reflexive, symmetric, and transitive
partial order	iff	R is reflexive, antisymmetric, and transitive
strict order	iff	R is irreflexive and transitive
preorder	iff	R is reflexive and transitive
total (linear) order	iff	R is a total partial order

Obvious properties

1. Every partial order is a preorder.

2. Every total order is a partial order.

3. Every total order is a preorder.

4. If $R \subseteq A \times A$ is a relation such that there are $a, b \in A$ with
$$a \neq b,\ (a,b) \in R \text{ and } (b,a) \in R,$$
then R is not a partial order, nor a total order, nor a strict order.

Operations on relations

Let $R \subseteq A \times B$ and $S \subseteq B \times C$ be two relations. Their composition is the relation

$$R \circ S = \{(a,c) \in A \times C \mid \text{there is } b \in B \text{ s.t. } (a,b) \in R \text{ and } (b,c) \in S\}$$

relational composition is associative $(R \circ S) \circ T = R \circ (S \circ T)$

so again we write
$$R^n = \underbrace{R \circ R \circ \ldots \circ R}_{n \text{ times}}$$

Let $R \subseteq A \times B$ be a relation. The inverse relation of R is the relation

$$R^{-1} = \{(b,a) \in B \times A \mid (a, b) \in R\}$$

Characterizations

Lemma: Let R be a relation over the set A. Then

1. R is reflexive iff $\Delta_A \subseteq R$
2. R is symmetric iff $R \subseteq R^{-1}$
3. R is transitive iff $R^2 \subseteq R$

Important equivalence on $\mathbb{Z}$

Def. For a natural number n, the relation $\equiv_n$ is defined as

$i \equiv_n j$ iff $n \mid i - j$

[iff i-j is a multiple of n]

[iff there exists $k \in \mathbb{Z}$ s.t. $i-j = k \cdot n$]

[iff $\exists k\, (k \in \mathbb{Z} \;\wedge\; i-j = k \cdot n)$]

logical formula

quantifier

logical connective

Lemma: The relation $\equiv_n$ is an equivalence for every n.

Equivalences classes

Def. Let R be an equivalence over A and $a \in A$. Then

$$[a]_R = \{ b \in A \mid (a, b) \in R\}$$

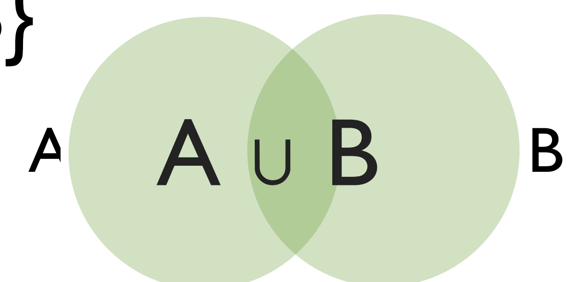
the equivalence class of a

Lemma: Let R be an equivalence over the set A. Then for all $a, b \in A$, $[a]_R = [b]_R$ or $[a]_R \cap [b]_R = \varnothing$

Task: Describe the equivalence classes of $\equiv_n$
How many classes are there?

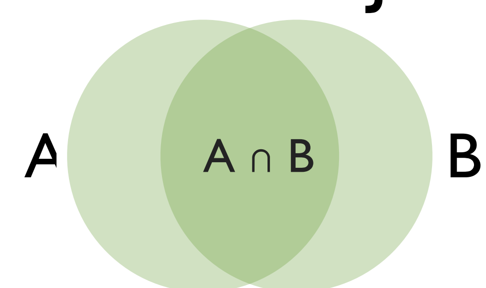
Unions and intersections of multiple sets

Union (Vereinigung) $A \cup B = \{x \mid x \in A \text{ or } x \in B\}$



Intersection (Durchschnitt) $A \cap B = \{x \mid x \in A \text{ and } x \in B\}$

A and B are disjoint if $A \cap B = \emptyset$



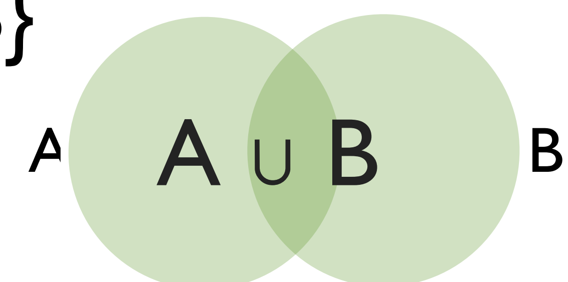
In general, for sets $A_1, A_2, \ldots, A_n$ with $n \geq 1$,

$$A_1 \cup A_2 \cup \ldots \cup A_n = \bigcup_{1 \leq i \leq n} A_i = \{x \mid x \in A_i \text{ for some } i \in \{1,..n\}\}$$

$$A_1 \cap A_2 \cap \ldots \cap A_n = \bigcap_{1 \leq i \leq n} A_i = \{x \mid x \in A_i \text{ for all } i \in \{1,..n\}\}$$

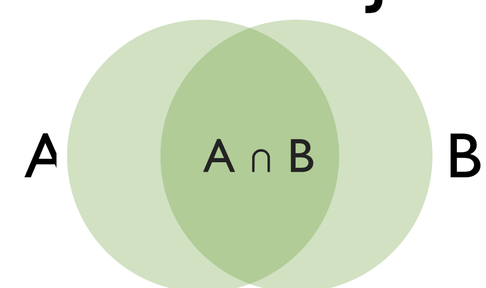
Unions and intersections of multiple sets

Union (Vereinigung) $A \cup B = \{x \mid x \in A \text{ or } x \in B\}$



Intersection (Durchschnitt) $A \cap B = \{x \mid x \in A \text{ and } x \in B\}$

A and B are disjoint if $A \cap B = \varnothing$



In general, for a family of sets $(A_i \mid i \in I)$

$$\bigcup_{i \in I} A_i = \{x \mid x \in A_i \text{ for some } i \in I\}$$

$$\bigcap_{i \in I} A_i = \{x \mid x \in A_i \text{ for all } i \in I\}$$

Back to equivalence classes

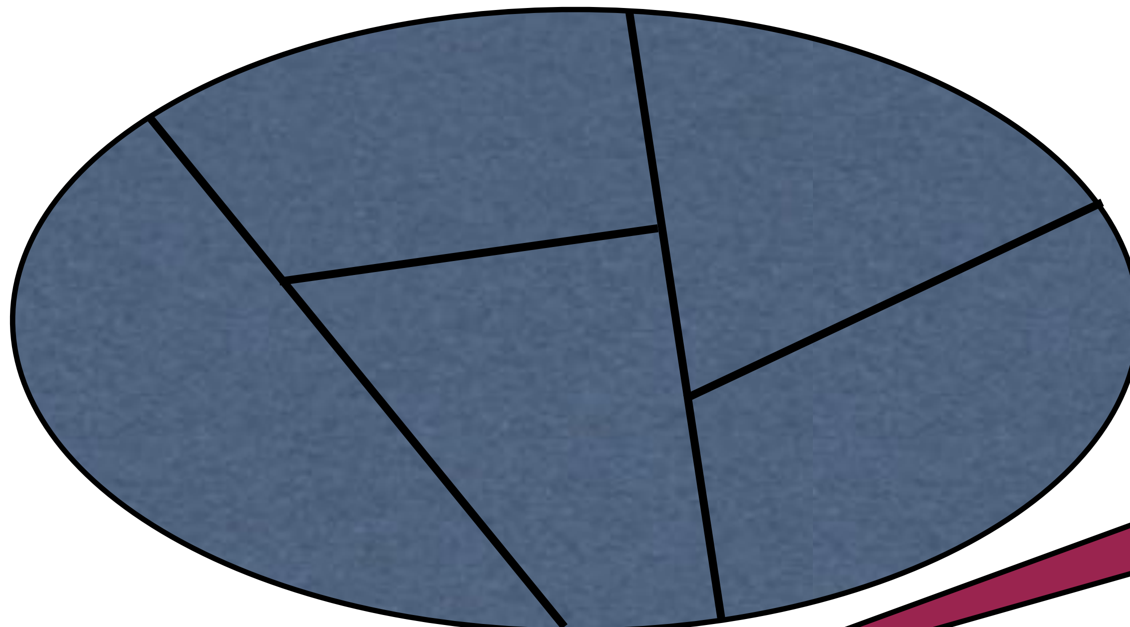
Example: Let R be an equivalence over A and $a \in A$. Then

$([a]_R , a \in A)$ is a family of sets.

all equivalence classes of R

Lemma E2: $A = \bigcup_{a \in A} [a]_R$. The union is disjoint.

Partitions



hence, a collection of subsets of X

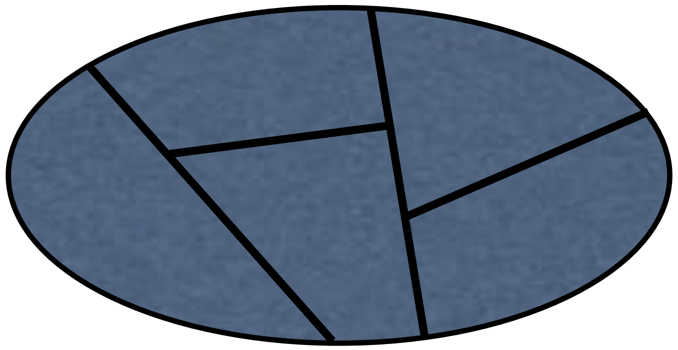
Def. Let X be a set. A subset P of the powerset $\mathcal{P}(X)$ is a partition (Klasseneinteilung) of X if it satisfies:

(1) For all $A \in P$, $A \neq \emptyset$

(2) For all $A, B \in P$, if $A \neq B$ then $A \cap B = \emptyset$

(3) $\bigcup_{A \in P} A = X$

that are non-empty, pairwise disjoint, and their union equals X



Partitions = Equivalences

Theorem PE: Let X be a set.

(1) If R is an equivalence on X, then the set

$$P(R) = \{ [x]_R \mid x \in X \}$$

is a partition of X.

(2) If P is a partition of X, then the relation

$$R(P) = \{(x,y) \in X \times X \mid \text{there is } A \in P \text{ such that } x,y \in A\}$$

is an equivalence relation.

Moreover, the assignments $R \mapsto P(R)$ and $P \mapsto R(P)$ are inverse to each other, i.e., $R(P(R)) = R$ and $P(R(P)) = P$.

Transitive closure

Let R be a relation on a set X. The transitive closure (transitive Hülle) of R, notation R^+, is the relation

$$R^+ = \bigcup_{n \in \mathbb{N}, n \neq 0} R^n$$

$R^{n+1} = R^n \circ R$

The reflexive and transitive closure (reflexive und transitive Hülle) of R, notation R^*, is the relation

$$R^* = \bigcup_{n \in \mathbb{N}} R^n$$

$R^0 = \Delta_R$

Proposition TC: Let R be a relation on X. The transitive closure of R is the smallest transitive relation that contains R. The reflexive and transitive closure of R is the smallest reflexive and transitive relation that contains R.