Lecture notes

Jiaqi Wang

November 12, 2023

Contents

1 Logic

1.1 Statements

Definition 1.1.1 – Statement A *statement* is a sentence that is either true or false but never both. A *proposition*, *logical statement* or *assertion* can also be used to refer to a statement.

1.2 Logical operations

- Logical and: $\vee$
- Logical or: $\wedge$
- Logical not: $\neg$

Definition 1.2.1 – Implication If A and B are assertions, then the assertion if A then B ($A \Rightarrow B$) is true if and only if one of the following occurs:

- A is true and B is true
- A is false and B is true
- A is false and B is false

Definition 1.2.2 – Biimplication (if and only if) $A \Leftrightarrow B \equiv (A \Rightarrow B) \wedge (B \Rightarrow A)$

1.3 Proposition Calculus

Using logical operators and assertions $P_1, P_2, \ldots, P_k$ to form new assertions and analyze them.

Theorem 1.3.1 – Some true assertions Suppose P,Q, and R are assertions. Then the following assertions are true:

(a) $P \vee \neg P$

(b) $P \Leftrightarrow \neg(\neg P)$

(c) $\neg(P \wedge \neg P)$

(d) $P \Rightarrow Q \Leftrightarrow \neg P \vee Q$

(e) $\neg(P \vee Q) \Leftrightarrow \neg P \wedge \neg Q$

(f) $\neg(P \wedge Q) \Leftrightarrow \neg P \vee \neg Q$

(g) $P \Rightarrow Q \Leftrightarrow \neg Q \Rightarrow \neg P$

(h) $(P \vee Q) \wedge R \Leftrightarrow (P \wedge R) \vee (Q \wedge R)$

(i) $(P \wedge Q) \vee R \Leftrightarrow (P \vee R) \wedge (Q \vee R)$

(j) $(P \vee Q) \Rightarrow R \Leftrightarrow (P \Rightarrow R) \wedge (Q \Rightarrow R)$

1.4 Methods of proof

If the statement is of the form

If P then Q.

1.4.1 Direct proof

We only need to consider the case where P is true and deduce the truth of Q.
A direct proof of $P \Rightarrow Q$ looks like:

Assume that P is true.

Then we use arguements that imply that Q is also true and end the proof with:

Hence Q is true.

1.4.2 Proof by contraposition

In instead of proving the statement $P \Rightarrow Q$ we prove its contrapositive ($\neg Q \Rightarrow \neg P$).

1.4.3 Proof by contradiction

In order to prove P we assume the opposite $\neg P$ to be true and deduce a condradiction with some obviously true statement Q.

Thus, we prove that $\neg Q \Rightarrow \neg P$. But then the contrapositive $Q \Rightarrow P$ must also be true. And the obvious truth of Q implies P to be true.

1.5 Excercises

1.5.1 Suppose p is false and q is true. What about:

(a) $p \Rightarrow (p \Rightarrow q)$ is true

(b) $p \Rightarrow (q \Rightarrow p)$ is true

(c) $q \Rightarrow (p \Rightarrow q)$ is true

(d) $q \Rightarrow (q \Rightarrow p)$ is false

2 Sets

2.1 Sets and subsets

Definition 2.1.1 – Set A is set any collection of "things" or "objects

Definition 2.1.2 – subset Suppose A and B are sets. The A is called a *subset* of B, if for every element $a \in A$ we also have that $a \in B$.
If A is a subset of B,then we write $A \subset B$ or $A \subseteq B$. We also say that B conatins A.
By $B \supset A$ or $B \supseteq A$ we mean $A \subset B$ or $A \subseteq B$.

Example 2.1.3 It is true that $1 \in \{1,2,3\}$ and $\{1\} \subseteq \{1,2,3\}$, but *not* that $1 \subseteq \{1\} \in \{1,2,3\}$ or $\{1\} \in \{1,2,3\}$

Example 2.1.4 Notice that $\emptyset \in \{\emptyset\}$ and $\emptyset \subseteq \{\emptyset\}$

Example 2.1.5 To following inclusions are proper

$$\mathbb{N} \subsetneq \mathbb{Z} \subsetneq \mathbb{Q} \subsetneq \mathbb{R} \subsetneq \mathbb{C}$$

Definition 2.1.6 – Power set If B is a set, then by $\mathscr{P}(B)$ we denote the set of all subsets A of B. The set $\mathscr{P}(B)$ is called the *power set* of B.
! The power set of a set is never empty.

Example 2.1.7 Suppose $A = \{x,y,z\}$m then $\mathscr{P}(A)$ consists of 8 subsets of A.

Proposition 2.1.8 – Let A be a set with n elements. Then its power set $\mathscr{P}(A)$ contains 2^n elements.

Proposition 2.1.9 – Suppose A,B and C are sets. Then the following holds:

1. If $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.
2. If $A \subseteq B$ and $B \subseteq A$, then $A = B$

Proof: Statement 1. Suppose $A \subseteq B$ and $B \subseteq C$. Let $a \in A$. Since $A \subseteq B$, $a \in B$. Now since $B \subseteq C$, $a \in C$. Since for every $a \in A : a \in C$, $A \subseteq C$ □

2.2 How to describe a set

Definition 2.2.1 – Set description Let P be a predicate with reference set X, then

$$\{x \in X \mid P(x)\}$$

denotes the subset of X consisting of all elements $x \in X$ for which the statement $P(x)$ is true.

Example 2.2.2 The set $\{x \in \mathbb{R} \mid x > 0\}$ consists of all posistive real numbers.

2.3 Operations on sets

Definition 2.3.1 – Let A,B be sets.

1. *intersection*: $A \cap B$ - the set of all elements contained in both A and B.
2. *union*: $A \cup B$ - the set of elements that are in at least on of A or B.
3. Two sets A and B are called *disjoint*, if their intersection $A \cap B$ is the empty set.

Proposition 2.3.2 – Let A,B and C be sets. Then the following holds:

(a) $A \cup B = B \cup A$

(b) $A \cup \emptyset = A$

(c) $A \subseteq (A \cup B)$

(d) If $A \subseteq B$, then $A \cup B = B$

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

(f) $A \cap B = B \cap A$

(g) $A \cap \emptyset = \emptyset$

(h) $A \cap B \subseteq A$

(i) If $A \subseteq B$, then $A \cap B = A$

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

Definition 2.3.3 – Big Unions and Intersections of sets Suppose I is a set and for each element i there exists a set A_i, then

$$\bigcup_{i \in I} A_i := \{x \mid \text{there is an } i \in I \text{ with } x \in A_i\}$$

and

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

(the set I is called the index set)
If $\mathscr{C}$ is a set/collection of sets, then we can define

$$\bigcup_{A \in \mathscr{C}} A := \{x \mid \text{there is an } A \in \mathscr{C}\}$$

and

$$\bigcap_{A \in \mathscr{C}} A := \{x \mid \text{for all } A \in \mathscr{C} \text{ we have } x \in A\}$$

Example 2.3.4 Suppose for each $i \in \mathbb{N}$ the set A_i is defined as $\{x \in \mathbb{R} \mid 0 \leq x \leq i\}$. Then

$$\bigcap_{i \in \mathbb{N}} A_i = \{0\}$$

(here we assume that $0 \in \mathbb{N}$) and

$$\bigcup_{i \in \mathbb{N}} A_i = \mathbb{R}_{\geq 0} = \{x \in \mathbb{R} \mid x \geq 0\}$$

Definition 2.3.5 – Setminus and symmetric difference Let A and B be sets. The *difference* of A and B, notation $A \setminus B$, is the set of all elements from A that are *not* in B.
The *symmetric difference* of A and B, notation $A \triangle B$, is the set of all elements in *exactly one* of A or B.

Proposition 2.3.6 – Let A,B and C be sets. Then the following holds:

1. $A \setminus B \subseteq A$

2. If $A \subseteq B$, then $A \setminus B = 0$

3. $A = (A \setminus B) \cup (A \cap B)$

4. $A \triangle B = (A \setminus B) \cup (B \setminus A)$

5. $A \triangle B = B \triangle A$

6. If $A \subseteq B$, then $A \triangle B = B \setminus A$

7. $A \triangle (B \triangle C) = (A \triangle B) \triangle C$

Proposition 2.3.7 – Let A,B and C be sets. Then the following hold:

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

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

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

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

Definition 2.3.8 – Set Complement If one is working inside a fixed set U and only cnsidering subsets of U, then the difference $U \setminus A$ is also called the *complement* of A in U. We write A^* or A^c for the complement of A in U. In this case the set U is also called the *universe*.

Proposition 2.3.9 – For subsets A,B and C of the universe U we have:

1. $A \cup A^* = U$

2. $B \setminus C = B \cap C^*$

3. $(A^*)^* = A$

4. If $A \subseteq B$ then $B^* \subseteq A^*$

5. $(A \cup B)^* = A^* \cap B^*$

6. $(A \cap B)^* = A^* \cup B^*$

2.4 Cartesian product

Definition 2.4.1 – Cartesian Product The Cartesian product $A_1 \times A_2 \times \cdots \times A_k$ of sets $A_1, \ldots, A_k$ is the set of all ordered k-tuples $(a_1, a_2, \ldots, a_k)$ where $a_i \in A_i$ for $1 \leq i \leq k$.
In particular, if A and B are sets, then

$$A \times B = (a, b) \mid a \in A \text{ and } b \in B$$

2.5 Partitions

Definition 2.5.1 – Partition Let S be a none-empty set. A collection Π of subsets of S is called a *partition* if and only if

1. $\emptyset \notin \Pi$

2. $\bigcup_{X\in\Pi} X = S$

3. for all $X \neq Y \in \Pi$ we have $X \cap Y = \emptyset$

Example 2.5.2 The set $\{1,2,\ldots,10\}$A can be partiioned into the sets $\{1,2,3\},\{4,5\},\{6,7,8,9,10\}$

Example 2.5.3 Suppose $\mathscr{L}$ is the set of all lines in $\mathbb{R}^2$ parallel to a fixed line ℓ. Then $\mathscr{L}$ partitions $\mathbb{R}^2$

Example 2.5.4 Let $n > 1$ be an integer. Then the set $\mathbb{Z}$ can be partitioned into the following subsets:

$$\begin{gathered}\{z \in \mathbb{Z} \mid z = 0 + nx \text{ for some } x \in \mathbb{Z}\}\\ \{z \in \mathbb{Z} \mid z = 1 + nx \text{ for some } x \in \mathbb{Z}\}\\ \vdots \\ \{z \in \mathbb{Z} \mid z = (n-1) + nx \text{ for some } x \in \mathbb{Z}\}\end{gathered}$$

2.6 Quantifiers

Definition 2.6.1 – Quantifiers Let P be a predicate on a reference set X. Then by

$$\forall x \in X\,[P(x)]$$

we denote the assertion "For all $x \in X$ the assertion $P(x)$ is true".
$\forall$ is called the *for all*-quantifier or *universal quantifier*.
By

$$\exists x \in X\,[P(x)]$$

we denote the assertion "There exists an $x \in X$ with $P(x)$ true".
$\exists$ is called the *existential quantifier*.

Example 2.6.2 The following statements are true:

$$\forall x \in \mathbb{R}\,[x \geq 0 \implies |x| = x],$$

$$\exists x \in \mathbb{R}\,[|x| = x]$$

$$\forall x \in \mathbb{Q}\,[-1 < \sin(x) < 1]$$

Here a few statements that are false:

$$\forall x \in \mathbb{R}\,[|x| = x]$$

$$\forall x \in \mathbb{R}\,[-1 < \sin(x) < 1]$$

Example 2.6.3 We can make combinations of quantifiers to create various assertions. For example

$$\forall x \in \mathbb{Z} \exists y \in \mathbb{Z}\,[x + y = 0]$$

Proposition 2.6.4 – DeMorgan's rule

$$\neg(\forall x \in X\,[P(x)]) \iff \exists x \in X\,[\neg P(x)]$$

$$\neg(\exists x \in X\,[P(x)]) \iff \forall x \in x\,[\neg P(x)]$$

Example 2.6.5 Let $X = \{1, 2, \ldots, 9\}$ and consider the following statements.

$$P = \forall x \in X \exists y \in X \, [x + y = 10]$$

$$Q = \exists x \in X \forall y \in X \, [x + y = 10]$$

The assertion P is clearly true.
The assertion Q is false. We prove $\neg Q$. By DeMorgan's rule the assertion $\neg Q$ is equivalent with

$$R = \forall x \in X \exists y \in X \, [x + y \neq 10]$$

2.7 Exercises

2.7.1 Which of the following sets are equal to each other: $\emptyset, \{0\}, \{\emptyset\}$

None

2.7.2 What are the sets that have no proper subset?

Since the empty set is a subset of any set, all non-empty sets have at least one proper subset, namely $\emptyset$.

2.7.3 How many elements does the set $\{\emptyset, \{\emptyset\}, \emptyset\}$

Since we do not count multiplicity there are 2 elements.

2.7.4 Suppose $A = \{\{1\}, \{2,3\}\}$. Which of the following is true:

- $\{1\} \subseteq A$ - Since $1 \notin A$, it is false.
- $\{2,3\} \subseteq A$ - Since $2 \notin A$ and $3 \notin A$, it is false.
- $\{\{2,3\}\} \subseteq A$ - Since $\{2,3\} \in A$, it is true.

2.7.5 Suppose A = {0, {1,2}}. Give all subsets of $\mathscr{P}(A)$

$\mathscr{P}(A) = \{\emptyset, \{0\}, \{\{1,2\}\}, A\}$
$\mathscr{P}(\mathscr{P}(A)) = \{$
$\emptyset,$
$\{\emptyset\}, \{0\}, \{\{1,2\}\}, A,$
$\{\emptyset, \{0\}\}, \{\emptyset, \{\{1,2\}\}\}, \{\emptyset, A\}, \{\{0\}, \{\{1,2\}\}\}, \{\{0\}, A\}, \{\{\{1,2\}, A\}\}$
$\{\emptyset, \{0\}, \{\{1,2\}\}\}, \{\emptyset, \{0\}, \{A\}\}, \{\{0\}, \{\{1,2\}\}, A\},$
$\{\emptyset, \{0\}, \{\{1,2\}\}, A\}$
$\}$

2.7.6 Suppose a set A contains n elements. How many elements does P(A) have?

$|A| = n \Rightarrow |\mathscr{P}(A)| = 2^n$

2.7.7 Which of the following statements is true for all sets A, B and C? Give a proof or a counter example

(a) $A \subseteq ((A \cap B) \cup C) \rightarrow false$

Proof. take $a \in (A \backslash B \backslash C)$, then $a \notin (A \cap B)$ and $a \notin C$
hence $a \notin (S \cap B) \cup C$
we conclude $A \nsubseteq ((A \cap B) \cup C)$ $\square$

(b) $(A \cup B) \cap C = (A \cap B) \cup C \rightarrow false$

Proof. take $a \in C \backslash (A \cup B)$
then $a \in (A \cap B) \cup C$
but $a \notin (A \cup B)$, so $a \notin (A \cup B) \cap C$
we conclude $(A \cup B) \cap C \neq (A \cap B) \cup C$ $\square$

(c) $(A \setminus B) \cap C = (A \cap C) \setminus (B \cap C) \rightarrow true$

Proof. take $a \in (A \setminus B) \cap C$, so $a \in (A \cap C) \setminus (B \cap C)$ □

Let A,B and C be sets. Prove the following.

(a)

3 Relations

3.1 Binary relations

Definition 3.1.1 – Ralation A relation R between the sets S and T is a subset of the Cartesian product $S \times T$.
Suppose R is a relation between S and T. If $(a,b) \in R$, we say a is in relation R to b (aRb).
S is called the domain, while S - *codomain*.
If $S = T$ we say R is a relation on S.

Example 3.1.2 We give some examples:

1. $R\{(0,0),(1,0),(2,1)\}$ is a relation between sets $S = \{0,1,2\}$ and $T = \{0,1\}$
2. $R = \{(x,y) \in \mathbb{R}^2 \mid y = x^2\}$ is a relation on $\mathbb{R}$
3. Let Ω be a set, then "is a subset of" $\subseteq$ is a relation on the set $S = \mathscr{P}(\Omega)$ of all subsets of Ω

Definition 3.1.3 – Image Let R be a relation from a set S to a set T. Then for each element $a \in S$ we define $[a]_R$ to be the set

$$[a]_R := \{b \in T \mid aRb\}$$

(Sometimes this set is also denoted by $R(a)$) This set is called the $(R-)$ image of a.
For $b \in T$ the set

$${}_R[b] := \{a \in S \mid aRb\}$$

Relations between finite sets can be described using matrices.

Definition 3.1.4 – Adjecency Matrix If $S = \{s_1, s_2, \ldots, s_n\}$ and $T = \{t_1, t_2, \ldots, t_m\}$ are finite sets and $R \subseteq S \times T$ is a binary relation, then the *adjecency* matrix A_R of the relation R is the $n \times m$ matrix whose rows are indexted by S and columns by T defined by:

$$A_{s,t} = \begin{cases} 1 & \text{if } (s,t) \in R \\ 0 & \text{otherwise} \end{cases}$$

Example 3.1.5

1. The adjecency matrix of the relation $R = \{(0,0),(1,0),(2,1)\}$ between the sets $S = \{0,1,2\}$ and $T = \{0,1\}$ equals

$$\begin{pmatrix} 1 & 0 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}$$

2. The adjecency matrix of the identity relation on a set S of size n:

$$I_n = \begin{pmatrix} 1 & 0 & \ldots & 0 & 0 \\ 0 & 1 & \ldots & 0 & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \ldots & 1 & 0 \\ 0 & 0 & \ldots & 0 & 1 \end{pmatrix}$$

3. The adjecency matrix of relation $\leq$ on the set $\{1,2,3,4,5\}$ is the upper triangular matirx:

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Some relations have special properties:

Definition 3.1.6 – Special relation properties Let R be a relation on set S. Then R is called

- *Reflexive* if for all $x \in S$ we have $(x,x) \in R$
- *Irreflexive* if for all $x \in S$ we have $(x,x) \notin R$
- *Symmetric* if for all $x,y \in S$ we have $xRy \implies yRx$
- *Antisymmetric* if for all $x,y \in S$ we have that xRy and $yRx \implies x = y$
- *Transitive* if for all $x,y,z \in S$ we have that xRy nd $yRz \implies xRz$

3.2 Relations and Directed Graphs

Definition 3.2.1 – Directed graph A *directed edge* of a set V is an element of $V \times V$. If $e(v,w)$ is a directed edge of V, then v is called its *tail* and w its *head*. Both v and w are called *end points* of the edge e. The *reverse* of the edge e is the edge (w,v). A *loop* is an edge from a vertex to itself.
A *directed graph* (also called (digraph)) $\Gamma = (V,E)$ consists of a set of *vertices* and a subset E of $V \times V$ of (directed) *edges*. The elements of V are called teh vertices of Γ and the elements of E the *edges* of Γ

3.2.2 Some graph theoretical language

Suppose $\Gamma = (V,E)$ is a digraph. A *walk* from v to w, where $v,w \in V$, is a sequence $v_0, v_1, \ldots, v_k$ of vertices with $v_0 = v, v_k = w$ and $(v_i, v_{i+1}) \in E$ for all $0 \leq i \leq k$. A *path* from v to w is a walk from v to w in which all vertices, except possibly the first vertex v and the last vertex w are different.

An *undericted walk* from v to w is a sequence $v_0, v_1, \ldots, v_k$ of vertices with $(v_i, v_{i+1}) \in E$ or $(v_{i+1}, v_i) \in E$ for all $0 \leq i \leq k$, while an *undirected path* from v to w is an undirected walk in which all vertices except possibly the first and last are different. The *length* of the (directed or undirected) walk or path is k. A *cycle* is a path from v to v of length at least 1.

If $v,w \in V$ are vertices of the digraph Γ, then the *distance* from v to w is the minimum of the lengths of the paths from v to w. The distance is set to ∞ (infinity) if there is no path from v to w.

The digraph is called *weakly connected* if for any two vertices v and w there is an undirected path between v and w. It is *called strongly* connected if there exist paths in both directions.

Proposition 3.2.3 – Let (V,E) be a directed graph. Then we have the following.

1. E is reflexive if and only if every vertex $v \in V$ is in a loop.
2. E is symmetric if and only if for every edge $e \in E$, also its reverse is in E.
3. E is transitive if and only if for each walk of length at least 1 starting from x and ending in y we have that $(x,y) \in E$.

Example 3.2.4 The complete directed graph on a vertex set V is the graph in which all vertices are adjacent to each other and tehmselves. This graph is clearly strongly connected.

So, te corresponding relation is reflexive, symmetric and transitive.

Proposition 3.2.5 – Let R be a relation on the set V which is reflexive, symmetric and transitive. Then all (weakly) connected components of the graph $\Gamma = (V, R)$ are complete graphs.

Definition 3.2.6 – Indegree / Outdegree Let $\Gamma = (V, E)$ be a digraph and $v \in V$ a vertex. The *indegree* of v is the number of edges with v as head. The *outdegree* of v is teh number of edges with v as tail.

3.3 Equivalence relations

Definition 3.3.1 – Equivalence Relation A relation R on a set S is called an *equivalence relation* on S if and only if it is relfexive, symmetric and transitive.

Example 3.3.2 Consider the plane $\mathbb{R}^2$ and in it the set S of straight lines. We call two lines parallel in S if and only if they are equal or do not intersect. Notice that two lines in S are parallel if and only if thir slopes are equal. Being parallel defines an equivalence relation on the set S.

Example 3.3.3 Fix $n \in \mathbb{Z}$, and consider the relation R on $\mathbb{Z}$ by aRb if an only if $a - b$ is divisible by n. We also write $a = b \pmod{n}$.

The relation R is an equivalence realtion. Indeed, suppose $a, b, c \in \mathbb{Z}$. Then

1. aRa as $a - a = 0$ is divisible by n.
2. If aRb, then $a - b$ is divisible by n and hence also $b - a$. Thus bRa.
3. If aRb, bRc, then n divides both $a - b$ and $b - c$ and then also $(a - b) + (b - c) = a - c$. So aRc

Example 3.3.4 Let Π be a partition of the set S. We define the relation R_Π as follows: $a, b \in S$ are in relation R_Π if and only if there is a subset X of S in Π containing both a and b. We check that the relation R_Π is an equivalence relation on S.

- Reflexivity: Let $a \in S$. Then there is an $X \in \Pi$ containing a. Hence, $a, a \in X$ and $aR_\Pi a$
- Symmetry: Let $aR_\Pi b$. Then there is an $X \in \Pi$ with $a, b \in X$. But then also $b, a \in X$ and $bR_\Pi a$
- Transitivity: If $a, b, c \in S$ with $aR_\Pi b$ and $bR_\Pi c$, then there are $X, Y \in \Pi$ with $a, b \in X$ and $b, c \in Y$. However, then b is in both X and Y. But then, as Π partitions S, we have $X = Y$. So $a, c \in X$ and $aR_\Pi c$

Lemma 3.3.5 – Let R be an equivalence relation on a set S. If $b \in [a]_R$, then $[b]_R = [a]_R$

Proof. Suppose $b \in [a]_R$. Thus aRb. If $c \in [b]_R$, then bRc and, as aRb, we have by transitivity aRc. In particular, $[b]_R \subseteq [a]_R$.

Since, by symmetry of R, aRb implies bRa and hence $a \in [b]_R$, we similarly get $[a]_R \subseteq [b]_R$. $\square$

Definition 3.3.6 – Equivalence classes Let R be an equivalence relation on a aset S. Then the sets $[s]_R$, where $s \in S$ are called the *R-equivalence* calsses on S.
We denote the set of R-equivalence classes by S/R

Theorem 3.3.7 – Let R be an equivalence relation on a set S. Then the set S/R of R-equivalence classes partions the set S.

Proof. Let Π_R be the set of R-equivalence classes. Then by reflexivity of R we find that each element $a \in S$ is inside the class $[a]_R \Pi_R$.

If an element $a \in S$ is in the classes $[b]_R and [c]_R$ of Π, then by the previous lemma we find $[b]_R = [a]_R$ and $[c]_R = [a]_R$. In particular, $[b]_R = [c]_R$. Thus each element $a \in S$ is inside an unique member of Π_R, which therefore is a partition of S. □

Example 3.3.8 Construction of $\mathbb{Q}$ The rational numbers can be constructed from integers with the help of an equivalence relation.

We consider the set $V = Z \times Z \setminus \{0\}$. On V we define the relation $\equiv$ by

$$(a,b) \equiv (c,d) \iff a \cdot d = b \cdot c$$

for all (a,b) and (c,d) in V.

Now we denote the $\equiv$-equivalence class of a pair (a,b) by $\frac{a}{b}$.

3.4 Composition of relations

If R_1 and R_2 are relations between a set S and a set T, then we can form new relations by taking the intersection $R_1 \cap R_2$ or the union $R_1 \cup R_2$. Also the complement of R_1 in R_2, $R_1 \setminus R_2$ is a new relation. Furhtermore, we can consider the relation $R^\top$ (sometimes also denoted by $R^{-1}, R^\sim$ or $R^\vee$) from T to S as the relation $\{(t,s) \in T \times S \mid (s,t) \in R\}$

Another way of making new relations out of old ones is the following. If R_1 is a relation between S and T and R_2 is a relation between T and U, then the *composition* or product $R = R_1;R_2$ (sometimes denoted by $R_2 \circ R_1$ or $R_1 * R_2$) is the relation between S and U defined by sRu for $s \in S$ and $u \in U$, if and only if there is a $t \in T$ with sR_1t and tR_2u.

Example 3.4.1 $R_1 = \{(1,2),(2,3),(3,3),(2,4)\}$ and $R_2 = \{(1,a),(2,b),(3,c),(3,d)\}$. Then $R_1;R_2 = \{(1,b),(2,c),(3,c),(2,d)\}$.

We get the adjecency matrix of a composition by multiplying the respective adjecency matrices and then replacing all non-zero entries with 1.

Example 3.4.2 Suppose $R_1 = \{(1,2),(2,3),(3,3),(2,4),(3,1)\}$ and R_2 is the relation $\{(1,1), (2,3), (3,1), (3,3), (4,2)\}$ Then the adjecency matrices A_1 and A_2 for R_1 and R_2 are

$$A_1 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}, A_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

The product of these matrices equals

$$M = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 1 & 1 \\ 2 & 0 & 1 \end{pmatrix}$$

So the adjecency matrix of $R_1;R_2$ is

$$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}$$

Proposition 3.4.3 – Suppose R_1 si a relation from S to T, R_2 a relation from T to U and R_3 a realtion from U to V. Then $R_1;(R_2;R_3) = (R_1;R_2);R_3$.
Composing relations is associative.

3.5 Transitive Closure

Lemma 3.5.1 – Let $\mathscr{C}$ be a collection of relations R on a set S. If all relations R in $\mathscr{C}$ are transitive (symmetric or reflexive), then the relation $\bigcap_{R\in\mathscr{C}} R$ is also transitive (symmetric or transitive, respectively).

Proof. Let $\bar{R} = \bigcap_{R\in\mathscr{C}} R$. Suppose all memebers of $\mathscr{C}$ are transitive. Then for all $a,b,c \in S$ with $a\bar{R}b$ and $b\bar{R}c$ we have aRb and bRc for all $R \in \mathscr{C}$. Thus by transitivity of each $R \in \mathscr{C}$ we also have aRc for each $R \in \mathscr{C}$. Thus we find $a\bar{R}c$. Hence $\bar{R}$ is transitive. □

The above lemma makes it possible to define the *reflexive, symmetric, or transitive closure* of a relation R on a set S. It is the smallest refexive, symmetric or transitive relation containing R. This means, as follows from lemma 3.5.1, it is the intersection $\bigcap_{R'\in\mathscr{C}} R'$, where $\mathscr{C}$ is the collection of all reflexive, symmetric, or transitive relations containing R.

Proposition 3.5.2 – $\bigcup_{n>0} R^n$ is the transitive closure of the relation R.

Proof. Define $\bar{R} = \bigcup_{n>0} R^n$. We prove transitivity of $\bar{R}$. Let $a\bar{R}b$ and $b\bar{R}c$, then there are sequence $a = a_1, \ldots, a_k = b$ and $b = b_1, \ldots, b_l = c$ with a_iRa_{i+1} and b_iRb_{i+1}. But then the sequence $a = a_1 = c_1, \ldots, c_k = a_k = b_1, \ldots, c_{k+l-1} = b_l = c$ is a sequence from a to c with c_iRc_{i+1}. Hence $aR^{k+l-2}c$ and $a\bar{R}c$. □

The transitive, symmetric and reflexive closure of a relation R is an equivalence relation. In terms of the graph Γ_R, the equivalence classes are the strongly connected componenets of Γ_R.

Algorithm 3.5.3 – H Warhall's Algorithm

3.6 Exercises

4 Maps

4.1 Definition

Definition 4.1.1 – A relation F from a set A to a set B is called a map or function from A to B if for each $a \in A$ there is one and only one $b \in B$ with aFb
If F is a map from A to B, we write $F : A \to B$
The set of all maps from A to B if denoted by B^A
A *partial map* F from A to B is a relation with the property that for each $a \in A$ there is at most one $b \in B$ with aFb.

Example 4.1.2

1. polynomial functions like $f : \mathbb{R} \to \mathbb{R}$, with $f(x) = x^3$ for all x
2. functions like $\cos, \sin, \tan$
3. $\sqrt{} : \mathbb{R}^+ \to \mathbb{R}$, taking square roots
4. $\ln : \mathbb{R}^+ \to \mathbb{R}$, the natural logarithm

Proposition 4.1.3 – Let $f : A \to B$ and $g : B \to C$ be maps, then the composition $g \circ f = f;g$ is a map from A to C.

Let A and B be two sets and $f : A \to B$. The set A is called the *domain* of f, the set B the *codomain*. If $a \in A$, then the element $b = f(a)$ is called the *image* of a under f. The subset of B consisting of the images of the elements of A under f is called the *image* or *range* of f and is denoted by $\mathrm{Im}(f)$. So

$$\mathrm{Im}(f) = \{b \in B \mid \text{ there is an } a \in A \text{ with } b = f(a)\}$$

If A' is a subset of A, then the image of A' under f is the set $f(A') = \{f(a) \mid a \in A'\}$ If A' is a subset of A, then the image of A' under the set $f(A') = \{f(a) \mid a \in A'\}$. So, $\mathrm{Im}(f) = f(A)$.

If $a \in A$ and $b = f(a)$, then the element a is called a *pre-image* of b. Notice that b can have more than one pre-image. The set of all pre-images of b is denoted by $f^{-1}(b)$. So

$$f^{-1}(b) = \{a \in A \mid f(a) = b\}$$

If B' is a subset of B, then the pre-image of B', denoted by $f^{-1}(B')$ is the set of elements a from A tjhat are mapped to an element b of B'. In particular

$$f^{-1}(B') = \{a \in A \mid f(a) \in B'\}$$

Example 4.1.4

1. Let $f : \mathbb{R} \to \mathbb{R}$ with $f(x) = x^2$ for all $x \in \mathbb{R}$. Then $f^{-1}([0,4]) = [-2,2]$
2. Consider the map from $\mathbb{Z}$ to $\mathbb{Z}$, which maps an integer a to the unique element b in $0,\ldots,7$ with $a = b \pmod 8$. The inverse image of 3 is the set $\{\ldots,-5,3,11,\ldots\}$. The inverse image of 11, however, is the emptyset.

Theorem 4.1.5 – Let $f : A \to B$ be a map.

- If $A' \subseteq A$, then $f^{-1}(f(A')) \supseteq A'$
- If $B' \subseteq B$, then $f(f^{-1}(B')) \subseteq B'$

Proof. Let $a' \in A'$, then $f(a') \in f(A')$ and hence $a' \in f^{-1}(f(A'))$. Thus $A' \subseteq f^{-1}(f(A'))$
Let $a \in f^{-1}(B')$, then $f(a) \in B'$. Thus $f(f'(B')) \subseteq B'$ □

Theorem 4.1.6 – Let $f : A \to B$ and $g : B \to C$ be maps. Then $\mathrm{Im}(g \circ f) = g(f(A)) \subseteq \mathrm{Im}(g)$

4.2 Special maps

Definition 4.2.1 – Surjective, injective and bijective maps A map $f : A \to B$ is called *surjective*, if for every $b \in B$ there is an $a \in A$ with $b = f(a)$. In other words if $\mathrm{Im}(f) = B$.
The map f is called *injective*, if for each $b \in B$, there is at most one a with $f(a) = b$. So the pre-image of b is either empty or consists of a unique element. In other words, f is injective if for any elements a and b from A we find that $f(a) = f(b)$ implies $a = b$.
The map f is *bijective* if it is both surjective and injective. So, if for each $b \in B$ there is a unique $a \in A$ with $f(a) = b$.

Example 4.2.2 (a) The map $\sin : \mathbb{R} \to \mathbb{R}$ is not surjective, nor injective

(b) The map $\sin : [-\pi/2, \pi/2] \to \mathbb{R}$ is injective, but not surjective

(c) The map $\sin : \mathbb{R} \to [-1, 1]$ is a surjective, but not injective map

(d) The map $\sin : [-\pi/2, \pi/2] \to [-1, 1]$ is a bijective map

Theorem 4.2.3 – Pigeonhole Principle Let A be a set of size n and B be a set of size m. Let $f : A \to B$ be a map between sets A and B.

(a) If $n < m$, then f cannot be surjective.

(b) If $n > m$, then f cannot be injective.

(c) If $n = m$, then f is injective if and only if f is surjective.

Remark 4.2.4. The above result is called the pigeonhole principle because of the following. If one has n pigeons (the set A) and the same number of holes (the set B), then one pigeonhole is empty if and only if one of the other holes contains at least two pigeons.

Example 4.2.5 Suppose you have to pick seven distinct numbers of the set $\{1, 2, \dots, 11\}$. Then among these seven numbers there is a pair that adds up to 12.

Suppose S is the set of 7 numbers picked. Now consider the following six subsets

$$\{1, 11\}, \{2, 10\}, \{3, 9\}, \{4, 8\}, \{5, 7\}, \{6\}$$

partitioning $\{1, \dots, 11\}$. The map that assigns to each of the seven elements of S the unique part of this partition to which it belongs can not be injective. So, there is a pair of this partition that is contained in S providing us with two numbers in S adding up to 12.

Proposition 4.2.6 – Let $f : A \to B$ be a bijection. Then for all $a \in A$ and $b \in B$ we have $f^{-1}(f(a)) = a$ and $f(f^{-1}(b)) = b$. In particular, f is the inverse of f^{-1}.

Theorem 4.2.7 – Let $f : A \to B$ and $g : B \to C$ be two maps.

(a) If f and g are surjective, then so is $g \circ f$

(b) If f and g are injective, then so is $g \circ f$

(c) If f and g are bijective, then so is $g \circ f$

Proposition 4.2.8 – If $f : A \to B$ and $g : B \to A$ are maps with $f \circ g = I_B$ and $g \circ f = I_A$ where I_A and I_B denote the identity maps on A and B, respectively. Then f and g are bijections. Moreover, $f^{-1} = g$ and $g^{-1} = f$.

Lemma 4.2.9 – Suppose $f : A \to B$ and $g : B \to C$ are bijective maps. Then the inverse of the map $g \circ f$ equals $f^{-1} \circ g^{-1}$.

4.3 Permutations and Symmetric groups

Definition 4.3.1 – **Permutations and Symmetric groups** Let X be a set.

- A bijection on X to itself is also called a *permutation* of X. The set of all permutations of X is denoted by $\mathrm{Sym}(X)$. It is called the *symmetric group* on X.
- The product $g \cdot h$ of two permutations $g, h \in \mathrm{Sym}(X)$ is defined as the composition $g \circ h$ of g and h. Thus for all $x \in X$ we have $g \cdot h(x) = g(h(x))$.
- If $X = \{1, \ldots, n\}$, we also write Sym_n instead of $\mathrm{Sym}(X)$. Furthermore, a permutation f of X is often given by $[f(1), f(2), \ldots, f(n)]$.

Theorem 4.3.2 – Sym_n has exactly $n!$ elements.

Definition 4.3.3 – **Order of a permutation** The order of a permutation g is the smallest positive integer m such that $g^m = e$.

4.4 Cycles

Definition 4.4.1 – **Fix points and Support** The *fixed points* of g in X are the elements of x in X for which $g(x) = x$ holds. The set of all fix points is $\mathrm{fix}(g) = \{x \in X \mid g(x) = x\}$.
The *support* of g is the complement in X of $\mathrm{fix}(g)$. It is denoted by $\mathrm{support}(x)$

Example 4.4.2 Consider the permutation $g = [1, 3, 2, 5, 4, 6] \in \mathrm{Sym}_6$. The fixed points of g are 1 and 6. So $\mathrm{fix}(g) = \{1, 6\}$. Thus the points moved by g form the set $\mathrm{support}(g) = \{2, 3, 4, 5\}$.

Cycles are elements in Sym_n of special importance.

Definition 4.4.3 – **Cycles** Let $g \in \mathrm{Sym}_n$ be a permutation with $\mathrm{support}(g) = \{a_1, \ldots, a_m\}$, where the a_i are pairwise distict. We say g is an m-cycle if $g(a_i) = g(a_{i+1})$ for all $i \in \{1, \ldots, m-1\}$ and $g(a_m) = a_1$. For such a cycle g we also use the cycle notation $(a_1, \ldots, a_m)$.
2-cycles are called *transpositions*.

Theorem 4.4.4 – Every permutation in Sym_n is a product of disjoint cycles. This product is unique up to rearrangement of the factors.

Definition 4.4.5 – **Cycle structure** The cycle structure of a permutation is the unordered sequence of the cycle lenghts in an expression of g as a product of disjoint cycles.

4.5 Alternating groups

Theorem 4.5.1 – If a permutation is written in two ways as a product of transpositions, then both products have even length or both have odd length.

Definition 4.5.2 – Let g be an element of Sym_n. the sign of g, denoted by $\mathrm{sign}(g)$, is defined as

- 1 if g can be written as a product of an even number of 2-cycles, and
- -1 if g can be writeen as a product of an odd number of 2-cycles.

We say that g is even $\mathrm{sign}(g) = 1$ and odd if $\mathrm{sign}(g) = -1$.

Theorem 4.5.3 – **Multiplicative property of sign** For all permutations g, h in Sym_n, we have

$$\mathrm{sign}(g \cdot h) = \mathrm{sign}(g) \cdot \mathrm{sign}(h)$$

Corollary 4.5.4 – If a permutation g is written as a product of cycles, then $\mathrm{sign}(g) = (-1)^w$, where w is the number of cycles of even length.

Definition 4.5.5 – **Alternating group** By Alt_n we denote the set of even permutations in Sym_n. We call Alt_n the *alternating group* on n letters.
The alternating group is closed with respect to taking products and inverse elements.

There are exactly as many even as odd permutations in Sym_n.

Theorem 4.5.6 – **Size of Alt_n** For $n > 1$, the alternating group Alt_n contains precisely $\frac{n!}{2}$ elements.

Theorem 4.5.7 – Every even permutation is a product of 3-cycles.

4.6 Exercises

4.6.1 Which of the following relations are maps from $A = \{1,2,3,4\}$ to A?

(a) $\{(1,3),(2,4),(3,1),(4,2)\}$: As for all $a \in A$ there is one and only $b \in A$, the relation is a map.

(b) $\{(1,3),(2,4)\}$: As 3 and 4 are not mapped to any element, this relation is not a map from A to A.

(c) $\{(1,1),(2,2),(3,3),(4,4),(1,3),(2,4),(3,1),(4,2)\}$: As elements from A are not mapped uniquely to another element, it is not a map.

(d) $\{(1,1),(2,2),(3,3),(4,4)\}$: As for all $a \in A$ there is one and only $b \in A$, the relation is a map.

4.6.2 Suppose f and g are maps from R to R defined by $f(x) = x^2$ and $g(x) = x+1$ for all $x \in R$. What is $g \circ f$ and what is $f \circ g$?

$$g \circ f = g(f(x)) = x^2 + 1$$
$$f \circ g = f(g(x)) = (x+1)^2$$

4.6.3 Which of the following maps is injective, surjective or bijective?

(a) $f : \mathbb{R} \to \mathbb{R}, f(x) = x^2$ for all $x \in \mathbb{R}$
Take $b = -4$, then there is no $a \in A$ such that $f(a) = b$. Therefore it is not surjective.
Take $c = -2, d = 2, e = 4$, then $f(c) = f(d) = e$. Therefore it is not injective.
Consequently, it is not bijective.

(b) $f : \mathbb{R} \to \mathbb{R}_{\geq 0}, f(x)x^2$ for all $x \in \mathbb{R}$
It is surjective, since $\forall b \in \mathbb{R}_{\geq 0}[\exists a \in \mathbb{R} : f(a) = b]$
Take $c = -2, d = 2, e = 4$, then $f(c) = f(d) = e$. Therefore it is not injective.

(c) $f : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}, f(x) = x^2$ for all $x \in \mathbb{R}$ It is bijective, since:

1. $\forall b \in \mathbb{R}_{\geq 0}[\exists a \in \mathbb{R} : f(a) = b]$
2. there is a one-to-one relation.:we

4.6.4 Suppose R_1 and R_2 are relations on a set S with $R_1;R_2 = I$ and $R_2;R_1 = I$. Prove that both R_1 and R_2 are bijective maps.

4.6.5 Let R be a relation from a finite set S to a finite set T with adjacency matrix A. Prove the following statements:

4.6.6

4.6.7

4.6.8

4.6.9

4.6.10 Let g be a permutation in Sym_n.Show that if $i \in$ support(g), then $g(i) \in$ support(g).

If $i \in \text{support}(g)$, then $g(i) \neq i \iff g(g(i)) \neq g(i)$

4.6.11 How many elements of Sym_5 have the cycle structure 2, 3?

First we choose two elements two permute and get the 2-cycle. The number of that is 5 choose 2 $\binom{5}{2}$. Then we permute the other 3 remaing elements which gives us 3! permutations, however, we need to subtract the 2-cycles that we get from those permutations, which are $\binom{3}{2}$. And also the case where we have 3 1-cycles. So for the number of permutations with cycle structure 2 3 we get:

$$\binom{5}{2} \cdot \left(3! - \binom{3}{2} - 1\right) = 20$$

4.6.12 Let g be the permutation

$$(1,2,3) \cdot (2,3,4) \cdot (3,4,5) \cdot (4,5,6) \cdot (5,6,7) \cdot (6,7,8) \cdot (7,8,9)$$

in Sym_6

(a) Write g as a product of disjoint cycles.
$(9\ 8) \cdot (7) \cdot (6) \cdot (5) \cdot (4) \cdot (3) \cdot (2\ 1)$

(b) Calculate the fixed points of g
fixed(g) = $\{3,4,5,6,7\}$

(c) Write g^{-1} as a product of disjoint cycles
$g^{-1} = g$, as applying a 2-cycle twice give us the identity.

(d) is g even?
g is composed two odd cycles, thus their product is even

4.6.13

(a) **If the permutations g and h in Sym$_n$ have disjoint supports, then g and h commute, i.e $g \cdot h = h \cdot g$. Prove this.**
Since they are g and h are disjoint, so support(g) $\cap$ support(h) $= \emptyset$. Then it would not matter in which order we take g and h as they will not permute the same element, thus they commute.

Proof. Let g and h be disjoint permutations
Let $i \in Fix(g)$. Then:

$$hg(i) = h(i)$$

Assume

$$h(i) \notin Fix(g)$$

So

$$h^2(i) = h(i)$$

Then

$$h^{-1}h^2(i) = h^{-1}h(i)$$
$$h(i) = i$$

Hence

$$i \in Fix(h)$$

However, this contradicts our assumption $i \in Fix(g)$
Therefore:

$$h(i) \in Fix(g)$$

So

$$gh(i) = h(i) = hg(i)$$

□

5 Orders

5.1 Orders and Posets

Definition 5.1.1 – Order and Partially ordered sets A relation $\sqsubseteq$ on a set P is called an *order* if it is reflexive, anitsymmetric and transitive. That means that for all x, y and z in P we have:

- $x \sqsubseteq x$
- if $x \sqsubseteq y$ and $y \sqsubseteq x$, then $x = y$
- if $x \sqsubseteq y$ and $y \sqsubseteq z$, then $x \sqsubseteq z$

The pair $(P, \sqsubseteq)$ is called a *partially ordered set*, or for short, a *poset*.
Two elements x and y in a poset $(P, \sqsubseteq)$ are called *comparable* if $x \sqsubseteq y$ or $y \sqsubseteq x$. The elements are called *incomparable* if $x \not\sqsubseteq y$ and $y \not\sqsubseteq x$.
If any two elements $x, y \in P$ are comparable, so we have $x \sqsubseteq y$ or $y \sqsubseteq x$, then the relation is called a *linear* order.

Example 5.1.2
- The identity relation I on a set P is an order.
- If $\sqsubseteq$ is an order on a set P, then $\sqsupseteq$ also defines an order on P. Here $x \sqsupseteq y$ if and only if $y \sqsubseteq x$. The order $\sqsupseteq$ is called the *dual* order of $\sqsubseteq$.
- On the set P of partitions of a set X we define the relation "refines" by the following. The partition Π_1 refines Π_2 if and only if each $\pi_1 \in \Pi_1$ is contained in some $\pi_2 \in \Pi_2$. The relation "refines" is a partial order on P.

If $\sqsubseteq$ is an order on the set P, then the corresponding directed graph with vertex P and edges (x, y), where $x \sqsubseteq y$ is *acyclic* (i.e. contains no cycles of length > 1).

If we want to draw a picture of the poset, we usually do not draw the whole digraph. Instead, we only draw an edge from x to y from P with $x \sqsubseteq y$ if there is no z, distinct from both x and y, for which we have $x \sqsubseteq z$ and $z \sqsubseteq y$. This digraph is called the *Hasse diagram* for $(P, \sqsubseteq)$, named after the German mathematician Helmut Hasse.

Definition 5.1.3 – Hasse diagram Let $(P, \sqsubseteq)$ be a poset. The graph with vertex set P and two vertices $x, y \in P$ adjacent if and only if $x \sqsubseteq y$ and there is no $z \in P$ different from x and y with $x \sqsubseteq z$ and $z \sqsubseteq y$.

5.1.4 New posets from old ones

- If P' is a subset of P, then P' is also a poset with order $\sqsubseteq$ restricted to P'. This is called an *induced* order on P'.
- Let S be some set. On the set of maps from S to P we can define an ordering as follows. Let $f : S \to P$ and $g : S \to P$, then we define $f \sqsubseteq g$ if and only if $f(s) \sqsubseteq g(s)$ for all $s \in S$.
- On the Cartesian product $P \times Q$ we can define an order as follows. For $(p_1, q_1), (p_2, q_2) \in P \times Q$ we define $(p_1, q_1) \sqsubseteq (p_2, q_2)$ if and only if $p_1 \sqsubseteq p_2$ and $q_1 \subseteq q_2$. This order is called the *product order*
- A second ordering on $P \times Q$ can be obtained by the following rule. For $(p_1, q_1), (p_2, q_2) \in P \times Q$ we define $(p_1, q_1) \sqsubseteq (p_2, q_2)$ if and only if $p_1 \sqsubseteq p_2$ and $p_1 \neq p_2$ or if $p_1 = p_2$ and $q_1 \sqsubseteq q_2$. This order is called the *lexicographic order* on $P \times Q$.

5.2 Maximal and minimal element

Definition 5.2.1 – Maximal and Minimal element Let $(P,\sqsubseteq)$ be a poset and $A \subseteq P$. An element $a \in A$ is called the *largest element* or *maximum* of A, if for all $a' \in A$ we have $a' \sqsubseteq a$. Notice that a maximum is unique.
An element $a \in A$ is called *maximal* if for all $a' \in A$ we have that either $a' \sqsubseteq a$ or a and a' are incomparable.
Similarly we can define the notion of *smallest element* or *minimum* and *minimal element*.
If the poset $(P,\sqsubseteq)$ has a maximum, then this is often denoted as $\top$ (top). A smallest element is denoted by $\perp$ (bottom).
If a poset $(P,\sqsubseteq)$ has a minimum $\perp$, then the minimal elements of $P \setminus \{\perp\}$ are called the *atoms* of P.

Lemma 5.2.2 – Let $(P,\sqsubseteq)$ be a poset. Then P contains at most one maximum and one minimum.

Example 5.2.3

- If we consider the poset of all subsets of S, then the empty set $\emptyset$ is the minimum of the poset, whereas the whole set S is the maximum. The atoms are the subsets of S that have 1 element.
- If we consider the $|$ as an order on $\mathbb{N}$, then 1 is the minimal element and 0 is the maximal element. The atoms are those natural numbers greater than 1, that are only divisible by 1 and itself, i.e. the prime numbers.

Lemma 5.2.4 – Let $(P,\sqsubseteq)$ be a finite poset. Then P contains a minimal and a maximal element.

Example 5.2.5 Notice that minimal elements and maximal elements are not necessarily unique. In fact, they do not even have to exist. In $(R,\leq)$ for example, there is no maximal nor a minimal element.

Algorithm 5.2.6 – H Minimal Element

Algorithm 5.2.7 – H Topological order

Definition 5.2.8 – If $(P,\sqsubseteq)$ is a poset and $A \subseteq P$, then an *upperbound* for A is an element u with $a \sqsubseteq u$ for all $a \in A$.
A *lowerbound* for A is an element u with $u \sqsubseteq a$ for all $a \in A$.
If the set of all upperbounds of A has a minimal element, then this element is called the *least upperbound* or *supremum* of A. Such an element, if it exists, is denoted by $\sup A$. If the set of all lowerbounds of A has a maximal element, then this element is called the *largest lowerbound* of *infimum* of A. If it exists, the infimum of A is denoted by $\inf A$.

Example 5.2.9 Let S be a set. In $(\mathscr{P}(S),\subseteq)$ any set A of subsets of S has a supremum and an infimum. Indeed,

$$\sup A = \bigcup_{X \in A} X \text{ and } \inf A = \bigcap_{X \in A} X$$

Definition 5.2.10 – Ascending/Descending chain An *ascending chain* in a $(P,\sqsubseteq)$ is a (finite or infinte) sequence $p_0 \sqsubseteq p_1 \sqsubseteq \dots$ of elements p_i in P. A *descending chain* in $(P,\sqsubseteq)$ is a (finite or infinite) sequence of elements $p_i, i \geq 0$ with $p_0 \sqsupseteq p_1 \sqsupseteq \dots$ of elements $p_i \in P$
The poset $(P,\sqsubseteq)$ is called *well founded* if any descending chain if finite.

Example 5.2.11 The natural numbers $\mathbb{N}$ with the ordinary ordering $\leq$ is well founded. Also the ordering $|$ on $\mathbb{N}$ is well founded.

However, on $\mathbb{Z}$ the order $\leq$ is not well founded.

5.3 Exercises

6 Recursion and Induction

6.1 Recursion

A *recursive definition* tells us how to build objects by using ones we have already built. Let us start with some examples of some common functions from $\mathbb{N}$ to $\mathbb{N}$ which can be defined recursively.

Example 6.1.1 Factorial The function $f(n) = n!$

Example 6.1.2 Sum The sum $1+2+3+\cdots+n$, also written as $\sum_{i=1}^{n} i$

Example 6.1.3 Fibonachi sequence

$$F(1) = 1 \tag{1}$$
$$F(2) = 1 \tag{2}$$
$$F(n+2) = F(n+1) + F(n) \tag{3}$$

In the examples above we see that for a recursively defined function f we need two ingredients:

- a *base* part, where we define the function value $f(n)$ for some small values of n like 0 or 1.
- a *recursive* part in which we explain how to compute the function in n with the help of the values for integers smaller than n.

Of course, we do not have to restrict our attention to functions with domain $\mathbb{N}$. Recursion can be used at several places.

Example 6.1.4 Let S be the subset of $\mathbb{Z}$ defined by:
$3 \in S$;
if $x, y \in S$ then also $-x$ and $x+y \in S$.

Then S consists of all the multiples of 3. Indeed, if $n = 3m$ for some $m \in N$, then $n = (\dots(3+3)+3)+\cdots+3$, and hence is in S. But then also $-3m \in S$. Thus S contains all multiples of 3. On the other hand, if S contains only multiples of 3, then in the next step of the recursion, only multiples of 3 are added to S. So, since initially S contains only 3, S contains only multiples of 3.

6.2 Natural induction

Principle 6.2.1 – Principle of Natural Induction Suppose $P(n)$ is a predicate for $n \in \mathbb{Z}$. Let $b \in \mathbb{Z}$. If the following holds:

- P(b) is true:
- for all $k \in \mathbb{Z}$, $k \geq b$ we have that $P(k)$ implies $P(k+1)$

Then $P(n)$ is true for all $k \geq b$

6.3 Strong induction and Minimal counter examples

Principle 6.3.1 – Principle of Strong Induction Suppose $P(n)$ is a predicate for $n \in \mathbb{Z}$. Let $b \in \mathbb{Z}$. If the following holds:

- P(b) is true:
- for all $k \in \mathbb{Z}$, $k \geq b$ we have that $P(b), P(b+1), \dots, P(k)$ together imply $P(k+1)$.

Then $P(n)$ is true for all $k \geq b$

Principle 6.3.2 – Minimal counter example Let $P(n)$ be a predicate for all $n \in \mathbb{Z}$. Let $b \in \mathbb{Z}$. If the statement that $P(n)$ is true for all $n \in \mathbb{Z}, n \geq b$, is not true, then there is a minimal counter example. That means, there is an $m \in \mathbb{Z}$, $m \geq b$ with $P(m)$ false and $P(n)$ true for all $n \in \mathbb{N}$ with $b \leq n < m$.

6.4 Structural induction

Principle 6.4.1 – Structural Induction If a structure of data types is defined recursively, then we can use this recursive definition to derive properties by induction.
In particular,

- if all basic elements of a recursively defined structure satisfy some property P
- and if newly constructed elements satisfy P, assuming the elements used in the construction already satisfy P,

then all elements in the structure satisfy P.

Principle 6.4.2 – The Principle of Induction on a well founded order Let $(P, \sqsubseteq)$ be a well founded order. Suppose $Q(x)$ is a predicate for all $x \in P$ satisfying:

- $Q(x)$ is true for all minimal elements $b \in P$.
- If $x \in P$ and $Q(y)$ is true for all $y \in P$ with $y \sqsubseteq x$, but $u \neq x$, then $P(x)$ holds.

Then $Q(x)$ holds for all $x \in P$.

6.5 Exercises

7 Cardinalities

7.1 Cardinality

Definition 7.1.1 – Cardinality Two sets A and B have the same *cardinality* if there exists a bijection from A to B.

Example 7.1.2 Two finite sets have the same cardinality if and only if thery have the same number of elements.

Example 7.1.3 The sets $\mathbb{N}$ and $\mathbb{Z}$ have the same cardinality. Indeed, consider the map $f: \mathbb{N} \to \mathbb{Z}$ defined by $f(2n) = n$ and $f(2n+1) = -n$ where $n \in \mathbb{N}$. This map is clearly a bijection

Theorem 7.1.4 – Cardinality as equivalence relation Having the same cardinality is an equivalence relation.

7.2 Countable sets

Definition 7.2.1 – Finite/Inifinite sets A set is called *finite* if it is empty or has the same cardinality as the set $\mathbb{N}_n := \{1, 2, \dots, n\}$ and *infinite* otherwise.

Definition 7.2.2 – Countable/Uncountable sets A set is called *countable* if it is finite or has the same cardinality as the set $\mathbb{N}$.
An infinite set that is not countable is called *uncountable*.

Theorem 7.2.3 – Countable sets in infinite sets Every infinite set contains an infinite countable subset.

Proof. Suppose A is an infinite set. Since A is infinite, we can start enumerating the elements $a_1, a_2, \dots$ such that all the elements are distinct. This yields a sequence of elements in A. The set of all the elements in this sequence form a countable subset of A. $\square$

Theorem 7.2.4 – Let A be a set. If there is a surjective map from $\mathbb{N}$ to A, then A is countable.

Proof. Let $f: \mathbb{N} \to A$ be a surjection. Then consider the sequence $f(1), f(2), \dots$. Remove from this sequence (going from left to right) each element that you have seen before. The result is either a finite sequence, or an infinite sequence $f(n_1), f(n_2), \dots$ of which all elements are distinct. In the latter case, consider the map $g: \mathbb{N} \to A$ with $g(i) = f(n_i)$. This map is a bijection, which proves A to be countable. $\square$

Corollary 7.2.5 – Let A be countable and $f: A \to B$ surjective, then B is countable.

Proof. Suppose A is a countable set and $f: A \to B$ a surjective map. If A is finite, then so is B. Thus assume that A has infintely many elements. Since A is countable, there is a bijection $g: \mathbb{N} \to A$. But then $f \circ g$ is a surjection from $\mathbb{N}$ to B. Hence we can apply the previous result and find a bijection from $\mathbb{N}$ to B. This proves B to be countable. $\square$

Theorem 7.2.6 – Any subset of a countable set is countable.

Proof. Suppose A is an infinite subset of a countable set B. Let $f: \mathbb{N} \to B$ be bijective and fix an element $a \in A$. Now consider the map $g: \mathbb{N} \to A$ defined by $g(x) = f(x)$ if $f(x) \in A$ and $g(x) = a$ if $f(x) \in B \setminus A$. Then g is surjective, as f is surjective. Thus A is countable. $\square$

Proposition 7.2.7 – $\mathbb{N} \times \mathbb{N}$ is countable.

Proof. Let $n \in \mathbb{N}$. Let m be maximal with $\sum_{i=0}^{m} i < n$. Now let $k = n - \sum_{i=0}^{m} i$So, $1 \leq k \leq m+1$.

We define $f : \mathbb{N} \to \mathbb{N}$ in the following way:

$$f(n) = (k, m+2-k).$$

So, in a table this looks as follows:

$f(1) = (1,1)$	$f(2) = (1,2)$	$f(4) = (1,3)$	$f(7) = (1,4)$	
$f(3) = (2,1)$	$f(5) = (2,2)$	$f(8) = (2,3)$	$\dots$	
$f(6) = (3,1)$	$f(9) = (3,2)$	$\dots$		
$\vdots$	$\vdots$			

By construction, f is injective. Indeed, the m and k are uniquely defined by n.

So it only remains to prove surjectivity. Let $(k,l) \in \mathbb{N} \times \mathbb{N}$. Set $m = k+l-2$. Hence $(k,l) = (k, m+2-k)$ and $(k,l) = f(n)$ for n equal to $\sum_{i=0}^{m} i + k$. $\square$

Theorem 7.2.8 – Let A and B be countable sets. Then $A \times B$ is countable.

Proof. Suppose $f : \mathbb{N} \to A$ and $g : \mathbb{N} \to B$ are surjections. The map $h : \mathbb{N} \times \mathbb{N} \to A \times B$ defined by $h(i,j) = (f(i), h(i))$ is surjective. So, since $\mathbb{N} \times \mathbb{N}$ is countable, also $A \times B$ is countable. $\square$

Proposition 7.2.9 – The sets $\mathbb{Z}$ and $\mathbb{Q}$ are countable.

Proof. The map $g : \{-1,1\} \times \mathbb{N} \to \mathbb{Z}$ given by $g(x,y) = xy$ is surjective. Since $\{-1,1\} \times \mathbb{N}$ is countable, hence $\mathbb{Z}$ is also countable.

Now let $f : \mathbb{Z} \times \mathbb{N} \to \mathbb{Q}$ be defined by $f(i,j) = \frac{i}{j}$ for $(i,j) \in \mathbb{Z} \times \mathbb{N}$. This is clearly a surjective map. Since $\mathbb{Z}$ and $\mathbb{N}$ are countable so is $\mathbb{Z} \times \mathbb{N}$. Hence $\mathbb{Q}$ is also countable. $\square$

Theorem 7.2.10 – Let $\mathscr{C}$ be a countable collection of countable sets. Then $\bigcup_{A \in \mathscr{C}} A$ is countable.

Proof. For each $A \in \mathscr{C}$ there exists a bijection $f_A : \mathbb{N} \to A$. Moreover, as $\mathscr{C}$ is countable, there exists also a bijection $g : \mathbb{N} \to \mathscr{C}$. We write $A_i = g(i)$.

Now consider the map $f : \mathbb{N} \times \mathbb{N} \to \bigcup_{A \in \mathscr{C}} A$ defined by $f(i,j) = f_{A_i}(j)$. This is a surjection. Thus $\bigcup_{A \in \mathscr{C}} A$ is countable. $\square$

Example 7.2.11 Let S be the set of all finite subsets of $\mathbb{N}$. Then $S = \bigcup_{i \in \mathbb{N} S_i}$, where S_i is the set of subsets of size at most i of $\mathbb{N}$.

We already showed that $\mathbb{N}^i$ is countable. But the map $(a_1, \dots, a_i) \in \mathbb{N}^i \mapsto \{a_1, \dots, a_i\} \in S_i$ is clearly surjective. Thus S_i is also countable. Hence $S = \bigcup_{i \in \mathbb{N} S_i}$ is also countable.

Proposition 7.2.12 – If A is infinite and B is finite, then A and $A \cup B$ have the same cardinality.

Proof. Assume that A is infinite and, withouth loss of generality, that A and B are disjunct. Let A_0 be a countable subset of A. Then $A_0 \cup B$ is also countable. Then there exists a bijection $g : A_0 \cup B \to A_0$. Now define $f : A \cup B \to A$ by

$$f(x) \begin{cases} g(x) & \text{if } x \in A_0 \cup B \\ x & \text{if } x \notin A_0 \cup B, \end{cases}$$

Then clearly f is a bijection between $A \cup B$ and A. $\square$

7.3 Some uncountable sets

Proposition 7.3.1 – The set $\{0,1\}^{\mathbb{N}}$ is uncountable.

Proof. Let $F:\mathbb{N}\to\{0,1\}^{\mathbb{N}}$. By f_i we denote the function $F(i)$ from $\mathbb{N}$ to $\{0,1\}$.

We will show that F is not surjective by constructing a function $f\in\{0,1\}^{\mathbb{N}}$ which is different from all the function f_i with $i\in\mathbb{N}$.

For each $i\in\mathbb{N}$ let

$$f(i)=0 \text{ if } f_i(i)=1 \text{ and}$$

$$f(i)=1 \text{ if } f_i(i)=0$$

Clearly, for all $i\in\mathbb{N}$ we have $f(i)\neq f_i(i)$ and hence $f\neq f_i$. So F is not surjective. This shows that there is no surjection from $\mathbb{N}$ to $\{0,1\}^{\mathbb{N}}$. In particular, $\{0,1\}^{\mathbb{N}}$ is not countable. □

Remark 7.3.2 (Cantor's diagonal argument).

If A is a set, then for each subset B of A we define the *characteristic function* $\chi_B:A\to\{0,1\}^{\mathbb{N}}$ to be the function that takes the value 1 on all elements in B and the value 0 on all elements in $A\setminus B$.

Clearly, every element $f\in\{0,1\}^{\mathbb{N}}$ is the characteristic fucntion of the set $\{a\in A\mid f(a)=1\}$. So, we find the map $B\in\mathscr{A}\mapsto\chi_B$ to be a bijection between $\mathscr{P}(A)$ to $\{0,1\}^{\mathbb{N}}$.

Corollary 7.3.3 – The set $\mathscr{P}(A)$ has the same cardinality as $\{0,1\}^{\mathbb{N}}$ and hence is uncountable.

Proposition 7.3.4 – The interval $[0,1)$ is uncountable.

Proof. Consider the map $f\in\{0,1\}^{\mathbb{N}}\mapsto\sum_{i=1}^{\infty}\frac{f(i)}{10^i}$. This map is injective. So, if $[0,1)$ is countable, then so is $\{0,1\}^{\mathbb{N}}$, which is a contradiction.

This proves that $[0,1)$ is uncountable. □

Corollary 7.3.5 – $\mathbb{R}$ is uncountable.

Proof. As $\mathbb{R}$ contains the uncountable subset $[0,1)$, it is also uncountable. □

Theorem 7.3.6 – If A and B are sets with the same cardinality, then $\mathscr{P}(A)$ and $\mathscr{P}(B)$ also have the same cardinality.

Proof. Suppose A and B have the same cardinality. Let $f:A\to B$ be a bijection. Consider the map $\hat{f}:P(A)\to P(B)$ given by $\hat{f}(S)=\{f(s)|s\in S\}$. This map is a bijection. □

Corollary 7.3.7 – If A is an infinite set, then $\mathscr{P}(A)$ is an uncountable set.

Theorem 7.3.8 – Let X be a set, then $\mathscr{P}(X)$ does not have the same cardinality as X.

Remark 7.3.9. The above theorem shows us that we can get bigger and bigger sets in the following way:

$$X_1 := \mathbb{N} \tag{4}$$

$$\text{for } n>1, X_n := \mathscr{P}(X_{n-1}) \tag{5}$$

7.4 Cantor-Schröder-Bernstein Theorem

Theorem 7.4.1 – Contor-Schröder-Bernstein Tehorem Let A and B be sets and assume that there are two maps $f : A \to B$ and $g : B \to A$ which are injective. Then there exists a bijection $h : A \to B$.
In particular, A and B have the same cardinality.

Corollary 7.4.2 – Let A be a set and assume $B \subseteq A$ has the same cardinality as A. Then each subset C of A with $B \subseteq C \subseteq A$ has the same cardinality as A.

Proposition 7.4.3 – The sets $\{0,1\}^{\mathbb{N}}$ and $[0,1)$ have the same cardinality.

Theorem 7.4.4 – The sets $\mathbb{R}, \{0,1\}^{\mathbb{N}}, \mathscr{P}(N)$ have the same cardinality.

Theorem 7.4.5 – The sets $\mathbb{R}^n$ with $n > 0$, and $\mathbb{R}$ have the same cardinality.

7.5 Additional axioms of set theory

Principle 7.5.1 – Axiom of Choice Let $\mathscr{C}$ be a collection of nonempty sets. Then there exists a map

$$f : \mathscr{C} \to \bigcup_{A \in \mathscr{C}} A$$

with $f(A) \in A$.
The image of f is a subset of $\bigcup_{A \in \mathbb{C}} A$.
The function f is called a *choice function*.

Principle 7.5.2 – The following statements are equivalent to the Axiom of Choice.

- For any two sets A and B ther edoes exist a surjective map from A to B or from B to A.
- The cardinality of an infinte set A is equal to the cardinality of $A \times A$.
- Every vector space has a basis.
- For every surjective map $f : A \to B$ there is a map $g : B \to A$ with $f(g(b)) = b$ for all $b \in B$.

Principle 7.5.3 – Axiom of Regularity Let X be a nonempty set of sets. Then X contains an element Y with $X \cap Y = \emptyset$.

7.6 Exercises

8 Integer Arithmetic

8.1 Divisors and multiples

Definition 8.1.1 – Let $a, b \in \mathbb{Z}$.

- We call b a divisor of a, if there is an integer q such that $a = q \cdot b$
- If b is a non-zero divisor of a then the (unique) integer q with $a = q \cdot b$ is called the *quotient* of a by b and denoted by $\frac{a}{b}$, a/b or $\text{quot}(a,b)$.

If b is a divisor of a, we also say that b *divides* a, or a is a *multiple* of b, or a is *divisible* by b. We write this as $b|a$

Example 8.1.2 If $a = 13$ and $b = 5$ then b does not divide a. However, if $a = 15$ and $b = 5$, then b does divide a.

Example 8.1.3 For all integers n we find $n-1$ to be a divisor of $n^2 - 1$.

More generally, for all $m \geq 2$ we h:w ave $n^m - 1 = (n-1)(n^{m-1} + n^{m-2} + \cdots + 1)$. So, $n-1$ is a divisor of $n^m - 1$.

Lemma 8.1.4 – Suppose that a, b and c are integers.

1. If a divides b and b divides c, then a divide c.
2. If a divides b and c, then a divides $x \cdot a + y \cdot b$ for all integers x, y
3. If b is non-zero and a divide b, then $|a| \leq |b|$

Theorem 8.1.5 – **Division with Remainder** If $a \in \mathbb{Z}$ and $b \in \mathbb{Z} \setminus \{0\}$, then there are unique integers q, r such that $a = q \cdot b + r, |r| < |b|$ and $b \cdot r \geq 0$.

8.2 Euclid's algorithm

8.3 Linear diaphantine equtions

8.4 Prime numbers

8.5 Factorization

8.6 Number systems

8.7 Exercises

9 Modular Arithmetic

9.1 Arthimetic modulo n

Definition 9.1.1 – Let n be an integer. On the set $\mathbb{Z}$ of integers we define the relation *congruence modulo* n as follows: a and b are *congruent modulo* n if and only if $n \mid a-b$.
We write $a \equiv b \pmod{n}$ to denote that a and b are congruent modulo n.

Example 9.1.2 If $a = 342, b = 241$, and $n = 17$, then a is not congruent to b modulo n.

Proposition 9.1.3 – Let n be an integer. The relation congruence modulo n is an equivalence relation. For nonzero n, there are exactly n distinct equivalence classes
The set of equivalence classes of $\mathbb{Z}$ modulo n is denoted by $\mathbb{Z}/n\mathbb{Z}$.

Example 9.1.4 The relation modulo 2 partitions the integers into two clases, the even numbers and the odd numbers.

Theorem 9.1.5 – Addition and Multiplication On $\mathbb{Z}/n\mathbb{Z}$ we define two so-called binary operations, an *addition* and a *multiplication*, by:

- Addition: $x \pmod{n} + y \pmod{n} = x + y \pmod{n}$
- Multiplication: $x \pmod{n} \cdot y \pmod{n} = x \cdot y \pmod{n}$

Both operations are well defined.

Proposition 9.1.6 – Propoerties of Modular Arithmetic Let n be an integer bnigger than 1. For all integers a, b, c we have the following equalities.

- Commutativity of addition:
$$a + b = b + a \pmod{n}$$
- Commutativity of multiplication:
$$a \cdot b = b \cdot a \pmod{n}$$
- Associativity of additiono:
$$(a + b) + c = a + (b + c) \pmod{n}$$
- Associativity of multiplication:
$$(a \cdot b) \cdot c = a \cdot (b \cdot c) \pmod{n}$$
- Distributivity of multiplication over addition:
$$a \cdot (b + c) = a \cdot b + a \cdot c \pmod{n}$$

9.2 Invertible elements and zero divisors

Definition 9.2.1 – An element $a \in \mathbb{Z}/n\mathbb{Z}$ is called *invertible* if there is an element b, called *inverse* of a, such that $a \cdot b = 1$.
Of a is invertible, its inverse will be denoted by a^{-1}.
The set of all invertible elements in $\mathbb{Z}/n\mathbb{Z}$ will be denoted by $\mathbb{Z}/n\mathbb{Z}^{\times}$. This set is also called the *multiplicative group* of $\mathbb{Z}/n\mathbb{Z}$.

Proposition 9.2.2 – Uniqueness of the Inverse Let $n > 1$. If an element $a \in \mathbb{Z}/n\mathbb{Z}$ is invertible, then its inverse is unique.

In $\mathbb{Z}$ division is not always possible. Some nonzero elemetns do have an inverse, others don't. The following theorem tells us precisely which elements of $\mathbb{Z}/n\mathbb{Z}$ have an inverse.

Theorem 9.2.3 – Characterization of Modular Invertibility Let $n > 1$ and $a \in \mathbb{Z}$

(a) The class $a \pmod{n}$ in $\mathbb{Z}/n\mathbb{Z}$ has a multiplicative inverse if and only if $\gcd(a,n) = 1$

(b) If a and n are relatively prime, then the inverse of $a \pmod{n}$ is the class $\mathrm{Extgcd}(a,n)_2 \pmod{n}$

(c) In $\mathbb{Z}/n\mathbb{Z}$, every class distinct from 0 has an inverse if and only if n is prime.

Example 9.2.4 The invertible elements in $\mathbb{Z}/2^n\mathbb{Z}$ are the classes $x \pmod{2^n}$ for which x is an ood integer.

An arithmetical system such as $\mathbb{Z}/n\mathbb{Z}$ with p prime, in which every element not equal to 0 has a multiplicative inverse, is called a *field*, just like $\mathbb{Q}, \mathbb{R}, \mathbb{C}$.

Besides invertible elements in $\mathbb{Z}/n\mathbb{Z}$, which can be viewed as divisors of 1, one can also consider the divisors of 0.

Definition 9.2.5 – Zero Divisor An element $a \in \mathbb{Z}/n\mathbb{Z}$ not equal to 0 is called a *zero divisor* if there is a nonzero element b such that $a \cdot b = 0$.

The following theorem shows which elements of $\mathbb{Z}/n\mathbb{Z}$ are zero divisors. They turn out to be those nonzero elements that are not invertible.

Theorem 9.2.6 – Zero Divisor Characterization Let $n > 1$ and $n \in \mathbb{Z}$

1. The class $a \pmod{n}$ in $\mathbb{Z}/n\mathbb{Z}$ is a zero divisor if and only if $\gcd(a,n) > 1$ and $a \pmod{n}$ is nonzero.

2. The residue ring $\mathbb{Z}/n\mathbb{Z}$ has no zero divisors if and only if n is prime.

Let n be an integer. Inside $\mathbb{Z}/n\mathbb{Z}$, we can distinguish the set of invertible elements and the set of zero divisors. The set of invertible elements is closed under multiplication, the set of zero divisors together with 0 is even closed under multiplication by arbitrary elements.

Lemma 9.2.7 – Let n be an integer with $n > 1$.

1. If a and b are elements in $\mathbb{Z}/n\mathbb{Z}^{\times}$, then their product $a \cdot b$ is invertible and therefore also in $\mathbb{Z}/n\mathbb{Z}^{\times}$. The inverse of $a \cdot b$ is given by $b^{-1} \cdot a^{-1}$.

2. If a is a zero divisor in $\mathbb{Z}/n\mathbb{Z}$ and b is an item arbitrary element, then $a \cdot b$ is either 0 or a zero divisor.

9.3 Linear congruence

Algorithm 9.3.1 – Linear Congruence

Remark 9.3.2. There are exactly $\gcd(a,n)$ distict solutions.

Example 9.3.3 In order to find all solutions to the congruence $24x \equiv 12 \pmod{15}$ we first compute the $\gcd(24,15)$.Using the Extended Euclidean Algorithm we find

$$\gcd(24,15) = 3 = 2 \cdot 24 - 3 \cdot 15$$

Now 3 divide 12, so the solution set is

$$\{2 \cdot 12 + k \cdot 15 \mid k \in \mathbb{Z}\}$$

Instead of using the algorithm, we can also use the expression of the gcd as a linear combination of 24 and 15 to argue what the solution is. To this end, multiply both sides of the equality $3 = 2 \cdot 24 - 3 \cdot 15$ by 4. This gives $12 = 8 \cdot 24 - 12 \cdot 15$.

So, a solution of the confgurence is $x = 8 \pmod{15}$.

We extend the study of a single congruence to a method for solvin special systems of congruences.

Theorem 9.3.4 – Chinese Remainder Theorem Suppose that $n_1, \ldots, n_k$ are pairwise coprime integers. Then for all integers $a_1, \ldots, a_k$ the system of linear congruences

$$x \equiv a_1 \pmod{n_i}$$

with $i \in \{1, \ldots, k\}$ has solution.
Indeed, the integer

$$x = \sum_{i=1}^{k} a_i \cdot y_i \cdot \frac{n}{n_i}$$

where

$$n = \prod_{i=1}^{k} n_i$$

and for each i we have

$$y_i = \text{Extgcd}\left(\frac{n}{n_i}, n_i\right)_3$$

satisfies all congruences.

Any two solutions to the system of congruences are congruent modulo the product $\prod_{i=1}^{k} n_i$.

9.4 The theorems of Fermat and Euler

Let p be a prime. Consider $\mathbb{Z}/p\mathbb{Z}$, the set of equivalence classes of $\mathbb{Z}$ modulo p. In $\mathbb{Z}/p\mathbb{Z}$ we can add, subtract, multiply and divide by elemnts which are not 0. Moreover, it contains no zero divisors.

Theorem 9.4.1 – Fermat's Little Theorem Let p be a prime. For every integer a we have

$$a^p \equiv a \pmod{p}$$

In particular, if a is not in $0 \pmod p$ then

$$a^{p-1} \equiv 1 \pmod p$$

Example 9.4.2 The integer 1234^1234-2 is divisible by 7.

Indeed, if we compute modulo 7, then we find that $1234 \equiv 2 \pmod 7$. Moreover, by Fermat's Little Theorem we have $2^6 \equiv 1 \pmod 7$, so

$$1324^1234 = 2^1234 = 2^{6\cdot 205+4} = 2^4 = 2 \pmod 7$$

Fermat's Little Theorem states that the multiplicative group $\mathbb{Z}/p\mathbb{Z}^\times$, where p is a prime, contains precisely $p-1$ elements. For arbitrary positive n, the number of elements in the multiplicative group $\mathbb{Z}/n\mathbb{Z}^\times$ is given by the so-called *Euler totient function*.

Definition 9.4.3 – Euler totient function The Euler totient function $\Phi : \mathbb{N} \to \mathbb{N}$ is defined by

$$\Phi(n) = \left|\mathbb{Z}/n\mathbb{Z}^\times\right|$$

for all $n \in \mathbb{N}$ with $n > 1$, and by $\Phi(1) = 1$.

Theorem 9.4.4 – Euler Totient The Euler totient function satisfies the following properties.

1. Suppose that n and m are positive integers. If $\gcd(n,m) = 1$, then

$$\Phi(n \cdot m) = \Phi(n) \cdot \Phi(m)$$

2. If p is a prime and n is a positive integer, then

$$\Phi(p^n) = p^n - p^n - 1$$

Theorem 9.4.5 – Euler's Theorem Suppose n is an integer with $n \geq 2$. Let a be an element of $\mathbb{Z}/n\mathbb{Z}^\times$. Then

$$a^{\Phi(n)} = 1$$

Let n be an integer. The *order* of an element a in $\mathbb{Z}/n\mathbb{Z}^\times$ is the smallest positive integer m such that $a^m = 1$. By Euler's Theorem the order of a exists and is at most $\Phi(n)$. More precise statements on the order of elements in $\mathbb{Z}/n\mathbb{Z}^\times$ can be found in the following result.

Theorem 9.4.6 – Orders Let n be an integer greater than 1.

1. If $a \in \mathbb{Z}/n\mathbb{Z}$ satisfies $a^m = 1$ for some positive integer m, then a is invertible and its order divides m.
2. For all elements $a \in \mathbb{Z}/n\mathbb{Z}^\times$ the order of a is a divisor of $\Phi(n)$
3. If $\mathbb{Z}/n\mathbb{Z}$ contains an element a of order $n-1$, then n is prime.

Definition 9.4.7 – An element a from $\mathbb{Z}/p\mathbb{Z}$ is called a *primitive element* of $\mathbb{Z}/p\mathbb{Z}$ if every element of $\mathbb{Z}/p\mathbb{Z}^\times$ is a power of a.

Theorem 9.4.8 – For each prime p there exists a primitive element in $\mathbb{Z}/p\mathbb{Z}$.

9.5 The RSA cryptosystem

9.6 Exercises

9.7 Homework

Ex 5

Let's prove that if x is an element of order $\Phi(n)$ in $\mathbb{Z}/n\mathbb{Z}$ (where $\Phi(n)$ is Euler's totient function), then every invertible element in $\mathbb{Z}/n\mathbb{Z}$ is a power of x.

We'll use a few key concepts:

1. The order of an element in a group is the smallest positive integer k such that x^k is the identity element of the group.

2. Euler's totient function $\Phi(n)$ is the number of positive integers less than or equal to n that are coprime to n.

3. In $\mathbb{Z}/n\mathbb{Z}$, the invertible elements are precisely those that are coprime to n (i.e., $\gcd(a,n) = 1$).

Now, let y be an invertible element in $\mathbb{Z}/n\mathbb{Z}$. We want to show that y is a power of x. We'll use the properties of Euler's totient function and group theory to prove this.

Since y is invertible, $\gcd(y,n) = 1$. Now, consider the group generated by x in $\mathbb{Z}/n\mathbb{Z}$, denoted as $\langle x\rangle$. By definition, the order of x is $\Phi(n)$, which means that all the elements in $\langle x\rangle$ have orders that divide $\Phi(n)$.

We know that y is invertible, so $\gcd(y,n) = 1$. This means that y is coprime to n and, therefore, belongs to the group of invertible elements modulo n. This group is isomorphic to the group $\langle x\rangle$, so y must also have an order that divides $\Phi(n)$.

Let k be the order of y, where k divides $\Phi(n)$. By Lagrange's theorem, in any group, the order of an element divides the order of the group. Since the order of y divides $\Phi(n)$, it also divides $\Phi(n)$. This means that k divides $\Phi(n)$, and since $\Phi(n)$ is the order of x, k must be less than or equal to $\Phi(n)$.

Since x has the smallest positive integer order in $\langle x\rangle$ (which is $\Phi(n)$), and k divides $\Phi(n)$, we conclude that k must be $\Phi(n)$. This implies that y has the same order as x, so $y = x^t$ for some positive integer t.

Therefore, we have shown that every invertible element in $\mathbb{Z}/n\mathbb{Z}$ is a power of x, as desired.

List of Theorems

10 Exercises for exam

10.1 Logic

Exercise numberlike=subsubsection 1. *The statements P and Q can be true or false. When is the statement*

when is the statement

$$R = (P \wedge Q) \vee ((\neg P \vee Q) \wedge (P \vee \neg Q))$$

true?

1. If P and Q are true, then $P \wedge Q$ hence R is true

2. If P is true and Q is false, then $P \wedge Q$ and $\neg P \vee Q$ are false, hence R is false

3. If P is false and Q is true, then $P \wedge Q$ and $P \vee \neg Q$ are false, hence R is false

4. If P and Q are false, then $\neg P \vee Q$ and $P \vee \neg Q$ are true, hence R is true

Exercise numberlike=subsubsection 2. *Prove or disprove the following statement:*
For all statements p, q, r we have $((p \vee q) \wedge r) \iff ((p \wedge r) \vee (q \wedge r))$

Using the distribive property of the $\wedge$ over $\vee$ we get:

$$(p \vee q) \wedge r = (p \wedge r) \vee (q \wedge r)$$

Thus we see that $((p \vee q) \wedge r) \iff ((p \wedge r) \vee (q \wedge r))$

Exercise numberlike=subsubsection 3. *Prove or disprove the following statement: for all statements P, Q and R it holds that:*

$$[(P \implies R) \vee (P \implies Q)] \iff [P \implies (Q \vee R)]$$

When P is true we get true $\iff$ true which is true. When P is false we get $R \vee Q \iff Q \vee R$ which is also true. Hence for all P, Q, R the statement is true.

10.1.1 Sets

Exercise numberlike=subsubsection 4. *Prove or disprove*

$$\forall x \in U\, [x \in (A \cap B) \implies (x \in A \vee x \in B)] \iff A = B$$

The statement is false and a counter example is $A = \{1, 2\}, B = \{1\}$

Exercise numberlike=subsubsection 5. *Prove or disprove: For all sets A, B and C we have: A*

10.2 Final Exam 2022/2023

Exercise numberlike=subsubsection 6. *Which statement is true*

1. *For all sets A and B we have if $\mathscr{P}(A) = \mathscr{P}(B)$, then $A = B$*

2. *For all sets A, B, C we have $(A \cup B = A \cup C \wedge B \subseteq C) \implies A = B$*