1. Preliminaries

1.1. Sets

We will naively think of a set as a collection of mathematical objects, called its elements or members. To indicate that an object \( x \) is an element of the set \( A \) we write \( x \in A \), in words: \( x \) is in \( A \), or \( x \) belongs to \( A \). To indicate that an object \( x \) is not an element of the set \( A \) we write \( x \notin A \). We consider the sets \( A \) and \( B \) as the same set (notation: \( A = B \)) if and only if they have exactly the same elements. We often introduce a set via the bracket notation, listing or indicating inside the brackets its elements. For example, \( \{2, 4\} \) is the set with 2 and 4 as its only elements. Note that \( \{2, 4\} = \{4, 2, 4\} \) the same set can be described in many different ways. You should not confuse an object \( x \) with the set \( \{x\} \) that has \( x \) as its only element: for example, \( \{0, 1\} \) has two elements, but \( \{(0, 1)\} \) has only one element. (Why?)

Examples.

(i) The empty set \( \emptyset \). (It has no elements.)
(ii) The set of natural numbers \( \mathbb{N} = \{0, 1, 2, \ldots\} \).
(iii) The set of integers \( \mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\} \).
(iv) The set of rational numbers \( \mathbb{Q} \).
(v) The set of real numbers \( \mathbb{R} \).
(vi) The set of complex numbers \( \mathbb{C} \).

If all elements of the set \( A \) are in the set \( B \), then we say that \( A \) is a subset of \( B \) (and write \( A \subseteq B \)). Thus the empty set \( \emptyset \) is a subset of every set, and each set is a subset of itself. We often introduce a set \( A \) in our discussions by defining \( A \) to be the set of all elements of a given set \( B \) that satisfy some property \( P \). Notation: \( A := \{x \in B : x \text{ satisfies } P\} \).

Let \( A \) and \( B \) be sets. The we can form the following sets:

- \( A \cup B := \{x : x \in A \text{ or } x \in B\} \).
- \( A \cap B := \{x : x \in A \text{ and } x \in B\} \).
- \( A \setminus B := \{x : x \in A \text{ and } x \notin B\} \).
- \( A \times B := \{(a, b) : a \in A \text{ and } b \in B\} \).

The elements of \( A \times B \) are the so-called ordered pairs \( (a, b) \) with \( a \in A \) and \( b \in B \). The key thing about ordered pairs is that we have \( (a, b) = (c, d) \) if and only if \( a = c \) and \( b = d \). For example, you may think of \( \mathbb{R} \times \mathbb{R} \) as the set of points \((x, y)\) in the \( xy \)-plane of coordinate geometry. And if you wish to think of \((a, b)\) as a set, then the right way to do so is to think \((a, b) = \{\{a\}, \{a, b\}\}\).

We say that \( A \) and \( B \) are disjoint if \( A \cap B = \emptyset \), that is, they have no element in common. Sometimes it is useful to consider another operation between sets called disjoint union. The disjoint union of two sets \( A \) and \( B \) is denoted by \( A \sqcup B \) and is defined by

\[ A \sqcup B := \{(a, \emptyset) : a \in A\} \cup \{(b, \emptyset) : b \in B\} \]

Note that the sets \( \{(a, \emptyset) : a \in A\} \) and \( \{(b, \emptyset) : b \in B\} \) are disjoint no matter what \( A \) and \( B \) are.

1.2. Functions

Definition. A function is a triple \( f = (A, B, \Gamma) \) of sets \( A, B, \Gamma \) such that \( \Gamma \subseteq A \times B \) and for each \( a \in A \) there is exactly one \( b \in B \) with \( (a, b) \in \Gamma \); we write \( f(a) \) for this unique \( b \), and call it the value of \( f \) at \( a \) (or the image of \( a \) under \( f \)). We call \( A \) the domain of \( f \), \( B \) the codomain of \( f \), and \( \Gamma \) the graph of \( f \). We write \( f : A \to B \) to indicate that \( f \) is a function with domain \( A \) and codomain \( B \), and we also say then that \( f \) is a function from \( A \) to \( B \).
Examples.

(i) Given any set \( A \) we have the identity function \( 1_A : A \to A \) defined by \( 1_A(a) = a \) for all \( a \in A \).

(ii) Any polynomial \( f(X) = a_0 + a_1X + \cdots + a_nX^n \) with real coefficients \( a_0, \ldots, a_n \) gives rise to a function \( f : \mathbb{R} \to \mathbb{R} \). (We often use the “maps to” symbol \( \mapsto \) in this way to indicate the rule by which we associate, to each \( x \) in the domain, its value \( f(x) \).)

Definition. Given \( f : A \to B \) and \( g : B \to C \) we have a function \( g \circ f : A \to C \) defined by \( (g \circ f)(a) = g(f(a)) \) for all \( a \in A \). It is called the composition of \( g \) and \( f \).

Definition. Let \( f : A \to B \) be a function. It is said to be injective if for all \( a_1 \neq a_2 \) in \( A \) we have \( f(a_1) \neq f(a_2) \). It is said to be surjective if for each \( b \in B \) there exists \( a \in A \) such that \( f(a) = b \). It is said to be bijective if it is both injective and surjective. For \( X \subseteq A \) we put

\[ f[X] := \{ f(x) : x \in X \} \subseteq B \]

and call \( f[X] \) the direct image of \( X \) under \( f \). For \( Y \subseteq B \) we put

\[ f^{-1}[Y] := \{ x \in A : f(x) \in Y \} \subseteq A \]

and call \( f^{-1}[Y] \) the inverse image of \( Y \) under \( f \). (Thus the surjectivity of our function \( f \) is equivalent to \( f[A] = B \).)

Exercises.

(i) If \( f : A \to B \) is a bijection then one can define an inverse function \( f^{-1} : B \to A \) by \( f^{-1}(b) := \) the unique \( a \in A \) such that \( f(a) = b \). Prove that in such a case \( f^{-1} \) is well-defined, i.e., prove that it is a function.

(ii) Note that \( f^{-1} \circ f = 1_A \) and \( f \circ f^{-1} = 1_B \).

(iii) Suppose that \( f : A \to B \) and \( g : B \to A \) satisfy \( g \circ f = 1_A \) and \( f \circ g = 1_B \). Then show that \( f \) is a bijection with \( f^{-1} = g \).

Remark. The attentive reader will notice that we just introduced a potential conflict of notation. For bijective \( f : A \to B \) and \( Y \subseteq B \), both the inverse image of \( Y \) under \( f \) and the direct image of \( Y \) under \( f^{-1} \) are denoted by \( f^{-1}[Y] \); no harm is done, however, since these two subsets of \( A \) coincide.

It follows from the definition of “function” that \( f : A \to B \) and \( g : C \to D \) are equal \( (f = g) \) if and only if \( A = C, B = D, \) and \( f(x) = g(x) \) for all \( x \in A \). We say that \( g : C \to D \) extends \( f : A \to B \) (or \( g : C \to D \) is an extension of \( f : A \to B \), or \( f : A \to B \) is a restriction of \( g : C \to D \)) if \( A \subseteq C, B \subseteq D, \) and \( f(x) = g(x) \) for all \( x \in A \).

1.3. Cardinalities

Definition. A set \( A \) is said to be finite if there exists \( n \in \mathbb{N} \) and a bijection \( f : \{1, \ldots, n\} \to A \). (Here we use \( \{1, \ldots, n\} \) as a suggestive notation for the set \( \{ n \in \mathbb{N} : 1 \leq m \leq n \} \). For \( n = 0 \) this is just \( \emptyset \).) If \( A \) is finite there is exactly one such \( n \) (although if \( n > 1 \) there will be more than one bijection \( f : \{1, \ldots, n\} \to A \)): we call this unique \( n \) “the number of elements of \( A \)” or “the cardinality of \( A \)”, and denote it by \( |A| \). A set which is not finite is said to be infinite.

Definition. A set \( A \) is said to be countably infinite if there is a bijection \( f : \mathbb{N} \to A \). It is said to be countable if it is either finite or countably infinite.

Example. Consider the function \( g : \mathbb{R} \to \mathbb{R} \) defined by

\[ g(x) = \frac{1}{1 + 2|x| - x} \]

where for any \( x \in \mathbb{R}, \) \( |x| \) denotes the largest natural number less than or equal to \( x \). (For example, \( |\pi| = 3, |3| = 3, \) and \( |3.99999| = 3 \).) Let \( f : \mathbb{N} \to \mathbb{Q} \) be the function defined by the following rule:

\[ f(n) = \frac{(g \circ \cdots \circ g)(0)}{n+1\text{-times}}. \]

Then \( f \) is a bijection between \( \mathbb{N} \) and \( \mathbb{Q}^+ \), where \( \mathbb{Q}^+ \) denotes the set \( \{ x \in \mathbb{Q} : x \geq 0 \} \). (Convince yourself of this.)

Remark. The sets \( \mathbb{N}, \mathbb{Q}, \mathbb{Z} \) are countably infinite, but the infinite set \( \mathbb{R} \) is not countably infinite. Every infinite set has a countably infinite subset.
Let $I$ and $A$ be sets. Then there is a set whose elements are exactly the maps $f : I \to A$, and this set is denoted by $A^I$. For $I = \{1, \ldots, n\}$ we also write $A^n$ instead of $A^I$. Thus an element of $A^n$ is a function $a : \{1, \ldots, n\} \to A$; we usually think of such an $a$ as a the $n$-tuple $(a(1), \ldots, a(n))$, and we often write $a_i$ instead of $a(i)$. So $A^n$ can be thought of as the set of $n$-tuples $(a_1, \ldots, a_n)$ with each $a_i \in A$. For $n = 0$ the set $A^n$ has just one element — the empty tuple.

An $n$-ary relation on $A$ is just a subset of $A^n$, and an $n$-ary operation on $A$ is a function from $A^n$ into $A$. Instead of “1-ary” we usually say unary, and instead of “2-ary” we usually say binary. For example, $\{(a, b) : a < b\}$ is a binary relation on $\mathbb{Z}$ and integer addition is the binary operation $(a, b) \mapsto a + b$ on $\mathbb{Z}$.

**Definition.** $\{a_i\}_{i \in I}$ or $(a_i)_{i \in I}$ denotes a family of objects $a_i$ indexed by the set $I$, and is just a suggestive notation for the set $\{(i, a_i) : i \in I\}$, not to be confused with the set $\{a_i : i \in I\}$ of members of the family. For $I = \mathbb{N}$ we usually say “sequence” instead of “family”.

Given any family $(A_i)_{i \in I}$ of sets we can form its union:

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

If $I$ is finite and each $A_i$ is finite, then so is the union above defined and

$$
\left| \bigcup_{i \in I} A_i \right| \leq \sum_{i \in I} |A_i|.
$$

If $I$ is countable and each $A_i$ is countable then $\bigcup_{i \in I} A_i$ is countable.

### 1.4. Words

**Definition.** Let $A$ be a set. Think of $A$ as an **alphabet** of letters. A **word of length** $n$ on $A$ is an $n$-tuple $(a_1, \ldots, a_n)$ of letters $a_i \in A$; because we think of it as a word we shall write this tuple instead as $a_1 \cdots a_n$ (without parentheses or commas). There is a unique word of length 0 on $A$, called the **empty word** and denoted by $\epsilon$. The set of all words on $A$ is denoted by $A^*$ and it satisfies:

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

A subset of $A^*$ is also called a **language** on the alphabet $A$. When $A \subseteq B$ we can identify $A^*$ with a subset of $B^*$, and this will be done if convenient.

**Definition.** Given words $a = a_1 \cdots a_m$ and $b = b_1 \cdots b_n$ on $A$ of length $m$ and $n$ respectively, we define their **concatenation** $ab \in A^*$ by:

$$
ab = a_1 \cdots a_m b_1 \cdots b_n.
$$

Thus $ab$ is a word on $A$ of length $m + n$. Concatenation is a binary operation on $A^*$ that is associative: $(ab)c = a(bc)$ for all $a, b, c \in A^*$, with $\epsilon$ as two sided identity: $\epsilon a = a = a \epsilon$ for all $a \in A^*$, and with two-sided cancellation: for all $a, b, c \in A^*$, if $ab = ac$, then $b = c$, and if $ac = bc$, then $a = b$.

### 1.5. Equivalence relations

Given a binary relation $R$ on a set $A$ it is often more suggestive to write $aRb$ instead of $(a, b) \in R$.

**Definition.** An **equivalence relation** on a set $A$ is a binary relation $\sim$ on $A$ such that for all $a, b, c \in A$:

(i) $a \sim a$ (reflexivity)
(ii) $a \sim b$ implies $b \sim a$ (symmetry)
(iii) $(a \sim b$ and $b \sim c$) implies $a \sim c$ (transitivity)

**Example.** Given any $n \in \mathbb{N}$ we have the equivalence relation “congruence modulo $n$” on $\mathbb{Z}$ defined as follows: for any $a, b \in \mathbb{Z}$ we have

$$
a \equiv b \mod n \iff a - b = nc \text{ for some } c \in \mathbb{Z}.
$$

For $n = 0$ this is just equality on $\mathbb{Z}$.
Let \( \sim \) be an equivalence relation on a set \( A \). We define the equivalence class \( a^\sim \) of an element \( a \in A \) by \( a^\sim = \{ b \in A : a \sim b \} \) (a subset of \( A \)). For \( a, b \in A \) we have \( a^\sim = b^\sim \) if and only if \( a \sim b \) and \( a^\sim \cap b^\sim = \emptyset \) if and only if \( a \not\sim b \).

We define the quotient set of \( A \) by \( \sim \) to be the set of equivalence classes:
\[
A/\sim := \{ a^\sim : a \in A \}.
\]
This quotient set is a partition of \( A \), that is, it is a collection of pairwise disjoint nonempty subsets of \( A \). Every partition of \( A \) is the quotient set \( A/\sim \) for a unique equivalence relation \( \sim \) on \( A \).

In the previous example (congruence modulo \( n \)) the equivalence classes are called congruence classes modulo \( n \) (or residue classes modulo \( n \)) and the corresponding quotient set is often denoted \( \mathbb{Z}/n\mathbb{Z} \).

### 1.6. Posets

A partially ordered set (short: poset) is a pair \((P, \leq)\) consisting of a set \( P \) and a partial ordering \( \leq \) on \( P \), that is, \( \leq \) is a binary relation on \( P \) such that for all \( p, q, r \in P \),

(i) \( p \leq p \) (reflexivity);
(ii) if \( p \leq q \) and \( q \leq p \) then \( p = q \) (antisymmetry);
(iii) if \( p \leq q \) and \( q \leq r \) then \( p \leq r \) (transitivity).

Let \((P, \leq)\) be a poset. Here’s some useful notation. For \( x, y \in P \) we set \( x \geq y \iff y \leq x \), and \( x < y \iff y > x \iff x \leq y \text{ and } x \neq y \).

Note that \((P, \geq)\) is also a poset. A least element of \( P \) is a \( p \in P \) such that \( p \leq x \) for every \( x \in P \); a largest element is defined likewise, with \( \geq \) instead of \( \leq \). Of course, \( P \) can have at most one least element; therefore, we can refer to the least element of \( P \), provided it exists. Likewise, we can refer to the largest element of \( P \) if \( P \) has a largest element.

A minimal element of \( P \) is an \( p \in P \) such that there is no \( x \in P \) with \( x < p \). A maximal element is defined likewise, with \( > \) instead of \( < \). If \( P \) has a least element, then that least element is the unique minimal element. However, there are many posets that have several minimal elements.

Let \( X \subseteq P \). We call \( X \) a chain in \( P \) (or a totally ordered subset of \( P \)) if for all distinct \( x, y \in P \), either \( x < y \) or \( y < x \). A lowerbound (respectively, upperbound) of \( X \) in \( P \) is an element \( l \in P \) (respectively, an element \( u \in P \)) such that \( l \leq x \) for all \( x \in X \) (respectively, \( x \leq u \) for all \( x \in X \)). On a few occasions we shall use the following result.

**Zorn’s Lemma.** Suppose \( P \neq \emptyset \) and every nonempty chain in \( P \) has an upperbound in \( P \). Then \( P \) has a maximal element.

### 2. Propositional logic

Propositional logic is the fragment of logic where we construct new statements from given statements using so-called connectives like not, or, and and. The truth value of such a statement is then determined completely by the truth values of the given statements.

**Example.** If \( p \) and \( q \) are two given statements, then we can construct the statements \( \neg p \) (the negation of \( p \), pronounced “not \( p \)”), \( p \lor q \) (the disjunction of \( p \) and \( q \), pronounced “\( p \) or \( q \)”), and \( p \land q \) (the conjunction of \( p \) and \( q \), pronounced “\( p \) and \( q \)”).

We start with the five distinct symbols
\[
\top, \bot, \neg, \lor, \land
\]
to be thought of as true, false, not, or, and and, respectively. These symbols will be fixed throughout the course, and are called propositional connectives. In this section we also fix a set \( A \) whose elements will be called propositional atoms (or just atoms), such that no propositional connective is an atom. It may help to think of an atom \( a \) as a variable for which we can substitute arbitrary statements, assumed to be either true or false.

A proposition on \( A \) is a word on the alphabet \( A \cup \{ \top, \bot, \neg, \lor, \land \} \) that can be obtained by applying the following rules:

(i) \( \top, \bot, \) and each atom \( a \) (viewed as words of length 1) are propositions on \( A \).
(ii) If \( p \) and \( q \) are propositions on \( A \), then \( \neg p, p \lor q, \) and \( p \land q \) are propositions on \( A \).

**Remark.** For the rest of this section “proposition” means “proposition on \( A \)”, and \( p, q, r \) (sometimes with subscripts) will denote propositions.

**Example.** Suppose \( a, b, c \) are atoms. Then \( \land \lor \neg ab \land c \) is a proposition. This follows from the rules above: \( a \) is a proposition, so \( \neg a \) is a proposition, hence \( \lor \neg ab \) as well; also \( \neg c \) is a proposition, and thus \( \land \lor \neg ab \land c \) is a proposition.
We let \( \text{Prop}(A) \) denote the set of propositions on \( A \).

**Remark.** Having the connectives \( \lor \) and \( \land \) in front of the propositions they “connect” rather than in between, is called *prefix notation* or *Polish notation*. This is theoretically elegant, but for the sake of readability we usually write \( p \lor q \) and \( p \land q \) to denote \( \lor pq \) and \( \land pq \) respectively, and we also use parentheses and brackets if this helps to clarify the structure of a proposition. So the proposition in the example above could be denoted by \( [(-a) \lor b] \land (-c) \), or even by \( (-a \lor b) \land (-c) \) since we shall agree that \( \neg \) binds stronger than \( \lor \) and \( \land \) in this informal way of indicating propositions. (Because of the informal character of these notations, we don’t have to give precise rules for its use; it’s enough that each actual use is clear to the reader.)

**Lemma 2.1 (Unique Readability).** If \( p \) has length 1, then either \( p = \top \) or \( p = \bot \), or \( p \) is an atom. If \( p \) has length > 1, then its first symbol is either \( \neg \), or \( \lor \), or \( \land \). If the first symbol of \( p \) is \( \neg \) then \( p = \neg q \) for a unique \( q \). If the first symbol of \( p \) is \( \lor \) then \( p = \lor qr \) for a unique pair \((q,r)\). If the first symbol of \( p \) is \( \land \), then \( p = \land qr \) for a unique pair \((q,r)\).

For now we shall assume this lemma without proof.

**Remark.** Rather than thinking of a proposition as a statement, it’s better viewed as a function whose arguments and values are statements: replacing the atoms in a proposition by specific mathematical statements like “\( 2+2 = 4 \)”, “\( \pi^2 < 7 \)”, and “every even integer \( > 2 \) is the sum of two prime numbers”, we obtain again a mathematical statement.

We shall use the following notational conventions: \( p \rightarrow q \) denotes \( \neg p \lor q \), and \( p \leftrightarrow q \) denotes \( (p \rightarrow q) \land (q \rightarrow p) \). By recursion on \( n \) we define

\[
p_1 \lor \cdots \lor p_n =
\begin{cases}
\bot & \text{if } n = 0 \\
p_1 & \text{if } n = 1 \\
p_1 \lor p_2 & \text{if } n = 2 \\
(p_1 \lor \cdots \lor p_{n-1}) \lor p_n & \text{if } n > 2
\end{cases}
\]

Thus \( p \lor q \lor r \) stands for \( (p \lor q) \lor r \). We call \( p_1 \lor \cdots \lor p_n \) the disjunction of \( \{p_1, \ldots, p_n\} \). The reason that for \( n = 0 \) we take this disjunction to be \( \bot \) is that we want a disjunction to be true if and only if (at least) one of the disjuncts is true. Similarly, the conjunction \( p_1 \land \cdots \land p_n \) of \( \{p_1, \ldots, p_n\} \) is defined by replacing everywhere \( \lor \) by \( \land \) and \( \bot \) by \( \top \) in the definition of \( p_1 \lor \cdots \lor p_n \).

**Definition.** A *truth assignment* is a map \( t : A \rightarrow \{0, 1\} \). We extend such a \( t \) to \( \hat{t} : \text{Prop}(A) \rightarrow \{0, 1\} \) by requiring

(i) \( \hat{t}(\top) = 1 \)
(ii) \( \hat{t}(\bot) = 0 \)
(iii) \( \hat{t}(\neg p) = 1 - \hat{t}(p) \)
(iv) \( \hat{t}(p \lor q) = \max(\hat{t}(p), \hat{t}(q)) \)
(v) \( \hat{t}(p \land q) = \min(\hat{t}(p), \hat{t}(q)) \)

Note that there is exactly one such extension \( \hat{t} \) by unique readability. To simplify notation we often write \( t \) instead of \( \hat{t} \).

**Exercise.** Let \( t : A \rightarrow \{0, 1\} \). Show that \( t(p \rightarrow q) = 1 \) if and only if \( t(p) \leq t(q) \), and that \( t(p \leftrightarrow q) = 1 \) if and only if \( t(p) = t(q) \).

**Remark.** Suppose \( a_1, \ldots, a_n \) are the distinct atoms that occur in \( p \), and we know how \( p \) is built up from those atoms. Then we can compute in a finite number of steps \( t(p) \) from \( t(a_1), \ldots, t(a_n) \). In particular, if \( t, t' : A \rightarrow \{0, 1\} \) and \( t(a_i) = t'(a_i) \) for \( i = 1, \ldots, n \), then \( t(p) = t'(p) \).

**Definition.** We say that \( p \) is a *tautology* (notation: \( \vdash p \)) if \( t(p) = 1 \) for all \( t : A \rightarrow \{0, 1\} \). We say that \( p \) is *satisfiable* if \( t(p) = 1 \) for some \( t : A \rightarrow \{0, 1\} \).

Thus \( \top \) is a tautology, and \( p \lor \neg p, p \rightarrow (p \lor q) \) are tautologies for all \( p \) and \( q \). One can verify whether any given \( p \) with exactly \( n \) distinct atoms in it is a tautology by computing \( 2^n \) numbers and checking that these numbers all come out 1. (To do this accurately by hand is already cumbersome for \( n = 5 \), but computers can handle somewhat larger \( n \). Fortunately, other methods are often efficient for special cases.)

**Remark.** Note that \( \vdash p \leftrightarrow q \) if and only if \( t(p) = t(q) \) for all \( t : A \rightarrow \{0, 1\} \). We call \( p \) equivalent to \( q \) if \( \vdash p \leftrightarrow q \). Note that “equivalent to” defines an equivalence relation on \( \text{Prop}(A) \).

The lemma below gives a useful list of equivalences. We leave it to the reader to verify them.
Lemma 2.2.  

(i) \( \vdash (p \lor p) \leftrightarrow p \) and \( \vdash (p \land p) \leftrightarrow p \) (Idempotent Law)

(ii) \( \vdash (p \land q) \leftrightarrow (q \land p) \) and \( \vdash (p \lor q) \leftrightarrow (q \lor p) \) (Commutativity)

(iii) \( \vdash (p \lor (q \land r)) \leftrightarrow ((p \lor q) \land r) \) and \( \vdash (p \land (q \lor r)) \leftrightarrow ((p \land q) \lor r) \) (Associativity)

(iv) \( \vdash (p \land q) \leftrightarrow (q \land p) \) and \( \vdash (p \lor q) \leftrightarrow (q \lor p) \) (Distributivity)

(v) \( \vdash (p \lor (p \land q)) \leftrightarrow (p \land (p \lor q)) \leftrightarrow p \) (Absorption Law)

(vi) \( \vdash \neg (p \lor q) \leftrightarrow (\neg p \land \neg q) \) and \( \vdash (p \land q) \leftrightarrow (\neg p \lor \neg q) \) (De Morgan Law)

(vii) \( \vdash (p \lor \neg p) \leftrightarrow \top \) and \( \vdash (p \land \neg p) \rightarrow \bot \) (Double Negation Law)

Let \((p_i)_{i \in I}\) be a family of propositions with finite index set \(I\), and choose a bijection \(k \mapsto i(k) : \{1, \ldots, n\} \rightarrow I\) and set

\[
\bigvee_{i \in I} p_i = p_{i(1)} \lor \cdots \lor p_{i(n)} \quad \bigwedge_{i \in I} p_i = p_{i(1)} \land \cdots \land p_{i(n)}
\]

If \(I\) is clear from context we just write \(\bigvee_i p_i\) and \(\bigwedge_i p_i\) instead. Of course, the notations \(\bigvee_{i \in I} p_i\) and \(\bigwedge_{i \in I} p_i\) can only be used when the particular choice of bijection of \(\{1, \ldots, n\}\) with \(I\) does not matter.

Next we define “model of \(\Sigma\)” and “tautological consequence of \(\Sigma\).

Definition. Let \(\Sigma \subseteq \text{Prop}(A)\). A model of \(\Sigma\) is a truth assignment \(t : A \rightarrow \{0, 1\}\) such that \(t(\sigma) = 1\) for all \(\sigma \in \Sigma\). We say \(p\) is a tautological consequence of \(\Sigma\) (written \(\Sigma \models p\)) if \(t(p) = 1\) for every model \(t\) of \(\Sigma\). Note that \(\vdash\) \(p\) is the same as \(\emptyset \models p\).

Proposition 2.3. Let \(\Sigma \subseteq \text{Prop}(A)\) and \(p, q \in \text{Prop}(A)\). Then

(i) \(\Sigma \models p \land q\) if and only if \(\Sigma \models p\) and \(\Sigma \models q\).

(ii) \(\Sigma \models p\) implies that \(\Sigma \models p \lor q\).

(iii) \(\Sigma \cup \{p\} \models q\) if and only if \(\Sigma \models p \rightarrow q\).

(iv) If \(\Sigma \models p\) and \(\Sigma \models p \rightarrow q\) then \(\Sigma \models q\) (Modus ponens).