# The Foundation of Mathematics.

## A rigorous development from the beginning.

Eleftherios Gkioulekas.

# Chapter 1

# Mathematical logic

## Propositional logic

- A proposition is any statement that is either true or false. We say that the truth value of a proposition is 1 when the proposition is true, and 0 when the proposition is false.
- notation: We use latin letters, such as $p, q, r, s, t$, to denote propositions. We write $p \vdash 1$ when a proposition is true and $p \vdash 0$ when it is false.
- An atomic proposition is a proposition whose expression is not a combination of other propositions. With any mathematical theory we must postulate a collection of propositions that are atomic. We must also establish a mechanism for constructing more complicated propositions from atomic ones.
- In propositional logic, the only means for composing propositions is logical operations. In first-order logic, we may also compose propositions with quantifiers.

## Standard logical operations

- A logical operation defines a proposition from one or two other propositions, called consistuents, whose truth value depends only on the truth values of the consistuent propositions.
- The standard logical operations are defined by writing a table that lists all the possible combinations of the consistuent proposition truth values and the corresponding truth value of the composite proposition defined with the specific logical operation. We call such tables, truth tables.

- The following truth table summarizes the definitions of the standard logical operations.

| $p$ | $q$ | $p \wedge q$ | $p \vee q$ | $p \veebar q$ | $\neg p$ | $p \Rightarrow q$ | $p \Leftrightarrow q$ |
|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 0 | 0 | 1 | 1 |
| 1 | 0 | 0 | 1 | 1 | 0 | 0 | 0 |
| 0 | 1 | 0 | 1 | 1 | 1 | 1 | 0 |
| 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 |

## Interpretation of standard logical operations

### 1) Conjuction $\boxed{p \wedge q}$

Conjuction means "and". For example:

$p$ : Joe is a man
$q$ : Joe is bald
$p \wedge q$ : Joe is a man and he is bald.

### 2) Disjuction: $\boxed{p \vee q}$

Disjuction is a non-exclusive "or".

$p \vee q$ : $p$ is true or $q$ is true
: at least one of $p, q$ is true
: either $p$ is true, or $q$ is true, or they are both true.

### 3) Exclusive disjuction $\boxed{p \veebar q}$

Exclusive disjuction is "either ... or ..."

$p \veebar q$ : either $p$ is true or $q$ is true (but not both)
one of $p, q$ is true (but not both)
only one of $p, q$ is true

▶ When encoding sentences in propositional logic it is very important to distinguish carefully between disjuction and exclusive disjuction. ◀

### 4) Negation $\boxed{\neg p}$

Negation is "not".

$\neg p$ : $p$ is not true.
$p$ is false.
it is not true that $p$.

5) Implication $\boxed{p \Rightarrow q}$

$p \Rightarrow q$ : If $p$ is true, then $q$ is true
$p$ implies $q$
$q$ is true if $p$ is true
$p$ is true only if $q$ is true (!!)
$q$ is true provided that $p$ is true
$q$ is a necessary condition for $p$
$p$ is a sufficient condition for $q$.

▶ A proposition of the form $p \Rightarrow q$ is called a conditional proposition. We call $p$ the hypothesis and $q$ the conclusion. The statement $p \Rightarrow q$ is false if $p$ is true and $q$ is false. Otherwise, it is true, even when the hypothesis is false!! ◀

6) Equivalence $\boxed{p \Leftrightarrow q}$

$p \Leftrightarrow q$ : $p$ and $q$ are equivalent
$p$ is true if and only if $q$ is true
$p$ and $q$ are either both true or both false.
$p$ is a necessary and sufficient condition for $q$
$p$ and $q$ imply each other.

▶ A proposition of the form $p \Leftrightarrow q$ is called an equivalence and it means, if it is true, that $p$ and $q$ always have the same truth value. ◀

• Notation : For convenience we will also denote the negation $\neg p$ of $p$ as: $\overline{p}$. We will use this notation to reduce the number of parenthesis in involved expressions.

## Propositional expressions

A <u>propositional expression</u> is an expression that defines a proposition by a sequence of logical operations on atomic propositions.

<u>example</u>: $(p \wedge q) \Rightarrow r$ is a propositional expression.

▶ In a propositional expression we use parenthesis to indicate which logical operations are performed first. The following conventions allow us to drop some unnecessary parenthesis:

a) There is no need to place parenthesis in expressions of the form $p \vee q \vee \cdots \vee r$ and $p \wedge q \wedge \cdots \wedge r$ because any placement of parenthesis yields an equivalent expression.

b) Conjuction ("$\wedge$"), disjuction ("$\vee$"), and exclusive disjuction ("$\veebar$") have precedence over implication ("$\Rightarrow$") and equivalence ("$\Leftrightarrow$")

c) Negation ("$\neg$") has precedence over all the other logical operations. ◀

<u>examples.</u>

1) $p \wedge q \Rightarrow r$ means $(p \wedge q) \Rightarrow r$ and not $p \wedge (q \Rightarrow r)$

2) $p \vee q \wedge r$ is ambiguous. We need to distinguish $(p \vee q) \wedge r$ from $p \vee (q \wedge r)$.

3) $\neg p \wedge q$ means $(\neg p) \wedge q$ and not $\neg (p \wedge q)$.
However, the notation $\bar{p} \wedge q$ is prefered for such cases.

- A propositional expression is a <u>tautology</u> if and only if it is always true, for every possible combination of truth values assigned to the atomic propositions that compose it.
- A propositional expression is a <u>contradiction</u> if and only if it is always false, for every possible combination of truth values assigned to the atomic propositions that compose it.

## Examples

1. Show that the expression $\overline{p \wedge q} \leftrightarrow \bar{p} \vee \bar{q}$ is a tautology.

If $p \vdash 0$ and $q \vdash 0$, then

$$(\overline{p \wedge q} \leftrightarrow \bar{p} \vee \bar{q}) \vdash (\overline{0 \wedge 0} \leftrightarrow \bar{0} \vee \bar{0}) = (\bar{0} \leftrightarrow 1 \vee 1) = (1 \leftrightarrow 1) = 1$$

If $p \vdash 0$ and $q \vdash 1$, then

$$(\overline{p \wedge q} \leftrightarrow \bar{p} \vee \bar{q}) \vdash (\overline{0 \wedge 1} \leftrightarrow \bar{0} \vee \bar{1}) = (\bar{0} \leftrightarrow 1 \vee 0) = (1 \leftrightarrow 1) = 1$$

If $p \vdash 1$ and $q \vdash 0$, then.

$$(\overline{p \wedge q} \leftrightarrow \bar{p} \vee \bar{q}) \vdash (\overline{1 \wedge 0} \leftrightarrow \bar{1} \vee \bar{0}) = (\bar{0} \leftrightarrow 0 \vee 1) = (1 \leftrightarrow 1) = 1.$$

If $p \vdash 1$ and $q \vdash 1$, then

$$(\overline{p \wedge q} \leftrightarrow \bar{p} \vee \bar{q}) \vdash (\overline{1 \wedge 1} \leftrightarrow \bar{1} \vee \bar{1}) = (\bar{1} \leftrightarrow 0 \vee 0) = (0 \leftrightarrow 0) = 0.$$

Therefore, $\overline{p \wedge q} \leftrightarrow \bar{p} \vee \bar{q}$ is a tautology.

2. Show that the expression $p \wedge \bar{p}$ is a contradiction.

If $p \vdash 0$, then $p \wedge \bar{p} \vdash 0 \wedge \bar{0} = 0 \wedge 1 = 0$
If $p \vdash 1$, then $p \wedge \bar{p} \vdash 1 \wedge \bar{1} = 1 \wedge 0 = 0$
Therefore $p \wedge \bar{p}$ is a contradiction.

To show that an expression is a tautology or a contradiction, we evaluate its truth value for every possible combination of truth values of the atomic propositions that compose it.

# Exercises

1. Show that the following expressions are tautologies:
   a) $p \veebar q \leftrightarrow (p \wedge \bar{q}) \vee (\bar{p} \wedge q)$.
   b) $(p \Rightarrow q) \leftrightarrow \neg(p \wedge \bar{q})$.
   c) $(p \leftrightarrow q) \leftrightarrow (p \wedge q) \vee (\bar{p} \wedge \bar{q})$.

2. Translate the following sentences into a propositional expressions by introducing symbols for atomic propositions.
   a) Henry can see the bottom of the pool only if the water is clear.
   b) If John testifies and tells the truth, he will be found guilty; and if he does not testify, he will still be found guilty.
   c) Bob will go to hell, unless he repents his sins and praises the Lord Vader, or unless hell freezes over.
   d) Bill is not pleasent but he is very rich and greedy.
   e) Life is interesting when bad things happen, however life is also interesting when interesting things happen.
   f) A sentence is stupid when it makes no sense or when a stupid person says it.
   g) One of Bill or Steve murdered Bob, unless Bob commited suicide first.
   h) If you drink the poison you will either die or become ill, unless you are immune to it.

3. Show that $(p \Rightarrow q) \leftrightarrow (\bar{p} \Rightarrow \bar{q})$ is not a tautology, but that $(p \Rightarrow q) \leftrightarrow (\bar{q} \Rightarrow \bar{p})$ is a tautology.

## Remarkable tautologies.

1) Commutative laws

$(p \wedge q) \Leftrightarrow (q \wedge p)$.

$(p \vee q) \Leftrightarrow (q \vee p)$

$(p \veebar q) \Leftrightarrow (q \veebar p)$.

2) Associative laws

$(p \wedge q) \wedge r \Leftrightarrow p \wedge (q \wedge r)$

$(p \vee q) \vee r \Leftrightarrow p \vee (q \vee r)$

$(p \veebar q) \veebar r \Leftrightarrow p \veebar (q \veebar r)$.

3) Distributive laws

$p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r)$.

$p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r)$.

4) De Morgan's laws

$\overline{p \vee q} \Leftrightarrow \bar{p} \wedge \bar{q}$

$\overline{p \wedge q} \Leftrightarrow \bar{p} \vee \bar{q}$

5) Reduction laws.

$p \veebar q \Leftrightarrow (p \wedge \bar{q}) \vee (\bar{p} \wedge q)$.

$(p \Rightarrow q) \Leftrightarrow \neg(p \wedge \bar{q}) \Leftrightarrow \bar{p} \vee q$

$(p \Leftrightarrow q) \Leftrightarrow (p \wedge q) \vee (\bar{p} \wedge \bar{q})$.

6) Double negation

$\neg(\neg p) \Leftrightarrow p$

7) Law of excluded middle

$p \vee \bar{p}$

These tautologies can be proved by evaluating the truth value for every combination of truth values for $p, q, r$. Then, we can use them to prove other tautologies.

▶ **Natation:** We write: $p_1 \Rightarrow p_2 \Rightarrow p_3 \Rightarrow \cdots \Rightarrow p_n$ as abbreviation for:

$(p_1 \Rightarrow p_2) \wedge (p_2 \Rightarrow p_3) \wedge \cdots \wedge (p_{n-1} \Rightarrow p_n)$

Similarly, we write: $p_1 \Leftrightarrow p_2 \Leftrightarrow \cdots \Leftrightarrow p_n$ as abbreviation for:

$(p_1 \Leftrightarrow p_2) \wedge (p_2 \Leftrightarrow p_3) \wedge \cdots \wedge (p_{n-1} \Leftrightarrow p_n)$ ◀

▶ **Methodology:** One way to show that an expression is a tautology, is to show that it is equivalent to another expression which is obviously always true.

- •1 Use the reduction laws to obtain an expression that involves only conjuction, disjuction and negation.
- •2 Manipulate the resulting expression and simplify it using the law of the excluded middle. ◀

<u>example</u> : Show that $p\wedge(p\Rightarrow q)\Rightarrow q$ is a tautology:

$$[p\wedge(p\Rightarrow q)\Rightarrow q] \Leftrightarrow [\overline{(p\wedge(p\Rightarrow q))}\vee q] \Leftrightarrow$$

$$\Leftrightarrow [(\bar{p}\vee\overline{(p\Rightarrow q)})\vee q] \Leftrightarrow$$

$$\Leftrightarrow [(\bar{p}\vee(p\wedge\bar{q}))\vee q] \Leftrightarrow$$

$$\Leftrightarrow [((\bar{p}\vee p)\wedge(\bar{p}\vee\bar{q}))\vee q] \Leftrightarrow$$

$$\Leftrightarrow [(\bar{p}\vee\bar{q})\vee q] \Leftrightarrow [\bar{p}\vee(\bar{q}\vee q)] \Leftrightarrow$$

$$\Leftrightarrow [\bar{p}\vee 1] \Leftrightarrow 1. \quad \square$$

<u>Exercise</u> : Show that the following expressions are tautologies:

a) $\bar{p}\wedge(p\vee q)\Rightarrow q$.
b) $(p\Rightarrow q)\wedge(q\Rightarrow p)\Leftrightarrow(p\Leftrightarrow q)$.
c) $(p\Rightarrow q)\wedge(q\Rightarrow r)\Rightarrow(p\Rightarrow r)$.
d) $(p\Rightarrow q)\wedge\bar{q}\Rightarrow\bar{p}$
e) $(p\Rightarrow q)\Rightarrow(\bar{q}\Rightarrow\bar{p})$.

Write the meaning of these expressions using English sentences.

## ▼ Propositional theory of inference

Inference theory is the semantic interpretation of propositional logic. Even though propositional logic is not strong enough to express modern mathematics, it can still be used to solve simple problems, and it is a starting point for constructing first-order logic.

- A propositional mathematical theory $T$ is
  a) a collection of atomic propositions $\alpha_1, \alpha_2, \dots, \alpha_m$
  b) a collection of propositional expressions $p_1, p_2, \dots, p_n$ of the atomic propositions, which we call axioms., and which we assume to be true (have truth value $1$).
- We say that a theory $T$ is consistent if it is possible to assign truth values to the atomic propositions $\alpha_1, \alpha_2, \dots, \alpha_m$ such that $(p_1 \wedge p_2 \wedge \cdots \wedge p_n) \vdash 1$
  Otherwise we say that $T$ is inconsistent.

▶ In order for a theory to be useful and interesting, it must be consistent. ◀

▶ notation : If $T$ is a theory with axioms $p_1, p_2, \dots, p_n$ then we define $ax(T)$ to be the expression:

$$\boxed{ax(T) : p_1 \wedge p_2 \wedge \cdots \wedge p_n}$$

which represents the conjuction of all the axioms ◀

- Let $T$ be a theory and $q$ a propositional expression. We say that $T \models q$ (the theory $T$ predicts $q$) if and only if the expression:

$$ax(T) \Rightarrow q$$

is a tautology. When that happens, we can then claim that the truth value of $q$ is also $1$, within the theory $T$.

▶ Remark : Broadly speaking, mathematics is the systematic study of theories. In every theory, we have a collection of statements, the axioms, which we assume as true, and then we develop the theory by finding what other statements $q$ the theory predicts. Some of these statements are deemed important, either because they have some subjective practical value, or because they can be used to further develop the theory. We call these statements <u>theorems</u>. Some other statements, that follow from the theory, may be called:

a) <u>Corollaries</u>: if they are direct or obvious consequences of a theorem

b) <u>Lemmas</u>: if they are specialized statements which, so far as we can tell, are only useful in proving a given theorem, or a collection of theorems.

Of course, if we do not care to describe a statement by any of these names, we can simply call it a <u>proposition</u>.

The purpose of a mathematical theory is usually to model physical reality so that we can reason about it and make logical predictions. Sometimes we may develop <u>abstract</u> theories to

a) investigate a hypothetical "reality" that could have been true and compare it with, what we think is our reality.

b) generalize a collection of theories under a broader theory such that every one of these theories, and hopefully many more, can be shown to be special cases of the general theory. This way we only need to develop one theory instead of many.

Given a theory, the mathematical questions that we want to ask are:

a) What are the axioms of $T$?

b) Is the theory consistent?

c) Are any of the axioms redundant?
(An axiom $p$ of a theory $T$ is <u>redundant</u> if $T' \models p$ where $T'$ is the theory that we obtain if we remove the axiom $p$ from $T$)

d) What predictions can we make from the axioms?

A non-mathematical, but also important question, is:
"What reality does the theory $T$ model? Are the axioms strong enough to predict all the statements that 'should' be true in that reality?"

These questions are non-mathematical because they can ~~al~~ only be answered by subjective judgement. Nevertheless, a mathematician often needs to consider these issues seriously. ◀

## Further remarks about theories

1) When a theory $T$ is <u>inconsistent</u>, it predicts a contradiction. In symbols, $T \models 0$.
2) Two theories $T_1$ and $T_2$ are <u>equivalent</u> when they make the same predictions. That happens when
   $\alpha x(T_1) \Leftrightarrow \alpha x(T_2)$ is a tautology.
3) A theory $T'$ is an <u>extension</u> of another theory $T$ if all the predictions of $T$ are also predictions of $T'$. That happens when
   $\alpha x(T') \Rightarrow \alpha x(T)$ is a tautology.
   We obtain extensions when we add axioms to a theory or when we make the existing axioms stronger.
4) A theory $T$ is <u>trivial</u> when $\alpha x(T)$ is a tautology. A trivial theory has no essential content and the only statements that it is capable of "predicting" are already tautologies. In other words, a trivial theory is equivalent to a theory that has no axioms.

## ▼ Formal proofs in propositional logic

Let $T$ be a given theory. In propositional logic we give meaning to the statement $T \models q$ by saying that it is true if and only if the statement $ax(T) \Rightarrow q$ is a tautology. This <u>is</u> the inference theory for propositional logic. Unfortunately, the inference theory for first-order logic can not be stated so directly. It may only be expressed with the notion of "<u>formal proof</u>". We want to introduce first-order logic by extending the notion of formal proofs, as they are used in propositional logic. So we will first define what a formal proof is in propositional logic, and show you what conventions are used for writing down one.

- Let T be a propositional mathematical theory, and let $\mathcal{P} = (p_1, p_2, \dots, p_n)$ be an ordered sequence of propositions. We say that $\mathcal{P}$ is a <u>proof</u> in T if it can be constructed by the following rules:
  1) We may introduce any axiom of T at any place in $\mathcal{P}$.
  2) We may introduce a statement $p$ if there are preceding statements $q_1, q_2, \dots, q_k$ in the derivation and
     $q_1 \wedge q_2 \wedge \dots \wedge q_k \Rightarrow p$ is a tautology.
  3) We may introduce any statement $p$, if we use it at least once in rule 4. (we call $p$ an "<u>assumption</u>").
  4) If $p'$ is an assumption and there are statements $q_1, q_2, \dots, q_k$ such that
     $p' \wedge q_1 \wedge q_2 \wedge \dots \wedge q_k \Rightarrow r$ is a tautology
     then we may introduce the statement $p' \Rightarrow r$.
     (the statements $q_1, q_2, \dots, q_k$ may or may not be assumptions themselves but they don't count as used if they are).

- Let $\mathcal{P} = (p_1, p_2, \dots, p_n)$ be a proof in a theory T. For every proposition $p$ in $\mathcal{P}$ we define a list of propositions also from $p$, which we denote $\mathcal{D}(p)$, and call "the <u>dependencies</u> of $p$", according to the following rules:
  1) If $p$ was introduced by rule 1 (it is an axiom of T) then $\mathcal{D}(p) = \{p\}$. (it depends only on itself).
  2) If $p$ was introduced by rule 2, then it depends on all the dependencies of $q_1, q_2, \dots, q_k$: $\mathcal{D}(p) = \bigcup_{i=1}^{k} \mathcal{D}(q_i)$.
  3) If $p$ was an assumption, then it depends only on itself.
  4) If $p : p' \Rightarrow r$ was introduced by rule 4, using assumption $p'$ then it depends on all the dependencies of $r$ except for the dependencies of $p$. In set-theoretic notation (which we will introduce later)
     $$\mathcal{D}(p) = \mathcal{D}(r) - \mathcal{D}(p') = \bigcup_{i=1}^{k} \mathcal{D}(q_i).$$

  ► By construction, for every $p$, $\mathcal{D}(p)$ will contain either axioms of T or axioms and assumptions. Since the conjuction of the propositions in $\mathcal{D}(p)$ tautologically implies $p$, if $\mathcal{D}(p_n)$ contains only axioms then the proof $\mathcal{P}$ shows that $ax(T) \Rightarrow p_n$ is a tautology, therefore $T \vDash p_n$. We say then that $\mathcal{P}$ is a formal proof of the statement $p_n$. ◄

Based on this reasoning, we give the following definition:

► <u>Definition</u>: Let $T$ be a mathematical theory and $p$ a proposition. We say that $p$ can be <u>derived</u> from $T$, which we denote $T \vdash p$, if and only if there is a proof $\mathcal{P}$ on $T$ such that all of the following are true:
a) $p$ is the last proposition in $\mathcal{P}$.
b) $\mathcal{A}(p)$ contains only axioms of $T$. ◄

and we have the following "meta-theorem":

<u>Theorem</u>: If $T$ is a mathematical theory and $p$ a proposition then: $(T \vDash p) \Leftrightarrow (T \vdash p)$.

► <u>Remark</u>: We have "shown" that if there is a formal proof for $p$, then $p$ is true. If $p$ is true, we can construct a formal proof for it. Why are formal proofs useful? In general, to show that $T \vDash p$ we could show that $ax(T) \Rightarrow p$ is a tautology. Unfortunately:
1) This is often very difficult. With a formal proof we have to work with many simpler tautologies instead of one complicated one.
2) We may use the formal proof definition to make logic more powerful by adding more rules. This provides an intuitive way of defining 1st-order logic! ◄

► <u>Remark</u>: A paradox in our discussion is that we have used logic to prove that logic works! In fact we have used <u>2nd-order logic</u> to show that propositional logic works! There is no way to avoid this circular argument. It is important then to note that we have only shown that logic does not disprove itself; we have not <u>and can not</u> prove logic! ◄

▸ <u>notation</u>: To present a formal proof $\mathcal{P}$ we write a sequence of lines of the form:

| | | |
|---|---|---|
| $\mathcal{A}(p_1)$ | 1. $p_1$ | Remark |
| $\mathcal{A}(p_2)$ | 2. $p_2$ | Remark |
| ..... | ..... | ..... |
| $\mathcal{A}(p_n)$ | n. $p_n$ | Remark |

In the first column we list the dependencies of the step. In the second column we list the proposition of the step, and we label the step with a number. The remark, in the third column, explains which rule we have used to introduce this step and it can be one of the following:

Axiom $\mapsto$ if the proposition is an axiom
Assumption $\mapsto$ if the proposition is an assumption
$m, n, \dots, k$ T $\mapsto$ if the proposition is tautologically implied by the propositions labeled $m, n, \dots, k$.
$m, n, \dots, k$ CP $\mapsto$ if we have used rule 4 to use up an assumption.

If we use a tautology, we may mention the name of the tautology in parenthesis ◂

## Useful tautological implications

| | |
|---|---|
| $p \wedge (p \Rightarrow q) \Rightarrow q$ | law of detachment |
| $\overline{q} \wedge (p \Rightarrow q) \Rightarrow \overline{p}$ | modus tollendo tollens |
| $\overline{p} \wedge (p \vee q) \Rightarrow q$ | modus tollendo ponens |
| $p \wedge q \Rightarrow p$ | law of simplification |
| $(p \Rightarrow q) \wedge (q \Rightarrow r) \Rightarrow (p \Rightarrow r)$. | law of hypothetical syllogism |
| $[(p \wedge q) \Rightarrow r] \Rightarrow [p \Rightarrow (q \Rightarrow r)]$ | law of exportation |
| $[p \Rightarrow (q \Rightarrow r)] \Rightarrow [(p \wedge q) \Rightarrow r]$. | law of importation |
| $[p \Rightarrow (q \wedge \overline{q})] \Rightarrow \overline{p}$ | law of absurdity. |
| $p \Rightarrow p \vee q$ | law of addition |

▸ These tautologies can be derived using the remarkable tautologies that we have introduced earlier. We can use them when we write formal proofs to introduce T-steps ◂

<u>example</u>: Let T be a theory with the following axioms:

$A_1$ : $p \Rightarrow (q \Rightarrow r)$

$A_2$ : $\bar{s} \vee p$

$A_3$ : $q$

Show that $s \Rightarrow r$

<u>Proof</u>

| | | |
|---|---|---|
| {1} | 1. $s$ | Assumption |
| {2} | 2. $\bar{s} \vee p$ | Axiom |
| {1,2} | 3. $p$ | 1,2 T (modus tollendo ponens). |
| {4} | 4. $p \Rightarrow (q \Rightarrow r)$ | Axiom |
| {1,2,4} | 5. $q \Rightarrow r$ | 3,4 T (detachment). |
| {6} | 6. $q$ | Axiom |
| {1,2,4,6} | 7. $r$ | 5,6 T (detachment) |
| {2,4,6}. | 8. $s \Rightarrow r$ | 1,7 CP |

Since {2,4,6} are all axioms : $T \models (s \Rightarrow r)$. □.

<u>example</u>: Let T be a theory with the following axioms

A1 : $p \Rightarrow q \vee r$

A2 : $q \Rightarrow \bar{p}$

A3 : $s \Rightarrow \bar{r}$

Show that $p \Rightarrow \bar{s}$

<u>Proof</u>

| | | |
|---|---|---|
| {1} | 1. $p$ | Assumption |
| {2} | 2. $p \Rightarrow q \vee r$ | Axiom |
| {1,2} | 3. $q \vee r$ | 1,2 T (detachment). |
| {4} | 4. $q \Rightarrow \bar{p}$ | Axiom |
| {1,4} | 5. $\bar{q}$ | 1,4 T (modus tollendo tollens) |
| {1,2,4} | 6. $r$ | 3,5 T (modus tollendo ponens) |
| {7} | 7. $s \Rightarrow \bar{r}$ | Axiom |
| {1,2,4,7} | 8. $\bar{s}$ | 6,7 T (modus tollendo tollens) |
| {2,4,7} | 9. $p \Rightarrow \bar{s}$ | 1,8 CP |

Since {2,4,7} are all axioms $T \models (p \Rightarrow \bar{s})$.

▸ Remarks

a) Although formal proofs are completely mechanical, it is important to understand the <u>meaning</u> of every step. Use intuition to be sure you use the rules correctly. At the same time, be aware of which rule of logic (and later, which theorem or proposition) you invoke at every step.

b) It usually helps the clarity of a proof to introduce any axiom just before the first time that you need to use it. ◂

## Exercises

1. Suppose that $a1: p \vee q \Rightarrow r$ and $a2: r \Rightarrow q$ are true. Show that $p \Rightarrow q$.

2. Suppose that $\bar{q} \vee r \Rightarrow \bar{p}$ and $s \wedge q \Rightarrow r$, are both true. Show that $p \Rightarrow \bar{s}$

3. If prices are high, then wages are also high. It is not possible for prices to be low and to have price controls at the same time. Also, if there are price controls, then there is no inflation. Show that if there is an inflation, then the wages are high.

4. If Bill Gates is in jail, then he is not a nuisance to the world. If he is not in jail, then the stockholders are happy. Show that it's not possible to keep the stockholders happy, and keep Bill Gates from being a nuisance to the world at the same time.

## Consistency of propositional theories.

- A propositional theory is <u>inconsistent</u> if $T \vDash 0$, that is if it is possible to derive a contradiction from its axioms.
- A propositional theory is <u>consistent</u> if it is not inconsistent.

→ To show that a theory T is consistent, we demonstrate an assignment of truth-values to the atomic propositions such that all the axioms are true.

<u>example</u>: Show that $a_1: p \vee q \Rightarrow r$ $\quad a_2: \bar{p} \Rightarrow \bar{q}$ are consistent.

<u>Proof</u>: Let $p \vdash 1$, $q \vdash 0$, $r \vdash 1$.

Then $a_1 \vdash [(1 \vee 0) \Rightarrow 1] \vdash [1 \Rightarrow 1] \vdash 1$

$a_2 \vdash [\bar{1} \Rightarrow \bar{0}] \vdash [0 \Rightarrow 1] \vdash 1$

Therefore $a_1, a_2$ are consistent. □

→ To show that a theory T is a ~~contradiction~~ inconsistent, we write a formal proof that derives a contradiction.

<u>example:</u> Show that $a_1: p \Rightarrow q$, $a_2: q \Rightarrow r$, $a_3: s \Rightarrow \bar{r}$ and $a_4: p \wedge s$ are inconsistent.

<u>Proof</u>

| | | |
|---|---|---|
| $\{1\}$ | 1. $p \wedge s$ | Axiom |
| $\{1\}$ | 2. $p$ | 1T (simplification) |
| $\{1\}$ | 3. $s$ | 1T (simplification) |
| $\{4\}$ | 4. $p \Rightarrow q$ | Axiom |
| $\{1,4\}$ | 5. $q$ | 2,4T (detachment) |
| $\{6\}$ | 6. $q \Rightarrow r$ | Axiom |
| $\{1,4,6\}$ | 7. $r$ | 5,6T (detachment) |
| $\{8\}$ | 8. $s \Rightarrow \bar{r}$ | Axiom |
| $\{1,8\}$ | 9. $\bar{r}$ | 3,8T (detachment) |
| | 10. $r \wedge \bar{r}$ | 7,9T |

But $r \wedge \bar{r}$ is a contradiction, therefore the axioms $a_1, a_2, a_3, a_4$ are inconsistent. □

▶ To show inconsistency, the tedious alternative is to show that at least one axiom is violated by <u>any possible</u> assignment of truth values to the atomic propositions. Deriving a contradiction is obviously a smarter approach. ◀

One reason why we prefer theories to be consistent is because there is no practical usefulness to a theory from which we can derive a tautologically false proposition. A mathematical reason is that inconsistent theories are trivial; there is nothing worth proving because of the following metatheorem:

Theorem: Let $T$ be an inconsistent theory and $p$ an arbitrary proposition. Then $T \models p$.

Proof

If $T$ inconsistent, then $ax(T) \vdash 0$.
Because $[0 \Rightarrow 0] \vdash 1$ and $[0 \Rightarrow 1] \vdash 1$, $ax(T) \Rightarrow p$ is tautologically true. Then we have:

| | | | |
|---|---|---|---|
| $\{1\}$ | 1. $ax(T)$ | Axiom | |
| $\{2\}$ | 2. $p$ | 1T | $(ax(T) \Rightarrow p)$ |

therefore $T \models p$ □

Since any statement can be "derived" from an inconsistent theory, mathematically speaking, $T$ is very uninteresting.

## Exercises

(1) Which of the following theories are consistent? Which are inconsistent? Supply the appropriate proof.

a) $a_1: p \Rightarrow q \wedge r$, $a_2: q \Rightarrow p \wedge s$, $a_3: s \Rightarrow \bar{r}$
b) $a_1: p \Rightarrow q$, $a_2: q \Leftrightarrow r$, $a_3: r \vee s \Leftrightarrow \bar{q}$
c) $a_1: \neg(\bar{q} \vee p)$, $a_2: p \vee \bar{r}$, $a_3: q \Rightarrow r$
d) $a_1: \bar{p} \wedge q \Rightarrow \bar{r}$, $a_2: p \veebar (q \wedge r)$.
e) $a_1: p \wedge q \Rightarrow \bar{r}$, $a_2: q \wedge r \Rightarrow \bar{p}$, $a_3: r \wedge p \Rightarrow \bar{q}$
f) $a_1: p \Leftrightarrow (q \Rightarrow r)$, $a_2: p \veebar \bar{q}$, $a_3: q \vee r$
g) $a_1: \bar{p} \wedge q \Leftrightarrow r$, $a_2: q \wedge r$, $a_3: p \veebar q$.

## The reductio ad absurdum method

This is a method of indirect proof that is based on the following theorem:

<u>Theorem</u> : Let $T_1, T_2$ be two theories and $p$ a proposition such that $ax(T_2) : ax(T_1) \wedge \bar{p}$.
If $T_1$ consistent and $T_2$ inconsistent, then $T_1 \models p$.

<u>Proof</u>

$T_2$ inconsistent $\Rightarrow ax(T_2) \vdash 0 \Rightarrow ax(T_1) \wedge \bar{p} \vdash 0 \Rightarrow$
$\Rightarrow [ax(T_1) \wedge \bar{p} \rightarrow q \wedge \bar{q}]$ is tautologically true
In $T_1$ we can now construct a proof for $T_1 \models p$:

| | | | |
|---|---|---|---|
| $\{1\}$ | 1. | $ax(T_1)$ | Axiom |
| $\{2\}$ | 2. | $\bar{p}$ | Assumption |
| $\{1,2\}$ | 3. | $ax(T_1) \wedge \bar{p}$ | 1,2 T |
| $\{1,2\}$ | 4. | $q \wedge \bar{q}$ | 3 T $[ax(T_1) \wedge \bar{p} \rightarrow q \wedge \bar{q}]$. |
| $\{1\}$ | 5. | $\bar{p} \rightarrow (q \wedge \bar{q})$ | 2,4 CP |
| $\{1\}$ | 6. | $p$ | 5 T (law of absurd) |

theorefore: $T_1 \models p$. □

a) This proof uses the law of absurd which is the following tautology: $[\bar{p} \rightarrow (q \wedge \bar{q})] \rightarrow p$.
b) It is not necessary for the theory $T_1$ to be consistent. In fact, if $T_1$ is inconsistent then $T_1 \models p$ unconditionally. However such a derivation does not really have any meaning and it is not what a mathematician would ever intend to do. To prove $p$ true, the absurdity must be caused by assuming $p$, not by another inconsistency of our theory $T_1$.
c) This theorem essentially works like a "subroutine" in writing a formal proof. It allows us to use a derived law of logic, which we will denote as RAA, which is an implicit use of CP on the law of absurd. We use it like this:

| | | | |
|---|---|---|---|
| $\{1\}$ | 1. $\bar{p}$ | Assumption | |
| $\{2\}$ | 2. $ax(T)$ | Axioms. | |
| ........................ | | | |
| $\{1,2\}$ | 3. $q \wedge \bar{q}$ | All previous steps. | |
| $\{2\}$ | 4. $p$ | 1,3 RAA. | ← (*) short cut. |

d) The RAA method is usually useful for proving negative statements of the form $\neg p$. Then we just introduce $p$ as an assumption and prove a contradiction.

<u>Example</u>: Suppose that $a_1: p \Rightarrow q$, $a_2: \bar{q} \vee r$, $a_3: \neg(p \wedge r)$. Show that $p$ is false.

<u>Proof</u>

| | | | |
|---|---|---|---|
| $\{1\}$ | 1. | $p$ | Assumption |
| $\{2\}$ | 2. | $p \Rightarrow q$ | Axiom |
| $\{1,2\}$ | 3. | $q$ | 1,2 T (detachment). |
| $\{4\}$ | 4. | $\bar{q} \vee r$ | Axiom |
| $\{1,2,4\}$ | 5. | $r$ | 3,4 T (modus tollendo ponens). |
| $\{6\}$ | 6. | $\neg(p \wedge r)$ | Axiom |
| $\{6\}$ | 7. | $\bar{p} \vee \bar{r}$ | 6 T (De Morgan's law). |
| $\{1,2,4,6\}$ | 8. | $\bar{p}$ | 5,7 T (modus tollendo ponens) |
| $\{1,2,4,6\}$ | 9. | $p \wedge \bar{p}$ | 1,8 T |
| $\{2,4,6\}$. | 10. | $\bar{p}$ | 1,9 RAA □ |

▶ Note that the implicit invokation of CP in the RAA method removes the dependency of the assumption. As soon as that dependency is removed, we have a proof of the last proposition so far. Depending on what that is we may either want to continue the proof or stop at that point. ◀

## The separation by cases method

This method can be used to reduce a proof into two easier proofs. It uses the following result:

**Theorem**: Let $T$ be a theory and $T_1, T_2$ two extended theories with:

$$ax(T_1): \ ax(T) \wedge q$$
$$ax(T_2): \ ax(T) \wedge \bar{q}$$

where $q$ is an arbitrary proposition.
If $T_1 \models p$ and $T_2 \models p$, then $T \models p$.

**Proof**

$ax(T) \wedge q \Rightarrow p$ is a tautology, because $T_1 \models p$ (1)
$ax(T) \wedge \bar{q} \Rightarrow p$ is a tautology, because $T_2 \models p$ (2)
Now we prove that $T \models p$, using the RAA method.

| | | | |
|---|---|---|---|
| $\{1\}$ | 1. | $\bar{p}$ | Assumption. |
| $\{1\}$ | 2. | $\neg[ax(T) \wedge q]$ | 1T (contrapositive on (1)). |
| $\{1\}$ | 3. | $\overline{ax(T)} \vee \bar{q}$ | 2T (De Morgan's law) |
| $\{4\}$ | 4. | $ax(T)$ | Axioms. |
| $\{1,4\}$ | 5. | $\bar{q}$ | 3,4T (modus tollendo ponens). |
| $\{1,4\}$ | 6. | $ax(T) \wedge \bar{q}$ | 4,5T |
| $\{1,4\}$ | 7. | $p$ | 6T (tautology (2)). |
| $\{1,4\}$ | 8. | $p \wedge \bar{p}$ | 1,7T |
| $\{4\}$ | 9. | $p$ | 1,8 RAA |

therefore $T \models p$ □

This proof is a very elaborate example of a "meta-proof". It is a proof about logic, but it is a solid proof, just like the proof for the RAA method. The way you should think about these proofs is as patterns of derivation which always work, and which can be applied when the theorem applies on an arbitrary theory. It is always possible to take a proof that uses these methods and expand it by writting out the pertinent steps explicitly, and thus get a proof that uses only the elementary rules of logic and does indeed prove $T \models p$.

▶ <u>notation</u> : A formal proof that uses the seperation of cases method usually takes the following form:

| | | | |
|---|---|---|---|
| $\{1\}$ | 1. $ax(T)$ | Axioms | |
| $\{2\}$ | 2. $q$ | Assumption | |
| ........ | ........ | ........ | $T_1 \models p$ proof |
| $\{1,2\}$ | 3. $p$ | Previous steps. | |
| $\{4\}$ | 4. $\bar{q}$ | Assumption | |
| ........ | ........ | ........ | $T_2 \models p$ proof |
| $\{1,4\}$ | 5. $p$ | Previous steps. | |
| $\{1\}$ | 6. $p$ | 3,5 SCM ⟵ (*) | |

Steps 3 and 5 prove $T_1 \models p$ and $T_2 \models p$ correspondingly, but each by itself does not prove $T \models p$ because they depend on one of the assumptions that we have made — either $q$ or $\bar{q}$. However, combining steps 3,5, we can invoke the seperation by cases method (which we denote as SCM) to introduce $p$ again in a new statement removing the dependencies on steps 2 and 4. In other words, we claim $T \models p$, as the theorem of separation of cases concludes. Of course, like RAA, the SCM rule is a <u>derived rule</u>, a shorthand for omitting its elaborate proof from the body of this proof. ◀

<u>example</u>: Suppose that $a_1: q \Rightarrow p$, $a_2: q \vee r$, $a_3: \bar{q} \Rightarrow s$, $a_4: s \wedge r \Rightarrow p$. Show that $p$ is true.

<u>Proof</u>

| | | |
|---|---|---|
| $\{1\}$ | 1. $q$ | Assumption |
| $\{2\}$ | 2. $q \Rightarrow p$ | Axiom |
| $\{1,2\}$ | 3. $p$ | 1,2 T (detachment). |
| $\{4\}$ | 4. $\bar{q}$ | Assumption |
| $\{5\}$ | 5. $q \vee r$ | Axiom |
| $\{4,5\}$ | 6. $r$ | 4,5 T (modus tollendo ponens). |
| $\{7\}$ | 7. $\bar{q} \Rightarrow s$ | Axiom |
| $\{4,7\}$ | 8. $s$ | 4,7 T (detachment). |
| $\{4,9,7\}$ | 9. $s \wedge r$ | 6,8 T |
| $\{10\}$ | 10. $s \wedge r \Rightarrow p$ | Axiom |
| $\{4,5,7,10\}$ | 11. $p$ | 9,10 T (detachment). |
| $\{2,5,7,10\}$ | 12. $p$ | 3,11 SCM ▫ |