Mathematical (formal) logic and mathematical theories

A. Formal systems, Proof calculi

1. *General characteristics*

A ***proof calculus*** (of a theory) is given by:

- a language
- a set of axioms
- a set of deduction rules

A definition of the ***language*** of the system consists of:

- ***alphabet*** (a non-empty set of symbols)
- ***grammar*** (defines in an inductive way a set of well-formed formulas - WFF)

Example Language of the 1st-order predicate logic.

a) alphabet:
1. logical symbols:
   * (countable set of) individual variables *x, y, z, …*
   * connectives ¬, ∧, ∨, ⊃, ≡
   * quantifiers ∀, ∃
2. special symbols (of arity *n*)
   * predicate symbols P^n, Q^n, R^n, …
   * functional symbols f^n, g^n, h^n, …
   * constants *a, b, c,* – functional symbols of arity 0
3. auxiliary symbols (,), [,], …

b) grammar:
1. terms
   * each constant and each variable is an atomic *term*
   * if $t_1, …, t_n$ are terms, f^n a functional symbol, then $f^n(t_1, …, t_n)$ is a (functional) *term*
2. atomic formulas
   * if $t_1, …, t_n$ are terms, P^n predicate symbol, then $P^n(t_1, …, t_n)$ is an *atomic (well-formed) formula*
3. composed formulas
   * let A, B be well-formed formulas. Then ¬A, (A∨B), (A∧B), (A⊃B), (A≡B), are *well-formed formula*s.
   * let A be a well-formed formula, *x* a variable. Then ∀*x*A, ∃*x*A are *well-formed formulas.*
4. Nothing is a WFF unless it so follows from 1.-3.

Notes Outmost left/right brackets will be omitted whenever no confusion can arise. Thus, e.g., P(*x*) ∧ Q(*x*) is a well formed formula. Predicate symbols P, Q of arity 0 are WFF formulas as well (they correspond to the propositional logic formulas p, q, ...).

A set of axioms is a chosen subset of the set of WFF.

These axioms are considered to be basic formulas that are not being proved.

Example: {p ∨ ¬p, p ⊃ p}.

A set of deduction rules of a form: $A_1,\ldots,A_m$ |– $B_1,\ldots,B_m$ enables us to prove *theorems* (*provable formulas*) of the calculus. We say that each B_i is derived from the set of assumptions $A_1,\ldots,A_m$.

Example: $p \supset q, p$ |– q

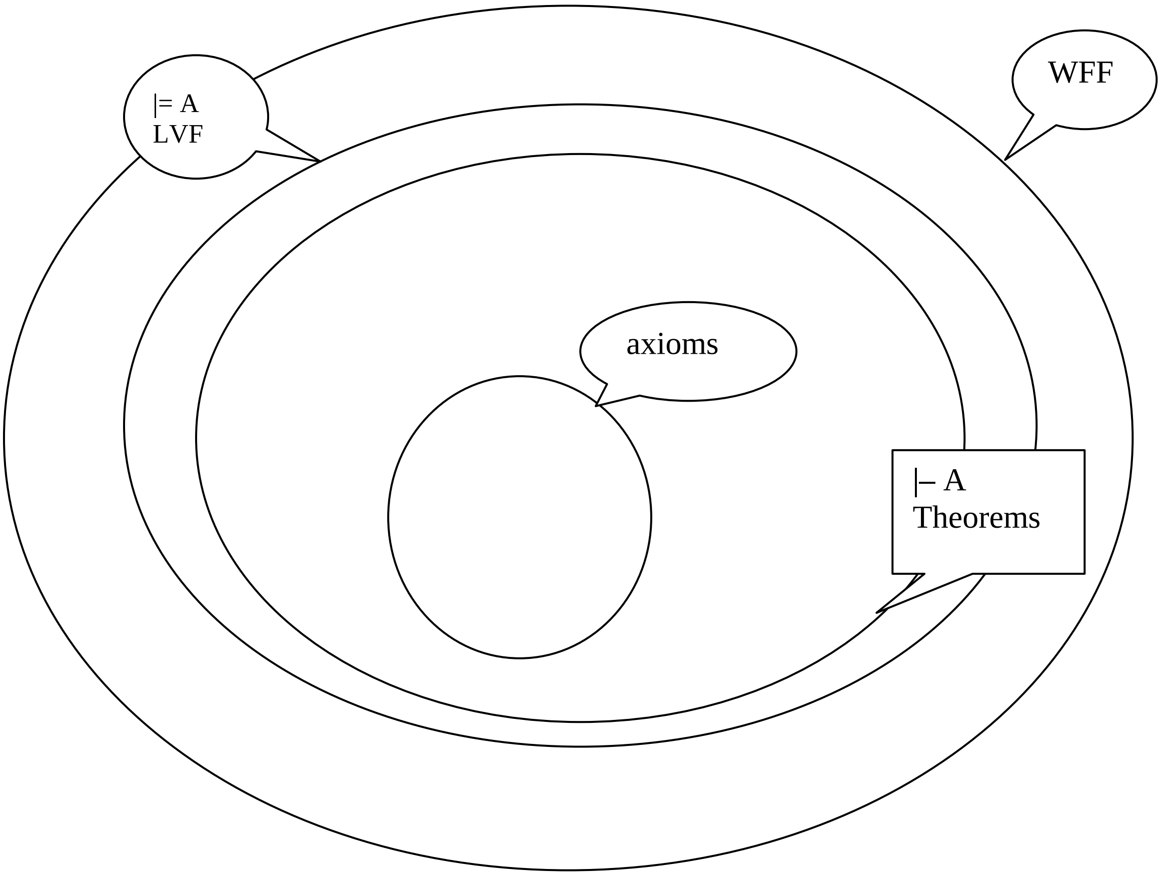
$p \wedge q$ |– p, q

A proof of a formula A (from logical axioms of the given calculus) is a sequence of formulas (proof steps) $B_1,\ldots B_n$ such that:

- $A = B_n$ (the proved formula A is the last step)
- each B_i ($i=1,\ldots,n$) is either
  - an axiom or
  - B_i is derived from the previous B_j ($j=1,\ldots,i-1$) using a deduction rule of the calculus.

A formula A is ***provable*** by the calculus, denoted |– A, if there is a proof of A in the calculus. A provable formula is called a ***theorem.***

The following Figure 1 illustrates particular sets of formulas:



A proof of a formula A from assumptions $A_1,\dots,A_m$ is a sequence of formulas (proof steps) $B_1,\dots B_n$ such that:

- $A = B_n$ (the proved formula A is the last step)
- each B_i ($i=1,\dots,n$) is either
  - an axiom, or
  - an assumption A_k ($1 \le k \le m$), or
  - B_i is derived from the previous B_j ($j=1,\dots,i-1$) using a rule of the calculus.

A formula ***A*** is ***provable from $A_1,\dots,A_m$***, denoted ***$A_1,\dots,A_m$ |– A***, if there is a proof of A from $A_1,\dots,A_m$.

Logical calculus is ***sound***, if each theorem is logically valid, symbolically:

If **|– A then |= A**, for all the formulas A.

An indirect proof of a formula A from assumptions $A_1,\dots,A_m$ is a sequence of formulas (proof steps) $B_1,\dots B_n$ such that:

- each B_i ($i=1,\dots,n$) is either
  - an axiom, or
  - an assumption A_k ($1 \le k \le m$), or
  - an assumption ¬A of indirect proof (formula A that is to be proved is negated)
  - B_i is derived from the previous B_j ($j=1,\dots,i-1$) using a rule of the calculus.
  - Some B_k contradicts to B_l , i.e., $B_k = \neg B_l$ ($k \in \{1,...,n\}$, $l \in \{1,...,n\}$)

A semantically correct (sound) logical calculus serves for proving logically valid formulas (tautologies). In this case axioms have to be logically valid formulas (true under all interpretations), and deduction rules have to make it possible to prove logically valid formulas. For that reason the rules are either truth-preserving or tautology preserving, i.e., $A_1,\dots,A_m$ |– $B_1,\dots,B_m$ can be read as follows: if all the formulas $A_1,\dots,A_m$ are logically valid formulas, then $B_1,\dots,B_m$ are logically valid formulas.

Logical calculus is ***complete***, if each logically valid formula is a theorem, symbolically:

If |= A then |– A, for all the formulas A.

In a sound and complete calculus the set of theorems and logically valid formulas (LVF) are identical:

|= A iff |– A

A sound proof calculus should meet the following Theorem of Deduction.

Theorem of deduction. A formula φ is provable from assumptions $A_1,\dots,A_m$, iff the formula $A_m \supset \varphi$ is provable from $A_1,\dots,A_{m-1}$.

Symbolically:

$A_1,\dots,A_m$ |– φ iff $A_1,\dots,A_{m-1}$ |– $A_m \supset \varphi$.

In a sound calculus meeting the Deduction Theorem the following implication holds:

If $\boldsymbol{A_1,\ldots,A_m} \models\!\!- \varphi$ then $\boldsymbol{A_1,\ldots,A_m} \models \varphi$.

If the calculus is sound and complete, then provability coincides with logical entailment:

$\boldsymbol{A_1,\ldots,A_m} |\!- \varphi$ iff $\boldsymbol{A_1,\ldots,A_m} \models \varphi$.

Proof. If the Theorem of Deduction holds, then

$A_1,\ldots,A_m |\!- \varphi$ iff $|\!- (A_1 \supset (A_2 \supset \ldots (A_m \supset \varphi)\ldots))$.
$|\!- (A_1 \supset (A_2 \supset \ldots (A_m \supset \varphi)\ldots))$ iff $|\!- (A_1 \wedge \ldots \wedge A_m) \supset \varphi$.
If the calculus is sound and complete, then
$|\!- (A_1 \wedge \ldots \wedge A_m) \supset \varphi$ iff $\models (A_1 \wedge \ldots \wedge A_m) \supset \varphi$.
$\models (A_1 \wedge \ldots \wedge A_m) \supset \varphi$ iff $A_1,\ldots,A_m \models \varphi$.

(The first equivalence is obtained by applying the Deduction Theorem *m*-times, the second is valid due to the soundness and completeness, the third one is the semantic equivalence.)

Remarks.

1) ***The set of axioms*** of a calculus is non-empty and ***decidable*** in the set of WFFs (otherwise the calculus would not be reasonable, for we couldn't perform proofs if we did not know which formulas are axioms). It means that there is an algorithm that for any WFF φ given as its input answers in a finite number of steps an output Yes or NO on the question whether φ is an axiom or not. A finite set is trivially decidable. The set of axioms can be infinite. In such a case we define the set either by an algorithm of creating axioms or by a finite set of ***axiom schemata.*** The set of axioms should be ***minimal,*** i.e., each axiom is independent of the other axioms (not provable from them).

2) ***The set of deduction rules*** enables us to perform proofs mechanically, considering just the symbols, abstracting of their semantics. Proving in a calculus is a ***syntactic method***.

3) A natural demand is a ***syntactic consistency*** of the calculus. A calculus is consistent iff there is a WFF φ such that φ is not provable (*in an inconsistent calculus everything is provable*). This definition is equivalent to the following one: a calculus is consistent iff a formula of the form A ∧ ¬A, or ¬(A ⊃ A), is not provable. A calculus is syntactically consistent iff it is sound (semantically correct).

4) For the 1st order predicate logic there are *sound* and *complete* calculi. They are, e.g., ***Hilbert style calculus, natural deduction*** and ***Gentzen calculus.***

5) There is another property of calculi. To illustrate it, let's raise a question: having a formula φ, does the calculus *decide* φ? In other words, is there an algorithm that would answer Yes or No, having φ as input and answering the question whether φ is logically valid or no? If there is such an algorithm, then the calculus is ***decidable.***

If the calculus is complete, then it proves all the logically valid formulas, and the proofs can be described in an algorithmic way. However, in case the input formula φ is not logically valid, the algorithm does not have to answer (in a final number of steps). Indeed, there are *no decidable 1st order predicate logic calculi, i.e.,* ***the problem of logical validity is not decidable***.

6) The relation of *provability* ($A_1,\ldots,A_n$ |– A) and the relation of *logical entailment* ($A_1,\ldots,A_n$ |= A) are ***distinct relations.*** Similarly, the set of theorems |– A (of a calculus) is generally not identical to the set of logically valid formulas |= A. The former is *syntactic and defined within a calculus,* the latter *independent of a calculus, it is* *semantic.* In a sound calculus the set of theorems is a subset of the set of logically valid formulas. In a sound and complete calculus the set of theorems is identical with the set of formulas.

The reason why proof calculi have been developed can be traced back to the end of 19th century. At that time formalization methods had been developed and various paradoxes arose. All those paradoxes arose from the assumption on the existence of actual infinities. To avoid paradoxes, D. Hilbert (a significant German mathematician) proclaimed the *program of formalisation of mathematics.* The idea was simple: to avoid paradoxes we will use only finitist methods: first, start with a decidable set of certainly (logically) true formulas, use truth preserving rules of deduction, and infer all the logical truths. Second, begin with some sentences true in an area of interest (interpretation), use truth-preserving rules of deduction, and infer all the truths of this area. In particular, he intended to axiomatise in this way mathematics, to avoid paradoxes.

Hilbert supposed that these goals can be met. Kurt **Gödel** (the greatest logician of the 20th century) proved *the completeness of the 1st order predicate calculus*, which was expected. He even proved the strong completeness: if SA |= T then SA **|–** T (SA – a set of assumptions). But Hilbert wanted more: he supposed that all the truths of mathematics can be proved in this mechanic finite way. That is, that a theory of arithmetic (e.g. Peano) is complete in the following sense: each formula is in the theory ***decidable***, i.e., the theory proves either the formula or its negation, which means that all the formulas true in *the intended interpretation* over the set of natural numbers are provable in the theory:

Gödel’s ***theorems on incompleteness*** give a surprising result: ***there are true but not provable sentences of natural numbers arithmetic***. Hence Hilbert program is not fully realisable.

2. Natural deduction calculus

Definition 1 *Axioms, deduction rules schemata***.**

Axioms:	$A \vee \neg A, A \supset A$		
conjunction:	$A, B \vdash A \wedge B$		IC
	$A \wedge B \vdash A, B$		EC
disjunction:	$A \vdash A \vee B$ or $B \vdash A \vee B$		ID
	$A \vee B, \neg A \vdash B$ or $A \vee B, \neg B \vdash A$		ED
Implication:	$B \vdash A \supset B$		II
	$A \supset B, A \vdash B$	EI	*modus ponens* **MP**
equivalence:	$A \supset B, B \supset A \vdash A \equiv B$		IE
	$A \equiv B \vdash A \supset B, B \supset A$		EE
General quantifier:	$A(x) \vdash \forall x A(x)$		I∀

The rule can be used only if formula $A(x)$ is not derived from any assumption that would contain variable x as free.

	$\forall x A(x) \vdash A(x/t)$	E∀

Formula $A(x/t)$ is a result of correctly substituting the term t for the variable x.

Existential quantifier	$A(x/t) \vdash \exists x A(x)$	I∃
	$\exists x A(x) \vdash A(x/c)$	E∃

where *c* is a constant not used as yet in the language. If the rule is used for distinct formulas A’, then a different constant has to be used. A more general form of the rule is:

$\forall y_1 \ldots \forall y_n \exists x\, A(x, y_1,\ldots,y_n) \vdash \forall y_1 \ldots \forall y_n\, A(\, x / f(y_1,\ldots,y_n), y_1,\ldots,y_n\,)$ E∃

Notes

1. In natural deduction calculus an indirect proof is often used.
2. Existential quantifier elimination has to be done in accordance to the rules of Scolemisation in the general resolution method.
3. Rules derivable from the above:

- $A(x) \supset B \vdash \forall x A(x) \supset B$, x is not free in B
- $A \supset B(x) \vdash A \supset \forall x B(x)$, x is not free in A
- $A(x) \supset B \vdash \exists x A(x) \supset B$, x is not free in B
- $A \supset B(x) \vdash A \supset \exists x B(x)$
- $A \supset \forall x B(x) \vdash A \supset B(x)$
- $\exists x A(x) \supset B \vdash A(x) \supset B$

Example Another useful rules and theorems of propositional logic (try to prove them):

Introduction of negation:	$A \vdash \neg\neg A$	IN
Elimination of negation:	$\neg\neg A \vdash A$	EN
Negation of disjunction:	$\neg(A \vee B) \vdash \neg A \wedge \neg B$	ND
Negation of conjunction:	$\neg(A \wedge B) \vdash \neg A \vee \neg B$	NK
Negation of implication:	$\neg(A \supset B) \vdash A \wedge \neg B$	NI
Tranzitivityof implication:	$A \supset B, B \supset C \vdash A \supset C$	TI
Transpozition:	$A \supset B \vdash \neg B \supset \neg A$	TR
Modus tollens:	$A \supset B, \neg B \vdash \neg A$	MT

a) $A \supset B, \neg B \vdash \neg A$ MT

Proof:

1.	$A \supset B$	assumption	
2.	$\neg B$	assumption	
3.	A	assumption of the indirect proof	
4.	B	MP: 1, 3	contradicts to 2., hence $\neg A$ Q.E.D

b) $C \supset D \vdash \neg C \vee D$

Proof:

1.	$C \supset D$	assumption	
2.	$\neg(\neg C \vee D)$	assumption of indirect proof	
3.	$\neg(\neg C \vee D) \supset (C \wedge \neg D)$	de Morgan (see c))	
4.	$C \wedge \neg D$	MP 2,3	
5.	C	EC 4	
6.	$\neg D$	EC 4	
7.	D	MP 1, 5	contradicts to 6, hence
8.	$\neg C \vee D$	(assumption of indirect proof is not true) Q.E.D.	

c) $(\neg A \wedge \neg B) \supset \neg(A \vee B)$ de Morgan

Proof:

1.	$(\neg A \wedge \neg B)$		assumption
2.	$A \vee B$		assumption of indirect proof
3.	$\neg A$		EC
4.	$\neg B$		EC
	5.1.	A	contradicts to 3
	5.2.	B	contradicts to 4.
6.	$\neg(A \vee B)$		Q.E.D. (assumption of indirect proof cannot be true)

d) $A \supset C, B \supset C \vdash (A \vee B) \supset C$

Proof:

1.	$A \supset C$	assumption	
2.	$\neg A \vee C$	rule b)	
3.	$B \supset C$	assumption	
4.	$\neg B \vee C$	rule b)	
5.	$A \vee B$	assumption	
6.	$\neg C$	assumption of indirect proof	
7.	$\neg B$	MT 4, 6	
8.	$\neg A$	MT 2, 6	
9.	$\neg A \wedge \neg B$	IC	
10.	$(\neg A \wedge \neg B) \supset \neg(A \vee B)$	theorem (de Morgan)	
11.	$\neg(A \vee B)$	MP 9, 10	contradicts to 5., hence
12.	C	(assumption of indirect proof is not true) Q.E.D.	

Example (*some proofs of FOL theorems*)

1) $\vdash \forall x\,[A(x) \supset B(x)] \supset [\forall x A(x) \supset \forall x B(x)]$

Proof:

1.	$\forall x\,[A(x) \supset B(x)]$	assumption	
2.	$\forall x A(x)$	assumption	
3.	$A(x) \supset B(x)$	E∀:1	
4.	$A(x)$	E∀:2	
5.	$B(x)$	MP:3,4	
6.	$\forall x B(x)$	I∀:5	Q.E.D.

According to the Deduction Theorem we prove theorems in the form of implication by means of the proof of consequent from antecedent:

$$\forall x\,[A(x) \supset B(x)] \vdash [\forall x A(x) \supset \forall x B(x)] \text{ iff}$$
$$\forall x\,[A(x) \supset B(x)],\ \forall x A(x) \vdash \forall x B(x)$$

2) $\vdash \neg\forall x\, A(x) \equiv \exists x\, \neg A(x)$ (De Morgan rule)

Proof:

⇒:	1.	$\neg\forall x\, A(x)$	assumption		
	2.	$\neg\exists x\, \neg A(x)$	assumption of indirect proof		
		3.1. $\neg A(x)$	hypothesis		
		3.2. $\exists x\, \neg A(x)$	I∃: 3.1		
	4.	$\neg A(x) \supset \exists x\, \neg A(x)$	II: 3.1, 3.2		
	5.	$A(x)$	MT: 4,2		
	6.	$\forall x\, A(x)$	Z∀:5	contradicts to:1	Q.E.D.
⇐:	1.	$\exists x\, \neg A(x)$	assumption		
	2.	$\forall x\, A(x)$	assumption of indirect proof		
	3.	$\neg A(c)$	E∃:1		
	4.	$A(c)$	E∀:2	contradicts to:3	Q.E.D.

Note: In the proof sequence we can introduce a hypothetical assumption H (in this case 3.1.) and derive conclusion C from this hypothetical assumption (in this case 3.2.). As a regular proof step we can then introduce implication H ⊃ C (step 4.).

According to the Theorem of Deduction this theorem corresponds to two rules of deduction:

$$\neg\forall x\, A(x) \vdash \exists x\, \neg A(x), \qquad \exists x\, \neg A(x) \vdash \neg\forall x\, A(x)$$

3) $\vdash \neg\exists x\, A(x) \equiv \forall x\, \neg A(x)$ (De Morgan rule)

Proof:

⇒:	1.	$\neg\exists x\, A(x)$	assumption		
		2.1. $A(x)$	hypothesis		
		2.2. $\exists x\, A(x)$	Z∃:2.1		
	3.	$A(x) \supset \exists x\, A(x)$	ZI: 2.1, 2.2		
	4.	$\neg A(x)$	MT: 3,1		
	5.	$\forall x\, \neg A(x)$	Z∀:4		Q.E.D.
⇐:	1.	$\forall x\, \neg A(x)$	assumption		
	2.	$\exists x\, A(x)$	assumption of indirect proof		
	3.	$A(c)$	E∃: 2		
	4.	$\neg A(c)$	E∀: 1	contradictss to: 3	Q.E.D.

According to the Theorem of Deduction this theorem corresponds to two rules of deduction:

$$\neg\exists x\, A(x) \vdash \forall x\, \neg A(x), \qquad \forall x\, \neg A(x) \vdash \neg\exists x\, A(x)$$

Note: In the second part of the proofs 2), 3) the rule of existential quantifier elimination (E$\exists$) has been used. This rule is not correct, for it is not truth preserving: formula $\exists x\, A(x) \supset A(c)$ is not logically valid (cf. Scolem rule in the resolution method). This rule, however, preserves satisfiability, and in an indirect proof can be used in a correct way.

4) $\vdash \forall x\, [A(x) \supset B(x)] \supset [\exists x A(x) \supset \exists x B(x)]$

Proof:

1.	$\forall x\, [A(x) \supset B(x)]$	assumption	
2.	$\exists x A(x)$	assumption	
3.	$A(a)$	E$\exists$: 2	
4.	$A(a) \supset B(a)$	E$\forall$: 1	
5.	$B(a)$	MP: 3,4	
6.	$\exists x B(x)$	Z$\exists$: 5	Q.E.D.

Note: this is another example of a correct using the rule E$\exists$.

5) $\vdash \forall x\, [A \vee B(x)] \equiv A \vee \forall x B(x)$, where A does not contain variable x free

Proof:

$\Rightarrow$: 1.	$\forall x\, [A \vee B(x)]$	assumption	
2.	$A \vee B(x)$	E$\forall$: 1	
3.	$A \vee \neg A$	axiom	
3.1.	A	1. hypothesis	
3.2.	$A \vee \forall x B(x)$	ZD: 3.1	
4.1.	$\neg A$	2. hypothesis	
4.2.	$B(x)$	ED: 2, 4.1	
4.3.	$\forall x B(x)$	Z$\forall$: 4.2	
4.4.	$A \vee \forall x B(x)$	ZD: 4.3.	
5.	$[A \supset (A \vee \forall x B(x))] \wedge [\neg A \supset (A \vee \forall x B(x))]$		II + IC
6.	$(A \vee \neg A) \supset (A \vee \forall x B(x))$		theorem + MP 5
7.	$A \vee \forall x B(x)$	MP 6, 2	

Q.E.D.

$\Leftarrow$: 1.	$A \vee \forall x B(x)$	Assumption, disjunction of hypotheses	
2.1.	A	1. hypothesis	
2.2.	$A \vee B(x)$	ZD: 2.1	
2.3.	$\forall x\, [A \vee B(x)]$	Z$\forall$: 2.2	
3.	$A \supset \forall x\, [A \vee B(x)]$		
4.1.	$\forall x B(x)$	2. hypothesis	
4.2.	$B(x)$	E$\forall$: 3.1	
4.3.	$A \vee B(x)$	ZD: 3.2	
4.4.	$\forall x\, [A \vee B(x)]$	Z$\forall$: 3.3	
5.	$\forall x B(x) \supset \forall x\, [A \vee B(x)]$	ZI 4.1., 4.4.	
6.	$[A \vee \forall x B(x)] \supset \forall x\, [A \vee B(x)]$	theorem, IC, MP – 3, 5	
7.	$\forall x\, [A \vee B(x)]$	MP 1, 6	Q.E.D.

6) $\vdash (A(x) \supset B) \supset (\forall x A(x) \supset B)$

Proof:

1.	$A(x) \supset B$	assumption
2.	$\forall x A(x)$	assumption
3.	$\neg A(x) \vee B$	rule b) $C \supset D \vdash \neg C \vee D$
4.	$A(x)$	E$\forall$: 2
5.	B	ED: 3,4 Q.E.D.

This theorem corresponds to the rule:

$$A(x) \supset B \vdash \forall x A(x) \supset B$$

Some more examples:

Example 2.3.5:

- Theorém: $(p \supset r) \supset (\neg p \vee r)$

1.	$p \supset r$	assumption
2.	$\neg(\neg p \vee r)$	assumption indirect proof
3.	$\neg(\neg p \vee r) \supset (\neg\neg p \wedge \neg r)$	Theorém ND (de Morgan)
4.	$\neg\neg p \wedge \neg r$	MP: 2.3.
5.	$p \wedge \neg r$	EN: 4.
6.	p	
7.	$\neg r$	EK
8.	r	MP: 1.6. – contr.
9.	$\neg p \vee r$	Q.E.D.

Example 2.3.6:

- Theorém: $[(p \supset r) \wedge (q \supset r)] \supset [(p \vee q) \supset r]$

1.	$[(p \supset r) \wedge (q \supset r)]$	assumption
2.	$(p \supset r)$	EK: 1
3.	$(q \supset r)$	EK: 1
4.	$p \vee q$	assumption
5.	$(p \supset r) \supset (\neg p \vee r)$	Theorém (Example 2.3.5)
6.	$\neg p \vee r$	MP: 2.5.
7.	$\neg r$	assumption indirect proof
8.	$\neg p$	ED: 6.7.
9.	q	ED: 4.8.
10.	r	MP: 3.9. – contr.
11.	r	Q.E.D

Technique of hypothetic assumptions (conditional proof):

In the sequence of formulas of a proof there can be introduced a hypothetical assumption H. If from H and as the case may be from other ordinary assumptions we derive formula D, then the formula $H \supset D$ can be introduced as an ordinary step.

Example 2.3.7:

- Theorém: $[(p \lor q) \supset r] \supset [(p \supset r) \land (q \supset r)]$

Direct proof by with hypothetic assumptions:

1.	$(p \lor q) \supset r$	assumption	
2.1.	p	hypothesis	
2.2.	$p \lor q$	ZD:2.1	
2.3.	r	MP:1,2.2	
3.	$p \supset r$	ZI: $2.1 \supset 2.3$	
4.1.	q	hypothesis	
4.2.	$p \lor q$	ZD:4.1	
4.3.	r	MP:1,4.2	
5.	$q \supset r$	ZI: $4.1 \supset 4.3$	
6.	$(p \supset r) \land (q \supset r)$	ZK:3,5	Q.E.D

- Theorem: $\neg(p \lor q) \supset \neg p \land \neg q$

Indirect proof with hypothetic assumptions:

1.	$\neg(p \lor q)$	assumption	
2.1.	p	hypothesis	
2.2.	$p \lor q$	ZD: 2.1	contr.:1
3.	$\neg p$	because p leads to contr.	
4.1.	q	hypothesis	
4.2.	$p \lor q$	ZD: 4.1	contr.:1
4.	$\neg q$	because p leads to contr.	
5.	$\neg p \land \neg q$	ZK: 3,4	Q.E.D.

The technique of the split proof from hypotheses:

Let in the proof sequence of formula F there is a formula in the form of disjunction: $C_1 \lor C_2 \lor ... \lor C_k$. If the formula F can be proved from each of the additional assumptions C_1, C_2,...,C_k, then the formula F has been proved.

Example 2.3.8:

- Theorém: $(p \supset q) \supset [(p \lor r) \supset (q \lor r)]$

Direct splitting proof:

1.	$p \supset q$	assumption	
2.	$p \lor r$	assumption, disjunction of cases	
3.1.	p	hypothesis of the 1. case	
3.2.	q	MP: 1, 3.1	
3.3.	$q \lor r$	ZD: 3.2	
3.	$p \supset q \lor r$	ZI	
4.1.	r	hypothesis of the 2. case	
4.2.	$q \lor r$	ZD: 4.1	
4.	$r \supset q \lor r$	ZI	
5.	$(p \supset q \lor r) \land (r \supset q \lor r)$	ZK: 3.4.	
6.	$(p \lor r) \supset (q \lor r)$	Theorém: Example 2.3.6, MP	Q.E.D.

- Theorém: $[(p \supset q) \wedge (r \supset s) \wedge \neg(q \vee s)] \supset \neg(p \vee r)$

Indirect splitting proof:

1.	$p \supset q$	assumption	
2.	$r \supset s$	assumption	
3.	$\neg(q \vee s)$	assumption	
4.	$p \vee r$	assumption of indirect proof in the form of disjunction	
5.1.	p	1. hypothesis	
5.2.	q	MP: 1, 5.1	
5.3.	$q \vee s$	ZD: 5.2, contr.:3	Q.E.D.
6.1.	r	2. hypothesis	
6.2.	s	MP: 2, 6.1	
6.3.	$q \vee s$	ZD: 6.2, contr.:3	Q.E.D.

3. Hilbert calculus.

Definition

- ***Language***: Language of the 1st-order predicate logic, but:
  from the *connectives only*: $\supset$ (implication), and $\neg$ (negation)
  the only quantifier: $\forall$ (general)
- ***Axiom schemas***:
  A1: $A \supset (B \supset A)$
  A2: $(A \supset (B \supset C)) \supset ((A \supset B) \supset (A \supset C))$
  A3: $(\neg B \supset \neg A) \supset (A \supset B)$
  A4: $\forall x A(x) \supset A(x/t)$ Term t substitutable for *x* in A
  A5: $(\forall x[A \supset B(x)]) \supset (A \supset \forall x B(x))$, *x* is not free in A
- ***Rule schemas***:
  MP: A, $A \supset B$ |– B (modus ponens)
  G: A |– $\forall x$A (generalization)

Notes:

1. A, B are not formulas, but meta-symbols denoting any formula. Each axiom schema denotes an infinite class of formulas of a given form. If axioms were specified by concrete formulas, like
   1. $p \supset (q \supset p)$
   2. $(p \supset (q \supset r)) \supset ((p \supset q) \supset (p \supset r))$
   3. $(\neg q \supset \neg p) \supset (p \supset q)$

   we would have to extend the set of rules with the *rule of substitution*:
   Substituting in a proved formula for each propositional logic symbol another formula, then the obtained formula is proved as well.
2. The axiomatic system defined in this way works only with the symbols of connectives $\neg$, $\supset$, and quantifier $\forall$. Other symbols of the other connectives and existential quantifier can be introduced as abbreviations *ex definicione*:
   $A \wedge B =_{df} \neg(A \supset \neg B)$
   $A \vee B =_{df} \neg A \supset B$
   $A \equiv B =_{df} (A \supset B) \wedge (B \supset A)$
   $\exists x A =_{df} \neg \forall x \neg A$

   The symbols $\wedge$, $\vee$, $\equiv$ and $\exists$ do not belong to the alphabet of the language of the calculus.
3. In Hilbert calculus we do not indirecet proof.
4. Hilbert calculus defined in this way is ***sound (semantically consistent)***.
   a) All the axioms are logically valid formulas.
   b) The modus ponens rule is truth-preserving.
   The only problem – as you can easily see – is the generalisation rule. This rule is obviously not truth preserving: formula $P(x) \supset \forall x P(x)$ is not logically valid. However, this rule is tautology preserving: if the formula A(*x*) at the left-hand side is logically valid, then $\forall x A(x)$ is logically valid as well. Since the axioms of the calculus are logically valid, the rule is correct.
   After all, this is a common way of proving in mathematics. To prove that something holds for all the triangles, we prove that for *any* triangle.

5. Note that any axiom is a theorem as well. Its proof is a trivial one step proof.

6. To make the proof more comprehensive, you can use in the proof sequence also previously proved formulas (theorems).

Examples:

1. Proof of a formula schema $A \supset A$:

1. $(A \supset ((A \supset A) \supset A)) \supset ((A \supset (A \supset A)) \supset (A \supset A))$	ax. A2	$B/A \supset A$, C/A
2. $A \supset ((A \supset A) \supset A)$	ax. A1	$B/A \supset A$
3. $(A \supset (A \supset A)) \supset (A \supset A)$	MP:2,1	
4. $A \supset (A \supset A)$	ax. A1	B/A
5. $A \supset A$	MP:4,3	Q.E.D.

Hence: $\vdash A \supset A$.

2. Proof of the schema $A \supset C$ from the assumptions $A \supset B$, $B \supset C$ (transitivity of implication TI):

1. $A \supset B$	1. assumption	
2. $B \supset C$	2. assumption	
3. $(A \supset (B \supset C)) \supset ((A \supset B) \supset (A \supset C))$	A2	
4. $(B \supset C) \supset (A \supset (B \supset C))$	A1	$A/(B \supset C)$, B/A
5. $A \supset (B \supset C)$	MP:2,4	
6. $(A \supset B) \supset (A \supset C)$	MP:5,3	
7. $A \supset C$	MP:1,6	Q.E.D.

hence: $A \supset B, B \supset C \vdash A \supset C$.

It is obvious that discovering proofs of even very simple formulas is in Hilbert calculus difficult. The reason is that in Hilbert calculus there are only two rules of deduction. However, when proving simple formulas, these theorems can be used in the other proofs. Since natural deduction (ND) calculus is much easier to use, it is useful to prove first the theorems of it, which can further make the proofs easier.

3. $\vdash A(x/t) \supset \exists x A(x)$
(the ND rule of introducing existential quantifier – existential generalisation)

Proof:

1.	$\forall x \neg A(x) \supset \neg A(x/t)$	ax. schema A4	
2.	$\neg\neg\forall x \neg A(x) \supset \forall x \neg A(x)$	theorem of type $\neg\neg C \supset C$ (see below)	
3.	$\neg\neg\forall x \neg A(x) \supset \neg A(x/t)$	$C \supset D, D \supset E \vdash C \supset E$: 2, 1 TI	
4.	$\neg\exists x A(x) \supset \neg A(x/t)$	Intr. $\exists$ acc. To the definition: 3	
5.	$[\neg\exists x A(x) \supset \neg A(x/t)] \supset [A(x/t) \supset \exists x A(x)]$	ax. schema A3	
6.	$A(x/t) \supset \exists x A(x)$	MP: 4, 5	Q.E.D.

3) $A \supset B(x) \vdash A \supset \forall x B(x)$ $\qquad$ x is not free in A

Proof:

1.	$A \supset B(x)$	assumption	
2.	$\forall x[A \supset B(x)]$	rule of Generalisation: 1	
3.	$\forall x[A \supset B(x)] \supset [A \supset \forall x B(x)]$	ax. schema A5	
4.	$A \supset \forall x B(x)$	MP: 2,3	Q.E.D.

Theorem of Deduction:

Let A be a *closed* formula, B any formula. Then:

$A_1, A_2, \ldots, A_k \vdash A \supset B$ *if and only if* $A_1, A_2, \ldots, A_k, A \vdash B$.

Remark: The statement *if* $\vdash A \supset B$, *then* $A \vdash B$

Is valid universally, not only for A being a closed formula (the proof is obvious – modus ponens).

On the other hand, the other statement

If $A \vdash B$, *then* $\vdash A \supset B$

is ***not valid*** for an open formula A (with at least one free variable).

Example: Let A = A(*x*), B = ∀*x*A(*x*). Then $A(x) \vdash \forall x A(x)$ is valid according to the generalisation rule. But the formula $A(x) \supset \forall x A(x)$ is generally not logically valid, and therefore not provable in a sound calculus.

Proof (we will prove the Deduction Theorem only for the propositional logic)**:**

1. → Let $A_1, A_2, \ldots, A_k \vdash A \supset B$. Then there is a sequence $B_1, B_2, \ldots, B_n$, which is the proof of $A \supset B$ from assumptions $A_1, A_2, \ldots, A_k$. The proof of B from $A_1, A_2, \ldots, A_k$, A is then the sequence of formulas $B_1, B_2, \ldots, B_n$, A, B, where $B_n = A \supset B$ and B is the result of applying modus ponens to formulas B_n and A.

2. ←Let $A_1, A_2, \ldots, A_k, A \vdash B$. Then there is a sequence of formulas $C_1, C_2, \ldots, C_r = B$, which is the proof of B from $A_1, A_2, \ldots, A_k$, A. We will prove by induction that the formula $A \supset C_i$ (for all i = 1, 2,...,r) is provable from $A_1, A_2, \ldots, A_k$. Then also $A \supset C_r$ will be proved.

a) Base of the induction: If the length of the proof is = 1, then for formula C_1 there can be three cases: C_1 is an assumption of A_i, C_1 is an axiom, C_1 is the formula A. In the first two cases the proof of $A \supset C_1$ is the sequence of formulas:

1.	C_1	assumption or axiom
2.	$C_1 \supset (A \supset C_1)$	A1
3.	$A \supset C_1$	MP: 1,2

In the third case we are to prove $A \supset A$ (see example 1).

b) Induction step: we prove that on the assumption of $A \supset C_n$ being proved for *n* = 1, 2, ..., i-1 the formula $A \supset C_n$ can be proved also for *n* = *i*. For C_i there are four cases: C_i is an assumption of A_i, C_i is an axiom, C_i is the formula A, C_i is an immediate consequence of the formulas C_j a $C_k = (C_j \supset C_i)$, where j, k < i. In the first three cases the proof is analogical to a). In the last case the proof of the formula $A \supset C_i$ is the sequence of formulas:

1.	$A \supset C_j$	induction assumption	
2.	$A \supset (C_j \supset C_i)$	induction assumption	
3.	$(A \supset (C_j \supset C_i)) \supset ((A \supset C_j) \supset (A \supset C_i))$	A2	
4.	$(A \supset C_j) \supset (A \supset C_i)$	MP: 2,3	
5.	$A \supset C_i)$	MP: 1,4	Q.E.D

Theorem of soundness (*semantic* consistence):

Each provable formula in the Hilbert calculus is also logically valid formula:

If $\vdash \mathbf{A}$, *then* $\models \mathbf{A}$.

Proof *(outline)***:**

Each formula of the form of an axiom schema of A1 – A5 is logically valid (i.e. true in every interpretation structure I for any valuation of free variables).

Obviously, MP (*modus ponens*) is a truth preserving rule.

A correct using of the generalisation rule $A(x) \vdash \forall x A(x)$ is guaranteed by the definition of satisfying the formula $\forall x A$ by a structure I. Let us assume that $A(x)$ is a proof step such that in the sequence preceding $A(x)$ the generalisation rule has not been used as yet. Hence the formula $A(x)$ must be logically valid (since it has been obtained from logically valid formulas by using at most the truth preserving *modus ponens* rule). It means that in any structure I the formula $A(x)$ is true for any valuation *e* of *x*. Which, by definition, means that $\forall x A(x)$ is logically valid as well.

Remark:

According to the deduction Theorem each theorem of the implication form corresponds to a deduction rule(s), and vice versa. For example:

Theorem:	Rule
$\vdash A \supset ((A \supset B) \supset B)$	$A, A \supset B \vdash B$ (MP rule)
$\vdash A \supset (B \supset A)$ /ax. schema A1/	$A \vdash B \supset A$, and $A, B \vdash A$
$\vdash A \supset A$	$A \vdash A$
$\vdash (A \supset B) \supset ((B \supset C) \supset (A \supset C))$	$A \supset B \vdash (B \supset C) \supset (A \supset C)$ and $A \supset B, B \supset C \vdash A \supset C$ /rule TI/

Example: a few simple theorems and the corresponding (natural deduction) rules:

1.	$\vdash A \supset (\neg A \supset B)$ $\vdash \neg A \supset (A \supset B)$	$A, \neg A \vdash B$	
2.	$\vdash A \supset A \vee B$, $\vdash B \supset A \vee B$	$A \vdash A \vee B$, $B \vdash A \vee B$	ID
3.	$\vdash \neg\neg A \supset A$	$\neg\neg A \vdash A$	EN
4.	$\vdash A \supset \neg\neg A$	$A \vdash \neg\neg A$	IN
5.	$\vdash (A \supset B) \supset (\neg B \supset \neg A)$	$A \supset B \vdash \neg B \supset \neg A$	TR
6.	$\vdash A \wedge B \supset A$, $\vdash A \wedge B \supset B$	$A \wedge B \vdash A, B$	EC
7.	$\vdash A \supset (B \supset A \wedge B)$, $\vdash B \supset (A \supset A \wedge B)$	$A, B \vdash A \wedge B$,	IC
8.	$\vdash A \supset (B \supset C) \supset (A \wedge B \supset C)$	$A \supset (B \supset C) \vdash A \wedge B \supset C$	

Some proofs:

Ad 1. $\vdash A \supset (\neg A \supset B)$, i.e.: $A, \neg A \vdash B$.

Proof:

1.	A	assumption	
2.	$\neg A$	assumption	
3.	$(\neg B \supset \neg A) \supset (A \supset B)$	A3	
4.	$\neg A \supset (\neg B \supset \neg A)$	A1	
5.	$\neg B \supset \neg A$	MP: 2,4	
6.	$A \supset B$	MP: 5,3	
7.	B	MP: 1,6	Q.E.D.

Ad 2. $\vdash A \supset A \lor B$, i.e.: $A \vdash A \lor B$. (the rule ID of the natural deduction)

Using the definition abbreviation $A \lor B =_{df} \neg A \supset B$, we are to prove the theorem: $\vdash A \supset (\neg A \supset B)$, i.e. the rule $A, \neg A \vdash B$, which has been already proved.

Ad 3. $\vdash \neg\neg A \supset A$, i.e.:. $\neg\neg A \vdash A$.

Proof:

1.	$\neg\neg A$	assumption
2.	$(\neg A \supset \neg\neg\neg A) \supset (\neg\neg A \supset A)$	ax. schema A3
3.	$\neg\neg A \supset (\neg A \supset \neg\neg\neg A)$	theorem ad 1.
4.	$\neg A \supset \neg\neg\neg A$	MP: 1,3
5.	$\neg\neg A \supset A$	MP: 4,2
6.	A	MP: 1,5 Q.E.D.

Ad 4. $\vdash A \supset \neg\neg A$, i.e.: $A \vdash \neg\neg A$.

Proof:

1.	A	assumption
2.	$(\neg\neg\neg A \supset \neg A) \supset (A \supset \neg\neg A)$	ax. schema A3
3.	$\neg\neg\neg A \supset \neg A$	theorem ad 3.
4.	$A \supset \neg\neg A$	MP: 3,2 Q.E.D.

Ad 5. $\vdash (A \supset B) \supset (\neg B \supset \neg A)$, i.e.: $A \supset B \vdash \neg B \supset \neg A$.

Proof:

1.	$A \supset B$	assumption
2.	$\neg\neg A \supset A$	theorem ad 3.
3.	$\neg\neg A \supset B$	TI: 2,1
4.	$B \supset \neg\neg B$	theorem ad 4.
5.	$A \supset \neg\neg B$	TI: 1,4
6.	$\neg\neg A \supset \neg\neg B$	TI: 2,5
7.	$(\neg\neg A \supset \neg\neg B) \supset \neg B \supset \neg A$	ax. schema A3
8.	$\neg B \supset \neg A$	MP: 6,7 Q.E.D.

Ad 6. $\vdash A \land B \supset A$, i.e.: $A \land B \vdash A$. (The rule EC of the natural deduction)

Using definition abbreviation $A \land B =_{df} \neg(A \supset \neg B)$ we are to prove $\vdash \neg(A \supset \neg B) \supset A$, i.e.: $\neg(A \supset \neg B) \vdash A$.

Proof:

1.	$\neg(A \supset \neg B)$	assumption
2.	$(\neg A \supset (A \supset \neg B)) \supset (\neg(A \supset \neg B) \supset \neg\neg A)$	theorem ad 5.
3.	$\neg A \supset (A \supset \neg B)$	theorem ad 1.
4.	$\neg(A \supset \neg B) \supset \neg\neg A$	MP: 3,2
5.	$\neg\neg A$	MP: 1,4
6.	$\neg\neg A \supset A$	theorem ad 3.
7.	A	MP: 5,6 Q.E.D.

Some meta-rules:

Let T is any finite set of formulas: $T = \{A_1, A_2,.., A_n\}$. Then the following rules are valid:

(a) *if* $T, A \vdash B$ and A is a theorem, *then* $T \vdash B$.
It is not necessary to state theorems in the assumptions.

(b) *if* $A \vdash B$, *then* $T, A \vdash B$.
(Monotonicity of proving)

(c) *if* $T \vdash A$ and $T, A \vdash B$, *then* $T \vdash B$.

(d) *if* $T \vdash A$ and $A \vdash B$, *then* $T \vdash B$.

(e) *if* $T \vdash A$, $T \vdash B$, $A, B \vdash C$, *then* $T \vdash C$.

(f) *if* $T \vdash A$ and $T \vdash B$, *then* $T \vdash A \wedge B$.
(Consequences can be composed in a conjunction way.)

(g) $T \vdash A \supset (B \supset C)$ *if and only if* $T \vdash B \supset (A \supset C)$.
(The order of assumptions is not important.)

(h) $T, A \vee B \vdash C$ *if and only if* both $T, A \vdash C$ and $T, B \vdash C$.
(Split the proof whenever there is a disjunction in the sequence – meta-rule of the natural deduction)

(i) *if* $T, A \vdash B$ *and if* $T, \neg A \vdash B$, *then* $T \vdash B$.

Notes:

1) meta-rules are useful rules defining relations not between formulas (as the deduction rules do), but between the deduction rules themselves.

2) A proof of the meta-rule is thus a sequence of rules.

Proofs of the meta-rules:

Ad (h):

Let $T, A \vee B \vdash C$, we prove that $T, A \vdash C$ and $T, B \vdash C$.
Proof:

1.	$A \vdash A \vee B$	the rule ID	
2.	$T, A \vdash A \vee B$	meta-rule (b): 1	
3.	$T, A \vee B \vdash C$	assumption	
4.	$T, A \vdash C$	meta-rule (d): 2,3	Q.E.D.
5.	$T, B \vdash C$	analogically to 4.	Q.E.D.

Let $T, A \vdash C$ and $T, B \vdash C$, we prove that $T, A \vee B \vdash C$.
Proof:

1.	$T, A \vdash C$	assumption
2.	$T \vdash A \supset C$	deduction Theorem:1
3.	$T \vdash \neg C \supset \neg A$	meta-rule (d): 2, (the rule TR of natural deduction)
4.	$T, \neg C \vdash \neg A$	deduction Theorem: 3
5.	$T, \neg C \vdash \neg B$	analogical to 4.
6.	$T, \neg C \vdash \neg A \wedge \neg B$	meta-rule (f): 4,5
7.	$\neg A \wedge \neg B \vdash \neg(A \vee B)$	de Morgan rule of natural deduction (prove it!)
8.	$T, \neg C \vdash \neg(A \vee B)$	meta-rule (d): 6,7

9.	$T \vdash \neg C \supset \neg(A \lor B)$	deduction theorem: 8	
10.	$T \vdash A\lor B \supset C$	meta-rule (d): 9. (the rule TR)	
11.	$T, A \lor B \vdash C$	deduction theorem: 10	Q.E.D.

Ad (i):

Let $T, A \vdash B$ and $T, \neg A \vdash B$, we prove $T \vdash B$.

Proof:

1.	$T, A \vdash B$	assumption
2.	$T, \neg A \vdash B$	assumption
3.	$T, A \lor \neg A \vdash B$	meta-rule (h): 1,2
4.	$T \vdash B$	meta-rule (a): 3

Remarks.

Hilbert calculus is ***sound*** and ***complete***: $T \vdash A$ *if and only if* $T \models A$.

The proof of soundness had been outlined above, the proof of the semantic completeness is much more complicated (Post theorem for PL, and so on).

Hilbert calculus is ***not decidable***. There are no decidable calculi for PL1 (the consequence of ***Goedel***'s theorems on incompleteness).

The problem of logical validity is not decidable in the 1st order predicate logic:

Decidability: The existence of an ***algorithm*** that decides every formula. When having a formula F as an input – the algorithm should answer YES or NO on the question whether F is logically valid or not.

The problem of logical validity is ***partially decidable*** in the 1st order predicate logic:
There are algorithms that partially decide every formula. When having a formula F as an input *and* when F is logically valid – the algorithm answers YES. But when A is not logically valid, the algorithm may answer NO, but does not have to answer at all.

B. Formal axiomatic theories

Introduction

1. History.

a) State of the arts: empirical theory describing the area of interest.

- Collecting facts is stressed, without taking into account particular consequences of them and relations-in-intension between them.
- Question “*What* is there?” is more important than the question “*Why* is it so?”.
- Typical problems are solved without any generalization

b) Informal theories:

- Primitive notions are given as basic, well understood, and by means of these primitives the other complex concepts are defined. Primitive basic knowledge is gathered, which is not being proved, but which the basis for deriving other knowledge is.
- A formal symbolic language is used.
- There are no formal rules of inferring and proving, logic is used just intuitively.
- Examples:
    - Euclidean (parabolic) geometry (4th century before Christ).
    - All the mathematical theories till the end of 19th century.
    - Physical theories: mechanics (classical, relativistic, quant), thermodynamics, electromagnetic field theory, optics, ...

c) Axiomatic formal theories:

- Not only knowledge is formalized, but also rules and process of deriving consequences of the knowledge base. Logic is an inseparable part of each theory.
- Formalizing the process of proving is not meaningless. The necessity of formal logic and semantics driven proving has been given by particular antinomies and paradoxes. When these paradoxes appeared in the very foundations of mathematics, a great effort has been devoted to building up correct consistent proof theories.
- Formal theory can be used in a syntactic automatic way, without knowing the semantics of proved statements.

2. ***Antinomies (paradoxes).***

a) Paradox of ***the set of all sets***.

- Let M be a set of all sets. It means that each subset of M is a member of M. From the above it follows, that the cardinality of M is at least (greater than or) equal to the cardinality of the set of all the subsets of M:

$$\text{card (M)} \geq \text{card } (2^{M}).$$

- On the other hand, obviously the set of all the subsets of a nonempty set M has more elements than M (besides having singleton (one member set) elements, it has also a lot of other subsets):

$$\text{card (M)} < \text{card } (2^{M}).$$

This contradicts the above inequality.

b) **Russell's antinomy**

(Russell discovered this contradiction in Frege's *Grundladen of Arithmetik* at the end of 19th century).

i) Obviously, a subset of a set S (in particular the S itself) should not be an element of S. Let us define a *normal set* N such a set which is not its own element. There is a question: Is the set M of all the normal sets normal?

ii) If we answer YES, then M does not contain M as its element, hence M should be normal, which means that M should be an element of M, otherwise M is *not* the set of *all* the normal sets. Contradiction.

iii) If we answer NO, then M is not normal, which means that M contains as its element a set, which is not normal – contradiction.

* ii) and iii) in symbols:

definition: M is a set of all x ($x \in$ M) such that $x \subseteq$ M, and x is normal ($x \notin x$) .

Question: Is M normal?

NO: M is not normal → M $\in$ M;

but M $\subseteq$ M, and *ex definitione* M is normal – contradiction.

YES: M $\notin$ M → M is normal;

but M $\subseteq$ M, and M is normal → M $\in$ M. Contradiction.

- To avoid such inconsistencies in mathematics, German mathematician and logician David **Hilbert** formulated in the beginning of the 20th century the so called

Program of Formalization of Mathematics.

The basic idea was extremely simple:

Choose some obviously ***true*** statements as ***axioms.*** Formulate ***truth preserving rules of inference***. Infer the consequences of axioms (***theorems***). In this way it is insured that all the theorems are true, no inconsistency can arise.

Hilbert believed that ***all the true statements of mathematics*** can be mechanically proved in this way, i.e., using a finite set of rules of inference, and inferring true consequences from a recursively given set of true axioms; hence mathematics would be saved, without inconsistencies. Note that all the inconsistencies arise from the necessity to work with actual ***infinity.***

Hilbert wanted to preserve all the classical mathematics (integral calculus, e.g.) working with infinities, but infinities recursively defined – potential infinities.

- **Goedel**'s results on ***incompleteness*** showed that this program cannot be realized in full.
  - The *consistency of arithmetic* cannot be formally proved by finite means
  - Each theory formalizing and containing arithmetic of natural numbers is *incomplete*. There are arithmetic statements that are neither provable nor refuted.
  - Consequences:
    - there are true arithmetic statements that cannot be proved in any formal theory, and are not consequences of any formal theory.
    - The theory of arithmetic is not decidable.
    - The problem of logical validity is not decidable
    - The set of theorems is not recursive

The most important theories are:

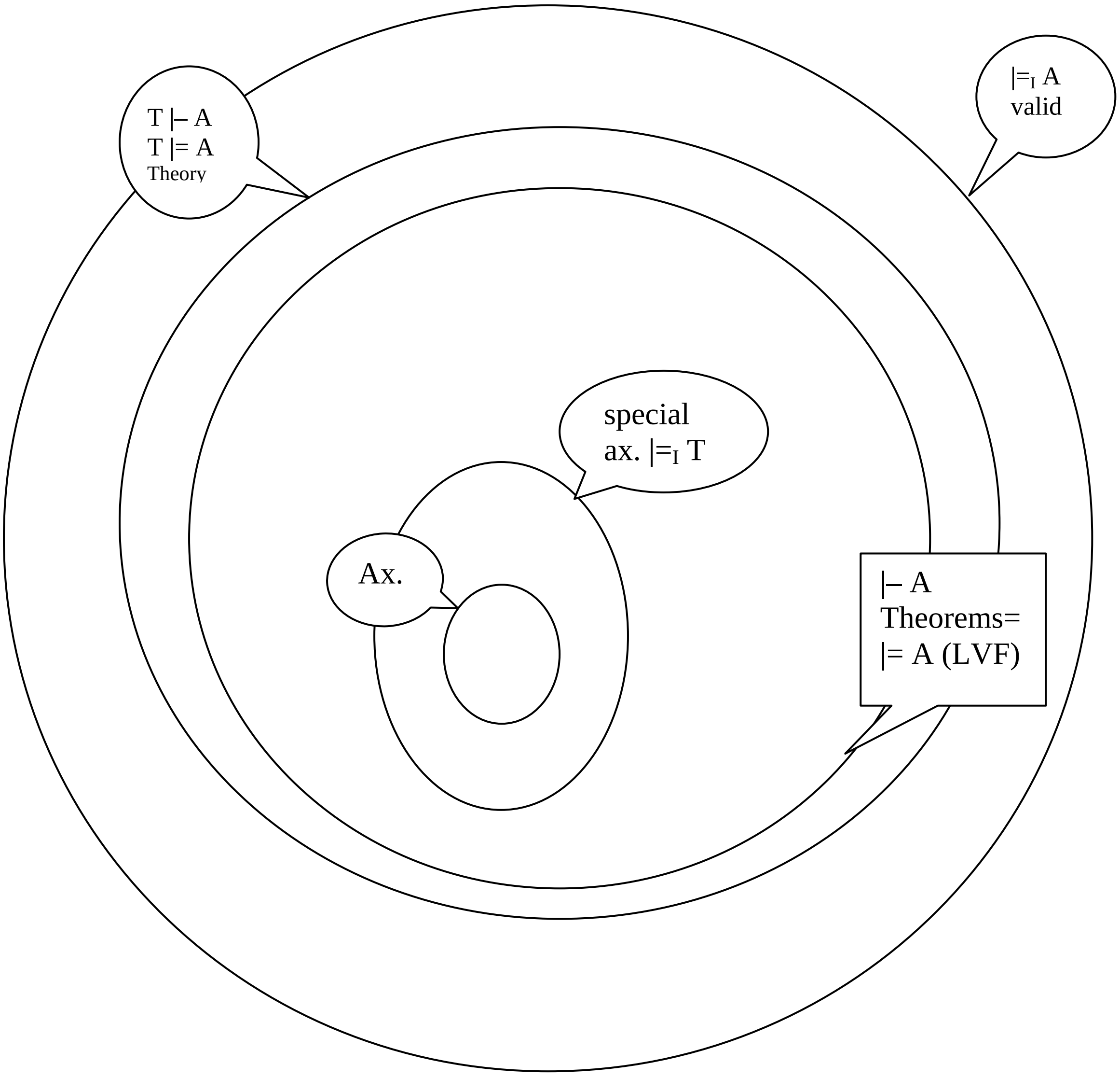
a) Arithmetic theories:

For instance Robinson’s arithmetic or Peano arithmetic, see the paper on Goedel’s results, in particular ***incompleteness***

b) Relational theories: for instance the theories of ordering, and of equivalence

c) Algebraic theories: for instance the theory of groups and lattices

The following figure illustrates ***incompleteness of arithmetic recursive theories***. Provable theorems of the theory (formulas provable from special axioms T |– A) are a subset of the set of all the formulas valid in the intended interpretation I (entailed by the axioms T |= A):
if $|=_I$ T and T |– A, then $|=_I$ A, but not vice versa.



B.1. Formal theory - definitions

Definition B.1.1:

Formal theory is given by:

- formal language
- a set of axioms
- a set of deduction rules

Formal language of the 1st-order theory is a language of the respective proof calculus: a set of well-formed formulas (WFF).

A set of axioms is a subset of the set of all WFF. It consists of:

- a set of ***logical*** axioms (of the respective calculus – logically valid formulas)
- a set of ***special*** axioms. The set of special axioms characterizes by means of formulas properties of relations between objects of a given area of interest. Hence, special axioms are chosen as true in the intended interpretation.

A set of deduction rules is the set of rules of the respective calculus.

In a broader sense a theory is the set of all the formulas that can be proved drom the axioms of the theory. Formal theory is characterized by its set of axioms.

Proof of a formula A in the theory T (denoted T |– A) is a sequence of WFFs (proof steps) such that:

- the last step is the formula A
- each step of the proof is either
  - a logical axiom, or
  - a special axiom, or
  - a formula that is obtained by applying a deduction rule to some previous formulas of the sequence.

Note B.1.1:

1. Proof calculus of FOL (e.g. Hilbert calculus or natural deduction) is a special case of an axiomatic theory. It is a theory without special axioms.

B.2. Relational Theories

B.2.1 Theory of equivalence:

Special constants:

$\Leftrightarrow$ ... binary predicate constant

Logical axioms: axioms of Hilbert calculus

Special axioms:

O1. $\forall x\ (x \Leftrightarrow x)$ reflexivity

O2. $\forall x\ \forall y\ [(x \Leftrightarrow y) \supset (y \Leftrightarrow x)]$ symmetry

O3. $\forall x\ \forall y\ \forall z\ [((x \Leftrightarrow y) \wedge (y \Leftrightarrow z)) \supset (x \Leftrightarrow z)]$ transitivity

B.2.2 Theory of sharp ordering:

1. **variant:**
   - Special constants:
     - = ... binary predicate constant
     - < ... binary predicate constant
   - Logical axioms: axioms of Hilbert calculus
   - Special axioms:

     O1. $\forall x\ (x = x)$ reflexivity
     O2. $\forall x\ \forall y\ [(x=y) \supset (y=x)]$ symmetry
     O3. $\forall x\ \forall y\ \forall z\ [(x=y \wedge y=z) \supset (x=z)]$ transitivity
     O4. $\forall x\ \forall y\ \forall z\ [(x=y \wedge x<z) \supset (y<z)]$
     O5. $\forall x\ \forall y\ \forall z\ [(x=y \wedge z<x) \supset (z<y)]$
     O6. $\forall x\ \forall y\ [(x<y) \supset \neg(y<x)]$ asymmetry
     O7. $\forall x\ \forall y\ \forall z\ [(x<y \wedge y<z) \supset (x<z)]$ transitivity
     O8. $\forall x\ \forall y\ [x=y \vee x<y \vee y<x]$
     O9. $\forall x\ \exists y\ [x<y]$
     O10.$\forall x\ \exists y\ [y<x]$
     O11.$\forall x\ \forall y\ \ [x<y \supset \exists z\ [x<z \wedge z<y]]$

2. **variant:**
   - Special constant:
     < ... binary predicate symbol
   - Logical axioms: axioms of Hilbert calculus
   - Special axioms:

     V1. $\forall x\ \forall y\ [x<y \supset \neg(y<x)]$ asymetry
     V2. $\forall x\ \forall y\ \forall z\ [x<y \wedge y<z \supset x<z]$ transitivity
     V3. $\forall x\ \forall y\ [x=y \vee x<y \vee y<x]$
     V4. $\forall x\ \exists y\ [x<y]$
     V5. $\forall x\ \exists y\ [y<x]$
     V6. $\forall x\ \forall y\ [x<y \supset \exists z\ (x<z \wedge z<y)]$

Some other examples:

- **Theory of equality**: O1-O3
  Models: identity on the set of natural numbers, rational numbers, real numbers, ...
- **Theory of sharp ordering** (O1-O7) or (V1-V2)
  Models: identity and sharp number ordering on the set of natural, rational, real numbers. Identity and proper inclusion on the set of all the subsets of a set S,...
- **Theory of linear sharp ordering**: O1-O8 or V1-V3
  Models: identity and sharp ordering on the set of natural, rational, real numbers;
  Identity and lexicographical ordering on the set of words over an alphabet,...
- **Theory of dense ordering**: O1-O11 or V1-V6
  Models: identity and sharp ordering on the set of rational or real numbers,...

B.2.3 Theory of partial ordering:

Special constants:

$\leq$ ... binary predicate constant

Logical axioms: axioms of Hilbert calculus

Special axioms:

PO1. $\forall x\ (x \leq x)$	reflexivity
PO2. $\forall x\ \forall y\ [((x \leq y) \wedge (y \leq x)) \supset x = y]$	anti-symmetry
PO3. $\forall x\ \forall y\ \forall z\ [((x \leq y) \wedge (y \leq z)) \supset (x \leq z)]$	transitivity

where '=' stands for ***identity.***

Structure <M, ≤ >, i.e., a nonempty set S, on which a binary relation $\leq$ ($\subseteq$ M × M) is defined, which satisfies the axioms of partial ordering PO1, PO2, PO3 is a model of the theory, and it is called a ***partially ordered set (poset)***.

Models:

- The set N of natural numbers ordered according to the common comparing greater or equal.
- The set of individuals ordered according to 'older or of the same age'.
- The set of natural numbers N ordered by the relation |, which is defined as follows: $m \mid n$ iff m is divisible by n (without a remainder).

The last example illustrates why this ordering is called 'partial': there are elements which are not comparable. For instance, numbers 3, 5 are not comparable.

It is often the case that the relation seems to be a partial ordering, but it is actually quasi-ordering. The problem is caused by the axiom of anti-symmetry.

Example: A model of axioms i) and iii) – ***quasi-ordered set***:

The set F of formulas of the FOL language ordered by the relation of logical entailment |= is a quasi-ordered set.

(If A |= B and B |= A, then formulas A, B are only equivalent but not identical: for instance A ⊃ B and ¬A ∨ B are equivalent but distinct formulas.)

Partial ordering of factor sets.

If we however wish to (partially) order a set the relation of which is just a quasi-ordering, we use the following tricky method: If a relation ≤ is a quasi-ordering on a set S, then we define on the set S a relation of ***equivalence*** (satisfying the reflexivity, symmetry and transitivity axioms) in this way: $a \Leftrightarrow b$ if and only if $a \leq b$ and $b \leq a$ ($a \in$ S, $b \in$ S).

It is a well-known fact that any equivalence relation ⇔ on a set S defines a ***partition*** of the set S into disjunctive classes (subsets of S) such that their union is equal to the whole set S. Members of a partition class are those elements of S that are equivalent according to the relation ⇔. Thus with respect to the relation ⇔ these elements are indistinguishable and any element of a class can serve as its representative. No members of distinct classes are equivalent. The set of partition classes is called the ***factor set*** of S, denoted **S/⇔**. The elements of S/⇔ are classes of equivalent elements denoted usually by [e], where e is a representative of the respective class.

Consider now the set F of all the formulas of the FOL language, and its factor set F/⇔. On this set of sets (classes) a relation of partial ordering can be defined as follows:

$[A_1] \leq [A_2]$ if and only if $A_1 \models A_2$.

The structure $< F/\Leftrightarrow, \leq >$ is a poset. To prove it, we have first to show that the relation ≤ is well-defined, and then second to prove that the axioms of partial ordering PO1-PO3 are satisfied. So that the above definition of ordering be correct, the defined relation must not depend on choosing particular representatives of classes.

Let $A_1' \in [A_1]$ a $A_2' \in [A_2]$, $[A_1] \leq [A_2]$. Then:
$A_1' \Leftrightarrow A_1$, hence $A_1' \models A_1$. By definition $A_1 \models A_2$, and $A_2 \models A_2'$, hence also $A_1' \models A_2'$, which means $[A_1'] \leq [A_2']$, and the definition is correct. Reflexivity and transitivity of the relation ≤ are obvious. We show that this relation is also anti-symmetric: if $[A_1] \leq [A_2]$ and $[A_2] \leq [A_1]$, then $A_1 \models A_2$ and $A_2 \models A_1$. This means that $A_1 \Leftrightarrow A_2$ and $[A_1] = [A_2]$.

B.3. Algebraic Theories

B.3.1. Theory of *groups*:

A structure <G, f> (ie. a non-empty set G, on which a binary *operation – mapping* f: $G \times G \rightarrow G$), which satisfies the following **axioms of the theory of groups**, is called a ***commutative (Abel) group.*** If the structure satisfies only the axioms i)-iii), it is called a (non-commutative) ***group***:

(f is a binary functional symbol)

i)	$\exists e \forall a\ f(e,a) = f(a,e) = a$	the existence of the unit element
ii)	$\forall a \forall b \forall c\ f(f(a,b),c) = f(a,f(b,c))$	associativity
iii)	$\forall a \exists \hat{a}\ f(a,\hat{a}) = f(\hat{a},a) = e$	the existence of an inverse element
iv)	$\forall a \forall b\ f(a,b) = f(b,a)$	commutativity

The theory of groups illustrates a method of axiomatic study. We generalize some similar “situations”, in which the way of proofs is identical up to some isomorphism. The (minimum set of) assumptions of these proofs are formulated in the language of logic in the form of axioms. By deductive methods we then infer their logical consequences (theorems) valid in any interpretation of the axioms. And we know that these theorems are true in particular interpretations. In this way we can even discover some unexpected properties of other structures (models) of the theory, which are identical to the intended original interpretation. We do not have to repeat particular proofs, they are common to the whole theory.

Note: in a commutative group the functional symbol f is often denoted by the sign for multiplying **‘.’** (the group is called *multiplicative*) or for adding **‘+’** (*additive group*). An inverse element is denoted multiplicative group by a^{-1}, or in additive group $-a$, respectively, the unit element by 1, or 0 respectively.

Let us illustrate the role of the group theory by a simple example.

Example 1. You may surely know the following arithmetic formulas:

a) $u - v + v - w = u - w$

b) $u/v \,.\, v/w = u/w$

c) $\log_v u \,.\, \log_w v = \log_w u$

These are valid for real numbers **R**.

Obviously, the set of real numbers with the adding operation, as well as multiplying operation, are commutative groups.

In any group the following theorem can be easily proved (***try to do it!***): if $\bullet$ is the binary group operation, then

Theorem $u \bullet v^{-1} \bullet v \bullet w^{-1} = u \bullet w^{-1}$

It is easy to see that formulas a) and b) are special cases of the theorem.

Let **<u>R</u>** be the set **R –** {0}**.** To show that the formula c) is also valid according to the Theorem, we have to characterize a commutative group the elements of which are logarithms. Let us define a binary operation $\bullet$ on the set **<u>R</u>:**

$u \bullet v = \log U \,.\, \log V$, where U, V are numbers such that $u = \log U$, $v = \log V$.

Since $u \bullet v = u \,.\, v$, it is obvious that <**<u>R</u>**, •> is a commutative group.
Now for $v \neq 0$ the following holds: $u \bullet v^{-1} = \log U \,.\, (\log V)^{-1} = \log_{10} U \,.\, \log_V 10 = \log_V U$.
We can see that according to the Theorem we get:

$\log_V U \,.\, \log_W V = u \bullet v^{-1} \bullet v \bullet w^{-1} = u \bullet w^{-1} = \log_W U$ (for $v, w \neq 0$).

Example 2. The set **Z** of positive and negative whole numbers is a commutative group with respect to the operation of adding: **Z**, **+**>.

Example 3. Consider the set **Z** with an equivalence relation defined as follows: $a \Leftrightarrow_n b$ modulo n iff $n \mid (a - b)$, i.e., the difference of numbers a, b is divisible by n. ***Try to prove that the relation $\Leftrightarrow_n$ is the equivalence relation !***
This equivalence defines (as every equivalence) the partition of **Z** into classes of numbers congruent modulo *n*.
Let us denote this factor set by **Z**/$\Leftrightarrow_n$ and its elements by [i], where I is a representative of the respective class. To adduce an example, let us illustrate the set **Z** / $\equiv_5$ modulo 5 by enumerating its elements:

[0] = {... -10, -5, 0, 5, 10, 15, ... }
[1] = {... -9, -4, 1, 6, 11, 16, ... }
[2] = {... -8, -3, 2, 7, 12, 17, ... }
[3] = {... -7, -2, 3, 8, 13, 18, ... }
[4] = {... -6, -1, 4, 9, 14, 19, ... }

Let $\oplus$ be a binary operation of class adding on **Z** /$\Leftrightarrow_n$ defined as follows:
[i] $\oplus$ [j] = [i+j].
This adding of classes is well-defined:
If [i] = [i’], [j] = [j’], then *n* | (i-i’) and *n* | (j-j’), hence *n* | (i-i’+j-j’), *n* | (i+j - i’+j’).
Which means [i+j] = [i’+j’]. It is easy to prove that the structure <**Z/$\Leftrightarrow_n$,** $\oplus$> is a commutative group. The unit element is the class [0], and for every [*a*] the inverse element is the class [-*a*].

B.3.2. Theory of lattices:

Let S be a set on which two binary operations (mappings from S × S → S) are defined that are denoted and called $\cap$ (meet) and $\cup$ (join). Let meet and join satisfy the following six axioms (a,b,c are elements of S):

i) $\forall(abc)\ (a \cup b) \cup c = a \cup (b \cup c)$ associativity
ii) $\forall(abc)\ (a \cap b) \cap c = a \cap (b \cap c)$ associativity
iii) $\forall(ab)\ a \cup b = b \cup a$ commutativity
iv) $\forall(ab)\ a \cap b = b \cap a$ commutativity
v) $\forall(ab)\ (a \cap b) \cup a = a$ Boole properties, or
vi) $\forall(ab)\ a \cap (b \cup a) = a$ idempotent properties

Then the structure <M, $\cap$, $\cup$> is called a ***lattice***.

In the lattice theory the following two theorems are valid. These theorems determine the relationship of the lattice theory and the theory of partial ordering. Actually, each lattice can be viewed as a poset, and a poset with the following properties can be viewed as a lattice:

Theorem 1: Let L = <S, $\cap$, $\cup$> be a lattice. Then the binary relation $\leq$ defined on S as follows:

$a \leq b \ \Leftrightarrow_{\mathrm{df}}\ a \cup b = b \ \equiv \ a \cap b = a$

is a partial ordering, and for all the two-element subsets there is a supremum and infimum in S:

$\forall(ab)\ [\sup\{a,b\} = a \cup b],\ \forall(ab)\ [\inf\{a,b\} = a \cap b]$.

Theorem 2: If S = <M, $\leq$ > is a partially ordered set such that each two-element subset of M has a supremum and infimum within M, then the structure L = <M, $\cap$, $\cup$> with meet and join defined: $a \cup b =_{\mathrm{df}} \sup\{a,b\}$, $a \cap b =_{\mathrm{df}} \inf\{a,b\}$, is a model of the lattice theory, i.e., L is a lattice.

In each lattice the following theorems are valid:

Theorem 3:
$\vdash\ (a \cap b) \cup (a \cap c)\ \leq\ a \cap (b \cup c)$
$\vdash\ (a \cup b) \cap (a \cup c)\ \geq\ a \cup (b \cap c)$

There are several important classes of lattices such that they satisfy the above lattice axioms and some additional axioms.

If the formulas of the theorem 3 are of the equality form, then the lattice is ***distributive***:

D1 $(a \cap b) \cup (a \cap c)\ =\ a \cap (b \cup c)$

D2 $(a \cup b) \cap (a \cup c)\ =\ a \cup (b \cap c)$

Another important lattices are ***modular lattices***:

M $\forall(a,b,c)\ (\ (a \leq c) \supset [a \cup (b \cap c) = (a \cup b) \cap c]\ )$

<u>Examples</u>:

- A set 2^M of all the subsets of M, where meet is defined as the set-theoretical union, and join as the set-theoretical intersection, is a *distributive lattice*.

- The factor set F/⇔ of classes of equivalent formulas is a distributive lattice, in which the meet and join are defined as follows:

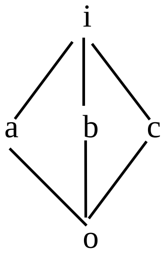
  $[A_1] \cup [A_2] = [A_1 \vee A_2]$, $[A_1] \cap [A_2] = [A_1 \wedge A_2]$,

  i.e., as a class formed by disjunction and conjunction, respectively.

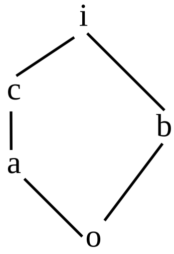
  (***Proof that the definition is correct!)***

Each distributive lattice is modular, but not vice versa:

- A set {o, a, b, c, i} ordered in this way: a ≤ i, b ≤ i, c ≤ i, a ≥ o, b ≥ o, c ≥ o is a modeular lattice which is not distributive. Using a Hasse diagram:



- A set {o, a, b, c, i} ordered according the the Hasse diagram is not a modular lattice:



The theory of lattices is used in informatics, for instance in the area of information retrieval, or the ***Formal Concept Analysis***.

Definition:

A ***theory*** T' ***is stronger than a theory*** T, iff each formula provable in T is also provable in T', but not vice versa.

Theories T ***and*** T' ***are equivalent*** (equally strong), iff each formula provable in T is also provable in T', and vice versa.

A ***Theory*** T' ***is an extension of a theory*** T, iff the set of special symbols used in T is a subset of the set of special symbols used in T', or if the set of axioms of T is a subset of the set of axioms of T'. If T' is equivalent to T, the ***extension is inessential***. If T' is stronger than T, the ***extension is essential***.

Example:

The theory of sharp ordering O1-O11 is stronger than the theory O1-O8.

The theory of sharp ordering O1-O11 is in the predicate logic with equality equivalent to the theory V1-V6 (in the predicate logic without equality).

Adding the axiom V6 to the theory V1-V5 is an essential extension of the former. Introducing a new relational symbol ≤ and an special axiom $x \leq y \equiv x < y \vee x = y$ is, however an inessential extension.