CS 576 lecture of 3/16/17

J. Meseguer

1. What do Theories Specify?

Words are essential, yet treacherous, because they can easily get us into *verbal confusions* suggested by their intuitive, but not critically analyzed meaning. Demagogues and all kinds of manipulators know this very well and exploit it systematically with great skill.

The word "theory" in logic, particularly when used, as we are doing, in the sense of a *theory presentation* is a good example of various potential verbal (and therefore mental) confusions that we must cut through by critically analyzing *a priori* (before the confusions can even insinuate themselves in one's mind) the given notion of *theory* (both syntactic and semantic in our treatment). So we can ask:

What do theories present/specify?

This has two answers:

1. *Semantically / Model-theoretically*:
   - a syntactic theory $((\Sigma,\Pi),\Gamma)$ presents/specifies the *class of models* $\underline{Mod}_{((\Sigma,\Pi),\Gamma)}$ that satisfy the axioms Γ;
   - a semantic theory $((\Sigma,\Pi),\mathbb{A})$ presents/specifies the *biggest class of models* $\mathbb{A}^{\#} = \underline{Mod}_{((\Sigma,\Pi),th(\mathbb{A}))}$

that satisfies the <u>same</u> set of FO formulas as $\mathbb{A}$.

2. <u>Syntactically / Proof-theoretically</u>:

- a syntactic theory $((\Sigma,\Pi),\Gamma)$ presents/specifies the set of its <u>theorems</u>, i.e., the set Γ° that we can <u>prove</u> from the axioms Γ, $\Gamma^\circ = \{\varphi \in FO(\Sigma,\Pi) \mid \Gamma \vdash \varphi\}$, which by Gödel's <u>Completeness Theorem</u> for first order logic coincides with the set of theorems <u>true</u> <u>in the class</u> $\underline{Mod}_{((\Sigma,\Pi),\Gamma)}$ i.e., $\Gamma^\circ = \{\varphi \in FO(\Sigma,\Pi) \mid \Gamma \models \varphi\}$;

- a semantic theory $((\Sigma,\Pi),\mathbb{A})$ specifies the set of <u>theorems</u> $th(\mathbb{A})$ that are <u>true</u> in $\mathbb{A}$, i.e., $th(\mathbb{A}) = \{\varphi \in FO(\Sigma,\Pi) \mid \forall \mathcal{M} \in \mathbb{A} \;\; \mathcal{M} \models \varphi\}$. Of course, if $th(\mathbb{A})$ can be effectively axiomatized by a recursive set Γ of axioms, then it also axiomatizes Γ°, which is also the set of theorems provable from Γ.

But note that, thanks to Gödel's Completeness Theorem and to the Galois Connection between sets of formulas and classes of models, viewpoints (1) and (2), although very different and conveying two radically different viewpoints (syntactic vs. semantic) are actually <u>isomorphic</u>!

Since isomorphism is a precise mathematical word, to avoid the charge that I am a charlatan in the style of a French philosopher of the Deconstruction school*, I should explain what I mean by isomorphism in this context.

(*) See, e.g., A. Sokal and J. Bricmont, "Fashionable Nonsense: Postmodern Intellectuals' Abuse of Science", Picador, 1988.

what I mean is very simple, namely, the semantic and syntactic meaning of a theory are systematically related by the poset isomorphism defined by the Galois connection when we restrict such a connection to the images of the functions $th_{(\Sigma,\Pi)}$ and $mod_{(\Sigma,\Pi)}$, since then we get a poset isomorphism:

$$\left(th_{(\Sigma,\Pi)}[\mathcal{P}(Mod_{(\Sigma,\Pi)})], \subseteq\right) \underset{\underset{mod(\Sigma,\Pi)}{\cong}}{\overset{\overset{\cong}{th(\Sigma,\Pi)}}{\rightleftarrows}} \left(mod_{(\Sigma,\Pi)}[\mathcal{P}(FO(\Sigma,\Pi))], \supseteq\right)$$

$$\Gamma^{\bullet} \longleftrightarrow \underline{Mod}_{((\Sigma,\Pi),\Gamma)}$$

$$th(\mathbb{A}) \longleftrightarrow \mathbb{A}^{\#}$$

(note how the inclusion order has been reversed for classes of models due to the anti-isomorphic nature of $th_{(\Sigma,\Pi)}$ and $mod_{(\Sigma,\Pi)}$).

It may be a good idea to visualize this poset isomorphism in the case of a very familiar example and of well-known theories, since this will also illustrate the combined power of syntactic and semantic theories and of theory transformations. Before doing so, let us add one more theory transformation, namely closure under elementary equivalence:

$$\_\_{\equiv} : \mathcal{P}(\underline{Mod}_{(\Sigma,\Pi)}) \ni \mathbb{A} \longmapsto \mathbb{A}_{\equiv} \in \mathcal{P}(\underline{Mod}_{(\Sigma,\Pi)})$$

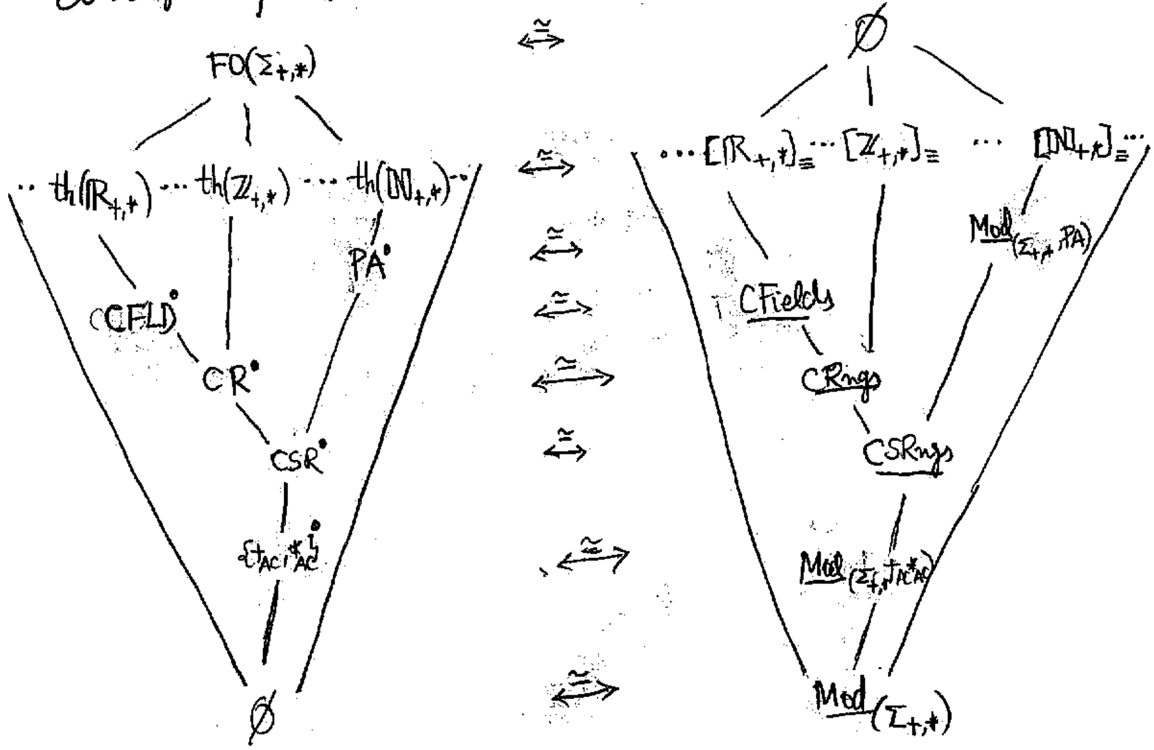
where $\mathbb{A}_{\equiv} = \{ M' \in \underline{Mod}_{(\Sigma,\Pi)} \mid \exists M \in \mathbb{A} \text{ s.t. } M \equiv M' \}$

where $M \equiv M'$ iff $\forall \varphi \in FO(\Sigma,\Pi)\ M \models \varphi \Leftrightarrow M' \models \varphi$, which induces the theory transformation $((\Sigma,\Pi),\mathbb{A}) \mapsto ((\Sigma,\Pi),\mathbb{A}_{\equiv})$.

The example in question is based on the unsorted signature $\{+,*,0,1\} = \Sigma_{+*}$ where we can consider the following syntactic and semantic theories:

0. $(\Sigma_{+,*}, \{+_{AC}, *_{AC}\})$ the theory where both $+$ and $*$ are associative-commutative
1. $(\Sigma_{+*}, \emptyset)$
2. $(\Sigma_{+,*}, CSR)$, the theory of <u>commutative semirings</u>, whose equational axioms are: $CSR = \{+_{AC}, *_{AC}, x+0=x, x*1=x, x*(y+z) = x*y+x*z\}$
3. $(\Sigma_{+,*}, CR)$, the theory of <u>commutative rings</u>, where we add to CSR the axiom: $\forall x \exists y . \ x+y=0$
4. $(\Sigma_{+,*}, PA)$, the theory of <u>Peano arithmetic</u>, where we add to $\Sigma_{+,*}$ the <u>Peano axioms</u> for the natural numbers (expressing $s(x)$ as $x+1$) where induction is captured as the <u>axiom scheme</u> (recursive set of formulas):
$$\left(\varphi(0) \wedge \forall x\,(\varphi(x) \Rightarrow \varphi(x+1))\right) \Rightarrow \varphi(x)$$
where $x \in fvars(\varphi)$ and $\varphi \in FO(\Sigma_{+,*})$.
5. $(\Sigma_{+,*}, CFLD)$, the theory of commutative fields, where we add to CR the axiom:
$$\forall x . \ x \neq 0 \Rightarrow (\exists y . \ x \cdot y = 1)$$
6. $(\Sigma_{+,*}, \{\underline{Init}(CSR)\})$, the theory of the natural numbers with addition and multiplication
7. $(\Sigma_{+,*}, \{\mathbb{R}\})$, the theory of the real numbers with addition and multiplication
8. $(\Sigma_{+,*}, \{\mathbb{Z}\})$ the theory of the <u>integers</u>

Let us see how all these theories come out in the wash of the just-mentioned Galois isomorphism by <u>picturing</u> their corresponding specifications there:



Note the following:

1. The left top element (all FO formulas) corresponds to the <u>inconsistent</u> theory presentation) (no models).
   <u>theory</u> call inconsistent theory presentation)
2. The <u>maximal elements</u> below such top are, proof theoretically the <u>complete theories</u>, and model-theoretically the <u>equivalence classes</u> of models in the <u>elementary equivalence</u> relation $\equiv$.
3. By Gödel's Incompleteness Theorem or, more simply, by Matiyasevich's negative answer to Hilbert's 10^{th} problem which consists in proving that <u>CSR-unification is undecidable</u> we know that $th(\mathbb{Z}_{+,*})$ and $th(\mathbb{N}_{+,*})$ are complete theories that <u>cannot be axiomatized</u> by a recursive set of axioms

so that the inclusion $PA^\circ \subset th(\mathbb{N}_{+,*})$ is <u>strict</u> and must remain so for any axiomatizable theory $(\Sigma_{+,*}, \Gamma)$ such that $PA^\circ \subset \Gamma^\circ \subset th(\mathbb{N}_{+,*})$.

4. Although usually $CSR \not\subseteq PA$, the theorems $+_{AC}$ and $*_{AC}$ are provable in Peano arithmetic by the usual inductive proofs, so that $CSR^\circ \subsetneq PA^\circ$ where the containment is easily shown to be strict.

5. By Tarski's theorem, the theory $th(\mathbb{R}_{+,*})$ <u>is decidable</u>. In particular, linear arithmetic over the reals (where we restrict to linear polynomials as opposed to arbitrary ones) and over the rationals (since $[\mathbb{R}_{+,*}]_\equiv = [\mathbb{Q}_{+,*}]_\equiv$) is decidable (by more efficient algorithms than Tarski's).

6. As we just saw last week, QF satisfiability, and therefore validity, in the theories $(\Sigma_{+,*}, \emptyset)$ (resp. $(\Sigma_{+,*}\{+_{AC}, *_{AC}\})$) is decidable by congruence closure (resp. AC-congruence closure).

2. Theory (Presentation) Isomorphism as Presentation-Independence

<u>Q1</u>: When are two theory (presentations) <u>equivalent</u>?

<u>A1</u>: When they present the <u>same</u> (syntactic or semantic: it makes no difference) theorems / classes of models.

<u>Q2</u>: How is the notion of equivalence captured categorically?

<u>A2</u>: By the notion of isomorphism.

Q3: Is the above notion of theory equivalence captured indeed by the notion of theory isomorphism in the (preorder) category of theory inclusions?

A3: Yes!

Let us introduce some notation and make some observations

1. Let ThIncl denote the (preorder) category of theory inclusions, with inclusion composition as arrow composition
2. For each theory T, its identity 1_T is the trivial inclusion $T \subseteq T$.
3. Recall that an isomorphism $A \simeq B$ in any category is characterized by arrows $f : A \to B$, $g : B \to A$ such that $f;g = 1_A$ and $g;f = 1_B$. Therefore, in our context T and T' will be isomorphic, $T \cong T'$, iff we have theory inclusions $T \subseteq T'$ and $T' \subseteq T$, so that:

$$\underbrace{T \subseteq T' \subseteq T}_{1_T} \qquad \underbrace{T' \subseteq T \subseteq T'}_{1_{T'}}$$

4. Define the following auxiliary notation:
   - $sign(T)$ defined by $sign((\Sigma,\Pi),\Gamma) = sign((\Sigma,\Pi),\mathbb{A}) = (\Sigma,\Pi)$
   - $th(T)$ defined by $th((\Sigma,\Pi),\Gamma) = \Gamma^{\bullet}$, and $th((\Sigma,\Pi),\mathbb{A}) = th(\mathbb{A})$
   - $mod(T)$ defined by $mod((\Sigma,\Pi),\Gamma) = \mathbf{Mod}_{((\Sigma,\Pi),\Gamma)}$, and $mod((\Sigma,\Pi),\mathbb{A}) = \mathbb{A}^{\#}$

We can now back the claim that theory equivalence (presenting the same models/theorems) is exactly theory isomorphism:

<u>Lemma</u>. The following are equivalent for theories T, T':

1. $T \cong T'$ in <u>ThIncl</u>
2. $mod(T) = mod(T')$
3. $thm(T) = thm(T')$

<u>Proof</u>. By the Galois isomorphism it is enough to prove either $(1) \Leftrightarrow (2)$ or $(1) \Leftrightarrow (3)$. We have three cases for $T \cong T'$:

(a) T and T' are <u>syntactic</u> theories. But by $T \subseteq T'$ and $T' \subseteq T$ we <u>must</u> have $sign(T) = sign(T')$, so $T = ((\Sigma, \Pi), \Gamma)$, $T' = ((\Sigma, \Pi), \Gamma')$, and by $T \subseteq T'$, $\Gamma^{\bullet} \subseteq \Gamma'^{\bullet}$, and by $T' \subseteq T$, $\Gamma'^{\bullet} \subseteq \Gamma^{\bullet}$, so that, $th(T) = th(T')$, proving $(1) \Leftrightarrow (3)$.

(b) T and T' are syntactic theories; again, we must have $sign(T) = sign(T')$, so that $T = ((\Sigma, \Pi), \mathbb{A})$ and $T' = ((\Sigma, \Pi), \mathbb{B})$. By $T \subseteq T'$ we must have $\mathbb{A} \subseteq \mathbb{B}^{\#}$, and by $T' \subseteq T$ we must have $\mathbb{B} \subseteq \mathbb{A}^{\#}$, so that $mod(T) = mod(T')$, proving $(1) \Leftrightarrow (2)$.

(c) T is a syntactic theory $((\Sigma, \Pi), \Gamma)$ and T' a semantic theory $((\Sigma, \Pi), \mathbb{A})$. By $T \subseteq T'$ we must have $\Gamma \subseteq th(\mathbb{A})$, and by $T' \subseteq T$ we must have $\underline{Mod}_{((\Sigma,\Pi),\Gamma)} \subseteq \mathbb{A}^{\#}$.

But by the Galois connection we must have

$\mathbb{A}^{\#} = mod(th(\mathbb{A})) \supseteq \underline{Mod}_{((\Sigma,\Pi),\Gamma')}$, so that $mod(T) = mod(T')$,

proving (1) $\Leftrightarrow$ (3). $\square$

Note that isomorphism defines an equivalence relation $\cong$ theories. What does that equivalence class $[T]_{\cong}$ capture?

It can be described in two equivalent ways:

(a) theory equivalence, as already pointed out, and

(b) presentation-independence, i.e., we abstract away the details of every different presentation of the same theorems/models.

Note also that, as it happens for any preorder, the quotient category $\underline{ThIncl}/_{\cong}$ is a poset. Furthermore, if we restrict this poset to the set of (equivalence classes of) theories with the same signature (Σ,Π), denoted $\underline{ThInc}/_{\cong}|_{(\Sigma,\Pi)}$ what do we get?

We exactly get a poset isomorphic to the poset $(th_{(\Sigma,\Pi)}[\mathcal{P}(\mathrm{Mod}_{(\Sigma,\Pi)})], \subseteq)$ in the Galois isomorphism, since this trivially follows from the above Lemma, which tells us that $T \simeq T'$ iff $th(T) = th(T')$.

Q: But then, why bother with <u>ThIncl</u> and with theory <u>presentations</u>? why couldn't we <u>define</u> a theory syntactically as a pair $((\Sigma,\Pi), \Gamma)$ with Γ <u>deduction</u> <u>closed</u>, i.e., $\Gamma = \Gamma^{\bullet}$, and semantically as $((\Sigma,\Pi), \mathbb{A})$ with $\mathbb{A}$ <u>FO-model closed</u>, i.e., $\mathbb{A} = \mathbb{A}^{\#}$?

A: This is a <u>very dumb</u> question. Of course we can do so. But what do we gain? A very misleading sense of simplicity. In fact, nothing we didn't already have. And what do we lose? The capacity to make <u>crucial</u> <u>distinctions</u>, and to <u>specify</u> the axioms/models of interest. For example:

1. The notion of an <u>axiomatizable</u> theory is verified by exhibiting a recursive set Γ of axioms such that generate $\Gamma^{\bullet}$.
2. Likewise, the notion of a <u>finitely axiomatizable</u> theory is verified by exhibiting a finite set Γ of axioms generating $\Gamma^{\bullet}$
3. The property of a theory $((\Sigma,\Pi),\Gamma)$ being <u>complete</u> can be very hard to establish proof-theoretically, but becomes <u>trivial</u> to establish by specifying it semantically as $((\Sigma,\Pi), \{\mathbb{M}\})$, or, if you wish, as $((\Sigma,\Pi), Th(\mathbb{M}))$. And is even easier to do so as $((\Sigma,\Pi), \underline{Init}((\Sigma,\Pi),\Gamma))$ for $((\Sigma,\Pi),\Gamma)$ a Horn theory.

3. Satisfiability is Independent of Theory Presentation

The question may arise about whether satisfiability in a *semantic* theory (for isomorphic syntactic theories the question is mute) may or not depend on the presentation. That is whether if we have $T \cong T'$, with $T = ((\Sigma, \Pi), \mathbb{A})$ and $T' = ((\Sigma, \Pi), \mathbb{B})$ and $\varphi \in FO(\Sigma)$, then φ is satisfiable in $\mathbb{A}$ iff it is satisfiable in $\mathbb{B}$. This question was settled, in the positive, in Lecture 2, but the argument is worth recalling.

- First of all note that $T \cong T'$ iff $\mathbb{A}^\# = \mathbb{B}^\#$. Therefore it is enough to prove φ satisfiable in $\mathbb{A}$ iff φ satisfiable in $\mathbb{A}^\#$.
- Second note that $\varphi \in th(\mathbb{A})$ iff $\forall \varphi \in th(\mathbb{A})$, where $\forall \varphi$ denotes the universal closure of φ.
- Third note that if φ is satisfiable in $\mathbb{A}$ then it is trivially satisfiable in $\mathbb{A}^\#$, since $\mathbb{A} \subseteq \mathbb{A}^\#$.
- So all boils down to proving that φ satisfiable in $\mathbb{A}^\#$ implies φ satisfiable in $\mathbb{A}$.

Proof. Suppose φ satisfiable in $\mathbb{A}^\#$ but unsatisfiable in $\mathbb{A}$. This means $\forall \mathcal{M} \in \mathbb{A}$, $\forall a \in [vars(\varphi) \to M]$, $\mathcal{M}, a \not\models \varphi$, i.e., $\mathcal{M}, a \models \neg\varphi$. But this means $\forall \neg\varphi \in th(\mathbb{A})$, and, equivalently, $\neg\varphi \in th(\mathbb{A})$. But by the Galois connection we then have,

$$\neg\varphi \in th(\mathbb{A}) = th(mod(th(\mathbb{A}))) = th(\mathbb{A}^\#)$$

contradicting the assumed satisfiability of φ in $\mathbb{A}^\#$. $\square$