Ax-Grothendieck talk(s)

Will Troiani

November 2021

Definition 0.0.1. A **first order signature** (or **first order language**) Σ consists of the following data.

- A set Σ-Sort of **sorts**. For each sort A of a signature Σ there exists a countably infinite set $\mathcal{V}_A$ of **variables** of sort A. We write $x : A$ for $x \in \mathcal{V}_A$.

- A set Σ-Fun of **function symbols**, together with a map assigning to each $f \in \Sigma$-Fun its **type**, which consists of a finite, non-empty list of sorts (with the last sort in the list enjoying a distinguished status): we write

$$f : A_1 \times \ldots \times A_n \longrightarrow B \tag{1}$$

  to indicate that f has type $A_1, ..., A_n, B$. The integer n is the **arity** of f, in the case $n = 0$, the function symbol f is a **constant** of sort B.

- A set Σ-Rel of **relation symbols**, together with a map assigning to each $R \in \Sigma$-Rel its **type**, which consists of a finite list of sorts: we write

$$R \rightarrowtail A_1 \times \ldots \times A_n \tag{2}$$

  to indicate that R has type $A_1, ..., A_n$. The integer n is the **arity** of R, in the case $n = 0$, the relation symbol R is an **atomic proposition**.

1. A finite amount of *sorts* (or types). We require the ability to identify particular sorts, and also to distinguish sorts. We also require that a new sort may be introduced if needed. The limit of the number of sorts is the limit of the ones abilities, means, and resources to perform the first two requirements of this dotpoint.

2. For each sort a finite set of *variables* associated to that sort with the same requirements as that of 1.

3. A finite amount of *function symbols* and a finite amount of *relation symbols*, both with the same requirements needed as 1.

Example 0.0.2.

Definition 0.0.3. We define $\mathcal{F}$, the first order theory of fields, beginning with the first order language of fields. Let Σ be a signature consisting of a single sort A. We introduce 5 function symbols.

- $0, 1 : A$,

- $- : A \longrightarrow A$,

- $+, \cdot : A \times A \longrightarrow A$.

The first order language of fields has no relation symbols.

Definition 0.0.4. Terms and their types:

- **Variables**:
$$x : A \tag{3}$$

- **Compound terms and their types**: let $f : A_1 \times \ldots \times A_n \longrightarrow B$ be a function symbol and $t_1 : A_1, ..., t_n : A_n$ be terms.
$$f(t_1, ..., t_n) : B \tag{4}$$

Definition 0.0.5. Formulas and their free variables:

- **Relations**: if $R \rightarrowtail A_1 \times \ldots \times A_n$ is a relation symbol and $t_1 : A_1, \ldots, t_n : A_n$ are terms then
$$R(t_1, ..., t_n), \qquad \mathrm{FV}(R(t_1, ..., t_n)) = \bigcup_{i=1}^{n} \mathrm{FV}(t_i) \tag{5}$$

- $s : A, t : A$ terms:
$$s = t, \qquad \mathrm{FV}(s = t) = \mathrm{FV}(s) \cup \mathrm{FV}(t) \tag{6}$$

2

- $\top, \bot$ are formulas, $\mathrm{FV}(\top) = \mathrm{FV}(\bot) = \varnothing$.

- ϕ, ψ formulas, $x : A$ a variable.

$$\phi \vee \psi, \phi \wedge \psi, \phi \Rightarrow \psi, \neg\phi, \forall x : A\phi, \exists x : A\phi \tag{7}$$

  where
$$\mathrm{FV}(\phi \vee \psi) = \mathrm{FV}(\phi) \cup \mathrm{FV}(\psi), \text{etc...} \tag{8}$$
$$\mathrm{FV}(\forall x : A, \phi) = \mathrm{FV}(\exists x : A, \phi) = \mathrm{FV}(\phi) \setminus \{x\} \tag{9}$$

Definition 0.0.6. A **first order theory** over a first order language Σ is a set of formulas on Σ.

Example 0.0.7. We extend the first order language $\mathcal{F}$ of fields to a first order theory.

The axioms are given as follows.

$$(x + y) + z = x + (y + z) \tag{10}$$
$$x + y = y + x \tag{11}$$
$$x + 0 = x \tag{12}$$
$$(x \cdot y) \cdot z = x \cdot (y \cdot z) \tag{13}$$
$$x \cdot 1 = 1 \cdot x = x \tag{14}$$
$$x \cdot (y + z) = x \cdot y + x \cdot z \tag{15}$$
$$x + (-x) = 0 \tag{16}$$
$$x \neq 0 \Rightarrow \exists y, xy = 1 \tag{17}$$

This set of formulas forms the axioms of $\mathcal{F}$.

We consider the special case when the number of sorts is equal to 1.

Definition 0.0.8. An **interpretation** $\mathcal{I}$ of a first order language consists of the following data.

- A non-empty set $\mathcal{I}(D)$ called the **domain**.

- For any function symbol $f : A_1 \times \ldots \times A_n \longrightarrow B$ a function

$$\mathcal{I}(f) : D^n \longrightarrow D \tag{18}$$

  If f is 0-ary then $\mathcal{I}(f)$ is simply a choice of element from D.

3

- For any relation symbol $R \rightarrowtail A_1 \times \ldots \times A_n$ a function

$$\mathcal{I}(R) : D^n \longrightarrow \{0, 1\} \tag{19}$$

Definition 0.0.9. Let D be a set. A **valuation** over Σ in a set D is a function

$$\nu : \mathcal{V} \longrightarrow D \tag{20}$$

We also introduce the following notation. If $d \in D$ is an element of D, $x \in \mathcal{V}$, and $\nu : \mathcal{V} \longrightarrow D$ is some valuation, then we have the following valuation.

$$\nu_{x \mapsto d}(y) = \begin{cases} d, & x = y, \\ \nu(y), & x \neq y \end{cases} \tag{21}$$

We now extend an interpretation of a language to a model of a first order theory (given a choice of valuation).

Definition 0.0.10. Let $\mathbb{T}$ be a first order theory over a first order language L. Let $\mathcal{I}$ be an interpretation of L and ν a valuation in the domain D of $\mathcal{I}$. We extend the interpretation to terms in the following way.

- $\mathcal{I}_\nu(x) = \nu(x)$, for any variable x,

- $\mathcal{I}_\nu(f(t_1, ..., t_n)) = \mathcal{I}(f)(\mathcal{I}_\nu(t_1), ..., \mathcal{I}_\nu(t_n))$, where $f(t_1, ..., t_n)$ is a term constructed from an n-ary function symbol f and n terms t_i.

Then the interpretation is extended to the formulas:

$$\mathcal{I}_\nu(R(t_1, ..., t_n)) = 1 \text{ iff } \mathcal{I}(R)(\mathcal{I}_\nu(t_1), ..., \mathcal{I}_\nu(t_n)) = 1 \tag{22}$$
$$\mathcal{I}_\nu(s = t) = 1 \text{ iff } \mathcal{I}_\nu(s) = \mathcal{I}_\nu(t) \tag{23}$$
$$\mathcal{I}_\nu(\top) = 1 \tag{24}$$
$$\mathcal{I}_\nu(\bot) = 0 \tag{25}$$
$$\mathcal{I}_\nu(\phi \vee \psi) = 1 \text{ iff } \mathcal{I}_\nu(\phi) = 1 \text{ or } \mathcal{I}_\nu(\psi) = 1 \tag{26}$$
$$\mathcal{I}_\nu(\phi \wedge \psi) = 1 \text{ iff } \mathcal{I}_\nu(\phi) = 1 \text{ and } \mathcal{I}_\nu(\psi) = 1 \tag{27}$$
$$\mathcal{I}_\nu(\phi \Rightarrow \psi) = 1 \text{ iff } \mathcal{I}_\nu(\phi) = 0 \text{ or } \mathcal{I}_\nu(\psi) = 1 \tag{28}$$
$$\mathcal{I}_\nu(\neg\phi) = 1 \text{ iff } \mathcal{I}_\nu(\phi) = 0 \tag{29}$$
$$\mathcal{I}_\nu((\exists x : A)\phi) = 1 \text{ iff there exists } d \in D \text{ such that } \mathcal{I}_{\nu_{x \mapsto d}}(\phi) = 1 \tag{30}$$
$$\mathcal{I}_\nu((\forall x : A)\phi) = 1 \text{ iff for all } d \in D \text{ we have } \mathcal{I}_{\nu_{x \mapsto d}}(\phi) = 1 \tag{31}$$

Let $\mathbb{T}$ be a first order theory over a first order language L. Then a **model** for $\mathbb{T}$ is an interpretation $\mathcal{I}$ of L such that for all valuations ν, each formula ϕ in $\mathbb{T}$ we have:

$$\mathcal{I}_\nu(\phi) = 1 \tag{32}$$

Example 0.0.11. Let $\mathbb{R}$ denote the real numbers. Set $\mathcal{I}(A) = \mathbb{R}$. Define

$$\mathcal{I}(0) := 0 \in \mathbb{R}$$
$$\mathcal{I}(1) := 1 \in \mathbb{R}$$
$$\mathcal{I}(-) : \mathbb{R} \longrightarrow \mathbb{R}$$
$$x \longmapsto -x$$
$$\mathcal{I}(+) : \mathbb{R}^2 \longrightarrow \mathbb{R}$$
$$(x, y) \longmapsto x + y$$
$$\mathcal{I}(\cdot) : \mathbb{R}^2 \longrightarrow \mathbb{R}$$
$$(x, y) \longmapsto xy$$

Then $\mathcal{I}$ is a model of $\mathcal{F}$.

We recall also the Natural Deduction proof system, which consists of the following deduction rules.

1 Proof (natural deduction)

So far we have discussed *language* and *meaning*, or what is the same, *syntax* and *semantics*. Now we discuss *proof*.

Definition 1.0.1. The deduction rules for the **natural deduction** are given as follows.

- Conjunction:

$$\frac{A \quad B}{A \wedge B} \wedge I \qquad \frac{A \wedge B}{A} \wedge E1 \qquad \frac{A \wedge B}{B} \wedge E2$$

- Disjunction

$$\frac{A}{A \vee B} \vee I1 \qquad \frac{B}{A \vee B} \vee I2 \qquad \frac{A \vee B \quad \overset{[A]^i}{\underset{\vdots}{C}} \quad \overset{[B]^j}{\underset{\vdots}{C}}}{C} \wedge E^{i,j}$$

- Implication

$$\frac{\overset{[A]^i}{\underset{\vdots}{B}}}{A \Rightarrow B} \Rightarrow I^i \qquad \frac{A \Rightarrow B \quad A}{B} \Rightarrow E$$

- Negation

$$\frac{\overset{[A]^i}{\underset{\vdots}{\bot}}}{\neg A} \neg I^i \qquad \frac{\neg A \quad A}{\bot} \neg E$$

- Universal quantification. The $\forall I$ rule can only be employed in the context where the formula B does not occur in A nor in any assumption formula upon which $\forall x A$ depends.

$$\frac{A[x := B]}{\forall x A} \forall I \qquad \frac{\forall x A}{A[x := B]} \forall E$$

- Existential quantification. The $\exists E$ rule can only be employed in the context where the formula B does not occur in A nor in C.

$$\frac{A[x := B]}{\exists x A} \exists I \qquad \frac{\exists x A \quad \overset{[A[x := B]]^i}{\underset{\vdots}{C}}}{C} \exists E^i$$

- (Respectively) equality, falsum, contradiction.

$$\frac{A = B \quad C}{C[B := A]} = \qquad \frac{\bot}{A} \bot E \qquad \frac{\overset{[\neg A]^i}{\underset{\vdots}{\bot}}}{A} \bot C^i$$

6

A **proof** is a finite, rooted planar tree with edges labelled by formulas and all vertices except for the root vertex labelled by a valid instance of a deduction rule. The leaves of the proof are the **assumptions** and if there exists a proof π where the edge connected to the root node is labelled by formula A and Γ is the set of assumptions of π we write

$$\Gamma \vdash A \tag{33}$$

Question 1.0.2. How does proof relate to truth?

Definition 1.0.3. Let $\mathcal{I}$ be an interpretation of a first order language L, let A be a formula in L, and let Γ be a set of formulas.

- $\mathcal{I} \models A$ if $\mathcal{I}_\nu(A) = 1$ for all valuations ν.

- $\mathcal{I} \models \Gamma$ if $\mathcal{I} \models A$ for all $A \in \Gamma$.

- $\Gamma \models A$ if $\mathcal{I} \models A$ for all interpretations $\mathcal{I}$ which satisfy $\mathcal{I} \models \Gamma$.

Theorem 1.0.4. *In classical natural deduction, we have*

$$\Gamma \vdash A \text{ if and only if } \Gamma \models A \tag{34}$$

Definition 1.0.5. A first order theory $\mathbb{T}$ over a first order language Σ is **complete** if every statement is either proveable or disproveable. That is, for every formula ϕ of Σ we have

$$\mathbb{T} \vdash \phi \quad \text{or} \quad \mathbb{T} \vdash \neg\phi \tag{35}$$

The point: this has all been motivated from a philosophical perspective, but we will use this structure as a mathematical tool and use it to prove the following statement.

Theorem 1.0.6 (Ax-Grothendieck Theorem)**.** *Let $f : \mathbb{C}^n \longrightarrow \mathbb{C}^n$ be a polynomial (that is, a polynomial in each entry). If f is injective then it is surjective.*

Sketch.   • We will prove the stronger statement:

     Claim 1.0.7. Let k be a field and denote by $\overline{k}$ its algebraic closure. Let $f : k^n \longrightarrow k^n$ by a polynomial. If f is injective then it is surjective.

- We will first prove the Claim 1.0.7 for the case when $k = \mathbb{F}_p$, the finite field of characteristic p.

- Define the first order theory $\mathcal{ALG}_0$ of algebraically closed fields of characteristic 0 and prove that this theory is complete.

- Write Claim 1.0.7 in the case when $k = \mathbb{Q}$ as first order statement ϕ.

- Assume that Claim 1.0.7 is *false*. By completeness of the $\mathcal{ALG}_0$ there exists a proof

$$
\begin{array}{c}
\pi \\
\vdots \\
\Gamma \vdash \neg\phi
\end{array}
$$

- Write Claim 1.0.7 in the case when $k = \mathbb{F}_p$ as a first order statement ψ.

- Use π to construct a proof $\Gamma \vdash \neg\psi$.

$$
\begin{array}{c}
\pi' \\
\vdots \\
\Gamma \vdash \neg\psi
\end{array}
$$

- Using the Completeness Theorem 1.0.4

$\square$