Mathematical Logic

Benjamin Church

July 3, 2022

Contents

1 Introduction

Mathematical logic is divided into two parts: semantics and syntactics. Semantics is the study to interpretations and models of a theory, think examples. Syntactics is the study of formal deduction systems and provability. We will study first-order or predicate quantifier logic which has an extremely powerful metatheory. Higher-order logics also exist but do not admit complete proof theory and many of the desirable metalogical properties of first-order logic fail to hold. A first-order logic has two pieces, a class of first-order formal languages which we will define inductivly and a deduction system defined by rules of inference.

1.1 First-Order Languages

.

Definition 1.1.1. A *vocabulary* or *signature* σ is a set of "nonlogical" symbols which may be of three types:

(a) Constant symbols (e.g. 0)

(b) n-ary function symbols (e.g. $+$)

(c) n-ary relation symbols (e.g. $\in$)

Along with the signature, a first-order language has a set of "logical" symbols:

(a) A countable list of variable symbols: $x_1, x_2, x_3, \cdots$

(b) Logical connectives: $\neg, \vee, \wedge, \rightarrow$

(c) Quantifiers: $\forall$ (we get $\exists \iff \neg\forall\neg$ for free)

(d) An equality relation: $=$

(e) Punctuation: ( ) , etc.

Definition 1.1.2. The set of *terms* of a first-order language L with vocabulary σ is defined inductively as follows:

(a) Any variable or constant symbol is a term.

(b) If f is an n-ary function symbol and $t_1, \ldots, t_n$ are terms then $f(t_1, \ldots, t_n)$ is a term. For a binary operator (2-ary function), say $\circ$, we will often write $(t_1 \circ t_2)$ to mean $\circ(t_1, t_2)$.

Definition 1.1.3. The set of *formulas* of a first-order language L with vocabulary σ is defined inductivly as follows:

(a) If s, t are terms then $(s = t)$ is a fomula. Furthermore if $R \in \sigma$ is an n-ary relation symbol and $t_1, \ldots, t_n$ are terms then $R(t_1, \ldots, t_n)$ is a formula. For a 2-ary relation we will often write sRt to mean $R(s, t)$.

(b) If A and B are formulas then $\neg A$, $(A \vee B)$, $(A \wedge B)$, and $(A \rightarrow B)$ are all formulas.

(c) If x is a variable symbol and φ a formula in which x is free (φ contains x but no quantifiers over x) then $\forall x\, \varphi$ and $\exists x\, \varphi$ are formulas.

Definition 1.1.4. A *sentence* of a first-order language is a formula with no free variables.

Definition 1.1.5. A first-order theory is a first-order language L along with a set Γ of first-order L-sentances which are refered to as axioms.

1.2 Proof Theory

There are many possible first-order deduction systems each with its own unique flavor. A deduction system has logical axioms and rules of inference on formulas of L. A formal proof begining with some assumptions is a sequence of L-formulas each of which is either a logical axiom, an assumption, or the result of a rule of inference applied to previous formulas.

Definition 1.2.1. We say that a first-order theory Γ *syntactically entails* or, more simply, *proves* A if there exists a formal proof using axioms of Γ and first-order rules of inference. We write this as $\Gamma \vdash A$.

Definition 1.2.2. A first-order theory Γ is *consistent* if there does not exist a statement A such that $\Gamma \vdash A$ and $\Gamma \vdash \neg A$.

Definition 1.2.3. A first-order theory Γ is *complete* if for every L-sentence A we have either $\Gamma \vdash A$ or $\Gamma \vdash \neg A$.

Lemma 1.2.4 (Deduction)**.** Let A be an L-sentence. If $\Gamma \cup \{A\} \vdash B$ then $\Gamma \vdash A \to B$.

Proof. This proof is a simple induction on theorems. We suppose it is true for all proofs of length n or less and show that any proof of B with length $n+1$ must contain a subproof of B' with length at most n such that a single rule of inference can take B' to B. Using the induction hypothesis we get $\Gamma \vdash A \to B'$. It is then a simple yet tedious excersize in first-order logic to arrive at $A \to B$ from $A \to B'$ and the rule of inference which takes B' to B. $\square$

Lemma 1.2.5 (Categorization of Consistency)**.** Γ is proof-theoretically consistent if and only if there exists a first-order sentence A such that $\Gamma \nvdash A$.

Proof. If Γ is consistent and $\Gamma \vdash A$ then $\Gamma \nvdash \neg A$. If Γ is not consistent then $\Gamma \vdash A$ and $\Gamma \vdash \neg A$ for some A. However, for any B, we have $\Gamma \vdash A \vee B$ since $\Gamma \vdash A$ and also $\Gamma \vdash \neg A$ so $\Gamma \vdash B$. Thus, if Γ is inconsistent then it proves everything. $\square$

Lemma 1.2.6. $\Gamma \cup \{\neg A\}$ is consistent $\iff$ $\Gamma \nvdash A$.

Proof. Suppose $\Gamma \cup \{\neg A\}$ is inconsistent. Then it proves anything including A. By the deduction lemma, $\Gamma \vdash \neg A \to A$ and thus $\Gamma \vdash A$.

Conversely, if $\Gamma \vdash A$ then $\Gamma \cup \{\neg A\} \vdash A$ and clearly $\Gamma \cup \{\neg A\} \vdash \neg A$ so it is inconsistent. $\square$

1.3 Interpretations, Models, and Truth

Definition 1.3.1. Let L be a first-order language with signature σ. An L-interpretation or σ-structure $\mathcal{M} = (M, I)$ is a nonempty set M called the domain and an interpretation function I satisfying,

(a) For each constant symbol $c \in \sigma$, an element of the domain, $c^{\mathcal{M}} = I(c) \in M$.

(b) For each n-ary function symbol $f \in \sigma$, n-ary function $f^{\mathcal{M}} = I(f) : M^n \to M$.

(c) For each n-ary relation symbol $R \in \sigma$, an n-ary relation $R^{\mathcal{M}} = I(R) \subset M^n$. Furthermore $=^{\mathcal{M}}$ is the diagonal relation Δ_M.

Definition 1.3.2. Let $\mathcal{M}$ be an L-interpretation and given a map $\alpha : \mathrm{VAR}_L \to M$ we extend α to an *assignment* on terms inductivly,

(a) If t is a constant symbol c then $\alpha(t) = c^{\mathcal{M}}$

(b) If $t = f(t_1, \dots, f_n)$ then $\alpha(t) = f^{\mathcal{M}}(\alpha(t_1), \dots, \alpha(t_n))$.

For a tuple $\underline{a} \in M$ we write $[\underline{x} := \underline{a}]$ for the assigment sending $x_i \mapsto a_i$.

Definition 1.3.3. Let $\mathcal{M}$ be an L-interpretation and α an assigment. Let φ be an L-formula then we define *satisfaction* of a formula by α, denoted $\mathcal{M}[\alpha] \models \varphi$ inductively:

(a) If φ is $R(t_1, \dots, t_n)$ then $\mathcal{M}[\alpha] \models \varphi \iff (\alpha(t_1), \dots, \alpha(t_n)) \in R^{\mathcal{M}}$.

(b) If φ is $(s = t)$ then $\mathcal{M}[\alpha] \models \varphi \iff \alpha(s) = \alpha(t) \iff (\alpha(s), \alpha(t)) \in \Delta_M$.

(c) If φ is $\neg A$ then $\mathcal{M}[\alpha] \models \varphi \iff \mathcal{M}[\alpha] \not\models A$.

(d) If φ is $A \to B$ then $\mathcal{M}[\alpha] \models \varphi \iff \mathcal{M}[\alpha] \models A$ implies $\mathcal{M}[\alpha] \models B$.

(e) If φ is $A \vee B$ then $\mathcal{M}[\alpha] \models \varphi \iff \mathcal{M}[\alpha] \models A$ or $\mathcal{M}[\alpha] \models B$.

(f) If φ is $A \wedge B$ then $\mathcal{M}[\alpha] \models \varphi \iff \mathcal{M}[\alpha] \models A$ and $\mathcal{M}[\alpha] \models B$.

(g) If φ is $\forall x\, A$ then $\mathcal{M}[\alpha] \models \varphi \iff \mathcal{M}[\alpha'] \models A$ for every assigment α' such that $\alpha(z) = \alpha'(z)$ for all variables besides x.

(h) If φ is $\exists x\, A$ then $\mathcal{M}[\alpha] \models \varphi \iff \mathcal{M}[\alpha'] \models A$ for some assigment α' such that $\alpha(z) = \alpha'(z)$ for all variables besides x.

An L-formula φ is true in the interpretation $\mathcal{M}$, written as $\mathcal{M} \models \varphi$, if $\mathcal{M}[\alpha] \models \varphi$ for each assignment α. The satisfaction of a sentence A does not depend on the choice of assignment and thus either $\mathcal{M}[\alpha] \models A$ for all α or for no α. Therefore, either $\mathcal{M} \models A$ or $\mathcal{M} \models \neg A$. A formula can be neither true nor false in $\mathcal{M}$ when it has free variables since different assigments may disagree on its satisfaction. However, sentences are always either true or false. If φ is a formula with free variables amoung $\underline{x}$ then for a tuple $\underline{a} \in M$ we write $\mathcal{M} \models \varphi(\underline{a})$ to mean $\mathcal{M}[\underline{x} := \underline{a}] \models \varphi$.

Definition 1.3.4. Let Γ be a first-order theory and $\mathcal{M}$ an L interpretation. If $\mathcal{M} \models \Gamma$ i.e. every axiom of Γ is satisfied in $\mathcal{M}$, then we say that $\mathcal{M}$ is a *model* of Γ.

Definition 1.3.5. Let $\mathcal{M}$ be an L-interpretation. Then $\mathrm{Th}_L(\mathcal{M})$, the theory of $\mathcal{M}$, is the set of true L-sentances of $\mathcal{M}$.

Definition 1.3.6. Two L-interpretations $\mathcal{M}$ and $\mathcal{N}$ are said to be elementary equivalent, written $\mathcal{M} \equiv \mathcal{N}$, if they have the same set of true L-sentences.

Lemma 1.3.7. If $\mathrm{Th}_L(\mathcal{M}) \subset \mathrm{Th}_L(\mathcal{N})$ then $\mathrm{Th}_L(\mathcal{M}) = \mathrm{Th}_L(\mathcal{N})$ and thus $\mathcal{M} \equiv \mathcal{N}$.

Proof. Let A be an L-sentence. If $\mathcal{M} \models A$ then by hypothesis $\mathcal{N} \models A$. However, if $\mathcal{M} \not\models A$ then, because A is a sentence, $\mathcal{M} \models \neg A$ so $\mathcal{N} \models \neg A$ and thus $\mathcal{N} \not\models A$. $\square$

Definition 1.3.8. Two L-interpretations $\mathcal{M}$ and $\mathcal{N}$ are said to be isomorphic, written $\mathcal{M} \cong \mathcal{N}$, if there is a bijection $\sigma : M \to N$ such that,

(a) For each constant symbol c, we have $\sigma(c^{\mathcal{M}}) = c^{\mathcal{N}}$.

(b) For each relation R and tuple $\underline{a} \in M$ we have $\underline{a} \in R^{\mathcal{M}} \iff \sigma(\underline{a}) \in R^{\mathcal{N}}$.

(c) For each function f and tuple $\underline{a} \in M$ we have $\sigma(f^{\mathcal{M}}(\underline{a})) = f^{\mathcal{N}}(\sigma(\underline{a}))$.

Proposition 1.3.9. Let $\sigma : \mathcal{M} \to \mathcal{N}$ be an isomorphism of L-interpretations. Then we have

$$\mathcal{M} \models \varphi(\underline{a}) \iff \mathcal{N} \models \varphi(\sigma(\underline{a}))$$

for any $\underline{a} \in M$ and L-fomula φ with parameters.

Proof. Induction on the complexity of a formula. □

Corollary 1.3.10. If $\mathcal{M} \cong \mathcal{N}$ then $\mathcal{M} \equiv \mathcal{N}$.

Proof. The above proposition applied to parameter-free formulas i.e. sentences says,

$$\mathcal{M} \models A \iff \mathcal{N} \models A$$

which is exactly the content of $\mathcal{M} \equiv \mathcal{N}$. □

Definition 1.3.11. A first-order theory Γ *semantically entails* or simply *entails* an L-formula A, written $\Gamma \models A$, if A is true in every model of Γ i.e. whenever $\mathcal{M} \models \Gamma$ then $\mathcal{M} \models A$.

Definition 1.3.12. A first-order theory is *satisfiable* (or consistent) if it admits a model.

Definition 1.3.13. A first-order theory is *model complete* if any two models are elementary equivalent.

2 The Completeness of First-Order Logic

The crowning achievment of mathematical logic is to join syntactics and semantics into a unified theory. This was accomplished in one fell swoop by the greatest logician to ever live, Kurt Gödel, in his celebrated "completeness theorems" for first-order logic. Care must be taken to not mistake the "completeness theorems" with Gödel's most famous work, his "incompletness theorems." The situation seems designed for confusion. Hopfully this distinction will clear things up. The *incompletness* theorems deal with the technical notion of proof-theoretic and model-theoretic completeness we discussed earlier and show that various theories cannot be complete in this sense. On the other hand, the *completness* theorems consider the informal notion of the completness of first-order logic as a whole in the sense that proof theory and model theory complete eachother.

Theorem 2.0.1 (Model Existence)**.** A first-order theory is satisfiable if and only if it is consistent in the proof-theoretic sense. Furthermore, any consistent L-theory has a model of cardinality at most $|L|$.

Proof. The proof of this theorem is long and highly technical so we cannot cover it here. The proof first constructs a maximally consistent set (consistent and every sentence or its negation is included) of sentances containing the theory and then constructs a model in which these are exactly the true sentances. □

Theorem 2.0.2 (Adequacy)**.** If $\Gamma \models A$ then $\Gamma \vdash A$. That is, if A is true in every model then there exists a formal proof of A.

Proof. Suppose that $\Gamma \nvdash A$ then we know that $\Gamma \cup \{\neg A\}$ is consistent. By the model existence theorem there exists a model of $\Gamma \cup \{\neg A\}$. However, this is a model of Γ in which A is false. Thus $\Gamma \not\models A$. ☐

Theorem 2.0.3 (Soundness)**.** If $\Gamma \vdash A$ then $\Gamma \models A$ i.e. A is true in every model.

Proof. The proof is quite simple and uses induction on proofs. The only piece of input is to check that one application of a rule of inference preserves truth value for any truth assignment. This follows easily from the inductive definition of truth assigments. ☐

Theorem 2.0.4. All models of Γ are elementary equivalent if and only if Γ is complete in the proof-theoretic sense.

Proof. Suppose that Γ is complete and let $\mathcal{M}$ be a model of Γ. For any first order sentence A, if $\Gamma \vdash A$ then $\mathcal{M} \models A$. Furthermore if $\Gamma \nvdash A$ then by completeness $\Gamma \vdash \neg A$ and thus $\mathcal{M} \models \neg A \iff \mathcal{M} \not\models A$. Thus,

$$\mathcal{M} \models A \iff \Gamma \vdash A$$

Therefore, every model of Γ has the same set of true first-order sentences and are thus all elementary equivalent.

Conversely, suppose that all models of Γ are elementary equivalent. For any model $\mathcal{M}$ of Γ and any sentence A either $\mathcal{M} \models A$ or $\mathcal{M} \models \neg A$. Furthermore, for any other model $\mathcal{N}$ we have $\mathcal{M} \equiv \mathcal{N}$ so either A or $\neg A$ is true in every model of Γ. Therefore, by the adequacy theorem, either $\Gamma \vdash A$ or $\Gamma \vdash \neg A$ so Γ is proof-theoretically complete. ☐

A finaly elegant summary of these results is given by Gödel's monumentous theorem:

Theorem 2.0.5 (Gödel)**.** For any first-order theory, $\Gamma \vdash A \iff \Gamma \models A$.

3 The Compactness of First-Order Logic

Here we will dive into model-theory proper in which we want to study properties of the set of all possible models of a given theory. However, it is often the case that proof-theoretic methods will provide insight and clever proofs even for purely model-theoretic statements.

Theorem 3.0.1 (Compactness)**.** A first-order theory is satisfiable if and only if it is finitely satifiable.

Proof. Suppose that Γ is not satisfiable. By the model existence theorm, Γ must be incomplete so there exist proofs $\Gamma \vdash A$ and $\Gamma \vdash \neg A$. However, every proof is finite so each can only use a finite set of axioms in Γ. Call the set of all axioms in Γ used in either proof $\Delta \subset \Gamma$. Thus, $\Delta \vdash A$ and $\Delta \vdash \neg A$ so Δ cannot admit a model and is finite. Therefore, if every finite subtheory $\Delta \subset \Gamma$ has a model then Γ must have a model. ☐

Remark. There exist purely model-theoretic proofs of the Compactness theorem but they require more sophisticated ideas such as ultra-products.

3.1 Ultra-Products

4 The Löwenheim–Skolem Theorem

Definition 4.0.1. Consider the first-order statments of the form,

$$\exists x \exists y \exists z : x \neq y \wedge y \neq z \wedge z \neq x$$

which express that there exist at least n elements. Call Σ the set of all such statments. Furthermore, for any set of constant symbols C, define,

$$\Sigma_C = \{\neg(a = b) \mid a, b \in C \text{ such that } a \neq b\}$$

the set of all sentances of the form $a \neq b$.

Theorem 4.0.2. Let Γ be a first order theory. If Γ has arbitrarily large finite modeles then Γ admits an infinite model.

Proof. Consider the first-order theory $\Gamma \cup \Sigma$. Since Γ has arbitrarily large finite models we know that any finite subset $\Delta \subset \Gamma \cup \Sigma$ is satisfiable by a large enough finite model of Γ. By the Compactness theorem, there exists a model of $\Gamma \cup \Sigma$ which is a model of Γ which cannot have any finite number of elements. $\square$

Remark. This theorem about deducing the sizes of possible models gives a small taste of the powerful Löwenheim–Skolem theorem yet to come. However, the finite version is very important for proving the consistency of a new theory. Furthermore, the technique of adding an infinite set of first-order theorem which together impose a strict condition but in isolation are easily satisfied and then applying the compactness theorem comes up over and over in mathematical logic.

Theorem 4.0.3 (Löwenheim–Skolem)**.** Let L be a first-order language and $\mathcal{M}$ an infinite L-interpretation. Then for any cardnal $\kappa \geq |L|$ there exists an L-interpretation $\mathcal{N}$ such that $\mathcal{M} \equiv \mathcal{N}$ and $|\mathcal{N}| = \kappa$. We call such an $\mathcal{N}$ an elementary substructure or elementary extension.

Proof. First suppose that $\kappa > \max(|\mathcal{M}|, |L|) \geq \aleph_0$. Let C be a set of constant symbols with $|C| = \kappa$ and construct the language L^+ generated by $L \cup C$. Now, consider the L^+-theory $\Gamma_{\mathcal{M}} = \mathrm{Th}_L(\mathcal{M}) \cup \Sigma_C$. For any finite subtheory $\Delta \subset \Gamma_{\mathcal{M}}$, I claim that $\mathcal{M} \models \Delta$. This is because Δ contains only true L-sentences of $\mathcal{M}$ and a finite number of Σ_C statements which can be interpreted by sending any distinct elements of $\mathcal{M}$ to the finite number of C-constants which appear in Δ. Thus, $\Gamma_{\mathcal{M}}$ is finitely satisfiable so, by compactness, $\Gamma_{\mathcal{M}}$ is satisfiable and thus consistent. By the model existence theorem there exists a model $\mathcal{M}' \models \Gamma_{\mathcal{M}}$ such that $|\mathcal{M}'| \leq |L^+| = |C| = \kappa$ (since $\kappa > |L| \geq \aleph_0$). However, since $\Sigma_C \subset \Gamma_{\mathcal{M}}$ we must have an injection $C \to M'$ because not two C-constants can be interpreted as equal (since $a \neq b$ is true in $\Gamma_{\mathcal{M}}$ for all $a, b \in C$). Thus, $|\mathcal{M}'| = |C| = \kappa$. We may view $\mathcal{M}'$ as an L-interpretation since $L \subset L^+$. Furthermore, $\mathrm{Th}_L(\mathcal{M}) \subset \Gamma_{\mathcal{M}}$ and $\mathcal{M}' \models \Gamma_{\mathcal{M}}$ so $\mathrm{Th}_L(\mathcal{M}) \subset \mathrm{Th}_L(\mathcal{M}')$ and thus $\mathcal{M} \equiv \mathcal{M}'$ as L-interpretations. $\square$

Remark. An immediate consequence of the preceeding theorems is that having arbitrarily large finite models implies having models of every infinite cardinality. This is very powerful and surprising. The Löwenheim–Skolem theorem and they compactness theorem show that first-order logic is insufficient to constrain the size of its models. We will make this notion percise within the framework of first-order properties.

5 Skolem's Paradox and Higher-Order Logic

5.1 First-Order Properties

(FINITENESS) (SIZE) (REAL NUMBERS)

5.2 Higher-Order Logic

5.3 Nonstandard Models of Set Theory

6 Categoricity

Definition 6.0.1. A first-order theory is κ-categorical if all models of size κ are isomorphic.

Theorem 6.0.2 (Vaught)**.** Supppose that Γ is κ-categorical for some $\kappa \geq |L|$ and has only infinite models then Γ is model complete.

Proof. Let $\mathcal{M} \models \Gamma$ and $\mathcal{N} \models \Gamma$ be models. By the Löwenhiem-Skolem theorem, there exists models $\mathcal{M}'$ and $\mathcal{N}'$ of cardinaility κ such that $\mathcal{M} \equiv \mathcal{M}'$ and $\mathcal{N} \equiv \mathcal{N}'$. However, by κ-categoricity, we know that $\mathcal{M}' \cong \mathcal{N}'$ since $|\mathcal{M}'| = |\mathcal{N}'| = \kappa$. Therefore, $\mathcal{M} \equiv \mathcal{M}' \equiv \mathcal{N}' \equiv \mathcal{N}$ so Γ is model complete. ☐

7 Applications To Algebraic Geometry

Definition 7.0.1. The first-order language of fields, denoted F, is generated by the signature $\sigma_F = \{0, 1, +, \cdot\}$ where 0 and 1 are constant symbols and $+$ and $\cdot$ are 2-ary function symbols.

Definition 7.0.2. The theory ACF is the first-order theory of algebraically closed fields is defined over F and has axioms:

(a) Field Axioms.

(b) Algebraic Closure: for each positive integer n, the sentence,

$$\forall a_0 \forall a_2 \cdots \forall a_n \exists x \ [a_n \cdot x^n + \cdots + a_1 \cdot x + a_0 = 0]$$

where exponentiation by a fixed integer is shortand for repeated multiplication.

Definition 7.0.3. The theory ACF_p is the first-order theory of algebraically closed fields of characteristic p is defined over F and has axioms $\mathrm{ACF}_p = \mathrm{ACF} \cup C_p$ where C_p limits the characteristic. Let σ_k be the sentence,

$$1 + 1 + \cdots + 1 = 0$$

with exactly k ones. Then $C_p = \{\neg\sigma_k \mid k < p\} \cup \{\sigma_p\}$ and $C_0 = \{\neg\sigma_p \mid k \in \mathbb{Z}^+\}$.

Theorem 7.0.4 (Steinitz)**.** All algebraically closed fields of the same uncountable cardinality and characteristic are isomorphic. That is, ACF_p is uncountably-categorical for any characteristic.

Proof. This theorem uses the axiom of choice and equivalences of transendence bases. It is not wildly difficult but is outisde the scope of this discussion. ☐

Corollary 7.0.5. ACF_p is complete.

Proof. There are infinitely many irreduicble polynomials and each have distinct roots. Thus any algebraially closed field is infinite. Let $\mathcal{M} \models \text{ACF}_p$ and $\mathcal{N} \models \text{ACF}_p$ be models. By the Löwenhiem-Skolem theorem, there exists a model $\mathcal{M}'$ of cardinaility $|\mathcal{N}|$ (since it is infinite) such that $\mathcal{M} \equiv \mathcal{M}'$. However, by categoricity, we know that $\mathcal{M}' \cong \mathcal{N}$ since they are models with the same cardinality. Therefore, $\mathcal{M} \equiv \mathcal{M}' \equiv \mathcal{N}$ so ACF_p is model complete. $\square$

Theorem 7.0.6 (Lefschetz Principle)**.** The true first-order sentences about $\mathbb{C}$ and about $\overline{\mathbb{Q}}$ are the same. This is often stated as, the first-order theory of algebraic geometry over $\mathbb{C}$ is the same as over $\overline{\mathbb{Q}}$.

Proof. By the completeness of ACF_0 we have $\overline{\mathbb{Q}} \equiv \mathbb{C}$. $\square$

Theorem 7.0.7 (Cross-Characteristic Transfer)**.** Let A be a first order F-sentence. Then $\text{ACF}_0 \models A$ if and only if $\overline{\mathbb{F}_p} \models A$ for all but finitely many p.

Proof. Consider any finite subtheory $\Delta \subset \text{ACF}_0 \cup \{A\}$. Since Δ may contain only finitely many sentences constraining the characteristic and for large enough p we know that $\overline{\mathbb{F}_p} \models A$, we can choose p large enough such that $\overline{\mathbb{F}_p} \models \Delta$. Therefore, Δ is satisfiable so $\text{ACF}_0 \cup \{A\}$ is finitely-satisfiable. Thus, by the compactness of first-order logic, $\text{ACF}_0 \cup \{A\}$ is satisfiable so there exists a model of ACF_0 in which A is true. Thus, by the completeness of ACF_0 we know that $\text{ACF}_0 \models A$.

Conversely suppose we can find arbitrarily large p such that $\overline{\mathbb{F}_p} \models \neg A$. Again, take a finite subtheory $\Delta \subset \text{ACF}_0 \cup \{\neg A\}$ and choose p large enought that it satisfies the finite number of sentences in Δ constraining the characteristic in which A is false. Thus, $\overline{\mathbb{F}_p} \models \neg A$ so $\text{ACF}_0 \cup \{\neg A\}$ is finitely satisfiable and thus, by compactness, satisfiable. As before, there exists a model of ACF_0 in which A is false so, by completeness, $\text{ACF}_0 \models \neg A$. $\square$

Theorem 7.0.8 (Ax-Grothendiek)**.** If a polynomial map $f : \mathbb{C}^n \to \mathbb{C}^n$ is injective then it is surjective.

Proof. For a fixed natural number d consider the first order sentence,

$$AG = \forall \underline{a}_0 \forall \underline{a}_1 \cdots \forall \underline{a}_d \Bigg[\forall \underline{x} \forall \underline{y} \Big[\Big(\underline{a}_d \cdot \underline{x}^d + \cdots + \underline{a}_1 \cdot \underline{x} + \underline{a}_0 = \underline{a}_d \cdot \underline{y}^d + \underline{a}_1 \cdot \underline{y} + \cdots + \underline{a}_0 \Big) \to \underline{x} = \underline{y} \Big]$$
$$\to \Big[\forall \underline{y} \exists \underline{x} : \underline{a}_d \cdot \underline{x}^d + \cdots + \underline{a}_1 \cdot \underline{x} + \underline{a}_0 = \underline{y} \Big] \Bigg]$$

which expresses the Ax-Grothendiek theorem for degree n. Here exponentiation is short for multiplication written a fixed number of times and underlined variables represent n-tuples with operations and comparisions defined componentwise i.e. each comparision is a conjunction of n comparisions on the components. Furthermore, suppose that a map $f : \overline{\mathbb{F}_p}^n \to \overline{\mathbb{F}_p}^n$ given by polynomials is injective. For each element $\underline{y} \in \overline{\mathbb{F}_p}^n$ consider the field extension $k = \mathbb{F}_p[\underline{a}_0, \dots, \underline{a}_d, \underline{y}]$ given by adjoing the coefficients of f and coordinates of y. Since these are elements of $\overline{\mathbb{F}_p}$ each is algebraic and thus k is a finite extension of $\mathbb{F}_p$ and thus a finite field. Furthermore f restricts to a map $f : k^n \to k^n$ since it is given by polynomials with coefficients in k. However, this restriction is still injective and therefore surjective because k^n is a finite set. Thus, $\exists \underline{x} \in k^n$ such that $f(\underline{x}) = \underline{y} \in k^n$ so f is surjective.

Since $\overline{\mathbb{F}_p} \models AG$ for every p we know that $\text{ACF}_0 \models AG$ and thus the Ax-Grothendiek theorem is true for every algebracially closed field of characteristic zero inculuding $\mathbb{C} \models AG$. $\square$

Theorem 7.0.9 (Strong Ax-Grothendiek)**.** Let V be an affine variety over an algebraically closed field and $f : V \to V$ a morphism. If f is injective then it is surjective.

Theorem 7.0.10. Every extension of algebracially closed fields is elementary.

Proof. This follows from quantifier elimination. $\square$

Theorem 7.0.11 (Hilbert's Nullstellensatz)**.** Let $I \subset \overline{K}[\underline{X}]$ be a proper ideal then the common vanishing set $V(I) = \{p \in \bar{K}^n \mid \forall f \in I : f(p) = 0\}$ is nonempty.

Proof. The ideal I is contained in a maximal ideal. Consider the field $L = \overline{\overline{K}[\underline{X}]/\mathfrak{m}}$ and projecton map $\overline{K}[\underline{X}] \to L$. Since $I \subset \mathfrak{m}$ the image of I is zero in L and thus the image of $\underline{X}$ is a common solution for I. Since $K \subset L$ it is an elementary extension. Since $\overline{K}[\underline{X}]$ is Noetherian, we can find generators $I = (f_1, \ldots, f_n)$. Let $\underline{a} \in \overline{K}$ a tuple encoding the coefficients of the polynomials $f_1, \ldots, f_n$ and $\psi(\underline{a})$ the first order formula encoding the idea that the polynomials with coefficients $\underline{a}$ have a common zero. Since the extension is elementary and $\underline{a} \in K$ we have,

$$K \models \psi(\underline{a}) \iff L \models \psi(\underline{a})$$

However, $\underline{X}$ is a solution in L so $K \models \psi(\underline{a})$. Thus any proper ideal has nonempty vanishing set. $\square$

8 Incompletness and Decidability

9 Provability Logic