MODEL THEORY FOR ALGEBRAIC GEOMETRY

VICTOR ZHANG

Abstract. We demonstrate how several problems of algebraic geometry, i.e. Ax-Grothendieck, Hilbert's Nullstellensatz, Noether-Ostrowski, and Hilbert's 17th problem, have simple proofs when approached from using model theory. The proofs use two general transfer principles. The first is the Lefschetz principle, which allows sentences that are true in algebraically closed fields of infinitely many prime characteristics to transfer to algebraically closed fields of characteristic 0. The second is model completeness, which allows sentences that are true in an algebraically closed field or real closed field to transfer down to an algebraically closed subfield or real closed subfield, respectively.

Contents

Date: August 2015.

1. Introduction

Model theory studies the duality between language and meaning. More precisely, theorems of model theory relate theories, which are sets of sentences, and models, which are mathematical objects for which those sentences are true. Examples of theorems in model theory are the completeness theorem, which establishes an equivalence of a set of sentences T being syntactically consistent, i.e. not proving a contradiction, and being semantically satisfiable, i.e. the existence of some mathematical structure where the sentences of T are true.

This duality in model theory mirrors a similar duality in algebraic geometry, one between formal and symbolic structures such as polynomials and geometric structures such as curves. Stated in model theoretic terms, for a field $F \supseteq \mathbb{Q}$, every set of $n-$valued polynomial equations $S \subseteq \mathbb{Q}[x_1, ..., x_n]$ can be thought of as a quantifier-free formula of one free variable $\phi(v)$ in the language $\mathcal{L} =\{0, 1, +, \times\}$, such that the solution set of S is precisely the definable set defined by $\phi(x)$ in F^n.

The similarity between model theory and algebraic geometry is supported by how a great deal of the applications of model theory have been in algebra. In this paper, we prove several theorems of algebraic geometry using model theoretic approaches, and exhibit the approach of proving theorems about mathematical objects by analysis of language, on the level of strings of first-order logic.

For example, in Ax's proof of the Ax-Grothendieck theorem, which states that every injective map $\mathbb{C}^n \to \mathbb{C}^n$ that is polynomial in all variables is surjective, the key step is the observation that every injective self map of finite sets is surjective. This reduction of the theorem is made possible by writing down in first-order logic the sentences that express the statement 'every injective polynomial map is surjective', and then counting the number of $\forall$ and $\exists$ quantifier inversions in these strings.

Important concepts of model theory used for the proofs in this paper are compactness of first-order logic, completeness of a theory, and quantifier elimination. They allow us to develop two transfer principles, which are used to prove the theorems mentioned above. The Lefschetz principle states that if some sentence is true for sufficiently large algebraically closed fields of finite characteristic, then it is true for all algebraically closed fields of characteristic zero. The model completeness property states that in a theory with quantifier elimination, such as the theory of algebraically closed fields or the theory of real closed fields, to check whether a sentence is true in a model it is sufficient to check it in a submodel or supermodel.

2. Model Theoretic Preliminaries

The reader familiar with the notions of model theory may skip this section. We aim to give a working intuition of the notions of languages, models, syntactic and semantic implication, definable sets, completeness and compactness of first-order logic, and the Lowenheim-Skolem theorems, and thus omit some technical details that are not useful, and cite the relevant sources when needed.

2.1. **Models and Theories, Syntactic and Semantic Implication, Definable Sets.**

Definition 1. A **language**

$$\mathcal{L} = \{c_i,\, f_j,\, r_k : i \in I,\, j \in J,\, k \in K\}$$

is a set of symbols. The symbols c_i are **constant symbols**, f_j are **function symbols** and r_k are **relation symbols**. We require that associated to each function symbol f_j and relation symbol r_k is a unique natural number n_{f_j} or n_{r_k} respectively, defined as the the **arity** of the function or relation symbol. The arity is meant to represent the intended number of inputs of a function or relation represented by the function or relation symbol.

The following are examples of languages, with the first example being the most important for this paper.

Example 2. 1. The **language of rings** $\mathcal{L}_{ring} = \{0, 1, +, -, \cdot\}$, with constant symbols $0, 1$ and function symbols $+$ and $\cdot$ with $n_+ = 2$ and $n_\cdot = 2$. (i.e. both $+$ and $\cdot$ are binary functions).

2. The language of sets, $\mathcal{L}_{set} = \{\in\}$ with one relation symbol $\in$ with $n_\in = 2$.

3. The language of orderings, $\mathcal{L}_{order} = \{\leq\}$ with one relation symbol $\leq$ with $n_\leq = 2$.

Languages are the lexicon of non-logical symbols from which sentences and formulas of first-order are built. The logical symbols are the standard symbols of first-order logic, i.e. quantifiers, implication symbols, a binary relation symbol representing equality, negation, parentheses, conjunction and disjunction

$$\forall,\ \exists,\ \rightarrow, \leftrightarrow, =,\ \neg,\ (\ ,\ ),\ \wedge,\ \vee$$

and countably many variable symbols.

Regardless of choice of language, we allow logical symbols to be included as valid building blocks for any formula, which we explain soon.

In practice, we use roman symbols other than v as variable symbols, e.g. x, y, or $x_1, ..., x_n$, etc. when the context is clear.

We now explain what we mean by formulas, sentences and free and bound variables. Intuitively, a formula $\phi(x, y)$ with free variables x, y is a "valid" string of symbols such that when when we replace (x, y) with a pair of elements (a, b) from a real mathematical object M, the resulting expression $\phi(a, b)$ is something that can be evaluated as true or false in M.

For example, in the language of rings and when $M = \mathbb{Z}$ and $\phi(x, y) \coloneqq x+y = 0$, then $\phi(1, -1) \coloneqq 1+(-1) = 0$ is true, while $\phi(0, 1) \coloneqq 0+1 = 0$ is false.

The actual definition of formulas and sentences is by a tedious induction, so instead we give illustrating examples.

Example 3. The following are examples of **formulas** in their respective languages $\mathcal{L}$. Consistent with the usage of mathematics, we require that formulas be of finite length. We write $\phi(\overline{x})$ to denote a formula with free variables in $\overline{x}$ where $\overline{x}$ is a finite vector of variable symbols in x, i.e. $\overline{x} = (x_1, ..., x_k)$ for some $k \in \mathbb{N}$. For each example we include in parentheses an interpretation of what the formula is meant to express.

(1) $\mathcal{L} = \mathcal{L}_{ring}$; $\phi(x, y) \coloneqq x + y = 0$ (i.e. x and y sum to 0)
(2) $\mathcal{L} = \mathcal{L}_{ring}$; $\phi(x) \coloneqq x^2 - 2 = 0 \coloneqq ((x \cdot x) - 1) - 1 = 0$ (i.e. x a a square root of 2).
(3) $\mathcal{L} = \mathcal{L}_{order}$; $\phi \coloneqq \exists x \forall y (x < y)$ (i.e. there exists a lower bound)

Example 4. A **bounded variable** is a variable referred to by quantifiers. The variables x, y in example 3 are bounded variables. A **free variable** is a variable that is not bounded. The formula in 1 has two free variables, the one in 2 has one free variable. A formula with no free variables is called a **sentence**. The formula in 3 is a sentence.

Definition 5. A **theory** of $\mathcal{L}$ is a set of sentences T each with symbols only from $\mathcal{L}$ and logical symbols. We say T is an $\mathcal{L}-$**theory**.

Most mathematical theorems can be formulated as a sentence in the language of sets, $\mathcal{L}_{set}$, and are proved from the theory $T = ZFC$ where ZFC is the axioms of ZFC. We explain what we mean by a proof. The formal definition of a proof is inductive and tedious, so we only give a working idea of it. Let σ be a sentence in $\mathcal{L}$ that we think of as a theorem to be proved, and let T be a $\mathcal{L}-$theory that we think of as a set of axioms. In addition to T we also make available for the purposes of proof standard axioms of logic, e.g. the law of the excluded middle, that we do not need to define explicitly here. A **proof of σ from T** is a sequence of sentences $\sigma_1, ..., \sigma_{n-1}, \sigma_n \equiv \sigma$ that ends in σ such that each σ_i is an axiom, i.e. an element of T or a standard axiom of logic, or deduced from previous elements of the sequence following the rules of deduction of first-order logic. We omit a formal definition of the rules of deduction.

In order to avoid confusion between the equality symbol $=$ that may appear in strings and equality as identity, given formulas ϕ, ψ, we write $\phi \equiv \psi$ to mean ϕ and ψ are identical strings, or possibly that ϕ and ψ are equivalent, i.e. each is provable from the other from only the rules of deduction and axioms of logic.

Definition 6. Let T be an $\mathcal{L}-$theory and let σ be an $\mathcal{L}-$sentence.

1. We say $T \vdash \sigma$ or T **proves** σ or T **syntactically implies** σ if there is a proof of σ from T.

2. We say T is **complete** if it proves every sentence or its negation, i.e. for every $\mathcal{L}-$ sentence ϕ, $T \vdash \phi$ or $T \vdash \neg\phi$.

3. We say T is **consistent** if it does not prove a contradiction, i.e. if $T \vdash \phi$ then $T \not\vdash \neg\phi$ for every $\mathcal{L}-$ sentence ϕ.

We now define what it means for some mathematical object M to satisfy a set of sentences T, i.e. be such that every sentence of T is true.

Definition 7. Let $\mathcal{L} =\{c_i,\, f_j,\, r_k : i \in I,\, j \in J,\, k \in K\}$ be a language. A **model** or **$\mathcal{L}-$structure** is a set M and elements c_i', functions f_j' and relations r_k' for $i \in I$, $j \in J$ and $k \in K$ such that:

1. For every constant symbol $c_i \in \mathcal{L}$, $c_i' \in M$.

2. For every function symbol $f_j \in \mathcal{L}$ with arity n, f_j' is a function $M^n \to M$.

3. For every relation symbol $r_k \in \mathcal{L}$ with arity s, r_k' is a $s-$ary relation of M, i.e. $r_k' \subseteq M^s$.

When there is no confusion, we use the syntactic symbols c_i, f_j and r_k to denote the actual constants, actual functions and actual relations of M, e.g. $f_j : M^n \to M$ would denote the function f_j'.

Example 8. The following are $\mathcal{L}-$structures of their respective languages.

1. The complex numbers $\mathbb{C}$ with the usual binary operations of addition and multiplication and usual additive and multiplicative identities 0 and 1 is a $\mathcal{L}_{ring}-$structure.

2. The natural numbers $\mathbb{N}$ with the usual ordering is a $\mathcal{L}_{order}-$structure.

The constants, functions and relations c_i, f_j and r_k of a model that correspond to the symbols c_i, f_j and r_k allow us to evaluate the truth of a sentence ϕ in M. The actual definition of truth in a model is again by a tedious induction, so instead we give illustrating examples. An important thing to note is that the truth of a sentence is only defined relative to a model, because all variables are only allowed to vary over elements of the model, and all quantification is over elements of the model.

Definition 9. If an $\mathcal{L}-$sentence σ is true in an $\mathcal{L}-$structure M, we say $M \models \sigma$ or M **is a model of** σ or M **models** σ. For an $\mathcal{L}-$theory T, we say $M \models T$ or M **models** T if M models every sentence in T. The following sentences are **true** in their respective models.

Example 10. 1. The following sentence expressing "-1 has a square root" is true in $\mathbb{C}$, but not in $\mathbb{R}$

$$\mathbb{C} \models (\exists x) x^2 = -1$$

$$\mathbb{R} \not\models (\exists x) x^2 = -1$$

2. Let $p(x) \in \mathbb{Z}[x]$ be a polynomial in the integers. Observe $p(x)$ is expressible purely as a string of symbols in $\mathcal{L}_{ring}$, for example $3x^2 + 2$ is expressible as $(1+1+1) \cdot x \cdot x + 1 + 1$. Since $\mathbb{C}$ is algebraically closed, we have

$$\mathbb{C} \models (\exists x) p(x) = 0$$

or $\mathbb{C}$ models a sentence expressing "$p(x)$ has a root".

If we define $T = \{p(x) = 0 : p(x) \in \mathbb{Z}[x]\}$ to be the set of all sentences expressing the existence of roots of polynomials in the integers, we have $\mathbb{C} \models T$.

3. The sentence "there exists a least element" is true in the natural numbers with the natural order, $\mathbb{N} \models (\exists n)(\forall m)\, n \leq m$.

4. The sentence $\phi \coloneqq (\exists n)(\forall m) m \leq n$ saying "there exists a greatest element" is not true in the natural numbers, we say it is **false**. We say $\mathbb{N}$ does not model ϕ or $\mathbb{N} \not\models \phi$; in fact, $\mathbb{N} \models \neg\phi$, i.e. the negation of ϕ is true in $\mathbb{N}$, because it is true that there does not exist a greatest element in $\mathbb{N}$. $\mathbb{N} \models \neg\sigma$ implies $\mathbb{N} \not\models \sigma$ or else both σ and $\neg\sigma$ will be true of the natural numbers, a contradiction.

Definition 11. (semantic implication of theories) Let T be an $\mathcal{L}-$theory and σ a $\mathcal{L}-$sentence. We say $T \models \sigma$ if every model of T models σ, i.e. for all $\mathcal{L}-$structures M such that $M \models T$, $M \models \sigma$. If T' is a set of $\mathcal{L}$ sentences, we say $T \models T'$ if $T \models \sigma$ for every $\sigma \in T'$. Define **the**

theory of a model $\mathrm{Th}(M)$ to be the set of all sentences σ such that $M \models \sigma$.

We now introduce the notion of definable sets.

Definition 12. 1. Let T be an $\mathcal{L}-$theory, and M a model of T. Let $X \subseteq M$ be a set which we call the set of **parameters** in M. Let $S \subseteq M^n$. We say S is **definable with parameters** from X if there exists a formula $\phi(x_1, ..., x_n, y_1, ..., y_k)$ with $n + k$ free variables and elements $b_1, ..., b_k \in X$ such that for all $\overline{a} := (a_1, ..., a_n) \in M^n$, $\overline{a} \in S$ if and only if $M \models \phi(\overline{a}, \overline{b}) := \phi(a_1, ..., a_n, b_1, ..., b_k)$. We simply say S is **definable** if S is definable with parameters from the empty set, i.e. S is definable without parameters. For a nonzero natural number m, we say S is $m-$**definable** if S is definable with $k \leq m$ parameters from M.

2. Let $c \in M$ be a fixed element. c is definable if $\{c\}$ is definable.

3. Let $f : M^k \to M$ be a function. f is definable if the set $S = \{(\overline{a}, b) : \overline{a} \in M^k, b \in M, f(\overline{a}) = b\}$ is definable, i.e. functions are definable if their graphs are definable.

4. Let $r \subseteq M^k$ be a relation. r is definable if it is definable, i.e a relation is definable if it is definable as a subset of the Cartesian product. This definition is technically not necessary, but we include it to highlight it.

Remark 13. Suppose in addition to the symbols in $\mathcal{L}$, we have definable constants, functions and relations c, f, r. Then when writing out $\mathcal{L}-$formulas, without loss of generality we may include symbols for c, f, r in the language because every instance of the new symbols is just a shorthand of the formulas defining c, f, r. (the case of a definable function is more technically involved and inductive, but not particularly enlightening).

Example 14. 1. As seen before in item (2) of the previous example, each integer is definable in $\mathbb{C}$ in $\mathcal{L}_{ring}$.

2. Division is definable in any field F in $\mathcal{L}_{ring}$ because $\frac{a}{b} = c$ if and only if $a = bc$. Therefore each rational number is definable if F is of characteristic 0.

3. Every rational function with coefficients in $\mathbb{Q}$, given by the evaluation map, is definable in a field of characteristic 0 in $\mathcal{L}_{ring}$.

2.2. The Completeness and Compactness Theorems, Lowenheim-Skolem Theorems.

The completeness theorem establishes an equivalence between the notions of syntactic consistency and semantic satisfiability, i.e. a theory is consistent if and only if it has a model. The proof of the completeness theorem, however, is technically involved, so we only give the main idea. We first introduce a definition below.

Definition 15. Let I be the set of all $\mathcal{L}-$sentences of the form $\exists x\, \phi(x)$ where $\phi(x)$ is a $\mathcal{L}$ formula. Let $C = \{c_i : i \in I\}$ be a new set of symbols and $\mathcal{L}' = \mathcal{L} \cup \mathrm{C}$. Let T' be an $\mathcal{L}'-$theory. We say T' is a **blueprint set** if T' is complete, and for each $\mathcal{L}-$sentence of the form $\psi := \exists x\, \phi(x)$, $T' \vdash \phi(c_\psi) \leftrightarrow \exists x\, \phi(x)$. We say c_ψ is a **witness** for ψ.

The idea of the proof of the completeness theorem is that to explicitly construct a model M for a consistent set of sentences T, we take a "free model" F and take a quotient by a relation $\sim$. Intuitively, in a theory T, the only sentences forcing elements to exist are sentences of the form $\psi := \exists x \phi(x)$, which asserts 'an element with property ϕ exists'. We give each such existential sentence a token constant symbol c_ψ, and take $F = C$ to be the set of all such token constants. We define $\sim$ and the corresponding constant, function and relations on $F/\sim$ according to some blueprint set.

Theorem 16. *(Completeness Theorem): Let T be an $\mathcal{L}-$theory. Then T is consistent if and only if T has a model*

Proof. ($\leftarrow$) This direction is immediate. For if M is a model of T, then if T is inconsistent, T will prove a contradiction, and thus, every sentence, including the sentence $(\exists x)(x \neq x)$. But in no model is there an element not equal to itself.

($\rightarrow$) Via transfinite induction (and hence a form of the axiom of choice), extend T to a blueprint set T'. Define a model $M = F/\sim$ as $F = C$ and $\sim$to be defined by $c_i \sim c_j$ if and only if $T' \vdash c_i = c_j$. In defining the interpretations for the constant, function and relation symbols in M, the blueprint set T' will contain sentences that literally assert what the constant, function and relations should be. We refer to [2, Tserunyan] for the details. □

Definition 17. We say an $\mathcal{L}-$theory T is **satisfiable** if it has a model. We say T is **finitely satisfiable** if every finite subset of T has a model.

Theorem 18. *(Compactness Theorem): Let T be a $\mathcal{L}-theory$. Then T is satisfiable if and only if T is finitely satisfiable.*

Proof. Observe that a theory is consistent if and only if every finite subset is consistent. This is because proofs are finitely long, and any deduction of a contradiction uses only finitely many axioms. By the completeness theorem, a theory is satisfiable if and only if every finite subset is satisfiable. □

Example 19. (non-noetherian ring with the same theory as the integers) Let $\mathcal{L}' = \mathcal{L}_{ring} \cup \{c\}$ be the language of rings with one constant symbol added in. Let T be Th($\mathbb{Z}$) union the set

$$\{\bigwedge_{i=1}^{k} [(\exists x) x \cdot (p_1 \cdot ... \cdot p_i) = c] \wedge \left[(\forall x) x \cdot p_i^2 \neq c\right] : p_i \text{ are prime, } k \in \mathbb{N}\}$$

be the theory of the integers, with infinitely many new sentences for initial segment of primes $p_1, ..., p_k$ asserting that c is divisible by p_i but not by p_i^2 for $i = 1, ..., k$. T is finitely satisfiable, because for every finite subset of T referencing primes $p_1, ..., p_n$, the integers with $c = p_1 \cdot ... \cdot p_n$ is a model. Then T is satisfiable, by some model M. In particular, this model M contains an element c that is divisible by every prime exactly once. If we consider M as an $\mathcal{L}_{ring}$ model by forgetting the constant symbol, M is a model of Th($\mathbb{Z}$), i.e. it satisfies all the same first-order sentences as the integers, but it has an element divisible by each prime exactly once. M has an infinite ascending chain of ideals given by repeatedly dividing c by the prime numbers one by one:

$$(c) \subseteq (\frac{c}{p_1}) \subseteq (\frac{c}{p_1 p_2}) \subseteq ...$$

Since c is divisible by both p_1 and $p_1 p_2$, there exists elements x, y such that $c = x p_1 = y p_1 p_2$, and $x = \frac{c}{p_1}$, which implies $\frac{x}{p_1} = y p_2$ so $\frac{x}{p_1}$ is divisible by p_2. We repeat this analysis with $\frac{c}{p_1}$ being divisible by both p_2 and $p_2 p_3$ to conclude that $\frac{c}{p_1 p_2}$ is divisible by p_3 and and so forth for the rest of the inclusions. This shows that this chain of ideals is defined. Furthermore, it is proper because since c is divisible by p_1 but not p_1^2, $c \in (c)$ but $c \notin (\frac{c}{p_1})$, and similarly so for the rest of the inclusions.

This shows the property of being a noetherian ring is not expressible as a set of sentences in first-order logic, otherwise Th($\mathbb{Z}$) would model such a set and our example model would be a noetherian ring.

Since we proved the compactness theorem by the completeness theorem, what the compactness theorem does is apply the completeness theorem in the background. i.e. if a set T is finitely satisfiable, then it is consistent, the completeness theorem generates a model for T, which shows T is satisfiable. Assuming T has no finite models, if we inspect the cardinality of the model generated by the completeness theorem, we see that is it countable, given that the language is countable, because it is constructed from the set of all sentences in $\mathcal{L}$. By cardinal arithmetic on the size of $\mathcal{L}$, this generalizes to the following theorem.

Theorem 20. *(Lowenheim-Skolem Theorems). Let T be a consistent theory in $\mathcal{L}$ with no finite models. Let M be a model of T.*

1. (Downward Lowenheim-Skolem) T has a model of size $|\mathcal{L}| + \aleph_o$.

2. (Upward Lowenheim-Skolem) for every cardinality $\kappa \geq M$, T has a model of size at least κ.

Corollary 21. *For every cardinality $\kappa \geq |M|$, T has a model of cardinality κ.*

Proof. (1) follows by counting the size of the set of all finite strings in $\mathcal{L}$. (2) follows by compactness, by adding in κ many constants c_i for $i \in \kappa$, then taking the theory $T' = T \cup \{c_\alpha \neq c_\beta :\ \alpha,\ \beta \in \kappa\}$ which is T but with infinitely new sentences asserting that the κ many constants are all distinct. T' has a model M', as M is model of every finite subset, and M' contains at least κ many elements. The corollary follows by applying (1) to T'. □

3. The Lefschetz Principle, Ax-Grothendieck Theorem and Noether-Ostrowski Irreducibility Theorem

We are now ready to begin applying these model theoretic tools to algebraic geometry. We assume some knowledge of abstract algebra and cardinal numbers, with the most important theorem being

Theorem 22. *(Steinitz Classification of Algebraically Closed Fields): An algebraically closed field F is determined up to isomorphism by its transcendence degree (over its prime sub-field, i.e. $\mathbb{F}_p$ where $p = charF$ or $\mathbb{Q}$ if $charF = 0$) and its characteristic.*[1, Erdos et. al]

By cardinal arithmetic and the fact there can only ever be countably many polynomials with coefficients in a prime sub-field, every field of degree κ has transcendence degree κ.

Definition 23. Let p be a prime. **The theory of algebraically closed fields of characteristic** p is denoted by ACF_p, defined as

$$ACF_p = \text{FIELD} \cup \text{AC} \cup \{p \cdot 1 = 0\}$$

And the theory of algebraically closed fields of characteristic 0 is defined similarly as:

$$ACF_0 = \text{FIELD} \cup \text{AC} \cup \{p \cdot 1 \neq 0 :\ p > 0 \text{ is prime}\}$$

where FIELD is the set of field axioms, AC is the set of sentences expressing algebraic closure:

$$AC \coloneqq \{(\forall a_0, ..., a_n \exists x)\, a_0 + a_1 x + ... + a_n x^n = 0 :\ n \in \mathbb{N}\}$$

and $p \cdot 1$ is short hand for $1 + ... + 1$, where there are p many 1's.

Theorem 24. *(Los-Vaught Test): Suppose T is a satisfiable theory with no finite models. Suppose for some $\kappa \geq |\mathcal{L}|$, all models of size κ are isomorphic to each other. Then T is complete.*

Proof. If T is not complete, then there exists a sentence ϕ such that both $T_1 = T \cup \{\phi\}$ and $T_2 = T \cup \{\neg\phi\}$ are consistent, hence satisfiable by infinite models. Applying Lowenheim-Skolem, we obtain models M_1 and M_2 of size κ such that $M_1 \models \phi$ and $M_2 \models \neg\phi$, contradicting the fact that M_1 and M_2 are isomorphic. □

Corollary 25. *ACF_p is complete for p prime or $p = 0$.*

Proof. For all uncountable κ, all models of size κ of ACF_p have transcendence degree κ, but an infinite field is determined by its characteristic and its transcendence degree by the Steinitz classification of algebraically closed fields. By the Los-Vaught test, ACF_p is complete. □

The first lemma we prove is a principle commonly used in algebraic geometry, but not often explicitly written out.

Lemma 26. *(Lefschetz Principle) Let ϕ be a sentence in $\mathcal{L}_{ring}$. The following are equivalent:*

1. *For sufficiently large primes p, there is a model $K \models ACF_p \cup \{\phi\}$.*
2. *$ACF_0 \models \phi$*
3. *$\mathbb{C} \models \phi$*

Proof. (2) $\leftrightarrow$ (3) Follows by completeness of ACF_0.

(1) $\to$ (2) Define $T = ACF_0 \cup \{\phi\}$. By the definition of ACF_0,

$$T = \text{FIELD} \cup \text{AC} \cup \{p \cdot 1 \neq 0 : p > 0 \text{ is prime}\} \cup \{\phi\}$$

T is finitely satisfiable because every finite subset T_0 can contain only finitely many sentences of the form $p \cdot 1 \neq 0 :\ p > 0$ is prime, so take a sufficiently large p such that there is a model $K \models ACF_p \cup \{\phi\}$. By compactness, T is satisfiable, hence there exists a model $K' \models ACF_0$ such that $K' \models \phi$, hence $ACF_0 \models \phi$ by completeness of ACF_0.

(2) $\to$ (1) Suppose $ACF_0 \models \phi$. Suppose for contradiction that there are arbitrarily large primes p such there is no model of $ACF_p \cup \{\phi\}$. Then ϕ is not consistent with ACF_p for arbitrarily large primes p, i.e. by completeness of ACF_p for arbitrarily large primes p, $ACF_p \models \neg\phi$. By a similar process in the previous step, define

$$T := ACF_0 \cup \{\neg\phi\} = \text{FIELD} \cup \text{AC} \cup \{p \cdot 1 \neq 0 : p > 0 \text{ is prime}\} \cup \{\neg\phi\}$$

T is finitely satisfiable by a similar reason to the previous step, hence by compactness, $ACF_0 \models \neg\phi$, a contradiction. □

The Ax-Grothendieck theorem states that any polynomial map, i.e. a map that is polynomial in all coordinates, from $\mathbb{C}^n \to \mathbb{C}^n$ that is injective is surjective. As an example of an application of the theorem, consider the polynomial map $\mathbb{C}^2 \to \mathbb{C}^2$ defined by

$$(u,\, v) \to (u^2 + u + v,\, u^2 + v\,)$$

This map does not trivially look surjective and can be proved to be injective. Solving the equations

$$u^2 + u + v = x^2 + x + y$$

$$u^2 + v = x^2 + y$$

by substituting $v = x^2 + y - u^2$ gives us $u + x^2 + y = x^2 + x + y$ and thus $u = x$, and plugging in $u = x$ into the second equation gives $y = v$. Hence the map is injective. By the Ax-Grothendieck theorem, the map is also surjective.

Once the Lefschetz principle is proven, the proof of the Ax-Grothendieck theorem amounts to counting quantifier inversions and observing that maps between finite sets are surjective if and only if they are injective.

Theorem 27. *(Ax-Grothendieck) Every polynomial map $\mathbb{C}^m \to \mathbb{C}^m$ is surjective if it is injective.*

The proof of the theorem shall be done in several steps, and in fact, we will prove something more general.

Definition 28. A $\mathcal{L}$ sentence ϕ is of **complexity level** Π_2 if ϕ is of the form

$$\forall(x_1, ..., x_n)\exists(y_1, ..., y_m)\, \varphi(x_1, ..., x_n, y_1, ..., y_m)$$

where $\varphi(x_1, ..., x_n, y_1, ..., y_m)$ is a formula without quantifiers. We say ϕ is Π_2.

Lemma 29. *Suppose $M_1 \subseteq M_2 \subseteq, ...$ is an increasing sequence of $\mathcal{L}$ structures indexed by some ordinal I and M is a $\mathcal{L}$ structure such that M is the union of the M_i, the constants of M are equal to the constants of M_i for any i, the relations in M are the union of the corresponding relations in M_i and the functions in M are the union of the corresponding functions in M_i. Suppose ϕ is a Π_2 $\mathcal{L}-$sentence. If $M_i \models \phi$ for all $i \in I$ then $M \models \phi$.*

Proof. Write

$$\phi = \forall x_1, ..., x_n \exists y_1, ..., y_m \varphi(x_1, ..., x_n, y_1, ..., y_m)$$

Let $a_1, ..., a_n \in M$. Each $a_i \in M_{k_i}$ for some $k_i \in I$. Let k be the maximum of such k_i. Since $M_k \models \phi$, there exists $b_1, ..., b_m \in M_k \subseteq M$ such that

$$M_k \models \varphi(a_1, ..., a_n, b_1, ..., b_n)$$

Since φ is quantifier-free,

$$M \models \varphi(a_1, ..., a_n, b_1, ..., b_n)$$

Thus

$$M \models \forall x_1, ..., x_n \exists y_1, ..., y_m \varphi(x_1, ..., x_n, y_1, ..., y_m)$$

□

Lemma 30. *Let ϕ be Π_2 in $\mathcal{L}_{ring}$ and suppose that for all finite fields F, $F \models \phi$. Then $ACF_p \models \phi$ for all primes p and $ACF_0 \models \phi$. (In particular, $\mathbb{C} \models \phi$).*

Proof. Observe that for all p, $\overline{\mathbb{F}}_p$ is a union of an increasing chain of finite fields $M_1 \subseteq M_2 \subseteq ...$ by adjoining the roots of all the polynomials over $\mathbb{F}_p$ one at a time, and by the fact that an algebraic extension of a finite field is finite. Then by the previous lemma, $\overline{\mathbb{F}}_p \models \phi$. By completeness, $ACF_p \models \phi$ for all primes p and by the Lefschetz principle, $ACF_0 \models \overline{\mathbb{F}}_p$. □

We now give a proof of the Ax-Grothendieck theorem.

Proof. (of Ax-Grothendieck Theorem). By the previous lemma, it suffices to demonstrate that fixing $n \in \mathbb{N}$, there exists a Π_2 sentence ϕ which asserts every injective polynomial map of degree n is surjective. This is because if such a sentence ϕ exists, all finite fields will model ϕ since set theoretically all injective self maps of finite sets are surjective. Accordingly, define

$$\phi := (\forall a_1, ..., a_N)\text{Injective}(a_1, ..., a_N) \rightarrow \text{Surjective}(a_1, ..., a_N)$$

where Injective$(a_1, ..., a_N)$ states that the polynomial map of degree n defined by coefficients $a_1, ..., a_N$ is injective as multivariate maps, and similarly so for Surjective$(a_1, ..., a_N)$. Let $f_{\overline{a}}$ be the polynomial map defined by $a_1, ..., a_n$ and let $\overline{x}$ and $\overline{y}$ be $m-$length vectors of variables. We explicitly define Injective$(a_1, ..., a_N)$ and $Surjective(a_1, ..., a_N)$ as follows.

$$\text{Injective}(a_1, ..., a_N) := (\forall \overline{x} \forall \overline{y}) f_{\overline{a}}(\overline{y}) = f(\overline{x}) \rightarrow \overline{x} = \overline{y}$$

$$\text{Surjective}(a_1, ..., a_N) := (\forall \overline{y})(\exists \overline{x}) f_{\overline{a}}(\overline{x}) = \overline{y}$$

where equality between two vectors of variables of equal length is taken to mean a conjunction of co-ordinate equality.

To see why ϕ can be made Π_2, observe that the following computation of moving the quantifiers to the front and replacing the variables $\overline{x}$ and $\overline{y}$ in $Surjective(a_1, ..., a_N)$ with new variables $\overline{w}$ and $\overline{k}$ as below gives rise to a Π_2 sentence equivalent to ϕ:

$$\phi := (\forall a_1, ..., a_N)\text{Injective}(a_1, ..., a_N) \to \text{Surjective}(a_1, ..., a_N)$$

$$\equiv (\forall a_1, ..., a_N)\left[(\forall \overline{x} \forall \overline{y}) f_{\overline{a}}(\overline{y}) = f(\overline{x}) \to \overline{x} = \overline{y}\right] \to \left[(\forall \overline{y})(\exists \overline{x}) f_{\overline{a}}(\overline{x}) = \overline{y}\right]$$

$$\equiv \left[\forall a_1, ..., a_N, \overline{x}, \overline{z}\right]\left[\exists \overline{w}\right]\left(f_{\overline{a}}(\overline{y}) = f(\overline{x}) \to \overline{x} = \overline{y}\right) \wedge \left(f_{\overline{a}}(\overline{w}) = \overline{z}\right)$$

□

The Noether-Ostrowski Irreducibility theorem is an even more immediate consequence of the Lefschetz principle. Given a polynomial $p \in R[\overline{x}]$ for some ring x, p defines a family of hyper surfaces, each over some field F where there exists a homomorphism $R \to F$. Each hyperspace is defined by mapping the coefficients of p through the homomorphism $R \to F$, and we call them 'fibers' of p. In the case where F is the fraction field of R, we call this the 'generic fiber of f. The Noether-Ostrowski Irreducibility theorem relates irreducibility of the generic fiber to the irreducibility of all the other fibers for the case where $R = \mathbb{Z}$.

Theorem 31. *Fix $f \in \mathbb{Z}[x_1, ..., x_n]$ and a prime p. Let $f_p \in \mathbb{F}_p[x_1, ..., x_n]$ be obtained from f by reducing each of its coefficients modulo p. Then for all such f, f is irreducible in $\overline{\mathbb{Q}}$ if and only if f_p is irreducible in $\overline{\mathbb{F}_p}$ for cofinitely many primes p.*

Proof. By the Lefschetz principle, and the fact that $\mathbb{Q} \models ACF_0$, we need only to show that there exists a sentence ϕ asserting that f is irreducible. Let n be the degree of f. Observe that a polynomial of degree n is irreducible if and only if it cannot be written as a product of two polynomials of degree less than n whose degrees add up to n. Given $k \in \mathbb{N}$, define f_{a^k} to be the general polynomial of degree k generated by coefficients $\overline{a}^k := (a_1^k, ..., a_{n_k}^k)$. Define ϕ by

$$\phi := \bigwedge_{k+l=n} \forall \overline{a}^k \forall \overline{b}^l \left(f_{a^k} \cdot f_{b^l} \neq f\right)$$

□

4. Quantifier Elimination for Algebraically Closed Fields

4.1. **Quantifier Elimination.**

Definition 32. 1. A $\mathcal{L}$ formula $\phi(\overline{a})$ is **quantifier-free** if there are no quantifiers in $\phi(\overline{a})$.

2. An $\mathcal{L}$ theory T has **quantifier elimination** if for every formula $\phi(\overline{x})$, there exists a quantifier-free formula $\psi(\overline{x})$ such that

$$T \vdash \forall \overline{x}(\phi(\overline{x}) \leftrightarrow \psi(\overline{x}))$$

3. If M is a $\mathcal{L}-$structure, we say M admits quantifier elimination if $\mathrm{Th}(M)$ admits quantifier elimination.

Quantifier elimination in a theory means that the theory proves every sentence is equivalent to a quantifier-free sentence. Quantifier elimination is an important property that we will focus on in proving the other theorems of algebraic geometry in this paper. The goal of this section is to show that ACF admits quantifier elimination. We first develop a test of quantifier elimination. We note that quantifier elimination is only possible if the language has a constant symbol, because every quantifier-free sentence must include a constant.

Definition 33. For an $\mathcal{L}$ structure A, and any subset $B \subseteq A$, define $\mathcal{L}_B$ to be $\mathcal{L}$ with new constant symbols added in for $b \in B$ and A_B to be the $\mathcal{L}_B-$structure where each formal symbol $b \in B$ is interpreted as itself. We define the **diagram**, $\mathrm{Diag}(A, B)$ as the set of all quantifier-free $\mathcal{L}_B$ sentences σ such that $A_B \models \sigma$. Define $\mathrm{Diag}(A) = \mathrm{Diag}(A, A)$.

The diagram of A with respect to B is just the set of all true quantifier-free sentences when we allow ourselves to use parameters from B.

Definition 34. An $\mathcal{L}-$theory T is **diagram complete** if for any $\mathcal{L}-$structure A such that $A \models T$ and any $\overline{a} \in A^n$ for any $n \in \mathbb{N}$, the $\mathcal{L}_{\overline{a}}$ theory $T \cup \mathrm{Diag}(A, \overline{a})$ is complete.

We observe that by the completeness theorem, the definition of diagram completeness is equivalent to to the following one.

Definition 35. 1. Fix $\mathcal{L}$ and let $\overline{c}$ be a tuple of new constant symbols. Call a set of $\mathcal{L}_{\overline{c}}$sentences $\Gamma_{\overline{c}}$ a $T-$**diagram** if every sentence of $\Gamma_{\overline{c}}$ is quantifier-free, $T \cup \Gamma_{\overline{c}}$ is consistent and for every quantifier-free $\mathcal{L}_{\overline{c}}$ sentence ψ, ψ or $\neg\psi$ is in $\Gamma_{\overline{c}}$. This means that fixing a new set of constants, a $T-$ diagram is a set of quantifier-free sentences that is closed under deduction and complete with respect to quantifier-free sentences in the language with the new constants.

2. An $\mathcal{L}-$theory T is diagram complete if and only if for any vector of new constants $\overline{c}$ and any T diagram $\Gamma_{\overline{c}}$, $T \cup \Gamma_{\overline{c}}$ is a complete $\mathcal{L}_{\overline{c}}$ theory.

Proposition 36. *If $\mathcal{L}$ has a constant symbol c, then an $\mathcal{L}-$theory T admits quantifier elimination if and only if T is diagram complete.*

Proof. ($\Leftarrow$) Suppose T is diagram complete. Let $\phi(\overline{x})$ be a $\mathcal{L}$ formula. By quantifier elimination we may assume $\phi(\overline{x})$ is quantifier-free. Either $A \models \phi(\overline{a})$ or $A \models \neg\phi(\overline{a})$, so $\mathrm{Diag}(A, \overline{a})$ contains either $\phi(\overline{a})$ or $\neg\phi(\overline{a})$.

($\Rightarrow$) This direction requires some technical definitions of notions of proof and symbolic manipulation and theorems including the deduction theorem and notions of substitution, which were omitted for a more intuitive exposition. We refer to [2, Tserunyan] in the references for a detailed proof. □

4.2. Quantifier Elimination of ACF.

To show that ACF has quantifier elimination, we need to show diagram-completeness, and we shall do so by the Los-Vaught test. The proof is similar to the proof of completeness of ACF_0.

Proposition 37. *For every $ACF-$diagram $\Gamma_{\overline{c}}$ and for every uncountable cardinal κ, every two $\mathcal{L}_{\overline{c}}$ models of $ACF \cup \Gamma_{\overline{c}}$ of cardinality κ are isomorphic to each other.*

Corollary 38. *ACF admits quantifier elimination.*

Proof. (of the proposition): Let $\Gamma_{\overline{c}}$ be an $ACF-$diagram and let F and K be two algebraically closed fields that are models of $\Gamma_{\overline{c}}$ of some uncountable cardinality κ. F and K must have the same characteristic, because the characteristic of a field is expressible by a set of quantifier-free sentences.

Let $\mathbb{F}_p$ be the prime subfield of F and K, which is unique up to isomorphism. Let $F_1 = \mathbb{F}_p(\overline{c_F})$ and $K_1 = \mathbb{F}_p(\overline{c}_K)$ where $\overline{c}_i$ are the interpretations of the constants $\overline{c}$ in i for $i = F, K$. Observe that $F_1 = \mathbb{F}_p(\overline{c})/\sim_F$ and $K_1 = \mathbb{F}_p(\overline{c})/\sim_K$ where $\sim_i$ are algebraic relations satisfied by $\overline{c}_i$. But algebraic relations are quantifier free formulas are in $\Gamma_{\overline{c}}$, and since F and K are models of $\Gamma_{\overline{c}}$, F_1 and K_1 are isomorphic. This isomorphism extends to an isomorphism of F and K, by counting the transcendence degree of F and K over F_1 and K_1 and the fact that κ is uncountable. □

5. Model Completeness and Hilbert's Nullstellensatz

An important consequence of quantifier elimination is model completeness, which we use to prove Hilbert's Nullstellensatz theorem. Model completeness asserts that substructures and superstructures are indistinguishable by sentences of first-order logic.

Definition 39. 1. Let T be an $\mathcal{L}-$theory, M and N models of T such that $N \subseteq M$. N is an **elementary substructure** of M if for all formulas $\phi(\overline{x})$ and tuples $\overline{a} \in N$, $N \models \phi(\overline{a})$ if and only if $M \models \phi(\overline{a})$. We write $N \preceq M$.

2. An $\mathcal{L}-$theory T is **model-complete** if all embeddings are elementary, i.e. whenever $B \subseteq A$ and A and B are models of T, then $A \preceq B$.

Proposition 40. *If T admits quantifier elimination, then T is model complete.*

Proof. Observe that if $B \subseteq A$ then A and B must agree on all quantifier-free formulas. But if T admits quantifier elimination, then all formulas are equivalent to quantifier-free ones, hence A and B are elementarily equivalent. □

Model completeness is incomparable with completeness, so one does not necessarily imply the other. The following examples illustrate this.

Example 41. 1. Define the theory of dense linear order with endpoints in $\mathcal{L}_{order}$ by

$$\text{DLOE} \coloneqq \text{ORDER} \cup \{\text{Density}\} \cup \{\text{Endpoints}\}$$

where ORDER is the set of axioms of total order, i.e. transitivity and trichotomy, and

$$\text{Density} \coloneqq [\forall (x, y) \exists z]\, x < z < y$$

$$\text{Endpoints} \coloneqq (\exists x \exists z \forall y)((y < x) \wedge (y > x))$$

We show below that DLOE is complete with all countable models isomorphic to $\mathbb{Q} \cap [0, 2]$ and $\mathbb{Q}\cap$[0,1]. However, DLOE is not model complete because $\mathbb{Q} \cap [0, 1]$ is a substructure of $\mathbb{Q} \cap [0, 2]$, but the inclusion embedding is not elementary, because $\mathbb{Q} \cap [0, 1] \models \neg(\exists x(x > 1))$ while $\mathbb{Q} \cap [0, 2] \models \exists x(x > 1)$.

Proof. (of completeness of DLOE) We use the Los-Vaught test on $\kappa = \aleph_0$. Given two countable dense linear orders with endpoints M and N, we construct an isomorphism as follows. Send the endpoints to endpoints. Order the remaining elements of M and N by a_1, a_2, ... and b_1, b_2, ... respectively. Next send a_1 of M to some remaining element b_{k_1} of N. Next consider a remaining element b_1 of N. Send b_1 to an element a_{k_1} in M to mirror b_1's relation to b_{k_1}, then take an element $a_2 \in M$ and and send it to an element $b_{k_2} \in N$ to mirror $a_2's$ relation to a_1 and a_{k_1}. Repeating this back and forth process, by induction we obtain a countable increasing sequence of partial isomorphisms (ϕ_n), each on increasing finite subsets M and N that eventually cover all elements.

The union ϕ of these partial isomorphisms is an isomorphism between M and N, because any a_1, $a_2 \in M$ both lie in some finite subset, which is eventually covered by some partial isomorphism. □

Example 42. The theory of algebraically closed fields is not complete, because there are algebraically closed fields of differing characteristics. However, it is model complete by quantifier elimination.

Hilbert's Nullstellensatz states that in an algebraically closed field, the vanishing set of a proper ideal in the polynomial ring is non-empty. A counter example in a non-algebraically closed setting is to take the real numbers, and consider the vanishing set of the ideal $(x^2 + 1)$. Since -1 does not have a square root, the vanishing set is empty. We see that the Nullstellensatz generalizes the fundamental theorem of algebra, since $F[x]$ is a principal ideal domain.

Theorem 43. *(Hilbert's Weak Nullstellensatz): Let F be an algebraically closed field and let I be a proper ideal of $F[x_1, ..., x_n]$. Then the vanishing set of V is nonempty; $V(I) \neq \phi$, i.e. there exists $\overline{a} \in F^n$ such that $f(\overline{a}) = 0$ for all $f \in I$.*

Proof. Since $F[x_1, ..., x_n]$ is noetherian, let $f_1, ..., f_k$ be a generating set for I. Let J be a maximal ideal containing I. Define

$$K = F[x_1, ..., x_n]/J$$

Since M is maximal, K is a field. Furthermore, we have $F \subseteq K$.

Let L be the algebraic closure of K. We have $F \subseteq K \subseteq L$ where $F \models ACF$ and $L \models ACF$. Observe that $\overline{a} := (x_1 + M, ..., x_n + M)$ is an element of $K^n \subseteq L^n$ such that $f_1(\overline{a}) = ... = f_k(\overline{a}) = 0$. Let $b_1, ..., b_M$ be the coefficients in F defining $f_1, ..., f_k$. We have

$$L \models \phi(b_1, ..., b_M) := (\exists \overline{a}) \left((f_1(\overline{a}) = 0) \wedge ... \wedge (f_k(\overline{a}) = 0) \right)$$

By model completeness of ACF

$$F \models \phi(b_1, ..., b_M) \equiv (\exists \overline{a}) \left((f_1(\overline{a}) = 0) \wedge ... \wedge (f_k(\overline{a}) = 0) \right)$$

Therefore there exists $\overline{a} \in F^n$ such that $f_1(\overline{a}) = ... = f_k(\overline{a}) = 0$. Since $f_1, ..., f_k$ generate I, $f(\overline{a}) = 0$ for all $f \in I$, hence $V(I) \neq \emptyset$. □

We see that similar to the proof of the Ax-Grothendieck theorem and the Noether-Ostrowski irreducibility theorem, once we establish some basic properties of the base theory, i.e. ACF or ACF_p, then the theorems fall into place by inspection of the translation of the theorems into first-order sentences.

6. Quantifier Elimination for Real Closed Fields

6.1. **Algebraic Preliminaries.** The concept of a real closed field is a generalization of the real numbers, defined such that every real closed field is elementarily equivalent to the real numbers. We will give a theory RCF consisting of the axioms of real closed fields.

Real closed fields do not admit quantifier elimination in $\mathcal{L}_{oring} \coloneqq \mathcal{L}_{ring} \cup \mathcal{L}_{order}$. To see this, first observe that for any quantifier-free formula $\phi(\overline{v})$ of $\mathcal{L}_{ring}$, the set defined by $\phi(\overline{v})$ in a field F is either finite or cofinite. This is because every quantifier-free formula is a boolean combination, i.e. obtained from finite unions and complements, of vanishing sets of polynomials, which is finite or cofinite because polynomials can have only finitely many roots. However, the formula asserting that "x is a square", i.e. "x is positive", $(\exists y)y^2 = x$ defines an infinite and coinfinite set in $\mathbb{R}$.

The reason why real closed fields do not have quantifier elimination is because they are orderable and that the order relation is definable in $\mathcal{L}_{ring}$. We see that by expanding the language to include an order relation, i.e. $\mathcal{L}_{oring} = \mathcal{L} \cup \{<\}$, then real closed fields do admit quantifier elimination. For example, the quantifier-free formula equivalent to $(\exists y)y^2 = x$ from above in the real numbers is $x > 0$.

Definition 44. 1. A field F is **formally real** if -1 is not the sum of squares.

2. A field is **real closed** if it is formally real with no proper formally real algebraic extensions.

We require some theorems from algebra to proceed. These are due to Artin and Schreier, cited from [3, Marker].

Theorem 45. *If F is formally real, then F is orderable, and in particular, if $a \in F$ is not the sum of squares, then there is an ordering of F where a is negative.*

Theorem 46. *Let F be a formally real field. The following are equivalent.*

1. F is real closed

2. $F(i)$ is algebraically closed, where $i^2 = -1$

3. For any $a \in F$, either a or $-a$ is a square and every polynomial of odd degree has a root.

This allows us to axiomatize RCF as follows.

Corollary 47. *The class real closed fields is given by the class of models of a set of sentences RCF, defined by*

I) field axioms

II) sentences asserting -1 is not the sum of squares, i.e. for each n, the sentence

$$(\forall x_1, ..., x_n)\, x_1^2 + ... + x_n^2 + 1 \neq 0$$

III) A sentence asserting each element or its negative is a square:

$$(\forall x \exists y) y^2 = x \vee y^2 + x = 0$$

IV) For each n, a sentence asserting that a polynomial of degree $2n+1$ has a root:

$$(\forall x_0, ..., x_{2n+1} \exists y) x_{2n+1} y^{2n+1} + ... + x_1 y + x_0 = 0$$

The fact that in a real closed field F, either a or $-a$ is a square allows us to define an ordering on F by $x < y$ if and only if $y - x$ is a nonzero square. It is a fact of algebra that this is the only possible ordering in F. This shows that order is definable in a real closed field with only symbols from $\mathcal{L}_{ring}$.

Definition 48. For a $\mathcal{L}_{ring}$ real closed field F with its addition and multiplication, define the $\mathcal{L}_{oring}$ real closed field F to be F with its canonical order, and its addition and multiplication.

Definition 49. For an ordered field F, the **real closure** of F is a real closed algebraic extension of F.

The real closure of a field exists by Zorn's lemma. The following fact justifies the statement that real closed fields have unique real closures that extend their ordering.

Theorem 50. *If F is an ordered field with ordering $<$, and R and R' are real closures of F where the canonical ordering extends $<$, then there is a unique field isomorphism $\phi : R \to R'$ that extends the identity on F.*

6.2. **Quantifier Elimination for RCF.** We proved quantifier elimination for ACF by the Los-Vaught test. There is another test for quantifier elimination which we shall use to prove quantifier elimination for RCF without using the Los-Vaught test. This test allows for the use of geometric intuitions about polynomial functions on real closed fields. This test and its adapted application is cited from [3, Marker].

Lemma 51. *(Second Quantifier Elimination Test): Let T be an $\mathcal{L}-$theory. Suppose that for all*

(1) quantifier-free formulas $\phi(\overline{v}, w)$

(2) models M and N of T
(3) common substructures A of M and N
(4) $\overline{a} \in A$ such that there is $b \in M$ such that $M \models \phi(\overline{a}, b)$,

there is $c \in N$ such that $N \models \phi(\overline{a}, c)$. Then T has quantifier elimination.

Theorem 52. *RCF admits quantifier elimination in $\mathcal{L}_{oring}$.*

Proof. Suppose $K, L \models RCF$ and $A \subseteq K \cap L$ is a common substructure. Note A has no zero divisors, because zero divisors in A are zero divisors in K and L. Let F_0 be the field of fractions of A extending the order of A by $\frac{a}{b} > 0$ if $a > 0$ and $b > 0$ and let F be the real closure of F_0. Since real closures are unique, without loss of generality, assume $F = \overline{F_0} \cap (K \cap L) \subseteq K \cap L$.

Let $\phi(v, \overline{w})$ be a quantifier-free formula and $\overline{a} \in F$, $b \in K$ be such that $K \models \phi(b, \overline{a})$. We show that there exists $x \in F$ such that $F \models \phi(x, \overline{a})$.

Since for every polynomial $p \in F[\overline{x}]$, $p(\overline{x}) \neq 0$ if and only if $p(\overline{x}) > 0$ or $-p(\overline{x}) > 0$ and $p(\overline{x}) \not> 0$ if and only if $p(\overline{x}) = 0$ or $-p(\overline{x}) > 0$, after placing ϕ in disjunctive normal form, we may assume ϕ is a disjunction of conjunctions of formulas of the form $p(v, \overline{w}) = 0$ or $p(v, \overline{w}) > 0$, i.e.

$$\phi(v, \overline{w}) \equiv \bigvee_{1 \leq i \leq n} \bigwedge_{1 \leq j \leq m} \theta_{i,j}(\overline{v}, w)$$

where $\theta_{i,j}(\overline{v}, w)$ is of the form $p(v, \overline{w}) = 0$ or $p(v, \overline{w}) > 0$. Since $K \models \phi(v, \overline{w})$, there exists $i' \in \{1, ..., n\}$ such that

$$K \models \bigvee_{1 \leq j \leq m} \theta_{i',j}(v, \overline{w})$$

So without loss of generality, assume there exists polynomials $p_1, ..., p_k$ and $q_1, ..., q_l$ such that

$$\phi(v, \overline{w}) \equiv \bigwedge_{1 \leq j \leq m} \theta_j(\overline{v}, w) \equiv \left(\bigwedge_{1 \leq i \leq k} p_i(v) = 0 \right) \wedge \left(\bigwedge_{1 \leq j \leq l} q_j(v) > 0 \right)$$

where $\theta_j(\overline{v}, w)$ is of the form $p(v, \overline{w}) = 0$ or $p(v, \overline{w}) > 0$.

The first case is that for some $1 \leq i \leq k$, $p_i(b) = 0$, b is algebraic over F. Since real closed fields have no proper real algebraic extensions, $b \in F$ and we are done.

The second case is that

$$\phi(v, \overline{w}) \equiv \bigwedge_{1 \leq j \leq l} q_j(v) > 0$$

Each q_j can only change signs at the zeroes of q_j in F, which are finitely many. For each q_j define I_j to be the set where $q_j > 0$. Note I_j is a finite union of intervals with endpoints, possibly including $\pm\infty$, in F. We have $I \coloneqq \bigcap_{1 \leq j \leq l} I_j$ is a finite union of interval in F and is nonempty, because $K \models \phi(v, \overline{w})$. Hence I contains some interval $[c, d]$ with endpoints $c < d$ in F such that $q_j(x) > 0$ for all $x \in [c, d] \cap F$. Since the order on real closed fields is dense, such x exist so $F \models K \models \phi(x, \overline{w})$. □

7. Model Completeness and Hilbert's 17th Problem

Since RCF admits quantifier elimination, it is model complete. This gives rise to a a simple proof of Artin's positive solution to Hilbert's 17th problem.

Definition 53. Let F be a real closed field and $f \in F(\overline{x})$ be a rational function in n variables. We say f is **positive semidefinite** if $f(\overline{a}) \geq 0$ for all $\overline{a} \in F^n$.

Hilbert's 17th problem asks whether every positive semidefinite polynomial in the reals can be written as a sum of squares of rational functions. The motivation comes from Hilbert's proof of the existence of positive semidefinite polynomials that cannot be written as the sum of squares of polynomials, with one example being the following

$$M(x, y) = x^4y^2 + x^2y^4 + 1 - 3x^2y^2$$

due to Motzkin, cited from [4, Schmudgen]. $M(x, y)$ is positive semidefinite by the arithmetic-geometric mean inequality. With the observation that $M(x, 0) = 1 = M(0, y)$, expressing $M(x, y)$ as a sum of squares of polynomials f_i would require each f_i to have only mixed non constant terms, i.e. $f_i = a_i + b_ixy + c_ix^2y + d_ixy^2$. The coefficient of x^2y^2 in $\sum f_i^2$ is $\sum b_i^2 = -3$, a contradiction because -3 is not a sum of squares in the reals.

However, we can write $M(x, y)$ as a sum of squares of rational functions as

$$M(x, y) = \frac{x^2y^2(x^2 + y^2 + 1)(x^2 + y^2 - 2) + (x^2 - y^2)^2}{(x^2 + y^2)^2}$$

Even though not every real positive semidefinite polynomial is a sum of squares of polynomials, Hilbert's 17th problem asks if it is a sum of squares of rational functions. The answer to Hilbert's 17th problem is yes, and more generally every rational positive semidefinite function can be written as a sum of squares of rational functions.

Theorem 54. *(Hilbert's 17th Problem) If $f \in F(\overline{x})$ is a positive semidefinite rational function (i.e. positive semidefinite as a function whenever it is defined) over a real closed field F, then f is a sum of squares of rational functions.*

Proof. Suppose for contradiction that f is a positive semidefinite rational function over F that is not a sum of squares. Let f be defined by coefficients $a_1, ..., a_M$ in F. Then there exists an ordering $\leq$ of $F(\overline{x})$ such that $f < 0$. Let $R \supseteq F(\overline{x})$ be real closed extending $\leq$. Take the element $\overline{x} \in R^n$ and observe that $f(\overline{x}) < 0$ because by the ordering, $f < 0$. So $\overline{x}$ witnesses the truth of the following existential statement in R:

$$R \models (\exists \overline{v}) f(\overline{v}) < 0$$

which is first-order in $\mathcal{L}_{oring}$ with parameters $a_1, ..., a_M$ in F. By model completeness, we may transfer this sentence to the substructure F and obtain

$$F \models (\exists \overline{v}) f(\overline{v}) < 0$$

implying that there exists $\overline{x} \in F^n$such that $f(\overline{x}) < 0$, a contradiction to positive semidefiniteness. □

Acknowledgments. I would like to thank Sean Howe for mentoring me in this independent study, and Peter May for organizing the REU at the University of Chicago. I would also like to thank Itay Neeman for organizing the UCLA summer school in logic where I learned some of the important model theory used in this paper and encountered some of the referenced course notes, and my instructors Sherwood Hatchman and John Susice at UCLA.

References

[1] An Isomorphism Theorem for Real Closed Fields, Annals of Mathematics, Vol 61, No.3, May 1955, https://www.math.hmc.edu/~henriksen/publications

[2] unpublished notes, http://www.math.ucla.edu/~znorwood/summer-school-2015/godel-incompleteness-anush.pdf

[3] various unpublished notes, http://homepages.math.uic.edu/~marker/orsay/

[4] Around Hilbert's 17th Problem, Documenta Mathematica, Extra Volume ISMP 2012 433-438, http://www.math.uiuc.edu/documenta/vol-ismp/61