THE THEORY OF GENERIC DIFFERENCE FIELDS

İREM YILDIRIM

DECEMBER 2003

THE THEORY OF GENERIC DIFFERENCE FIELDS

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES
OF
THE MIDDLE EAST TECHNICAL UNIVERSITY

BY

İREM YILDIRIM

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF SCIENCE
IN
THE DEPARTMENT OF MATHEMATICS

DECEMBER 2003

Approval of the Graduate School of Natural and Applied Sciences

Prof. Dr. Canan ÖZGEN
Director

I certify that this thesis satisfies all the requirements as a thesis for the degree of Master of Science.

Prof. Dr. Ersan AKYILDIZ
Head of Department

This is to certify that we have read this thesis and that in our opinion it is fully adequate, in scope and quality, as a thesis for the degree of Master of Science.

Assist. Prof. Dr. David PIERCE
Supervisor

Examining Committee Members

Assist. Prof. Halit OĞUZTÜZÜN _____

Assist. Prof. Andreas TIEFENBACH _____

Assoc. Prof. Dr. Süleyman ÖNAL _____

Prof. Dr. Mahmut KUZUCUOĞLU _____

Assist. Prof. Dr. David PIERCE _____

ABSTRACT

THE THEORY OF GENERIC DIFFERENCE FIELDS

Yıldırım, İrem
M.Sc., Department of Mathematics
Supervisor: Assist. Prof. Dr. David Pierce

December 2003, 53 pages

A difference field $\mathcal{M}$, is a field with a distinguished endomorphism, is called a ***generic difference field*** if it is existentially closed among the models of the theory of difference fields. In the language $L_d = \{+, -, \cdot, 0, 1, \sigma\}$, by a theorem of Hrushovski, it is characterized by the following: M is an algebraically closed field, σ is an automorphism of M, and if W and V are varieties defined over M such that $W \subseteq V \times \sigma(V)$ and the projection maps $\pi_1 : W \to V$ and $\pi_2 : W \to \sigma(V)$ are generically onto, then there is a tuple $\bar{a}$ in M such that $(\bar{a}, \sigma(\bar{a})) \in W$. This thesis is a survey on the theory of generic difference fields, called $ACFA$, which has been studied by Angus Macintyre, Van den Dries, Carol Wood, Ehud Hrushovski and Zoé Chatzidakis. $ACFA$ is the model completion of the theory of algebraically closed difference fields. It is very close to having full quantifier elimination, but it doesn't. We can eliminate quantifiers down to formulas with one quantifier and hence obtain the completions of $ACFA$. This entails the decidability of the theory $ACFA$ as well as its extensions obtained by specifying the characteristic. The fixed field of σ is a pseudo-finite field.

Keywords: Generic Difference Fields, Generic Automorphisms, $ACFA$.

ÖZ

JENERİK FARK CİSİMLERİNİN TEORİSİ

Yıldırım, İrem
Yüksek Lisans, Matematik Bölümü
Tez Yöneticisi: Yard. Doç. David Pierce

Aralık 2003, 53 pages

Fark cismi $\mathcal{M}$ ayırt edilmiş endomorfizması olan bir cisimdir. Bu cisme eğer fark cisimleri teorisinin modelleri arasında varoluşsal olarak kapalıysa jenerik fark cisimi denir. $L_d = \{+, -, \cdot, 0, 1, \sigma\}$ dilinde Hrushovski'nin bir teoremi ile şu şekilde karakterize edilir: M; cebirsel olarak kapalı bir cisimdir, σ; M'in bir otomorfizmasıdır, ve eğer W ve V, M'nin üzerinde tanımlanmış öyle değişken kümelerdir ki $W \subseteq V \times \sigma(V)$ ve projeksiyon haritaları $\pi_1 : W \to V$ ve $\pi_2 : W \to \sigma(V)$ jenerik olarak örtendir, o zaman M de öyle bir n-boyutlu afin uzay noktası $\bar{a}$ vardır ki $(\bar{a}, \sigma(\bar{a})) \in W$. Bu tez $ACFA$ denilen ve Angus Macintyre, Van den Dries, Carol Wood, Ehud Hrushovski ve Zoé Chatzidakis tarafından çalışılan jenerik fark cisimlerinin teorisi üzerine yapılmış bir incelemedir. $ACFA$ cebirsel olarak kapalı fark cisimleri teorisinin model tamamlayıcısıdır. Bu teori neredeyse tam niceleyici yokedilmesine sahiptir ama tamamen yok edilemez. Bu teoride biz niceleyicileri ancak bir niceleyiciye kadar yok edebilmekteyiz ve böylece $ACFA$'in tamamlayıcılarını da elde etmekteyiz. Bu işlem, cismin karakteristiğini de belirleyerek sağlanan genişlemeleri ile birlikte $ACFA$ teorisinin de kararlılığını gerektirir. σ'nın sabit cismi bir sahte-sonlu cisimdir.

Anahtar Kelimeler: Jenerik Fark Cismi, Jeneric Otomorfizmalar, $ACFA$.

To BERFU

ACKNOWLEDGMENTS

I would like to thank Assist. Prof. Dr. David Pierce, my supervisor, for his many suggestions and constant support during this research. I am also thankful to Prof. Dr. Mahmut Kuzucuoglu for his guidance.

I am grateful to my parents Gülhan & Yılmaz Yıldırım for their patience.

Finally, I wish to thank Bülent Basım and Cansu Betin for their support and guidance, Fulay and Elcin for their endless patience and moral support, Reside (for her unbelievable knowledge of english), Esin, Gamze, Yumak.

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

Model theory is a branch of mathematics which classifies mathematical structures by considering axioms satisfied by those structures. It uses first order logic because it satisfies the Compactness Theorem and Löwenheim-Skolem Theorem. In fact model theory is the analysis of the so-called definable subsets of a mathematical structure.

The definable subsets of classical mathematical structures are very important in algebraic and geometric investigations, for example: they are the constructible sets in algebraic geometry and the semi-algebraic sets in real geometry.

The second chapter includes some basic techniques to find out the model theory of a set of mathematical structures. It includes identifying elementary classes, finding axioms for these classes, and determining definable sets of the structures belonging to these classes. Quantifier elimination is an analysis of definable sets by considering the complexity of their formulas. Sometimes quantifier elimination fails in the natural language, but yet the definable sets in a structure have useful form; model completeness is a good way of understanding these situations. A trick of model theory shows that if we enrich the language of a structure sufficiently, structures can be made to have quantifier elimination, but this shows nothing about their definable sets. We need to find

an appropriate language in which a class of structures has quantifier elimination. Before giving these techniques I'll give some basic definitions in model theory and examples about them.

Chapter 3 starts with basic algebraic geometry which helps us to understand definable sets of a field. The quantifier free definable subsets of a field are the finite boolean combinations of Zariski closed sets called constructible sets. The constructible sets have much stronger closure properties if the field is algebraically closed.

So we'll come to the model theory of algebraically closed fields. By applying the techniques which I'll show in the second chapter I'll prove that the theory is model complete and has quantifier elimination. This fact yields the following: Let $\overline{\mathbb{Q}}$ be the field of algebraic numbers over $\mathbb{Q}$, then any finite system of polynomial equations and inequations with coefficients in $\overline{\mathbb{Q}}$ that has a solution in some extension field of $\mathbb{Q}$ has one in $\overline{\mathbb{Q}}$. In other words if an algebraic set is nonempty, then it has a point with coordinates in $\overline{\mathbb{Q}}$. This conclusion is closely related to Hilbert's Nullstellensatz.

I'll give the Lefschetz Principle, which is a consequence of the completeness and decidability of the theory of algebraically closed fields for a given characteristic. At the end there is an application of model theory to the algebra of fields which is due to Ax.

In the last chapter I'll study the fields to which a distinguished endomorphism has been adjoined: the so called difference fields. Since the distinguished endomorphism of a difference field extends to an automorphism of a larger field, I assume that all difference fields are inversive: in other words, the endomorphism is an automorphism. The first section of this chapter gives basic algebraic background about field automorphisms, difference fields and difference systems.

If we can understand the solvability of difference systems we can understand the elementary theory of difference fields.

The theory of difference fields has a model companion, the so-called theory of generic difference fields, which is called $ACFA$. That $ACFA$ axiomatizes the theory of generic difference fields was first proved by A. Macintyre in 1990 in a more complicated version and after that Hrushovski proved the isolated one. So the theory is model complete, therefore very near to eliminating quantifiers, but it doesn't in the natural language of difference fields. By adjoining predicates to the language which describe the isomorphism type of the prime subfield, we get a reasonable elimination theory. Actually what we get is: the theory of generic difference fields has elimination of quantifiers by adding extra predicates to the language, but the definable sets of a model are not in useful form.

The last section of this chapter deals with the fixed field of the automorphism. I'll give some results of Ax about finite fields and describe the relation between the finite fields and pseudo finite fields. We can conclude from the theorem of Lang-Weil that the fixed field of the automorphism is pseudo-finite.

CHAPTER 2

BASIC MODEL THEORY

In this chapter I'll give the basic definitions and primary results that play an important role through other chapters. These definitions and results can be found in [15]. For more details and historical background of model theory, *The Handbook of Mathematical Logic* is a very good source to use.

The first section gives the definition of languages, structures and formulas and some examples about them. The definition of a substructure and an elementary substructure are given in terms of the notion of L-embedding. Tarski's Test, which can be used to show model completeness of a theory, is given in Section 2. In Section 3 we define theories, connection between the theories and structures, and some important properties which they may satisfy. The definable sets of a structure are given by a recursive definition in Section 5 and the next section gives some basic techniques to find them.

First Order Logic

First order logic is the logic in which formulas are finite in length and quantification is limited to individual elements of a structure. For example, the formula $\bigvee_{n\in\mathbb{N}} x^n = e$, indexed by the natural numbers, which defines the torsion elements of a group $(G, \cdot, e)$, is not a first order formula since the disjunction is infinite. The quantification over all ideals of a ring $(R, +, \cdot, 0, 1)$

is not permitted in the first order logic since ideals are not elements of the ring. Throughout this paper every language and formula is first order.

2.1 Languages and Structures

This section gives the definition of languages, structures and formulas and some specific examples about them.

Informally, a structure is a set with distinguished functions, distinguished relations and distinguished elements. For example, the ordered additive group of integers has underlying set $\mathbb{Z}$, and we distinguish the binary functions $+$ and $-$, the binary relation $<$ and the identity element 0. Precisely,

A ***structure*** $\mathcal{M}$ is given by the following:

- a non-empty set M called the ***universe, domain*** or ***underlying set*** of $\mathcal{M}$.
- A collection of functions $\{f_i : i \in I_0\}$ where $f_i : M^{n_i} \to M$ for some $n_i \geq 1$.
- A collection of relations $\{r_i : i \in I_1\}$ where $r_i \subseteq M^{m_i}$ for some $m_i \geq 1$.
- A collection of distinguished elements $\{c_i : i \in I_2\} \subseteq M$.

I_0, I_1 and I_2 may be empty, and n_i and m_j are referred to as the ***arity*** of f_i and r_j.

The ***cardinality*** of $\mathcal{M}$ is the cardinality of the universe M, denoted by $|M|$.

For another example the ordered field of real numbers as a structure has domain $\mathbb{R}$, binary functions $+, -$ and $\times$, binary relation $<$, and distinguished elements 0 and 1.

In mathematical logic we study structures by examining the sentences of first order logic true in those structures. To any structure we attach a language L where we have an n_i-ary function symbol $\hat{f}_i$ for each f_i, an m_i-ary relation symbol $\hat{r}_i$ for each r_i and constant symbols $\hat{c}_i$ for each c_i.

Conversely an ***L-structure*** is a structure $\mathcal{M}$ where we can interpret all of the symbols of L.

Precisely, a ***language*** L can be defined as a disjoint union of $\mathcal{F}, \mathcal{R}, \mathcal{C}$, where:

$$\begin{aligned}\mathcal{F} &= \{\text{a set of function symbols}\},\\ \mathcal{R} &= \{\text{a set of relation symbols}\},\\ \mathcal{C} &= \{\text{a set of constant symbols}\}.\end{aligned}$$

Some examples are:

- $L_r = \{\hat{+}, \hat{-}, \hat{\cdot}, \hat{0}, \hat{1}\}$ is the language of rings, which has:

$$\begin{aligned}\mathcal{F} &= \{\hat{+}, \hat{-}, \hat{\cdot}\} \quad \text{each } \hat{f}_i \in \mathcal{F} \quad \text{is binary},\\ \mathcal{R} &= \emptyset,\\ \mathcal{C} &= \{\hat{0}, \hat{1}\}\end{aligned}$$

- $L_{or} = \{\hat{+}, \hat{-}, \hat{\cdot}, \hat{0}, \hat{1}, \hat{<}\}$ is the language of ordered rings, which has:

$$\begin{aligned}\mathcal{F} &= \{\hat{+}, \hat{-}, \hat{\cdot}\} \quad \text{each } \hat{f}_i \in \mathcal{F} \quad \text{is binary},\\ \mathcal{R} &= \{\hat{<}\} \quad \hat{<} \quad \text{is binary},\\ \mathcal{C} &= \{\hat{0}, \hat{1}\}\end{aligned}$$

If $\mathcal{R} = \emptyset$ in a language L then we say that L is a ***language of Algebras***.

If $\mathcal{M}$ is an L-structure where L is a language of algebras, then $\mathcal{M}$ is called an ***Algebra***.

We call $\hat{f}_i^{\mathcal{M}}$ (respectively for $\hat{r_j}^{\mathcal{M}}$ and $\hat{c_l}^{\mathcal{M}}$) ***the interpretation in*** $\mathcal{M}$ ***of*** the symbols $\hat{f}_i$ (respectively for $\hat{r_j}$ and $\hat{c_l}$) in L and the $\hat{f}_i^{\mathcal{M}}$ (respectively $\hat{r_j}^{\mathcal{M}}$ and $\hat{c_l}^{\mathcal{M}}$) are the so called fundamental functions (respectively relations and constants) on $\mathcal{M}$.

As an example take the language L_{or} and let the universe be $\mathbb{R}$, we have:

- the function symbols $\hat{+}, \hat{-}, \hat{\cdot}$ in L_{or} become the functions as:

$$\hat{+}^{\mathbb{R}} = ((a_1, a_2) \mapsto a_1 + a_2 : \mathbb{R}^2 \to \mathbb{R}),$$
$$\hat{-}^{\mathbb{R}} = ((a_1, a_2) \mapsto a_1 - a_2 : \mathbb{R}^2 \to \mathbb{R}),$$
$$\hat{\cdot}^{\mathbb{R}} = ((a_1, a_2) \mapsto a_1 \cdot a_2 : \mathbb{R}^2 \to \mathbb{R}),$$

  for $a_1, a_2 \in \mathbb{R}$,

- the relation symbol $\hat{<} \in L_{or}$ defines the set:

$$\hat{<}^{\mathbb{R}} : \{(a_1, a_2) \subseteq \mathbb{R}^2 : a_1 < a_2\},$$

- the constant symbols $\hat{0}, \hat{1}$ in L_{or} define constants:

$$\hat{0}^{\mathbb{R}} = 0 \in \mathbb{R}, \quad \text{the identity element for addition,}$$
$$\hat{1}^{\mathbb{R}} = 1 \in \mathbb{R}, \quad \text{the identity element for multiplication.}$$

If no confusion arises from now on we'll not use the $\hat{}$ on the symbols of L. Simply, we'll show the language of rings $L_r = \{+, -, \cdot, 0, 1\}$.

An L***-term*** is built by function symbols and constant symbols of L, equality symbol $=$ and the variables $x_1, x_2, \ldots$. Precisely, the recursive definition

of ***the set of*** L***-terms*** is the smallest set, say $\mathcal{T}(\mathcal{L})$, in the language L such that:

- $c \in \mathcal{T}(L)$ for every $c \in \mathcal{C}$,
- each variable symbol $x_1, x_2, \ldots \in \mathcal{T}(L)$ and
- if $t_1, \ldots, t_n \in \mathcal{T}(L)$ and $f \in \mathcal{F}$, then $f(t_1, \ldots, t_n) \in \mathcal{T}(L)$ where f is n-ary.

For example in L_r:

- 0,1 are constant terms,
- $\cdot(+(1,1), x_1)$ is a term (in the usual notation $(1+1) \cdot x_1$),
- $-(\cdot(x_1, x_2), \cdot(+(+(1,1),1), x_3)$ is a term. (in the usual notation $x_1 \cdot x_2 - ((1+1)+1) \cdot x_3$).

Let $\mathcal{M}$ be an L-structure and s be a term built using variables $\bar{x} = (x_1, \ldots, x_n)$. We interpret s is a function $s^{\mathcal{M}} : M^n \mapsto M$. For s and $\bar{a} = (a_1, \ldots, a_n) \in M$ we recursively define $s^{\mathcal{M}}(\bar{a})$ as follows:

- If s is a constant symbol c, then $s^{\mathcal{M}}(\bar{a}) = c^{\mathcal{M}}$,
- If s is the variable x_i, then $s^{\mathcal{M}}(\bar{a}) = a_i$,
- if $s = f(t_1, \ldots, t_n)$ where $t_1, \ldots, t_n \in \mathcal{T}(L)$ and $f \in \mathcal{F}$ then $s^{\mathcal{M}}(\bar{a}) = f^{\mathcal{M}}(t_1^{\mathcal{M}}(\bar{a}), \ldots, t_n^{\mathcal{M}}(\bar{a}))$.

The function $s^{\mathcal{M}}$ is defined by $\bar{a} \mapsto s^{\mathcal{M}}(\bar{a})$.

In a language L, the ***formulas*** are built from terms, the logical connectives $\wedge$, $\vee$, $\neg$, quantifiers $\exists$, $\forall$, parentheses and relation symbols of L. We interpret $\wedge$ as "and", $\vee$ as "or", $\neg$ as "not", quantifiers $\exists$ as "there exists" and $\forall$ as "for all".

We call an L-formula φ ***atomic*** if it's the combination of the terms and the relation symbols of L or the equality symbol. Indeed, it's one of the form:

- $t = s$ where t and s are terms of L, or
- $r(t_1, \ldots, t_n)$ where t_i's are terms of L, and r is an n-ary relation symbol of L.

The ***set of formulas*** in a language L is the smallest set say $F(L)$ containing all atomic L-formulas and satisfying the following:

- if $\varphi \in F(L)$ then $\neg\, \varphi \in F(L)$,
- if $\varphi \in F(L)$ then $\exists x_i\, \varphi$ and $\forall x_i\, \varphi$ are in $F(L)$,
- if φ_1, $\varphi_2 \in F(L)$ then $\varphi_1 \wedge \varphi_2$ and $\varphi_1 \vee \varphi_2$ are in $F(L)$.

In model theory we prove most of the results by induction on the complexity of the formulas: first for the terms by induction on terms, then for the atomic formulas by induction on atomic formulas, last for formulas by induction on formulas.

A variable x ***occurs freely*** (or is a ***free variable***) in a formula φ if it isn't inside the scope of a $\exists x$ or $\forall x$ quantifier, otherwise we say it is bound. For example:

$$\varphi(a, b, c) := \exists x(ax^2 + bx + c = 0),$$
$$\psi(x, a, b, c) := (ax^2 + bx + c = 0).$$

In the first example the variables a, b and c are free variables but the variable x is inside the quantifier $\exists x$ so it is bound. In the second example none of the variables are bound therefore all variables are free variables. Note that by using the above examples we can say that $\varphi(a, b, c) := \exists x \psi(x, a, b, c)$.

We write $\varphi(\bar{x})$ to show that the free variables of φ are among the variables $\bar{x} = x_1, \ldots, x_n$ and say that φ is an n-ary formula. I'll denote the set of all n-ary L-formulas by $F_n(L)$.

Let φ be a formula and $fv(\varphi)$ be the set of indices of its free variables. Then:

1. If φ is atomic, then $fv(\varphi)$ be the set of all indices of variables in it.
2. $fv(\varphi) = fv(\neg\, \varphi)$.
3. $fv(\varphi_1 \wedge \varphi_2) = fv(\varphi_1 \vee \varphi_2) = fv(\varphi_1) \cup fv(\varphi_2)$.
4. $fv(\exists x_i \varphi) = fv(\varphi) - \{i\}$

Precisely a ***quantifier free (or open) formula*** is defined by the following:

1. Atomic formulas are quantifier free.
2. If φ is quantifier free, then so is $\neg\, \varphi$.
3. If φ_1 and φ_2 are quantifier free, then so are $\varphi_1 \wedge \varphi_2$ and $\varphi_1 \vee \varphi_2$.

An L-formula φ is called an ***L-sentence*** if $fv(\varphi) = \emptyset$, precisely all variables of an L-sentence are bound. Imprecisely all axioms are sentences.

For example in L_r:

- $\exists x_1\ (x_1 \cdot x_1 = x_2)$ is not a sentence, since x_2 is a free variable.
- $\forall x_1 \exists x_2\ (x_1 \cdot x_2 = x_2 \cdot x_1)$ is a sentence.
- $\forall x_1 \forall x_2\ (x_1 \cdot x_2 = x_2 \cdot x_1)$ is a universal sentence.

The ***universal closure*** of a formula $\varphi(x_1, \ldots, x_n)$ is $\forall x_1, \ldots, \forall x_n \varphi(x_1, \ldots, x_n)$ [18]. For example: $\forall x_2 \exists x_1\ x_1 \cdot x_1 = x_2$ is the universal closure of the formula $\exists x_1\ x_1 \cdot x_1 = x_2$.

Remark 2.1.1. If no confusion arises I would like to use $\bar{x}$ for the n-tuple of variables $x_1, \ldots, x_n$ and $\bar{a}$ for the n-tuple of elements $a_1, \ldots, a_n$ of a set.

If we think of $\varphi(\bar{x})$ as a property of elements $\bar{a} \in M^n$ where M is the universe of an L-structure $\mathcal{M}$, we need to define $\varphi(\bar{x})$ holds for $\bar{a} \in M^n$. Let t, s and t_i's be terms and φ, ϕ be formulas of the language L, if $\varphi(\bar{x})$ holds for $\bar{a} \in M^n$, we denote this by $\mathcal{M} \models \varphi(\bar{a})$, and this means:

- if φ is $t = s$, then $t^{\mathcal{M}}(\bar{a}) = s^{\mathcal{M}}(\bar{a})$,
- if φ is $r(t_1, \ldots, t_n)$, then $r^{\mathcal{M}}(t_1^{\mathcal{M}}(\bar{a}), \ldots, t_n^{\mathcal{M}}(\bar{a})) \in r^{\mathcal{M}}$,
- if φ is $\neg\, \phi$, then $\mathcal{M} \not\models \phi(\bar{a})$,
- if φ is $\varphi_1 \wedge \varphi_2$, then $\mathcal{M} \models \varphi_1(\bar{a})$ and $\mathcal{M} \models \varphi_2(\bar{a})$,
- if φ is $\varphi_1 \vee \varphi_2$, then $\mathcal{M} \models \varphi_1(\bar{a})$ or $\mathcal{M} \models \varphi_2(\bar{a})$,
- if φ is $\exists y\ \phi(\bar{x}, y)$, then $\mathcal{M} \models \phi(\bar{a}, b)$ for some $b \in M$,
- if φ is $\forall y\ \phi(\bar{x}, y)$, then $\mathcal{M} \models \phi(\bar{a}, b)$ for all $b \in M$.

Then we say that $\mathcal{M}$ ***satisfies*** $\varphi(\bar{a})$ or $\varphi(\bar{a})$ is ***true*** in $\mathcal{M}$ or $\varphi(\bar{x})$ ***holds*** for $\bar{a} \in M^n$.

Note that we can use:

$$\varphi \to \phi \quad \text{for} \quad \neg\, \varphi \vee \phi \quad \text{and}$$
$$\varphi \leftrightarrow \phi \quad \text{for} \quad (\varphi \to \phi) \wedge (\phi \to \varphi).$$

Since we can think of $\varphi \vee \phi$ as $\neg\, (\neg\, \varphi \wedge \neg\, \phi)$ and $\forall x \varphi$ as $\neg\, (\exists x \neg\, \varphi)$ we can exclude their cases when proving theorems.

2.2 L-Embedding

By introducing the notion of L-embedding we define being a substructure and an elementary substructure. These definitions will be used in the next section and the other chapters frequently.

Let $\mathcal{M}$ and $\mathcal{N}$ be L-structures with underlying sets M and N respectively. An ***L-embedding*** $h : \mathcal{M} \to \mathcal{N}$ is an injective map that preserves the interpretation of all function symbols, relation symbols and constant symbols of L. Precisely, for all $\bar{a} \in M^n$:

- $h(f_i^{\mathcal{M}}(\bar{a})) = f_i^{\mathcal{N}}(h(\bar{a}))$ for all n-ary $f_i \in \mathcal{F} \subseteq L$.
- $\bar{a} \in r_j^{\mathcal{M}} \iff h(\bar{a}) \in r_j^{\mathcal{N}}$ for all n-ary $r_j \in \mathcal{R} \subseteq L$.
- $h(c_l^{\mathcal{M}}) = c_l^{\mathcal{N}}$ for all $c_l \in \mathcal{C} \subseteq L$.

A bijective L-embedding is called an ***L-isomorphism***.

We say either $\mathcal{M}$ is a ***substructure*** of $\mathcal{N}$ or $\mathcal{N}$ is an ***extension*** of $\mathcal{M}$ and write $\mathcal{M} \subseteq \mathcal{N}$ if $M \subseteq N$ and the inclusion map of $\mathcal{M}$ in $\mathcal{N}$ is an L-embedding. That is, for all $\bar{a} \in M^n$:

- for all n-ary $f_i \in \mathcal{F} \subseteq L$,

$$f_i^{\mathcal{M}} = f_i^{\mathcal{N}} \mid_{M^n},$$

- for all n-ary $r_j \in \mathcal{R} \subseteq L$

$$r_j^{\mathcal{M}} = r_j^{\mathcal{N}} \cap M^n,$$

- for all $c_l \in \mathcal{C} \subseteq L$

$$c_l^{\mathcal{M}} = c_l^{\mathcal{N}}.$$

Lemma 2.2.1. *Let $\mathcal{M}$ and $\mathcal{N}$ be L-structures. If $\mathcal{M} \subseteq \mathcal{N}$, $\bar{a}$ in M and $\varphi(\bar{x})$ is a quantifier free formula, then*

$$\mathcal{M} \models \varphi(\bar{a}) \text{ if and only if } \mathcal{N} \models \varphi(\bar{a}).$$

Proof. Suppose $\mathcal{M} \subseteq \mathcal{N}$, our aim is to show that the lemma is true for all quantifier free formula. Since the quantifier free formulas are defined recursively as on p.10, we need to check the lemma for atomic formulas. Atomic formulas are of the form $t = s$ where t and s are terms of L, or $r(t_1, \ldots, t_n)$ where t_i's are terms of L, so we need to check the validity of the lemma for terms. This is last because the lemma is true for all elements of the language by definition of a substructure.

Claim: If $t(\bar{x})$ is a term in L and $\bar{b}$ in M, then $t^{\mathcal{M}}(\bar{b}) = t^{\mathcal{N}}(\bar{b})$. This by induction on complexity of terms.

- If t is a constant symbol c then $c^{\mathcal{M}} = c^{\mathcal{N}}$.
- If t is the variable symbol x_i, then $t^{\mathcal{M}}(\bar{b}) = b_i = t^{\mathcal{N}}(\bar{b})$.
- Suppose $t = f(t_1, \ldots, t_n)$ where f is an n-ary function symbol, $t_1, \ldots, t_n$ are terms and $t_i^{\mathcal{M}}(\bar{b}) = t_i^{\mathcal{N}}(\bar{b})$ for $i = 1, \ldots, n$. Since $\mathcal{M} \subseteq \mathcal{N}$, $f^{\mathcal{M}} = f^{\mathcal{N}} \mid M^n$. Thus,

$$\begin{aligned} t^{\mathcal{M}}(\bar{b}) &= f^{\mathcal{M}}(t_1^{\mathcal{M}}(\bar{b}), \ldots, t_n^{\mathcal{M}}(\bar{b})) \\ &= f^{\mathcal{N}}(t_1^{\mathcal{M}}(\bar{b}), \ldots, t_n^{\mathcal{M}}(\bar{b})) \\ &= f^{\mathcal{N}}(t_1^{\mathcal{N}}(\bar{b}), \ldots, t_n^{\mathcal{N}}(\bar{b})) \\ &= t^{\mathcal{N}}(\bar{b}). \end{aligned}$$

Since the claim is true,

- If φ is $t_1 = t_2$, then

$$\begin{aligned} \mathcal{M} \models \varphi(\bar{a}) &\iff t_1^{\mathcal{M}}(\bar{a}) = t_2^{\mathcal{M}}(\bar{a}) \\ &\iff t_1^{\mathcal{N}}(\bar{a}) = t_2^{\mathcal{N}}(\bar{a}) \\ &\iff \mathcal{N} \models \varphi(\bar{a}) \end{aligned}$$

- If φ is $r(t_1, \ldots, t_n)$, where r is an n-ary relation symbol, then

$$\begin{aligned} \mathcal{M} \models \varphi(\bar{a}) &\iff (t_1^{\mathcal{M}}(\bar{a}), \ldots, t_n^{\mathcal{M}}(\bar{a})) \in r^{\mathcal{M}} \\ &\iff (t_1^{\mathcal{M}}(\bar{a}), \ldots, t_n^{\mathcal{M}}(\bar{a})) \in r^{\mathcal{N}} \\ &\iff (t_1^{\mathcal{N}}(\bar{a}), \ldots, t_n^{\mathcal{N}}(\bar{a})) \in r^{\mathcal{N}} \\ &\iff \mathcal{N} \models \varphi(\bar{a}). \end{aligned}$$

Thus, the lemma is true for all atomic formulas.

Suppose that the lemma is true for ψ and φ is $\neg\psi$. Then,

$$\begin{aligned} \mathcal{M} \models \varphi(\bar{a}) &\iff \mathcal{M} \models \neg\, \psi(\bar{a}) \\ &\iff \mathcal{M} \not\models \psi(\bar{a}) \\ &\iff \mathcal{N} \not\models \psi(\bar{a}) \\ &\iff \mathcal{N} \models \neg\, \psi(\bar{a}) \\ &\iff \mathcal{N} \models \varphi(\bar{a}). \end{aligned}$$

At last suppose that the lemma is true for $\varphi_1(\bar{x})$ and $\varphi_2(\bar{x})$, and $\varphi(\bar{x}) = \varphi_1(\bar{x}) \wedge \varphi_2(\bar{x})$, then:

$$\begin{aligned}
\mathcal{M} \models \psi(\bar{a}) &\iff \mathcal{M} \models \varphi_1(\bar{a}) \wedge \varphi_2(\bar{a}) \\
&\iff \mathcal{M} \models \varphi_1(\bar{a}) \quad \text{and} \quad \mathcal{M} \models \varphi_2(\bar{a}) \\
&\iff \mathcal{N} \models \varphi_1(\bar{a}) \quad \text{and} \quad \mathcal{N} \models \varphi_2(\bar{a}) \\
&\iff \mathcal{N} \models \varphi_1(\bar{a}) \wedge \varphi_2(\bar{a}) \\
&\iff \mathcal{N} \models (\varphi_1 \wedge \varphi_2)(\bar{a}) \\
&\iff \mathcal{N} \models \psi(\bar{a}).
\end{aligned}$$

□

Let $\mathcal{M}$ and $\mathcal{N}$ be L-structures with underlying sets M and N respectively, then an L-embedding $h : \mathcal{M} \to \mathcal{N}$ is called an ***elementary embedding*** if it preserves the interpretation of all formulas of L. Precisely for all n-ary L-formula $\varphi(\bar{x})$ and $\bar{a} \in M^n$:

$$\mathcal{M} \models \varphi^{\mathcal{M}}(\bar{a}) \iff \mathcal{N} \models \varphi^{\mathcal{N}}(h(\bar{a})).$$

We say either $\mathcal{M}$ is an ***elementary substructure*** of $\mathcal{N}$ or $\mathcal{N}$ is an ***elementary extension*** of $\mathcal{M}$ and write $\mathcal{M} \preccurlyeq \mathcal{N}$ if $\mathcal{M} \subseteq \mathcal{N}$ and the inclusion map $i : \mathcal{M} \hookrightarrow \mathcal{N}$ is an elementary embedding. Indeed $\mathcal{M} \preccurlyeq \mathcal{N}$ if and only if for all n-ary L-formulas $\varphi(\bar{x})$ and $\bar{a} \in M^n$,

$$\mathcal{M} \models \varphi(\bar{a}) \iff \mathcal{N} \models \varphi(\bar{a}).$$

2.3 Theories and Models

In the first section we took a set say M and choose a suitable language to work on it and obtained the structure $\mathcal{M}$. Now assume that we have a set Σ

of sentences and we want to find the structures which all the sentences in Σ holds.

Let Σ be a set of L-sentences. A ***model*** of Σ is an L-structure $\mathcal{M}$ such that $\mathcal{M} \models \varphi$ for all $\varphi \in \Sigma$; In this case we write $\mathcal{M} \models \Sigma$.

An L-sentence φ is a ***logical consequence*** of Σ and written $\Sigma \models \varphi$ if $\mathcal{M} \models \varphi$ for all $\mathcal{M} \models \Sigma$.

An ***L-theory*** $\mathcal{T}$ is a set of L-sentences that contains all of its logical consequences.

If $\mathcal{T}$ is a theory and $\Sigma \subseteq \mathcal{T}$, we say Σ is a ***set of axioms*** for $\mathcal{T}$ if $\mathcal{T} = Th(\Sigma)$. If there exists a finite set of axioms for $\mathcal{T}$, we say that $\mathcal{T}$ is finitely axiomatizable.

A class $\mathcal{K}$ of L-structures is said to be an ***elementary class*** if $\mathcal{K}$ is the class of all models of the same L-theory $\mathcal{T}$. In this case we said that $\mathcal{T}$ ***axiomatizes*** $\mathcal{K}$. For example the class of algebraically closed fields is an elementary class, but the class of finite fields is not, since not every model of the theory of finite fields is a finite field. There are infinite fields which satisfy every sentence true for finite fields. We will explain this situation for finite fields more clearly at the end of the last chapter.

Some examples of the theories in the language L_r:

- the class of fields is axiomatized by:
  - $\forall x_1 \forall x_2 \; x_1 + x_2 = x_2 + x_1$,
  - $\forall x_1 \forall x_2 \forall x_3 \; x_1 + (x_2 + x_3) \iff (x_1 + x_2) + x_3$,
  - $\forall x \; x + (-x) = 0$,
  - $\forall x_1 \forall x_2 \forall x_3 \; x_1 \cdot (x_2 \cdot x_3) = (x_1 \cdot x_2) \cdot x_3$,
  - $\forall x_1 \forall x_2 \forall x_3 \; x_1 \cdot (x_2 + x_3) = (x_1 \cdot x_2) + (x_1 \cdot x_3)$,
  - $\forall x \; x + 0 = 0$,

- $\forall x\ x.1 = x$,
- $\forall x_1 \forall x_2\ x_1 \cdot x_2 = x_2 \cdot x_1$,
- $\forall x\ x \neq 0 \rightarrow \exists y\ x \cdot y = 1$,
- $0 \neq 1$

(Note that if we weaken the last axiom to $\forall x \forall y\ (x \neq 0 \wedge y \neq 0 \rightarrow x \cdot y \neq 0)$ we get the axioms for the theory of integral domains.)

- by adding the following set of sentences to the theory of fields:

$$\forall a_0 \ldots \forall a_{n-1} \exists x\ x^n + \textstyle\sum_{i=0}^{n-1} a_i x^i = 0$$

for $n = 1, 2 \ldots$ we get the axiomatization for the theory of algebraically closed fields which we'll denote by ACF. Indeed these axioms are:

$$\forall a_0 \exists x\ x + a_0 = 0$$
$$\forall a_0 \forall a_1 \exists x\ x^2 + a_1 x + a_0 = 0$$

by continuing this way we get an infinite set of conditions which tell us that every monic polynomial for each degree has a root.

- to show the characteristic we add:

$$\varphi_p : \underbrace{1 + \ldots + 1}_{p-times} = 0$$

to ACF, p prime, then,

for $p\ > 0\ : ACF_p = ACF \cup \{\varphi_p\}$ and

for $p = 0\ : ACF_0 = ACF \cup \{\neg\ \varphi_p : p\ > 0\}$

where ACF_p (respectively ACF_0) is the axiomatization for the theory algebraically closed fields of characteristic p (respectively characteristic 0).

2.4 Definable Sets

By describing the simple sets on a structure we can construct more complicated ones. The first of these simple sets are the ones defined by atomic formulas.

A set $X \subseteq M^n$ is ***definable*** in the L-structure $\mathcal{M}$ if there are formulas $\varphi(x_1, \ldots, x_{n+m})$ and elements $\bar{b} \in M^m$ such that:

$$X = \{\bar{a} \in M^n : \mathcal{M} \models \varphi(\bar{a}, \bar{b})\}$$

We say that X is ***A-definable*** or ***definable over*** A, where $A \subseteq M$, if we can choose that $b_1, \ldots, b_m \in A$. If $m = 0$ we say X is $\emptyset$-definable.

For example:

- In L_{or} $\{x : x > \pi\}$ is definable over $\mathbb{R}$ but not $\emptyset$-definable, while $\{x : x > \sqrt{2}\}$ is $\emptyset$-definable by the L_{or} formula $x \cdot x > 1 + 1 \wedge x > 0$.
- Let F be a field and $\mathcal{M} = (F[X], +, -, \cdot, 0, 1)$ be the ring of polynomials over F. Then F is definable by the formula $x = 0 \vee \exists y(x \cdot y = 1)$ in $\mathcal{M}$.

Now I'll give a characterization of the definable sets.

Proposition 2.4.1. *Suppose D_n is the smallest collection of subsets of M^n for all $n \geq 1$ such that $D = (D_n : n \geq 1)$ is the smallest collection satisfying the following conditions hold:*

- *$M^n \in D_n$.*
- *For all n-ary functions f of $\mathcal{M}$, the graph of f is in D_{n+1}.*
- *For all n-ary relations r of $\mathcal{M}$, $r \in D_n$.*
- *For all $i, j \leq n$, $\{\bar{x} \in M^n : x_i = x_j\} \in D_n$.*

- *Each D_n is closed under complement, union and intersection.*
- *If $X \in D_m$ and $\pi : M^n \to M^m$ is a projection map $(x_1, \ldots, x_n) \mapsto (x_{i_1}, \ldots, x_{i_m})$, then $\pi^{-1}(X) \in D_n$.*
- *If $X \in D_n$ and π is as above, then $\pi(X) \in D_m$.*
- *If $X \in D_{n+m}$ and $\bar{b} \in M^m$, then $\{\bar{a} \in M^n : (\bar{a}, \bar{b}) \in X\} \in D_n$.*

Then $X \subseteq M^n$ is definable if and only if $X \in D_n$.

Proof. See [15], Proposition 1.3.4. □

$Diag_{el}(\mathcal{M})$ and $Diag(\mathcal{M})$

For an L-structure $\mathcal{M}$ let L_M be the language obtaining by adding new constants symbols for each element of the universe M of $\mathcal{M}$.

$Diag(\mathcal{M}) = \{\varphi : \varphi \text{ an open } L_M\text{-sentence and } \mathcal{M} \models \varphi\}$ and

$Diag_{el}(\mathcal{M}) = \{\varphi : \varphi \text{ an } L_M\text{-sentence and } \mathcal{M} \models \varphi\}$.

Note that $\mathcal{M}$ expands naturally to an L_M structure $\mathcal{M}'$, by interpreting the constant symbol corresponding to $m \in M$ by the element m itself.

2.5 Techniques

Recursively Axiomatizable Theories

A language L ***is recursive*** if there is an algorithm that decides whether a sequence of symbols is an L-formula [11, p.50].

An L-theory $\mathcal{T}$ is ***recursively axiomatizable*** if L is recursive and $\mathcal{T}$ has a recursive set of axioms (i. e. there is an algorithm that decides whether an L-sentence φ is in that set of axioms).

If a theory in a recursive language is axiomatized by a finite set of sentences, then it is clearly recursively axiomatizable. The theory of integral domains and the theory of fields of characteristic p ($p \neq 0$) are some examples of these theories. But there are recursive theories which are not equivalent to a finite set of sentences: for example, the theory of fields of characteristic zero and the theory of algebraically closed fields.

A proof of φ using assumptions from a set Σ of L-sentences is a finite sequence of L-formulas $\psi_1, \ldots \psi_n$ such that:

- $\psi_n = \varphi$ and,
- – $\psi_i \in \Sigma$ or,
  - ψ_i follows from $\psi_1, \ldots \psi_{i-1}$ by a simple logical rules [2].

If there exists a proof of φ from Σ then we write $\Sigma \vdash \varphi$.

Gödel's Completeness Theorem says that if these logical rules are chosen properly then

$$\Sigma \vdash \varphi \iff \Sigma \models \varphi.$$

Consistent Theories

We say that an L-theory $\mathcal{T}$ is ***satisfiable*** if it has a model. We say that $\mathcal{T}$ is ***consistent*** if and only if we can't formally derive a contradiction ($\mathcal{T} \vdash \varphi \wedge \neg \varphi$) from $\mathcal{T}$; otherwise, we say that $\mathcal{T}$ is ***inconsistent***. The following theorem is a reformulation of the above Gödel's Theorem:

Theorem 2.5.1. *(Completeness) An L-theory $\mathcal{T}$ is satisfiable if and only if $\mathcal{T}$ is consistent.*

Proof. Suppose that $\mathcal{T}$ is not satisfiable then $\mathcal{T}$ has no models, so $\varphi \wedge \neg \varphi$ is a logical consequence of $\mathcal{T}$. Thus $\mathcal{T} \models \varphi \wedge \neg \varphi$ so $\mathcal{T} \vdash \varphi \wedge \neg \varphi$ therefore $\mathcal{T}$ is inconsistent. Conversely, an inconsistent theory has no models. □

The completeness theorem has a simple consequence **Compactness**:

Theorem 2.5.2. *(Compactness) An L-theory $\mathcal{T}$ has a model if and only if every finite subset of $\mathcal{T}$ has a model.*

Proof. If $\mathcal{T}$ has a model then clearly every finite subset of $\mathcal{T}$ has a model. Assume $\mathcal{T}$ has no models; then every model of $\mathcal{T}$ is a model of $\varphi \wedge \neg\, \varphi$. Since proofs are finite (by the properties of the proof systems that we use), we can get $\varphi \wedge \neg\, \varphi$ by using finitely many assumptions from $\mathcal{T}$; therefore $\mathcal{T}$ has a finite subset which is inconsistent. □

Complete Theories

An L-theory $\mathcal{T}$ is ***complete*** if for any L-sentence φ either $\mathcal{T} \models \varphi$ or $\mathcal{T} \models \neg\, \varphi$.

Let $\mathcal{M}$ and $\mathcal{N}$ be L-structures. We say that they are ***elementarily equivalent*** if

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

for all L-sentences φ; we denote this by $\mathcal{M} \equiv \mathcal{N}$. Elementarily equivalence in the language L_A is denoted by $\equiv_A$ or is called elementarily equivalent over A.

The ***full theory*** of an L- structure $\mathcal{M}$ is $Th(\mathcal{M}) = \{\varphi :\ \varphi \text{ is an } L\text{-sentence and } \mathcal{M} \models \varphi\}$, which is complete. It is easy to see that $\mathcal{M} \equiv \mathcal{N}$ if and only if $Th(\mathcal{M}) = Th(\mathcal{N})$.

The following theorem shows that $Th(\mathcal{M})$ is an isomorphism invariant of $\mathcal{M}$.

Theorem 2.5.3. *Suppose that $j : \mathcal{M} \to \mathcal{N}$ is an isomorphism of L-structures; $\mathcal{M}$ and $\mathcal{N}$. Then, $\mathcal{M} \equiv \mathcal{N}$.*

Proof. By induction on formulas. See [15] Theorem 1.1.10. □

Proposition 2.5.4. *(Tarski's Test) Let $\mathcal{M} \subseteq \mathcal{N}$ be L-structures then $\mathcal{M} \preccurlyeq \mathcal{N}$ if and only if for every L-formula $\varphi(\bar{x}, y)$ and $\bar{a} \in M^n$ the following holds:*

$$\text{if } \mathcal{N} \models \exists y\, \varphi(\bar{a}, y) \text{ then there is } b \in M \text{ such that } \mathcal{N} \models \varphi(\bar{a}, b)$$

Proof. ($\Rightarrow$) Clear by the definition of elementary substructure.

($\Leftarrow$) We will prove that for each L-formula $\psi(\bar{x})$ and all $\bar{a} \in M^n$ we will have

$$\mathcal{M} \models \psi(\bar{a}) \iff \mathcal{N} \models \psi(\bar{a})$$

by induction on the complexity of ψ.

- It is clear by Lemma 2.2.1 that if $\psi(\bar{x})$ is atomic since $\mathcal{M} \subseteq \mathcal{N}$.

- For negation, suppose let $\psi(\bar{x}) = \neg\varphi(\bar{x})$ and we have it for φ, then,

$$\begin{aligned} \mathcal{M} \models \psi(\bar{a}) &\iff \mathcal{M} \models \neg\varphi(\bar{a}) \\ &\iff \mathcal{M} \not\models \varphi(\bar{a}) \\ &\iff \mathcal{N} \not\models \varphi(\bar{a}) \\ &\iff \mathcal{N} \models \neg\varphi(\bar{a}) \\ &\iff \mathcal{N} \models \psi(\bar{a}). \end{aligned}$$

- The $\wedge$ case can be proved similarly.

- For the case $\exists$, we will consider $\psi(\bar{x}) = \exists y\, \varphi(\bar{a}, y)$.

  If $\mathcal{M} \models \exists y\, \varphi(\bar{a}, y)$ then $\exists b \in M$ and $M \models \varphi(\bar{a}, b)$ by inductive hypothesis $\mathcal{N} \models \exists y\, \varphi(\bar{a}, y)$ which implies that $\mathcal{N} \models \exists y\, \varphi(\bar{a}, y)$. It remains to show that if $\mathcal{N} \models \exists y\, \varphi(\bar{a}, y)$ then $\mathcal{M} \models \exists y\, \varphi(\bar{a}, y)$.

Assume $\mathcal{N} \models \exists y\ \varphi(\bar{a}, y)$; by the assumption there is some b in M such that:

$$\mathcal{N} \models \varphi(\bar{a}, b).$$

By the inductive hypothesis on φ,

$$\mathcal{M} \models \varphi(\bar{a}, b)$$

finally which implies that

$$\mathcal{M} \models \exists y\ \varphi(\bar{a}, y).$$

□

Theorem 2.5.5. *(Löwenheim-Skolem Theorem) Let $\mathcal{T}$ be an L-theory, and assume that $\mathcal{T}$ has an infinite model, then $\mathcal{T}$ has models of every infinite cardinal κ greater than or equal to the cardinal of $\mathcal{T}$.*

See [11, p.63] for a proof.

Note that in the Löwenheim-Skolem Theorems κ denotes an infinite cardinal greater than or equal to the number of symbols in the language L (denoted by $|L|$).

The Downward Löwenheim-Skolem Theorem gives us a method for building small elementary submodels and The Upward Löwenheim-Skolem Theorem is useful for the Completeness Test of Vaught and also helps getting big elementary extensions of a model of the theory $\mathcal{T}$.

Theorem 2.5.6. *(Downward Löwenheim-Skolem Theorem) Suppose $X \subseteq N$ and $|X| \leq \kappa \leq |N|$. Then $\mathcal{N}$ has an elementary submodel $\mathcal{M} \preccurlyeq \mathcal{N}$ of cardinality κ such that $X \subseteq M$.*

Theorem 2.5.7. *(Upward Löwenheim-Skolem Theorem) Let $\mathcal{M}$ be an infinite structure for L. For every cardinal κ greater than or equal to the cardinality of $\mathcal{M}$ and the cardinality of L, $\mathcal{M}$ has an elementary extension of cardinal κ.*

Proof. See [11] §4 for proofs of both Löwenheim-Skolem Theorems. □

κ categorical

Let κ be an infinite cardinal and let $\mathcal{T}$ be an L-theory which has models of size κ, then we say that $\mathcal{T}$ is ***κ-categorical*** if any two models $\mathcal{M}$ and $\mathcal{N}$ of $\mathcal{T}$ satisfying $|M| = |N| = \kappa$ are isomorphic.

Proposition 2.5.8. *For each p (prime or zero), the theory ACF_p is κ-categorical for each uncountable κ.*

Proof. Algebraically closed fields are described up to isomorphism by the characteristic and the transcendence degree. Also any algebraically closed field with transcendence degree λ has cardinality $\lambda + \aleph_0$. If $\kappa > \aleph_0$, any algebraically closed field of cardinality κ has transcendence degree κ. Hence any two algebraically closed fields of the same characteristic and the same uncountable cardinality are isomorphic. □

Theorem 2.5.9. *(Vaught's Test) If all models of an L-theory $\mathcal{T}$ are infinite and $\mathcal{T}$ is κ-categorical for some infinite cardinal $\kappa \geq |L|$, then $\mathcal{T}$ is complete.*

Proof. Let $\mathcal{M}, \mathcal{N} \models \mathcal{T}$ with $|M| = \lambda_1$ and $|M| = \lambda_2$.

If $\lambda_1 < \kappa$ then by using Upward Löwenheim-Skolem Theorem we get a model $\mathcal{M}'$ of $\mathcal{T}$ such that $\mathcal{M} \preccurlyeq \mathcal{M}'$ with $|M'| = \kappa$. If $\lambda_1 > \kappa$ then by using Downward Löwenheim-Skolem Theorem we get again a model $\mathcal{M}'$ of $\mathcal{T}$ such that $\mathcal{M}' \preccurlyeq \mathcal{M}$ with $|M'| = \kappa$. So we get $\mathcal{M}' \equiv \mathcal{M}$. Then by doing the same process for $\mathcal{N}$ we get a new model $\mathcal{N}'$ of $\mathcal{T}$ such that $\mathcal{N}' \equiv \mathcal{N}$ with $|N'| = \kappa$. Since $\mathcal{T}$ is κ-categorical $\mathcal{M} \equiv \mathcal{N}$. □

The theory of algebraically closed fields is not complete since it doesn't decide the characteristic; however, the theory of algebraically closed fields with the fixed characteristic p (p prime or zero) is complete and will be proved in next chapter.

Decidability

An Σ of L-sentences is ***decidable*** if there is an algorithm that decides for a given sentence φ whether $\Sigma \models \varphi$.

Proposition 2.5.10. *Let $\mathcal{T}$ be a complete recursively axiomatizable satisfiable theory in a recursive language L. Then $\mathcal{T}$ is decidable.*

Proof. See [15] Lemma 2.2.8. □

Model Complete Theories

An L-theory $\mathcal{T}$ is ***model-complete*** if whenever $\mathcal{M}, \mathcal{N} \models \mathcal{T}$ and $\mathcal{M} \subseteq \mathcal{N}$ then $\mathcal{M} \preccurlyeq \mathcal{N}$.

Informally suppose $\mathcal{K}$ is an elementary class of L-structures with the theory $\mathcal{T}$, then $\mathcal{T}$ is model-complete if and only if each embedding in $\mathcal{K}$ is an elementary embedding.

Lemma 2.5.11. *An L-theory $\mathcal{T}$ is model-complete if and only if $\mathcal{T} \cup Diag(\mathcal{M})$ is complete whenever $\mathcal{M} \models \mathcal{T}$.*

Proof. ($\Leftarrow$) Assume $\mathcal{T} \cup Diag(\mathcal{M})$ is not complete for some $\mathcal{M} \models \mathcal{T}$ then there is an L-sentence φ and there are models $\mathcal{N}, \mathcal{N}'$ of $\mathcal{T} \cup Diag(\mathcal{M})$ such that:

$$\mathcal{N} \models \varphi, \text{ but } \mathcal{M} \models \neg\varphi.$$

Since $\mathcal{N}, \mathcal{N}' \models Diag(\mathcal{M})$ we may assume that $\mathcal{M} \subseteq \mathcal{N}, \mathcal{N}'$. Assume that $\mathcal{M} \models \varphi$ then $\mathcal{M} \preccurlyeq \mathcal{N}'$.

($\Rightarrow$) Assume that $\mathcal{T}$ is not model-complete then $\mathcal{M} \subseteq \mathcal{N}$ but $\mathcal{M} \not\preceq \mathcal{N}$ for some $\mathcal{M}, \mathcal{N} \models \mathcal{T} \cup Diag(\mathcal{M})$. So there is an L_M-sentence φ such that

$$\mathcal{N} \models \neg\varphi \text{ but } \mathcal{M} \models \varphi.$$

Since $\mathcal{N}, \mathcal{M} \models \mathcal{T} \cup Diag(\mathcal{M})$ we conclude that $\mathcal{T} \cup Diag(\mathcal{M})$ is not complete.

□

We say that two n-ary L-formulas $\varphi(\bar{x})$ and $\psi(\bar{x})$ are ***equivalent in an L-theory*** $\mathcal{T}$ if $\mathcal{T} \models \forall\bar{x}(\varphi(\bar{x}) \iff \psi(\bar{x}))$. In fact we may use Tarski's Test to prove a theory is model complete, but we use another lemma which is more convenient for the class of algebraically closed fields and the class of generic difference fields that we'll study in next chapters. First some definitions:

The ***universal part*** of an L-theory $\mathcal{T}$ is denoted by $\mathcal{T}_\forall$ and is the set of all universal consequences of $\mathcal{T}$. So $\mathcal{T}_\forall$ is the set which is generated by all of the universal sentences in $\mathcal{T}$ by logical rules.

For example the theory of integral domains is the universal part of the theory of algebraically closed fields.

Lemma 2.5.12. *Let $\mathcal{A}$ be an L-structure and $\mathcal{T}$ be an L-theory. Then $\mathcal{A} \models \mathcal{T}_\forall$ if and only if $\mathcal{A}$ extends to a model of $\mathcal{T}$.*

Proof. ($\Rightarrow$) Assume $\mathcal{T} \cup Diag(A)$ is inconsistent. Then for some $\varphi(\bar{a})$ in $Diag(A)$;

$$\mathcal{T} \models \neg\varphi(\bar{a})$$
$$\mathcal{T} \models \forall\bar{x}\neg\varphi(\bar{x})$$

which is a contradiction since $\forall\bar{x}\neg\varphi(\bar{x})$ is in $\mathcal{T}_\forall$.

($\Leftarrow$) Assume that $\mathcal{A}$ is not a model of $\mathcal{T}_\forall$. Then for some $\varphi =: \forall\bar{x}\psi(\bar{x})$ in $\mathcal{T}$ where ψ is quantifier free;

$$\mathcal{A} \models \neg\varphi$$
$$\mathcal{A} \models \exists\bar{x}\neg\psi(\bar{x})$$
$$\mathcal{A} \models \neg\psi(\bar{a})$$

for some $\bar{a}$ in A. Then $\neg\psi(\bar{a}) \cup \forall\bar{x}\psi(\bar{x})$ is inconsistent since $\neg\psi(\bar{a}) \in Diag(A)$. Therefore $\mathcal{T} \cup Diag(A)$ is inconsistent so there is no $\mathcal{M} \models \mathcal{T}$ such that $\mathcal{A} \subseteq \mathcal{M}$. □

Let $\mathcal{M}$ and $\mathcal{N}$ be L-structures and $\mathcal{M} \subseteq \mathcal{N}$. $\mathcal{M}$ is ***existentially closed*** in $\mathcal{N}$ if every existential sentence $\exists\bar{x}\varphi(\bar{x}, \bar{a})$ which holds in $\mathcal{N}$ where $\bar{a} \in M^n$ holds in $\mathcal{M}$. (Note that we mean $\exists x_1, \ldots, \exists x_m$ by $\exists\bar{x}$.)

A model $\mathcal{M}$ of an L-theory $\mathcal{T}$ is ***existentially closed among the models of*** $\mathcal{T}$ if every existential L_M-sentence which is satisfied in some model $\mathcal{N}$ of $\mathcal{T}$ extending $\mathcal{M}$ is already satisfied in $\mathcal{M}$ (indeed for each finite system of atomic formulas and negated atomic formulas with parameters $\bar{a} \in M$ if we can solve this system in an extension $\mathcal{N}$ of $\mathcal{M}$ then we can solve it in $\mathcal{M}$).

Proposition 2.5.13. *Let $\mathcal{K}$ be an elementary class of L-structures with the theory $\mathcal{T}$ then $\mathcal{T}$ is model complete if and only if every model of $\mathcal{T}$ is existentially closed.*

Proof. By [13] Theorem 5 and by [11] Proposition 2.16. □

Quantifier Elimination

Let $\mathcal{T}$ and $\mathcal{T}^*$ be two L-theories. We say that $\mathcal{T}^*$ is the ***model companion*** of $\mathcal{T}$ if the following holds:

- every model of $\mathcal{T}$ embeds in a model of $\mathcal{T}^*$,
- every model of $\mathcal{T}^*$ embeds in a model of $\mathcal{T}$.
- $\mathcal{T}^*$ is model complete.

If we have, in addition to the above properties, for any $\mathcal{A} \models \mathcal{T}$, $\mathcal{T}^* \cup Diag(\mathcal{A})$ is complete (or if $\mathcal{A} \models \mathcal{T}$, $\mathcal{M}, \mathcal{N} \models \mathcal{T}^*$, $\mathcal{A} \subseteq \mathcal{M}$ and $\mathcal{A} \subseteq \mathcal{N}$ then $\mathcal{M} \equiv_A \mathcal{N}$) then we say that $\mathcal{T}^*$ is the ***model completion*** of $\mathcal{T}$.

For example, the theory of algebraically closed fields is the model completion of the theory of integral domains.

Theorem 2.5.14. *Let $\mathcal{T}_0$, $\mathcal{T}_1$ be model companions of $\mathcal{T}$. Then $\mathcal{T}_0 = \mathcal{T}_1$.*

Proof. Given $\mathcal{A} \models \mathcal{T}_0$, we shall show that $\mathcal{A} \models \mathcal{T}_1$. We use an elementary chain argument. Let $\mathcal{A} = \mathcal{A}_0 \models \mathcal{T}_0$. By the definition of model completion, we can find $\mathcal{A}_1 \models \mathcal{T}_1$, $\mathcal{A}_0 \subseteq \mathcal{A}_1$. By generalizing this, given $\mathcal{A}_{2n} \models \mathcal{T}_0$ let $\mathcal{A}_{2n} \subseteq \mathcal{A}_{2n+1} \models \mathcal{T}_1$ and $\mathcal{A}_{2n+1} \subseteq \mathcal{A}_{2n+2} \models \mathcal{T}_0$. Put $\mathcal{A}' = \bigcup_{n\in\omega} \mathcal{A}_n$. Since $\mathcal{T}_0$ is model complete, we have $\mathcal{A}_{2n} \preccurlyeq \mathcal{A}_{2n+2}$ so by the elementary chain principle [11], $\mathcal{A} = \mathcal{A}_0 \preccurlyeq \mathcal{A}'$. But since $\mathcal{T}_1$ is model complete, we also have $\mathcal{A}_{2n+1} \preccurlyeq \mathcal{A}_{2n+3}$ so $\mathcal{A}' \models \mathcal{T}_1$. Hence $\mathcal{A} \models \mathcal{T}_1$. □

So we can conclude from the above theorem that if the model companion of a theory $\mathcal{T}$ is exists then it is unique.

As a general definition an L-theory $\mathcal{T}$ has ***quantifier elimination*** if for every formula $\varphi(\bar{x}) \in F_n(L)$ there is a quantifier free formula $\psi(\bar{x}) \in F_n(L)$ such that $\varphi(\bar{x})$ and $\psi(\bar{x})$ are equivalent in $\mathcal{T}$. Precisely:

$$\mathcal{T} \models \forall \bar{x}\ (\varphi(\bar{x}) \iff \psi(\bar{x}))$$

where $\forall \bar{x} = \forall x_1 \cdots \forall x_n$ and $\bar{x}, \varphi(\bar{x}), \psi(\bar{x})$ are as before.

Theorem 2.5.15. *Let L be a language containing at least one constant symbol c. Let $\mathcal{T}$ be an L- theory and let $\varphi(\bar{x})$ be an n-ary L- formula with free variables $\bar{x}$ (the case $n = 0$ allowed). Then the following are equivalent.*

1. *There is a quantifier free L-formula $\psi(\bar{x})$ such that:*

$$\mathcal{T} \models \forall(\bar{x})(\varphi(\bar{x}) \iff \psi(\bar{x}))$$

2. *If $\mathcal{M}, \mathcal{N}$ are models of $\mathcal{T}$, $\mathcal{A}$ is an L-structure, $\mathcal{A} \subseteq \mathcal{M}$ and $\mathcal{A} \subseteq \mathcal{N}$, then $\mathcal{M} \models \varphi(\bar{a})$ if and only if $\mathcal{N} \models \varphi(\bar{a})$ for all $\bar{a} \in \mathcal{A}$.*

Proof. See Theorem 3.1.4 of [15]. □

Lemma 2.5.16. *Let $\mathcal{T}$ be an L-theory. Suppose that for every quantifier free L formula $\theta(\bar{x}, w)$, there is a quantifier free $\psi(\bar{x})$ such that,*

$$\mathcal{T} \models \forall(\bar{x})\ (\exists w\ \theta(\bar{x}, w) \iff \psi(\bar{x})).$$

Then every L-formula $\varphi(\bar{x})$ is equivalent to a quantifier free L-formula.

Proof. We prove this by induction on the complexity of φ.

This is clear if $\varphi(\bar{x})$ is quantifier free.

For $i = 0, 1$ suppose that $\mathcal{T} \models \forall(\bar{x})\ (\theta_i(\bar{x}) \iff \psi_i(\bar{x}))$ where $\psi_i(\bar{x})$ is quantifier free.

If $\varphi(\bar{x}) = \neg\, \theta_0(\bar{x})$, then $\mathcal{T} \models \forall(\bar{x})\ (\varphi(\bar{x}) \iff \neg\, \psi_0(\bar{x}))$

If $\varphi(\bar{x}) = \theta_0(\bar{x}) \wedge \theta_0(\bar{x})$, then $\mathcal{T} \models \forall(\bar{x})\ (\varphi(\bar{x}) \iff \psi_0(\bar{x}) \wedge \psi_1(\bar{x}))$

In either case φ is equivalent to a quantifier free formula in $\mathcal{T}$.

Suppose that $\mathcal{T} \models \forall(\bar{x})\forall w\ (\theta(\bar{x}, w) \iff \psi_0(\bar{x}, w))$ where ψ_0 is quantifier free. Suppose $\varphi(\bar{x}) = \exists w\ \theta(\bar{x}, w)$. Then $\mathcal{T} \models \forall(\bar{x})\ (\varphi(\bar{x}) \iff \exists w\ \psi_0(\bar{x}, w))$.

But then by our assumptions there is a quantifier free $\psi(\bar{x})$ such that $\mathcal{T} \models \forall(\bar{x})(\varphi(\bar{x}) \iff \psi(\bar{x}))$. □

Thus to show that $\mathcal{T}$ has quantifier elimination we need only verify that condition (2) of Theorem 2.5.15 holds for every formula $\varphi(\bar{x})$ of the form $\exists w\, \theta(\bar{x}, w)$ where $\theta(\bar{x}, w)$ is quantifier free. Precisely:

Corollary 2.5.17. *Let $\mathcal{T}$ be an L-theory (in a language with at least one constant-symbol) has quantifier elimination if and only if $\mathcal{T} \cup Diag(A)$ is complete whenever $\mathcal{A} \models \mathcal{T}_\forall$. In particular, a theory with quantifier elimination is model-complete.*

Proof. By Theorem 2.5.15 and Lemma 2.5.16. □

Now we have a very useful proposition for quantifier elimination. Indeed we use this in the following chapters to prove the theory of algebraically closed fields admits elimination of quantifiers and the theory of generic difference fields is the model completion of the theory algebraically closed difference fields.

Proposition 2.5.18. *An L-theory $\mathcal{T}$ has quantifier elimination if and only if $\mathcal{T}$ is the model completion of a universal theory.*

Proof. ($\Rightarrow$) If $\mathcal{T}$ has quantifier elimination, then $\mathcal{T} \cup Diag(A)$ is complete whenever $\mathcal{A} \models \mathcal{T}_\forall$ by Corollary 2.5.17, so $\mathcal{T}$ is the model completion of $\mathcal{T}_\forall$ by definition.

($\Leftarrow$) If $\mathcal{T}^*$ is the model-companion of $\mathcal{U}$, then $\mathcal{T}_\forall = \mathcal{U}_\forall$, if also $\mathcal{U}$ is a universal theory then $\mathcal{T}_\forall = \mathcal{U}$; if $\mathcal{T}$ is the model-completion of $\mathcal{U}$, then by Corollary 2.5.17. □

Important Theorems and Some Remarks

In the following let $\mathcal{T}$ and $\mathcal{T}^*$ be the L-theories of the classes $\mathcal{K}$ and $\mathcal{K}^*$ of L-structures respectively.

Theorem 2.5.19. *$\mathcal{T}$ is model complete implies $\mathcal{T}$ has quantifier elimination down to existential formulas.*

Proof. Let $\theta(\bar{x})$ be an L-formula.

Define the set of $\exists$- formulas $\Gamma = \{\varphi \text{ an } \exists\text{-formula} : \mathcal{T} \models \varphi(\bar{x}) \Rightarrow \theta(\bar{x})\}$.

Suppose $\mathcal{M} \models \mathcal{T} \cup \{\theta(\bar{a})\}$ for some $\bar{a} \in M^n$. Then $\mathcal{T} \cup Diag(\mathcal{M}) \models \theta(\bar{a})$. By compactness $\mathcal{T} \cup \{\psi(\bar{a}, \bar{b})\} \models \theta(\bar{a})$ for some $\psi(\bar{a}, \bar{b}) \in Diag(\mathcal{M})$, and then

$$\mathcal{T} \models \exists \bar{y}\ \psi(\bar{x}, \bar{y}) \Rightarrow \theta(\bar{x}).$$

Let $\exists \bar{y}\ \psi(\bar{x}, \bar{y})$ be $\varphi(\bar{x})$; then $\varphi(\bar{x}) \in \Gamma$ and $\mathcal{M} \models \varphi(\bar{a})$. So $\mathcal{T} \models \theta(\bar{x}) \Rightarrow \bigvee \Gamma$. Therefore by compactness,

$$\mathcal{T} \models \varphi_1(\bar{x}) \wedge \cdots \wedge \varphi_n(\bar{x}) \iff \theta(\bar{x}) \text{ for some } \varphi_i \in \Gamma.$$

□

Remarks

Let $\mathcal{T} \subseteq \mathcal{T}^*$ and they have the same universal consequences. Then:

- If $\mathcal{T}^* \cup Diag(\mathcal{M})$ is complete whenever $\mathcal{M} \models \mathcal{T}^*$, then $\mathcal{T}^*$ is the model companion of $\mathcal{T}$ and $\mathcal{T}^*$ has quantifier elimination down to existential formulas.

- If $\mathcal{T}^*$ is the model companion of $\mathcal{T}$ and $\mathcal{T}^* \cup Diag(\mathcal{M})$ is complete whenever $\mathcal{M} \models \mathcal{T}$ then $\mathcal{T}^*$ is the model completion of $\mathcal{T}$.

- If $\mathcal{T} = \mathcal{T}^*{}_\forall$ and $\mathcal{T}^*$ is the model completion of $\mathcal{T}$ then $\mathcal{T}^*$ has full quantifier elimination.

We will give examples in the next chapters.

CHAPTER 3

ALGEBRAICALLY CLOSED FIELDS

3.1 Basic Algebraic Geometry

Varieties

Let M be an algebraically closed field. ***Affine n-space*** over M is the set of all n-tuples of elements of M, denoted by $A^n(M)$ or simply M^n. A subset X of M^n is an ***algebraic set*** defined over K where K is a subfield of M if there exists a subset S of the polynomial ring $K[\bar{X}]$ such that

$$X = V(S) = \{\bar{a} \in M^n : f(\bar{a}) = 0 \text{ for all } f \in S\}$$

where $\bar{a} = (a_1, \ldots, a_n)$, $a_i \in M$ and $\bar{X} = X_1, \ldots, X_n$.

The Zariski topology on M^n is constructed by letting algebraic sets be closed. [9]

$K[\bar{X}]$ is a Noetherian ring, therefore every ideal I has a finite set of generators (by Hilbert's Basis Theorem). If I is the ideal generated by S, then $V(S) = V(I)$. So there exists a finite set of polynomials such that we can express $V(S)$ as the common zeros of them.

Let X be an algebraic set, we define

$$I(X) = \{f \in K[\bar{X}] : f(\bar{a}) = 0, \forall \bar{a} \in X\}.$$

A Zariski closed subset X of M^n is ***irreducible*** if whenever $X = X_1 \cup X_2$ where X_1, X_2 are Zariski closed subsets of M^n, then $X = X_1$ or $X = X_2$.

A ***variety*** U of M^n is an irreducible Zariski closed set.

Remarks

Let U be a Zariski closed set of M^n. The ***Dimension*** of a variety U is the transcendence degree over K of the function field $K(U) = \{f(u)/g(u)$ where $f, g \in K[\bar{X}]\}$ (or simply $\text{trdeg}(K(U)/K)$) which is denoted by $\dim(U)$.

A ***generic point*** $\bar{a}$ of U over $K \subseteq M$ is a point in M^n such that $I(\bar{a}) = I(U)$.

An ***algebraic curve*** over a field K is an equation $f(X, Y) = 0$, where $f(X, Y)$ is a polynomial in indeterminate X and Y with coefficients in K. A solution of the equation $f(X, Y) = 0$ is a simply a point on this curve. A ***K-rational point*** of this curve is a solution (a, b) of this equation where $a, b \in K$.

Let $K \subseteq M_1, M_2$ be fields. M_1 and M_2 are ***algebraically independent*** over K, if for any $n \in \mathbb{N}$, whenever $a_1, \ldots, a_n \in M_1$ are algebraically independent over K, they remain algebraically independent over M_2.

Let $K \subseteq M_1, M_2$ be fields. M_1 and M_2 are ***linearly disjoint*** over K, if for any $n \in \mathbb{N}$, whenever $a_1, \ldots, a_n \in M_1$ are linearly independent over K, they remain linearly independent over M_2.

Tensor Product

Let M_1 and M_2 be linearly disjoint over K. Define $M_1 \otimes_K M_2$ as follows:

Let B_1 and B_2 be fixed bases of the K-vector spaces M_1 and M_2 respectively. Then $M_1 \otimes_K M_2$ has basis $\{a \otimes b : a \in B_1, b \in B_2\}$ as a K-vector space. Let $c \in M_1$ and $d \in M_2$ then we can write:

$$c = \sum_{i=1}^{n} c_a a \text{ and } d = \sum_{i=1}^{n} d_b b$$

where c_a's and d_b's are elements of K and all but finitely many of them are zero. Then we write an element $c \otimes d$ of $M_1 \otimes_K M_2$ as:

$$\sum_{a \in B_1, b \in B_2} c_a d_b (a \otimes b)$$

then since M_1 and M_2 are linearly disjoint over K, $M_1 \otimes_K M_2$ is a domain.

Also note that if K is an algebraically closed field, then M_1 and M_2 are ***algebraically independent*** over K if and only if they're linearly disjoint over K.

The ***prime subfield*** of a field M is the subfield of M generated by the multiplicative identity 1_M of M. It is isomorphic to either $\mathbb{Q}$ (if the characteristic is zero) or finite field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ (if the characteristic is p).

If r is a root of the polynomial equation

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0$$

where the a_i's are integers and r satisfies no similar equation of degree $< n$, then r is an ***algebraic number*** of degree n. If r is an algebraic number and $a_n = 1$, then it is called an ***algebraic integer***.

A ***separable polynomial*** with coefficients in K is a polynomial whose factors have distinct roots in some extension M of K.

M is a ***separable extention*** of a field K if the minimal polynomial of any element of M is a separable polynomial. In fact, in a field characteristic zero, every extension is separable, as is any finite extension of a finite field. If all algebraic extensions of a field K are separable, then K is called a ***perfect field***.

Note that the primitive element theorem says that a finite separable extension is generated by one element.

Theorem 3.1.1. *Let K have characteristic $p > 0$. Then K is perfect if and only if:*

$$K^p \equiv \{x^p : x \in K\} = K$$

3.2 The Model Theory of Algebraically Closed Fields

3.2.1 ACF

Any field M can be assumed as an L_r-structure $\mathcal{M}$. In Chapter I we saw that by adding the following infinite set of sentences into the theory of fields,

$$\forall a_0 \ldots \forall a_{n-1} \exists x \quad x^n + \sum_{i=0}^{n-1} a_i x^i = 0$$

for every positive integer n we get the first order axiomatization of the theory of algebraically closed fields.

Quantifier Elimination

Lemma 3.2.1. *ACF is the model completion of the theory of integral domains which is a universal theory.*

Proof. By definition of model completion we need to prove that $ACF \cup Diag(A)$ is complete whenever $A \models ACF_\forall$.

First note that the axioms for integral domains are universal consequences $ACF_\forall$ of ACF [15, p.85].

Let $M \models ACF$ and $D \subseteq M$ be an integral domain. Then D can be embedded in its field of fractions by $a \to a/1$ for $a \in D$. Since every field can be embedded in an algebraically closed field every model of the theory of integral domains can be embedded to a model of ACF.

For let D be an integral domain, A be its field of fractions. Let M_1 and M_2 be two algebraically closed fields extending A. Using Upward Löwenheim-Skolem theorem there are models M_1^* and M_2^* of ACF with the same cardinality κ and $\kappa > max(\aleph_0, |A|)$. By categoricity of ACF we have $M_1^* \cong M_2^*$ and therefore $M_1^* \equiv_A M_2^*$. □

Theorem 3.2.2. *ACF has quantifier elimination.*

Proof. By Proposition 2.5.18. □

Definable Sets

- The Zariski closed sets are definable.
- The finite boolean combinations (closure under finite intersection, finite union and complement) of the Zariski closed sets are definable. In fact they are exactly the sets definable by quantifier free formulas of L_r. Such sets are called constructible sets. By the property that ACF has quantifier elimination, the projection of a constructible set is also constructible. [15, p.88]

Completeness of ACF

Now we'll prove the following as we claimed in Chapter 2.

Theorem 3.2.3. *ACF_p is a complete theory.*

Proof. Since ACF_p is κ categorical by applying Vaught's test we need only to show ACF_p has only infinite models.

Fix $p \in \mathbb{N}$ and let $\mathcal{M} \models ACF_p$, assume $n = |M| < w_0$ and let

$$p(x) = 1 + \prod_{m \in M}(x - m);$$

then $p(x) = 1 \neq 0$ for every $m \in M$, so M is not algebraically closed. So ACF_p has only infinite models. □

Decidability of ACF

Theorem 3.2.4. *Lefschetz Principle*

- *If M and N are algebraically closed fields with the same characteristic p, then the L_r-structures $\mathcal{M}$ and $\mathcal{N}$ (with universes M and N) satisfy the same first order sentences of L_r.*
- *Suppose φ is an L_r-sentence, then TFAE*
  1. $\mathbb{C} \models \varphi$
  2. $ACF_0 \models \varphi$
  3. $ACF_p \models \varphi$ *for sufficiently large primes p*
  4. $ACF_p \models \varphi$ *for arbitrarily large primes p*

Proof. 1 and 2 are equivalent since ACF_0 is complete. $(2 \Rightarrow 3)$ Let $ACF_0 \models \varphi$, so φ is a logical consequences of the sentences in ACF_0. So only finitely many of the sentences $\neg\varphi_p$ are used, that is $ACF_p \models \varphi$ for sufficiently large primes p. $(3 \Rightarrow 4)$ is obvious.$(4 \Rightarrow 2)$ Suppose $ACF_0 \nvDash \varphi$. Then since ACF_0 is complete we have $ACF_0 \models \neg\varphi$. So $ACF_p \models \neg\varphi$ for sufficiently large primes p and (4) fails. □

The Lefschetz Principle has the following consequence.

Theorem 3.2.5. *(Ax) Let $n \in \mathbb{N}$, and let $F : \mathbb{C}^n \to \mathbb{C}^n$ be an injective polynomial map. Then F is surjective.*

Proof. Let $\varphi_{n,d}$ be the L_r-sentence which states that every injective polynomial $F = (f_1, \ldots, f_n)$ map of n variables and degree at most d is surjective. It suffices to show that $\mathbb{C} \models \varphi_{n,d}$ for all n, d.

Let M be a finite field: then $M \models \varphi_{n,d}$ for all n, d. The algebraic closure $\overline{M}$ of M is of the form $\overline{M} = M_0 \cup M_1 \cup M_2 \cup \cdots$, where $M_0 \subseteq M_1 \subseteq M_2 \subseteq \cdots$ are finite fields. Thus if $F : \overline{M}^n \to \overline{M}^n$ is an injective polynomial map a standard chain theorem tells us that F must be surjective as well. So $\overline{M} \models \varphi_{n,d}$ for all n, d. By completeness of ACF_p, we get $ACF_p \models \varphi_{n,d}$ for all n, p, d. Then by Theorem 2.2.6, we get $\mathbb{C} \models \varphi_{n,d}$ for all n, d. □

By Proposition 2.5.10, any recursively axiomatized complete theory is decidable, and since ACF_p is a recursively axiomatized complete theory, therefore it is decidable for p prime or 0. Indeed by the completeness of ACF_p and the completeness theorem either there is a proof of φ or a proof of $\neg\varphi$ from ACF_p. We can then search in a systematic way all finite sequences of symbols and test each one to see if it is a valid proof of either φ or $\neg\varphi$. At the end we'll get one of them.

Also ACF is decidable. Indeed, given a sentence φ, we can find N such that either φ or $\neg\varphi$ is a consequence of

$$ACF \cup \{\varphi_p : \ p < N\}.$$

(By the Lefchetz Principle and completeness of ACF_0, such N exists.)

Without loss of generality suppose that $ACF \cup \{\varphi_p : \ p < N\} \models \sigma$. Then $ACF \models \sigma$ if and only if $ACF_p \models \sigma$ whenever $p \leq N$; and we can determine whether the latter condition holds.

Since if we can't find a proof of φ from ACF, we can find a proof of $\neg\varphi$ from ACF_p for some p since for all p prime ACF_p is decidable.

CHAPTER 4

GENERIC DIFFERENCE FIELDS

In this chapter I'll study the theory of difference fields.

The first section deals with algebraic background which can be useful for us to understand some basics about difference fields. The details and proofs of this section can be found in [7].

Section 2 deals with the model companion of difference fields: the theory of so called generic difference fields. I started studying this subject with the paper of Angus Macintyre, *Generic Automorphisms of Fields* [12]. It has an advanced level of presentation of ideas. I found the papers of Zoé Chatzidakis, *A survey on the model theory of difference fields* [5] and *The Model Theory Of Difference Fields* [4] more explicit for me to understand the concept of generic difference fields. The paper of David Marker, $ACFA$ Seminar [16] also helps.

For further reading I advise [4] since it can be considered as a complete reference for all of the theory of difference fields.

4.1 Algebraic Background

Field Automorphism

A field automorphism fixes the prime field say K which is $\mathbb{Q}$, the rational numbers, in the case of field characteristic zero and is $\mathbb{F}_p$ in characteristic

$p > 0$. The set of automorphisms of a field M which fix a subfield K of M forms a group, by composition, called the ***Galois group***, written $Gal(M/K)$.

A ***difference field*** $\mathcal{M}$ is a field M with a distinguished automorphism σ.

Let $\bar{X} = X_1, \ldots, X_n$ be an n-tuple of indeterminates; then $M[\bar{X}]_\sigma$ is the difference polynomial ring in indeterminates:

$$X_1, \ldots, X_n, \sigma(X_1), \ldots, \sigma(X_n), \ldots, \sigma^m(X_1), \ldots, \sigma^m(X_n) \ldots.$$

Let $L_d = L_r \cup \{\sigma\}$, then $\mathcal{M}[\bar{X}]_\sigma$ can be considered as an L_d-structure. The elements $p(\bar{x})$ of the universe $M[\bar{X}]_\sigma$ of $\mathcal{M}[\bar{X}]_\sigma$ are called difference polynomials, and $p(\bar{x}) = 0$ is called a ***σ-equation***. The set $\{\bar{a} \in M^n : p(\bar{x}) = 0\}$ is called a ***σ-closed*** set. The ***order of*** $p(\bar{x})$ is the largest m such that some $\sigma^m(x_j)$ appears in $p(\bar{x})$.

Let M be an algebraically closed field, and let U be a variety over M defined by polynomial equations:

$$p_1(\bar{x}) = \cdots = p_k(\bar{x}) = 0.$$

Then $\sigma(U)$ is also a variety of over M defined by equations:

$$\sigma(p_1)(\bar{y}) = \ldots = \sigma(p_k)(\bar{y}) = 0$$

where $\sigma(x_i) = y_i$.

We can then form $U \times \sigma(U)$ as a variety over M by:

$$p_1(\bar{x}) = \cdots = p_k(\bar{x}) = 0$$
$$\sigma(p_1)(\bar{y}) = \ldots = \sigma(p_k)(\bar{y}) = 0.$$

Take a variety $W \subseteq U \times \sigma(U)$. The natural projection maps are:

$$\pi_1 : U \times \sigma(U) \to U \text{ and } \pi_2 : U \times \sigma(U) \to \sigma(U).$$

Let $(\bar{a}, \bar{b})$ be any generic point of W. If $\bar{a}$ is a generic point of U and $\bar{b}$ is a generic point of $\sigma(U)$ then we say that W ***projects generically onto*** U and $\sigma(U)$.

Basic Systems

Example 4.1.1. *Let (M, σ) be a difference field and let $f(\bar{x}) \in M[\bar{X}]_\sigma$. Assume that the degree of $f(\bar{x})$ is 2. Then*

$$f(\bar{x}) = f(x_1, \ldots, x_n, \sigma(x_1), \ldots, \sigma(x_n), \sigma^2(x_1), \ldots, \sigma^2(x_n)).$$

By letting $\sigma(x_1) = y_1, \ldots, \sigma(x_n) = y_n$ we can rewrite $f(\bar{x})$ as

$$f(x_1, \ldots, x_n, y_1, \ldots, y_n, \sigma(y_1), \ldots, \sigma(y_n)).$$

Therefore if one wants to know about solutions of the set of polynomial equations and inequations in

$$x_1, \ldots, x_n, \sigma(x_1), \ldots, \sigma(x_n), \sigma^2(x_1), \ldots, \sigma^2(x_n), \ldots,$$

the example shows that by adding extra variables this comes down to understanding polynomial systems which have polynomial equations and inequations in

$$x_1, \ldots, x_m, \sigma(x_1), \ldots, \sigma(x_m).$$

We will consider just σ-equations since by the help of the field axiom

$$\forall x \; x \neq 0 \iff \exists y \; x \cdot y = 1$$

we can replace inequations by equations in more variables.

We called these systems ***basic systems***. Precisely, the order of each difference polynomial equation occurring in a basic system equals at most 1.

Proposition 4.1.2. *A difference field (M,σ) is existentially closed (e.c) if whenever a basic system of (M,σ) is solvable in an extension $(M^{'},\sigma^{'})$ of (M,σ) then it is solvable in (M,σ).*

Proof. Let Σ be basic system of (M,σ) which has a solution in $(M^{'},\sigma^{'}) \supseteq (M,\sigma)$ where (M,σ) is e.c..

Since Σ is a basic system then we can write it as $\bigwedge_{\varphi} \varphi(\bar{x})$ where φ are atomic formulas over (M,σ). Since Σ has a solution in $(M^{'},\sigma^{'})$ then $(M^{'},\sigma^{'}) \models \exists \bar{x} \bigwedge_{\varphi} \varphi(\bar{x})$ so $(M,\sigma) \models \exists \bar{x} \bigwedge_{\varphi} \varphi(\bar{x})$ since (M,σ) is e.c..

For the other direction any $\exists$-formula can be written $\bigvee_{\psi} \psi$ where ψ are of the form $\exists \bar{x} \bigwedge_{\varphi} \varphi(\bar{x})$ and φ are atomic or negated atomic formulas. If $\varphi(\bar{x}) : f(\bar{x}) \neq g(\bar{x})$ by using $\exists \bar{x}\ \exists y \bigwedge y \cdot (f(\bar{x}) - g(\bar{x})) = 1$ and by adding extra variables as in the Example 4.1.1 we get a basic system over (M,σ). Then by assumption (M,σ) is e.c.. □

If no confusion arises throughout this chapter I'll use:

$$\bar{x} = (x_1, \ldots, x_n)$$
$$\sigma^n(\bar{x}) = (\sigma^n(x_1), \ldots, \sigma^n(x_n)).$$

4.2 Generic Automorphism of Fields

A difference field (M,σ) is called a ***generic difference field*** if (M,σ) is existentially closed among the models of the theory of difference fields.

Lemma 4.2.1. *There is a first order theory whose models (M,σ) are characterized by the following:*

1. *M is an algebraically closed field.*

2. *σ is an automorphism of M.*

3. *(By Hrushovski) If U and W are varieties defined over M, with $W \subseteq U \times \sigma(U)$ such that the projections W to U and to $\sigma(U)$ are generically onto, then there is a tuple $\bar{a}$ in M such that $(\bar{a}, \sigma(\bar{a})) \in W$.*

Proof. Clearly 1 and 2 are first order. But it is hard to see this for 3. We know that if U is a variety then $I(U)$ is an ideal. Let $I(U) = I$ which is in $M[\bar{X}]$ and $I(W) = J$ which is in $M[\bar{X}, \bar{Y}]$. Then the dual of the projection map gives a map $M[\bar{X}]/I \to M[\bar{X}, \bar{Y}]/J$, which is injective if and only if W projects generically onto U. So we need to say $J \cap M[\bar{X}] = I$ in a first order way [8].

So the third axiom is in fact the scheme of axioms: one for each triple (n, m, d) where

- n is an upper bound on the number of variables of U,
- m is an upper bound on the number of the polynomials used to define U and W,
- d is an upper bound on the degree of these polynomials.

□

The theory in Lemma 4.2.1 is called $ACFA$.

Theorem 4.2.2. *The models of $ACFA$ are exactly the generic difference fields.*

Proof. Let $(M, \sigma) \models ACFA$, and let $f_1(\bar{X}) = 0, \ldots, f_m(\bar{X}) = 0$ be a basic system of σ-equations over M. Let $(a_1, \ldots, a_n, \sigma(a_1), \ldots, \sigma(a_n))$ be a solution of this system in an extension field (L, σ') of (M, σ). Let U, W be varieties over M with generic points $(a_1 \ldots, a_n)$ of U and $(a_1, \ldots, a_n, \sigma(a_1), \ldots, \sigma(a_n))$ of W. Then $(\sigma(a_1), \ldots, \sigma(a_n))$ is a generic of $\sigma(U)$. By 3 in Lemma 4.2.1 there is $(b_1, \ldots, b_n, \sigma(b_1), \ldots, \sigma(b_n)) \in W$ with $b_i \in M$, $i = 1, \ldots, n$. Then

$$I(b_1, \ldots, b_n, \sigma(b_1), \ldots, \sigma(b_n)) \supseteq I(a_1, \ldots, a_n, \sigma(a_1), \ldots, \sigma(a_n))$$

over M and therefore $(b_1, \ldots, b_n, \sigma(b_1), \ldots, \sigma(b_n))$ is a solution of the system in M.

Conversely, let (M, σ) be a difference field which is generic. Then we need to show $(M, \sigma) \models ACFA$. Clearly M is algebraically closed. Let U and $\sigma(U)$ be varieties over M. Then $W \subseteq U \times \sigma(U)$ has a generic point $(\bar{\alpha}, \bar{\beta})$ of W in some extension $M^{'}$ of M. Assume that $\bar{\alpha}$ is a generic point of U and $\bar{\beta}$ is a generic point of $\sigma(U)$. Define,

$$\sigma^1 : M(\bar{\alpha}) \to M(\bar{\beta})$$

by $\sigma^1(\alpha_i) = \beta_i$ and acts as σ over M. So we can extend σ^1 to an automorphism $\sigma^{'}$ of $M^{'}$ hence we get

$$(\bar{\alpha}, \sigma^{'}(\bar{\alpha})) \in W.$$

Since (M, σ) is generic, we get some $(\bar{\gamma}, \sigma(\bar{\gamma})) \in W$ where $\bar{\gamma}$ in M. □

As a result of this theorem and by Proposition 2.5.12 we conclude that $ACFA$ is model complete and hence the model companion of the theory of difference fields. Therefore the following theorem holds immediately by the first property of being the model companion of a theory.

Theorem 4.2.3. *Every difference field embeds in a model of $ACFA$.*

Proposition 4.2.4. *Suppose (M_i, σ_i) $(i = 1, 2)$ are extensions of an algebraically closed (K, σ). Then they can be jointly embedded in some $(L, \sigma^{'})$.*

Proof. Let $h : M_2 \to M_2^{'}$ be a K isomorphism, and let $\sigma_2^{'} = h\sigma_2, h^{-1}$ where $M_2^{'}$ is free from M_1 over K. Since K is algebraically closed, $M_2^{'}$ and M_1 are linearly disjoint over K. Since (M_2, σ_2) and $(M_2^{'}, \sigma_2^{'})$ are K-isomorphic under h, they're elementarily equivalent over K.

Hence by replacing M_2 by M_2', we may assume that M_1 and M_2 are linearly disjoint over K. Then by algebraic properties $M_1 \otimes_K M_2$ is a domain and we can embed M_1 and M_2 in $M_1 \otimes_K M_2$ by

$$a \to a \otimes 1 \text{ and } b \to 1 \otimes b.$$

Define a new $\sigma(a \otimes b) = \sigma_1(a) \otimes \sigma_2(b)$ for $a \in M_1$ and $b \in M_2$. So σ extends to an automorphism σ' of the quotient field L of $M_1 \otimes_K M_2$, which agrees with each σ_i on M_i. □

Proposition 4.2.5. *If (M_i, σ_i) $(i = 1, 2)$ are generic and the σ_i's agree on the algebraic closure of the prime field then $(M_1, \sigma_1) \equiv (M_2, \sigma_2)$.*

Proof. By Proposition 4.2.4, the (M_i, σ_i) can be jointly embedded in some (L, σ). But then by Theorem 4.2.3 (L, σ) can be embedded in an e.c. (L', σ'). By model completeness: $(M_1, \sigma_1) \preccurlyeq (L', \sigma')$ and $(M_2, \sigma_2) \preccurlyeq (L', \sigma')$ which implies that $(M_1, \sigma_1) \equiv (M_2, \sigma_2)$. □

Similarly, by Proposition 4.2.4 we can conclude that the sentences satisfied by a tuple $\langle a_1, \ldots, a_n \rangle$ in a generic (M, σ) are determined by the algebraic closure of the smallest field which contains the tuple and closed under σ and σ^{-1}. Let A be a subset of the field M. We'll denote the smallest subfield of M containing A and closed under σ, σ^{-1} by $\langle A \rangle_\sigma$.

Lemma 4.2.6. *Let (M, σ) be a difference field, M_0 be the prime field of M and $A \subseteq M$. Then*

$$\langle A \rangle_\sigma = M_0(A, \sigma(A), \sigma^{-1}(A), \ldots)$$

Proof. Clear. □

Lemma 4.2.7. *Let B be the relative algebraic closure of $\langle A \rangle_\sigma$ in M. Then $\langle B \rangle_\sigma = B$.*

Proof. Let $b \in B$. Then there exist an F in

$$\mathbb{Z}[\bar{x}_0, \bar{x}_1, \bar{y}_1, \bar{x}_2, \ldots, \bar{y}_m, t]$$

such that:

$$F(a_1, \ldots, a_n, \ldots, \sigma^m(a_1), \ldots, \sigma^{-m}(a_1), \ldots, \sigma^{-m}(a_n), b) = 0$$

where $a_1, \ldots, a_n \in A$; but then,

$$F(\sigma(a_1), \ldots, \sigma(a_n), \ldots, \sigma^{m+1}(a_1), \ldots, \sigma^{-m+1}(a_1), \ldots, \sigma^{-m+1}(a_n), \sigma(b)) = 0$$

therefore $\sigma(b) \in B$. □

Lemma 4.2.8. *Let M be an algebraically closed difference field. Then $ACFA \cup Diag(M)$ is complete.*

Proof. Let $K_1, K_2 \models ACFA \cup Diag(M)$. Then $K_1, K_2 \models Diag(M)$ implies that K_1, K_2 contain substructures M_1 and M_2 respectively such that $M_1 \cong M$ and $M_2 \cong M$. So we may assume that both K_1 and K_2 contain M. Then the proof of Proposition 4.2.5 can be adjusted to show that we will get $K_1 \equiv K_2$ over M. □

Lemma 4.2.8 shows that $ACFA$ is the model completion of the theory of algebraically closed difference fields, which is not a universal theory. $ACFA$ doesn't admit quantifier elimination in L_d. For an example see [6, pg.23].

Quantifier Elimination

Let $\mathcal{T} = \text{Th}\{\text{difference fields}\}$, $(N, \sigma) \models \mathcal{T}$ and $\bar{a} \in N^n$. Let $(K, \sigma) = \langle \bar{a} \rangle_\sigma$ and let the algebraic closure of K in N be M ($K \subseteq M \subseteq N$).

Let $\Gamma = \{\theta(\bar{a}, b) \in \ Diag(M, \sigma)\}$ (i.e. the formulas in $Diag(M, \sigma)$ which has just one constant from $M \setminus K$ and the others are from K).

Note that Γ contains the following information about (M, σ):

1. that M is algebraically closed,

2. the characteristic of M,

3. surjectivity of σ on M.

The paper [12] has more complicated version of Γ which we will use proving the quantifier elimination in $ACFA$. In fact he gives more explicit definition of the formulas in Γ and he uses them proving the decidability of $ACFA$.

Theorem 4.2.9. *Every formula $\theta(\bar{x})$ in the language of difference fields is equivalent to a disjunction of formulas of the form $\exists y\, \varphi(\bar{x}, y)$ in the theory of generic difference fields.*

Proof. Claim: $T_\forall \cup \Gamma \models Diag(M, \sigma)$.

Let $(N', \sigma') \models T_\forall \cup \Gamma$ then there is an interpretation of elements of M into N'. i.e. let $b \in M$ then $b^{N'} = b'$ for some $b' \in N'$. Since $Diag(K, \sigma) \subseteq \Gamma$ we may assume that if $b \in K$, then $b^{N'} = b$. Then if $\operatorname{char} K = 0$ clearly $(K, \sigma) \cong (K, \sigma')$, but if $\operatorname{char} K = p$ go to $K^{p^{-\infty}}$. We need to check that σ extends uniquely to the perfect closure $K^{p^{-\infty}} = \bigcup_n K^{p^{-n}}$ say L of K. Let σ' satisfy $\sigma' \mid_K = \sigma$. If $\alpha \in L$, then $\alpha^{p^n} \in K$ for some minimal n; say $\alpha^{p^n} = \beta$. Then

$$\sigma(\beta) = \sigma(\alpha^{p^n}) = \sigma'(\alpha)^{p^n},$$

so $\sigma'(\alpha) = \sigma(\beta)^{p^{-n}}$.

Thus σ' is unique if it exists. It also exists, since on $K^{p^{-n}}$ the map

$$\alpha \mapsto \sigma(\alpha^{p^n})^{p^{-n}}$$

is $\tau^{-1} \circ \sigma \circ \tau$, where τ is the Frobenius isomorphism

$$\beta \mapsto \beta^{p^n} : K^{p^{-n}} \to K.$$

Since $(N^{'}, \sigma^{'}) \models \Gamma$, we have $(N^{'}, \sigma^{'}) \models Diag(\langle \bar{a}, b\rangle_{\sigma}, \sigma)$ for every $b \in M$; hence there is a substructure $(\langle \bar{a}, b^{'}\rangle_{\sigma'}, \sigma^{'})$ of $(N^{'}, \sigma^{'})$ such that:

$$(\langle \bar{a}, b\rangle_{\sigma}, \sigma) \cong \langle \bar{a}, b^{'}\rangle_{\sigma'}, \sigma^{'}).$$

Let $\theta(\bar{c}) \in Diag(M, \sigma)$. I need to show $(N^{'}, \sigma^{'}) \models \theta(\bar{c}^{'})$. But it's enough to show there is $b \in M$ such that $\langle \bar{a}, \bar{c}\rangle_{\sigma} \subseteq \langle \bar{a}, b\rangle_{\sigma}$. In fact its the same as to show $K(\bar{c}) \subseteq K(b)$. If $\operatorname{char} K = 0$ then K is perfect and if $\operatorname{char} K = p$ then by replacing K with its perfect closure we can use primitive element theorem to conclude there is such $b \in M$ that $K(\bar{c}) \subseteq K(b)$.

Then by the arguments on the proof of Theorem 2.5.19

$$ACFA \models \forall \bar{x}(\theta(\bar{x}) \iff \bigvee \exists y \wedge_{\varphi} \varphi(\bar{x}, y)).$$

□

Completeness of $ACFA$

$ACFA$ is not a complete theory since it doesn't decide the characteristic.

Proposition 4.2.10. *Every completion of $ACFA$ is of the form $ACFA \cup \Sigma$ where Σ is $\{\exists x\ \theta(x) :\ \theta(b) \in \Gamma$ for some $b \in \mathbb{F}^{alg}\}$ and $\mathbb{F}$ is the prime field.*

Proof. Let $(M, \sigma) \models ACFA$ with the prime subfield $\mathbb{F}$ of the field M. By Lemma 4.2.8, $ACFA \cup Diag(\mathbb{F}^{alg}, \sigma)$ is a complete theory but also by the proof of Theorem 4.2.9 $ACFA \cup \Gamma$ is also complete where $\Gamma = \{\theta(b) \in Diag(\mathbb{F}^{alg}, \sigma)\}$.

So $Th(M, \sigma)$ of (M, σ) is in fact $ACFA \cup \{\exists x\ \theta(x) : \theta(b) \in \Gamma$ for some $b \in \mathbb{F}^{alg}\}$ hence $ACFA \cup \Sigma$ is complete. □

Decidability

Let $ACFA_0^{\sigma} = ACFA \cup \{\exists x\ \theta(x) :\ \theta(b) \in \Gamma, b \in \mathbb{Q}^{alg}\}$ where $\Gamma = \{\theta(b) \in Diag(\mathbb{Q}^{alg}, \sigma)\}$, take an L_d-sentence ψ then by Theorem 4.2.9 it is equivalent

to sentence $\exists x \wedge_{\varphi} \varphi(x)$ modulo $ACFA$ where $\varphi(x)$ are atomic and over $\mathbb{Q}$. So the decision problem reduces to looking at the sentences of the form $\exists x\ \varphi(x)$.

One can show by using the same argument as proving Theorem 4.2.9 that in fact $\varphi(x)$ is a Boolean combination of sentences $\exists t\ [f_i(t) = 0 \wedge \sigma(rt) = h_i(t)]$ [12]. Where f and h are polynomials over $\mathbb{Z}$. Let L be the splitting field of f_i's, then by primitive element theorem $L = \mathbb{Q}(\beta)$ for some $\beta \in \mathbb{Q}^{alg}$. The action of σ on L is determined by choice of conjugate of β which is among some $F_1(\beta), \ldots, F_k(\beta)$. And since the roots of f_i are among $H_{ij}(\beta)$ then we can determine the action of σ on all roots of f_i. By this way we can find the automorphisms which satisfy φ.

4.3 The Fixed Field of σ

The fixed field is a particulary important definable subset of a model (M, σ) of $ACFA$. I'll show in this section that $Fix(\sigma) = \{x \in M : \sigma(x) = x\}$ is a ***pseudo-finite field***, i.e. an infinite model of the theory of finite fields. The model theory of finite fields is first studied by Ax, see for details [1].

We denote the theory of finite fields by $\mathcal{T}_f$ in the language L_r.

Let M be a field. M is pseudo-algebraically closed (PAC) if every variety defined over M has an M-rational point.

Pseudo-finite fields

Let Psf be the theory [21] whose models are axiomatized by the following:

1. F is a perfect field.
2. F has exactly one algebraic extension of degree n, for each $n \in \mathbb{N}$.
3. F is PAC.

Then Psf is in fact $T_f \cup \{$ models are infinite $\}$.

Theorem 4.3.1. *Let M be a model of $ACFA$ and let $F = Fix(\sigma)$. Then F is a pseudo-finite field.*

Proof. If F has characteristic $p > 0$ then a has a unique p^{th} root $a^{1/p}$ in F. Hence $\sigma(a) = a$ implies $\sigma(a^{1/p}) = a^{1/p}$. Therefore $Fix(\sigma)$ is closed under p^{th} roots thus perfect.

For item 3: Let U be a variety defined over F, and consider the diagonal subvariety $W \subseteq U \times U$. Then $U = \sigma(U)$, and U, W satisfy the axiom 3 of $ACFA$, so that there is $\bar{a} \in M$ with $(\bar{a}, \sigma(\bar{a})) \in W$ (i.e. $\bar{a} \in U$ and $\sigma(\bar{a}) = \bar{a}$ and hence $\bar{a} \in F$). So $Fix(\sigma)$ is PAC.

Assume that L and $L^{'}$ are two normal algebraic extensions of F of degree n. Since F is perfect, actually $L, L^{'}$ are Galois extensions of F. By Galois theory $Gal(LL^{'}/F)$ has subgroups $Gal(LL^{'}/L)$ and $Gal(LL^{'}/L^{'})$ of order say $d = [LL^{'} : F]/n$. But since F is fixed by the group generated by $\sigma \mid_{LL^{'}} \in Gal(LL^{'}/F)$ which is cyclic, it has only one subgroup of order d.

So in order to prove 2 it is enough to show that for each n, F has at least one Galois extension of degree n and all extensions of degree n are normal.

Since every algebraic extension of degree n of F is contained in a finite Galois extension of F and all subgroups of a cyclic group is normal, all extensions of degree n of F are normal.

Consider the difference field extension $L = M(X_1, \ldots, X_n)$ of M with $\sigma(X_i) = X_{i+1}$ for $i = 1, \ldots, n-1$, and $\sigma(X_n) = X_1$. Then

$$L \models \exists x \; \sigma^n(x) = x \wedge \bigwedge_{1 \leq i < n} \sigma^i(x) \neq x,$$

so that M satisfies the same sentence. Let $a \in M$ be such that $\sigma^n(a) = a$, $\sigma^i(a) \neq a$ for $1 \leq i < n$. So $F(a)$ is a Galois extension of F degree n over F. $\square$

REFERENCES

[1] J. Ax, *The theory of finite fields*, Ann. Math. 88 [1968] 239- 271.

[2] J. Barwise, *An Introduction to First Order Logic*, Handbook of Mathematical Logic, Part A, North Holland Publishing Company, New York, [1977].

[3] C. C. Chang, H. J. Keisler, *Model Theory*, Third ed., Studies in Logic and the Foundations of Math. 73, North Holland, Amsterdam, [1990].

[4] Zoé Chatzidakis, E. Hrushovski *Model Theory of Difference Fields*, pp.2997-3071 in Math. Ams. 351, New York, [1999].

[5] Zoé Chatzidakis,"A survey on the model theory of difference fields", pp.65-96 in *Model Theory, algebra and geometry* Math. Sci. Res. Inst. Publ. 39, New York, [2000].

[6] Zoé Chatzidakis, *Model Theory of Difference Fields*, Lecture Notes, Notre Dame, Sep [2000].

[7] R. M. Cohn, *Difference Algebra*, Tracts in Mathematics 17, Math., Interscience Pub, [1965].

[8] L. Van Den Dries, K. Schmidt *Bounds in the theory of polynomial rings over fields*, A nonstandard approach. Invent. Math.76, no. 1, 77- 91, [1984].

[9] R. Hartshorne, *Algebraic Geometry*, Springer- Verlag, New York, [1977].

[10] W. Hodeges, *Model Theory*, Cambridge University Press, [1993].

[11] H. J. Keisler, *Fundamantals of Model Theory*,Handbook of Mathematical Logic, Part A, North Holland Publishing Company, New York, [1977].

[12] A. Macintyre, *Generic automorphisms of fields*, Annals of Pure and Applied Logic. Math. 88, 165-180, [1977] .

[13] A. Macintyre, *Model-Completeness*, Handbook of Mathematical Logic, Part A, North Holland Publishing Company, New York, [1977].

[14] A Macintyre, "MSRI/ Evans Hall Lectures, Berkeley", [1998].

[15] D. Marker, *Model Theory: An Introduction*, Springer, New York [2002].

[16] D. Marker, *"ACFA Seminar"*, University of Ilinois, Chicago Fall [1997].

[17] A. Robinson, *Complete Theories*, North Holland Publishing Company, New York, [1956].

[18] G. E. Sacks, *Saturated Model Theory*, Math. Lecture Note Series W. A. , MA, [1972].

[19] L. Serge, *Introduction to Algebraic Geometry*, Math. New York, Interscience Publishers [1958].

[20] S. G. Simpson, Math: 563 *Model Theory*, www.math.psu.edu/simpson /courses/math563, [1998].

[21] J. Väänänen,"Pseudo-finite model theory", www.math.helsinki.fi/logic /people /jouko.vaananen/ qf-final.pdf November 12, [2001].