# Model Theory of Algebraically Closed Fields and The Ax-Grothendieck Theorem

Ahmed Osama Mohamed Sayed Sayed Elmwafy (ahmedelmwafy@aims.ac.za)
African Institute for Mathematical Sciences (AIMS)

Supervised by:
Dr. Gareth Boxall
University of Stellenbosch, South Africa
Dr. Charlotte Kestner
Imperial College London, United Kingdom

14 May 2020

*Submitted in partial fulfillment of a structured masters degree at AIMS South Africa*



# Abstract

We introduce the concept of an algebraically closed field with emphasis of the basic model-theoretic results concerning the theory of algebraically closed fields. One of these nice results about algebraically closed fields is the quantifier elimination property. We also show that the theory of algebraically closed field with a given characteristic is complete and model-complete. Finally, we introduce the beautiful Ax-Grothendieck theorem and an application to it.

**Keywords:** Model, Structure, Quantifier Elimination, Complete, Model-complete, Ax-Grothendieck theorem.



## Declaration

I, the undersigned, hereby declare that the work contained in this research project is my original work, and that any work done by others or by myself previously has been acknowledged and referenced accordingly.

Ahmed Osama Mohamed Sayed Sayed Elmwafy, 14 May 2020

# Contents

# 1. Introduction

Model theory explores the duality between any language of the mathematical objects and its meaning. Theorems of model theory connect theories, that are a collection of sentences, and models, which are mathematical structures that satisfy those sentences. This duality in model theory is similar to the duality in algebra, one between formal and symbolic structures in model parallel with polynomials and algebraic structures such as algebraically closed fields in algebra.

The shared history of model theory and algebra extends back to the first half of the 20th century when logicians started to understand that model theory was remarkably able to handle the algebraic structures. From that day forward, the algebraic model-theoretic has got its own name by verifying more algebraic results. In the middle of the 20th century, Alfred Taraski [Marker et al.] led the study of fields from a model-theoretic aspects. He developed the method of quantifier elimination. Quantifier elimination is a powerful tool in the model-theoretic investigation of the algebraic structures. A theory is said to have the quantifier elimination property if every formula is equivalent to a formula with no quantifiers. We will introduce a useful test for quantifier elimination as a result of the back and forth method which was developed in the fifties and sixties by Ronald Fraïssé [Tent and Ziegler]. We study the concept of completeness which states that a theory is complete if it proves every sentence or its negation. We simplify a test for verifying whether a theory is complete or not, this test depends on checking if any two models of the theory are elementarily equivalent, then the theory is complete. Last but not least in this part, we give the proof of model-completeness as a consequence of quantifier elimination, a theory is model complete if every embedding of one model in another is an elementary embedding. We introduce a simple model-theoretic proof of the Ax-Grothendieck theorem via a transfer principle, We use the principle of Lefschetz, which allows the transfer of true sentences in algebraically closed fields of infinitely many prime characteristics to algebraically closed fields of characteristic $0$.

The thesis consists of three main parts. Firstly, we give a fully detailed introduction of the fundamental algebraic concepts that needed in studying the structure of algebraically closed fields. Secondly, we introduce the basic concepts of model theory. Model theory is a powerful tool in mathematical logic used in studying the mathematical structures. Then we give a suitable language of the algebraically closed fields and study some important keys in model theory such as quantifier elimination, completeness, and model completeness. Last but not least, we introduce the beautiful Ax-Grothendieck theorem and an application to it in other areas of science.

In Chapter 2, we start by introducing all the necessary algebraic concepts needed to study the algebraically closed fields (ACF) which have an important property which states that every non-constant polynomial in its polynomial ring has a root in it. We show the existence of algebraically closed field extension for every field and show that it is necessary to be an infinite set. Moreover, we expose the property that any two transcendental bases of an algebraically closed field have the same cardinality. Finally, if $K_1$ and $K_2$ are two algebraically closed field extensions of $F_1$ and $F_2$ respectively, with the property that $tr.deg(K_1/F_1) = tr.deg(K_2/F_2)$, then every isomorphism of fields between $F_1$ and $F_2$ extends to an isomorphism between their algebraically closed fields $K_1$ and $K_2$.

In Chapter 3, we give in detail all the basic notation of model theory which is necessary for the following chapters. Model theory is the first theory studies mathematical objects as a language and expressing the mathematical objects as a structure and give every structure a suitable language. Model theory studies the duality between languages and interpretations. Theorems in model theory relate theories, which expressed as a set of first-order sentences, and models are mathematical objects for which those sentences are true.

In Chapter 4, we start by introducing a suitable language for the algebraically closed fields, and some model-theoretic properties of algebraically closed fields as quantifier elimination, model-completeness and completeness of algebraically closed fields with a given characteristic are proven.

In Chapter 5, we give a brief introduction about the Ax-Grothendieck theorem which states that every injective polynomial map $f : \mathbb{C}^n \to \mathbb{C}^n$ is bijective. The idea of the proof depends on the fact that every injective self map of finite sets is bijective. We prove algebraically that every self injective polynomial map of the algebraic closure of a finite field $K$ is bijective. Then we prove the Ax-Grothendieck theorem with the notation of first-order logic as a model-theoretic aspect. Finally, we give a brief idea about the concept of cellular automaton and the theorem Garden of Eden as an application to the Ax-Grothendieck theorem.

# 2. Algebra

In this chapter we introduce all the knowledge of algebra which is necessary for the study of algebraically closed fields and algebraic closure operator.

**2.0.1 Definition.** A field is a non-empty set $K$ with two binary operations $+$ and $\cdot$ such that:

1. $(K, +)$ is abelian group.
2. $(K \setminus \{0\}, \cdot)$ is abelian group.
3. $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$ $\forall x, y$ and $z$ in $K$.

## 2.1 Field Extension

The results in this section are mainly from Fraleigh (2003) and Lang (2002).

**2.1.1 Definition.** A subset $F$ of a field $K$ is called a subfield of $K$ if it satisfies the field axioms with respect to the same operations of $K$ and we write $F \leq K$.

**2.1.2 Definition.** Stewart (2015) A field $K$ is called a prime field if it has only trivial subfields.

**2.1.3 Definition.** Stewart (2015) If $K$ is a field, the prime subfield of $K$ is the intersection of all the subfields of $K$.

**2.1.4 Theorem.** *Stewart (2015) Every field $K$ has a prime subfield which is either isomorphic to the rational field $\mathbb{Q}$ or the field $\mathbb{Z}_p$ of integers modulo a prime number $p$.*

*Proof.* The proof of this theorem is given in [Stewart] Theorem 16.9. □



**2.1.5 Definition.** A field $K$ is said to be an extension field of a field $F$ if $F \subseteq K$ and $F$ itself is a field with respect to the same operations with $K$.

We denote $K/F$ to mean that $K$ is a field extension of $F$. We classify the elements of a field extension into two different categories as follows:

**2.1.6 Definition.** An element $\alpha$ in an extension field $K/F$ is algebraic if there exists a nonzero polynomial $p(x)$ in $F[x]$ such that $p(\alpha) = 0$. An element $\alpha$ is transcendental element over $F$ if $\alpha$ is not algebraic over $F$.

**2.1.7 Example.** The element $\pi$ in $\mathbb{C}$ is algebraic over $\mathbb{R}$ being a zero of $x - \pi$ in $\mathbb{R}[x]$ while $\pi$ is transcendental over $\mathbb{Q}$.

**2.1.8 Definition.** An extension field $K/F$ is called simple extension if there exist $\alpha$ in $K$ such that $K = F(\alpha)$.

**2.1.9 Remark.** We use $F[x]$ to denote the polynomial ring over $F$ while $F(\alpha)$ is to give the field extension of $F$ by adjoining the element $\alpha$.

**2.1.10 Example.** The complex field $\mathbb{C}$ is a simple extension of $\mathbb{R}$ since we have $\mathbb{C} = \mathbb{R}(i)$.

**2.1.11 Definition.** An extension field $K/F$ is algebraic extension if every element of $K$ is algebraic element over $F$.

**2.1.12 Theorem.** *If $K/F$ is an extension field and $\alpha$ in $K$ is algebraic over $F$ then $F(\alpha)/F$ is algebraic extension .*

*Proof.* The proof of this theorem is given in [Fraleigh] Theorem 29.18. □

**2.1.13 Definition.** If $K/F$ is an extension field of finite dimension $n$ as a vector space over $F$, then $K$ is a finite extension of degree $n$ over $F$, denoted by $[K : F] = n$.

**2.1.14 Theorem.** *Every finite extension field $K/F$ is algebraic extension.*

*Proof.* The proof of this theorem is given in [Fraleigh] Theorem 31.3. □

**2.1.15 Theorem.** *If $K/E$ is finite field extension and $E/F$ is finite field extension then $K/F$ is finite field extension.*

*Proof.* The proof of this theorem is given in [Fraleigh] Theorem 31.4. □

**2.1.16 Example.** We have that $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$ and $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ are finite field extensions then $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$ is a finite field extension.

**2.1.17 Theorem.** *Let $K/F$ be an extension field, and $\alpha$ in $K$ be an algebraic element over $F$. Then there exists an irreducible polynomial $p(x)$ in $F[x]$ such that $\alpha$ is a zero of $p(x)$. This $p(x)$ is uniquely determined up to a constant factor in $F$ and is a polynomial of minimal degree $\geq 1$ having $\alpha$ as a zero.*

*Proof.* The proof of this theorem is given in [Fraleigh] Theorem 29.13. □



**2.1.18 Definition.** Let $K/F$ be an extension field, and $\alpha$ in $K$ be an algebraic element over $F$. The unique monic irreducible polynomial which is of minimal degree $\geq 1$ having $\alpha$ as a zero is the irreducible polynomial for $\alpha$ over $F$ denoted by $irr(\alpha, F)$. The degree of $\alpha$ over $F$ is the degree of $irr(\alpha, F)$ and denoted by $deg(\alpha, F)$.

**2.1.19 Example.** The degree of $\sqrt{2}$ over the field $\mathbb{Q}$, denoted by $deg(\sqrt{2}, \mathbb{Q}) = 2$ since $\sqrt{2}$ is zero of the unique monic irreducible polynomial of minimal degree $\geq 1$, $x^2 - 2$ in $\mathbb{Q}[x]$.

**2.1.20 Corollary.** If $K/F$ is an extension field, $\alpha$ in $K$ is an algebraic element over $F$ and $\beta$ in $F(\alpha)$ then $deg(\beta, F)$ divides $deg(\alpha, F)$.

*Proof.* The proof of this corollary is given in [Fraleigh] Corollary 31.17. □

We use Corollary (2.1.20) to check the existence of zeros of some polynomials in a field or not.

**2.1.21 Example.** There is no element in $\mathbb{Q}(\sqrt{2})$ that is a root of $x^5 - 2$ since $deg(\sqrt{2}, \mathbb{Q}) = 2$ while a root of $x^5 - 2$ is of degree $5$ over $\mathbb{Q}$ but $5 \nmid 2$.

**2.1.22 Theorem.** *Let $K/F$ be an extension field which is algebraic then a finite number of elements $\alpha_1, \ldots, \alpha_n$ in $K$ exists with $K = F(\alpha_1, \ldots, \alpha_n)$ if and only if $K/F$ is an extension which is finite.*

*Proof.* The proof of this theorem is given in [Fraleigh] Theorem 31.11. □

**2.1.23 Theorem.** *Fraleigh (2003) If $K/E$ is an algebraic field extension and $E/F$ is an algebraic field extension. Then $K/F$ is an algebraic field extension.*

*Proof.* If $K/E$ is an algebraic field extension, then for every $\alpha$ in $K$ there exists a minimal polynomial $p(x) = a_0 + a_1x + \cdots + a_nx_n$ where $a_i$ in $E$ and $p(\alpha) = 0$. Let $F_1 = F(a_0, a_1, \ldots, a_n)$ is a finite extension of $F$ since each $a_i$ in $E$ is algebraic over $F$. We have $F_1(\alpha) = F(a_0, a_1, \ldots, a_n)(\alpha)$ is a finite extension of $F_1$, hence $F_1(\alpha)$ is a finite extension of $F$ by Theorem (2.1.15) which states that a finite extension of a finite extension is a finite extension over the original field. Finally $F_1(\alpha)$ is algebraic over $F$ by Theorem (2.1.14) which states that every finite extension is algebraic extension, so $\alpha$ is algebraic over $F$. □

**2.1.24 Corollary.** Lang (2002) If $K$ is a field with $F$ as a finite subfield of $K$ and $\alpha$ is an algebraic element over $F$, then $F(\alpha)$ is finite.

*Proof.* The proof of this corollary is in [Lang]. □

## 2.2 Algebraically Closed Fields (ACF)

In this section our goal is to prove the existence of an extension field which is algebraically closed for every field. The results in this section are mainly from Fraleigh (2003) and Lang (2002).

**2.2.1 Definition.** Lang (2002) A field $K$ is said to be ACF if every polynomial $p(x)$ in $K[x]$ with degree $\geq 1$ has a zero in $K$.



**2.2.2 Example.** The complex field $\mathbb{C}$ is ACF.

**2.2.3 Theorem.** *A field $K$ is ACF if and only if every non-constant polynomial $p(x)$ in $K[x]$ factors into linear factors.*

*Proof.* The proof of this theorem is given in [Fraleigh] Theorem 31.15. □

**2.2.4 Corollary.** An ACF has no proper algebraic extension.

*Proof.* The proof of this theorem is given in [Fraleigh] Corollary 31.16. □

**2.2.5 Proposition.** Lang (2002) Suppose that $F$ be a field. If $f$ is a polynomial of degree $\geq 1$ in $F[x]$, then there is an extension $K/F$ in which $f$ has a root.

*Proof.* The proof on this theorem is given in [Lang] Proposition 2.3. □

**2.2.6 Remark.** Lang (2002) Let $K/F$ be an extension field. If $\sigma : F \to E$ is an embedding of a field $F$ into a field $E$, then $\sigma$ induces an isomorphism of $F$ with its image $\sigma F$, written as $F^\sigma$. Similarly, Let $f$ be a polynomial in $F[x]$ that has a root in $K$. If $\tau : K \to L$ is an extension of $\sigma$, then we obtain that a zero of $\tau\sigma$ is a zero of $f^\sigma$.

Now we are going to reach our goal of this section.

**2.2.7 Theorem.** *Lang (2002) Let $K$ be a field then there exists an ACF that has $K$ as a subfield.*

*Proof.* Lang (2002) Construct a field $E_1$ which is an extension of $K$ such that every polynomial $f(x)$ of degree $\geq 1$ in $K[x]$ admits a zero as follows:

For each polynomial $f(x)$ in $K[x]$ with $deg(f(x)) \geq 1$, we associate new variables $x_f$ and construct the set $S$ of all the $x_f$ that are zeros for every $f(x)$ in $K[x]$. It is clear that the set $S$ and the set of all polynomials $f(x)$ in $K[x]$ are in bijection.

We construct $K[S]$ as a polynomial ring such that the ideal generated by all the polynomials $f(x_f)$ in $K[S]$ is not a unit ideal. To show that it is not unit, we can assume contrarily that it is unit so that there exists a finite linear combination of elements in this ideal which is $1$. Then we have

$$g_1 f_1(x_{f_1}) + \cdots + g_n f_n(x_{f_n}) \quad \text{where} \quad g_i \text{ in } K[S]$$

Replacing $x_{f_i}$by $x_i$ for simplicity, the polynomials $g_i$ will have only finite number of variables, say $x_1, \ldots, x_N$ where $N \geq n$. So our linear combination can be written as follows:

$$\sum_{i=1}^{n} g_i(x_1, \ldots, x_N) f_i(x_i) = 1.$$

Assume that $F$ is a finite extension in which each polynomial $f_1, \ldots, f_n$ admits a zero, say $\alpha_i$ in $F$ is a zero of $f_i$ for $i = 1, \ldots, n$ and $\alpha_i = 0$ for all $i > n$. Substituting by $\alpha_i$ in the linear combination, we have

$$0 = \sum_{i=1}^{n} g_i(\alpha_1, \ldots, \alpha_N) f_i(\alpha_i) = 1$$

which is contradiction.

Now, assume that $\mathfrak{m}$ be a maximal ideal of $K[S]$ containing the ideal generated by all the polynomials $f(x_f)$ in $K[S]$ so that $K[S]/\mathfrak{m}$ is a field. Consider the canonical map

$$\sigma : K[S] \to K[S]/\mathfrak{m}.$$

So for any polynomial $f(x)$ in $K[S]$ with $deg(f(x)) \geq 1$, by applying Remark (2.2.6), the polynomial $f^\sigma$ has a zero in $K[S]/\mathfrak{m}$ which is an extension of $\sigma K$, since for every field $K$ and a polynomial $f(x)$ in $K[x]$ with $deg(f(x)) \geq 1$ there exists an extension $E_1/K$ in which $f(x)$ has a zero.

Finally by induction we can obtain a chain of fields

$$E_1 \subset E_2 \subset \ldots E_n \subset \ldots$$

such that every $f(x)$ in $E_n[x]$ with $deg(f(x)) \geq 1$ has a zero in $E_{n+1}$. Let $E = \bigcup_n E_n$ , it is clear that $E$ is a field, since if we have two elements $a, b$ in the set $E$ then $n$ exists such that $a$ and $b$ in $E_n$ which implies that $a + b$ and $a \cdot b$ in $E_n$, this does not depend on how we choose $n$ such that $a$ and $b$ are in $E_n$ and it shows that we have a $E$ as a field.

Now, each polynomial $f(x)$ in E$[x]$ which has coefficients in one of the subfields $E_n$ has a zero in $E_{n+1}$ and hence there is a zero in $E$.

□

**2.2.8 Proposition.** Any ACF is infinite.

*Proof.* Let $F$ be any finite field, $p(x) = 1 + \prod_{a \in F} (x - a)$ be any polynomial in $F[x]$. We see that $p(a) = 1 \neq 0$ for every $a$ in $F$ so there is no zero for this polynomial in $F$ and hence $F$ is not ACF. Thus any ACF must be infinite. □

The following is called the fundamental theorem of algebra.

**2.2.9 Theorem.** *The complex field $\mathbb{C}$ is ACF.*

*Proof.* The proof of this theorem is in [Fraleigh] Th 31.18. □

## 2.3 Algebraic Closure

The main results of this section are mainly from Lang (2002). Our goal in this section is to prove the existence of algebraic closure for every field and showing that any two algebraic closures over the same field are isomorphic.

**2.3.1 Definition.** Let $K/F$ be an extension field then $\bar{K}_F = \{\alpha \in K : \alpha \text{ algebraic over } F\}$ is the algebraic closure of $F$ in $K$.

The following gives an equivalent definition for algebraic closure.

**2.3.2 Definition.** Any field extension $K/F$ such that $K$ is an algebraic extension of $F$ and $K$ is ACF is called the algebraic closure of $F$.

We denote $\bar{K}$ to express the algebraic closure of a field $K$.

**2.3.3 Theorem.** *Lang (2002) Let $K$ be a field then there is an extension $\bar{K}$ of $K$ which is ACF and this extension is algebraic over $K$.*

*Proof.* By Theorem (2.2.7), we proved that for every field $K$ there is a field extension $E/K$ which is ACF. Construct $\bar{K}$ to be the union of all the algebraic subextensions of $E$ over $K$, therefore $\bar{K}$ is an algebraic extension over $K$.

To prove that $\bar{K}$ is ACF, if $f(x)$ in $\bar{K}[x]$ with $deg(f(x)) \geq 1$ so since $E$ is ACF, $f(x)$ has a root $\alpha$ in $E$ and $\alpha$ is algebraic over $\bar{K}$, then $\alpha$ in $\bar{K}$ which means that $\bar{K}$ is ACF. Finally we obtained that $\bar{K}$ is algebraic over $K$ and ACF. Hence $\bar{K}$ exists as the algebraic closure of $K$. □

The following is to prove that any two algebraic closures of a field $F$ are isomorphic via an isomorphism which leaves $F$ fixed.

**2.3.4 Theorem.** *Lang (2002) Let $K$ be a field, $E/K$ be an algebraic extension, and $\sigma : K \to L$ be an embedding of $K$ into an ACF $L$. Then an extension of $\sigma$ to an embedding of the extension $E$ in $L$ exists. If $E$ is ACF and $L$ is algebraic over $\sigma K$, then any such extension of $\sigma$ is isomorphic of $E$ onto $L$.*

*Proof.* The proof of this theorem is given in [Lang] Theorem 2.8, the proof depends on Zorn's lemma. □

**2.3.5 Corollary.** Let $X, Y$ be two algebraic closures of a field $K$ and $\tau : X \to Y$ be an embedding over $K$. Then $\tau$ is an isomorphism.

*Proof.* Let $\tau$ be a homomorphism that leaves $K$ fixed. By Theorem (2.3.4), since $X$ is an ACF then $\tau X$ is an ACF and $\tau X \subset Y$. Since $Y$ is algebraic over $K$ so $Y$ is algebraic over $\tau X$, let $y$ in $Y$ so $y$ algebraic over $\tau X$ which implies that $y \in \tau X$ and hence $Y \subset \tau X$. Finally we obtain $Y = \tau X$ so $\tau$ is an isomorphism. □

## 2.4 Algebraic Closure Operator

In this section our goal is to define a closure operator inside ACF and check its properties. The results of this section are mainly from Tent and Ziegler (2012).

**2.4.1 Definition.** Let $S$ be a nonempty set, a function $cl : \mathcal{P}(S) \to \mathcal{P}(S)$ is called a pregeometry if it satisfying the following properties, for any set $A, B \subseteq S$ and $a, b$ in $S$

1. $A \subseteq cl(A)$ ($cl$ is extensive).
2. If $A \subseteq cl(B)$ then $cl(A) \subseteq cl(B)$ ($cl$ is transitive).
3. If $a$ in $cl(A)$ then there exists a finite $A_0 \subseteq A$ such that $a$ in $cl(A_0)$ ($cl$ is finite character).
4. If $a$ in $cl(A \cup \{b\}) \setminus cl(A)$ then $b$ in $cl(A \cup \{a\})$ (exchange principle).

**2.4.2 Definition.** A subset $A$ of a pregeometry is closed if $A = cl(A)$.

**2.4.3 Definition.** A pregeometry is called a geometry if the singletons and the empty set are closed.

**2.4.4 Definition.** Let $(S, cl)$ be a pregeometry, a subset $A \subseteq S$ is called :

1. an independent if $a$ is not in $cl(A \setminus \{a\})$ for all $a$ in $A$.
2. a generating set if $S = cl(A)$.
3. a basis if $A$ is independent generating.

We define a closure operator (pregeometry) inside an ACF as follows:

**2.4.5 Definition.** Let $K$ be ACF, $A \subset K$ and $b \in K$, we say that $b$ is algebraic over $A$, and we write $b$ in $acl(A)$, if $b$ belongs to an algebraic extension of the subfield of $K$ generated by $A$. Equivalently, $b$ in $acl(A)$ if there is a non-constant polynomial $p(x)$ with coefficients in the subfield of $K$ generated by $A$ such that $p(b) = 0$.

In the following theorem we will prove some few properties

**2.4.6 Theorem.** *Let $K$ be ACF, we have the following:*

1. *$A \subseteq acl(A)$ for all $A \subseteq K$ (acl extensive )*
2. *If $A \subseteq B$ then $acl(A) \subseteq acl(B)$ for all $A, B \subseteq K$ (acl monotonic).*
3. *$acl(A) = acl(acl(A))$ for all $A \subseteq K$.*

4. $A \subseteq acl(B)$ *then* $acl(A) \subseteq acl(B)$ *(acl transitive).*
5. *If* $a$ *in* $acl(A)$ *then there exists finite* $A_0 \subseteq A$ *such that* $a$ *in* $acl(A_0)$ *(acl finitary).*
6. *If* $b$ *in* $acl(A \cup \{c\}) \setminus acl(A)$ *then* $c$ *in* $acl(A \cup \{b\})$ *for all* $b, c$ *in* $K$ *(Exchange principle).*

*Proof.*
1. Let $a$ in $A$ then $a$ is a zero of the polynomial $x - a$ which has coefficients in the subfield generated by $A$ so $a$ in $acl(A)$.
2. Let $a$ in $acl(A)$, then there exists a nonzero polynomial $p(x) = a_n x^n + \cdots + a_0$ where $a_i$ in $A$ and $P(a) = 0$ but since $a_i$ in $A \subseteq B$ and $p(a) = 0$ then $a$ in $acl(B)$.
3. To show that $acl(acl(A)) = acl(A)$, by considering $acl(acl(A))$ as an algebraic field extension of the algebraic extension $acl(A)$, using Theorem (2.1.23) which states that algebraic extension of algebraic extension is algebraic over the original set $A$ so $acl(acl(A)) = acl(A)$.
4. It is given that $A \subseteq acl(B)$ then $acl(A) \subseteq acl(acl(B))$ since $cl$ is monotonic and we have $acl(acl(B)) = acl(B)$ and hence $acl(A) \subseteq acl(B)$.
5. If $a$ in $acl(A)$, then there exists an irreducible polynomial $p(x) = b_n x^n + \cdots + b_0$ such that $b_n, \ldots, b_0$ in the ring generated by $A$ and with $a$ as one, among finitely many roots so a finite subset $A_0$ of $A$ is enough to generate $b_n, \ldots, b_0$, and hence we obtain that $a$ in $acl(A_0)$.
6. Assume that $b$ in $acl(A \cup \{c\})$ then there exists a nonzero polynomial $p(x, y)$ in $K[x, y]$ such that $p(b, c) = 0$ while $p(x, c)$ is not zero for the variable $x$. If we have that $c$ is not in $acl(A \cup \{b\})$, it follows that $p(b, y) = 0$ for all the variables $y$ so there exists nonzero polynomial $p(x, y)$ where $p(b, y) = 0$ for every variable $y$ which implies that $b$ in $acl(A)$ since if $b$ is not in $acl(A)$, this means that the polynomial $p(x, y)$ is zero polynomial, and hence we obtain a contradiction.

□

## 2.5 Transcendence Degree



The main result in this section is Theorem (2.5.4) which is mainly from Hungerford (1980).

**2.5.1 Definition.** Let $K/F$ be an extension field of $F$. A subset $S$ of $K$ is algebraically independent over $F$ if for some positive integer $n$, there exists a nonzero polynomial $p(x)$ in $F[x_1, \ldots, x_n]$ such that $p(s_1, \ldots, s_n) \neq 0$ for some distinct $s_1, \ldots, s_n$ in $S$. A subset $S$ of $K$ is algebraically dependent over $F$ if it is not algebraically independent over $F$.

**2.5.2 Definition.** Let $K/F$ be an extension field. A transcendence basis of $K$ over $F$ is a subset $S \subseteq K$ which is maximal algebraically independent.

**2.5.3 Example.** For any $\alpha$ in $K/F$, $\{\alpha\}$ is algebraically dependent over $F$ if and only if $\alpha$ is algebraic over $F$.

**2.5.4 Theorem.** *Let* $A$ *and* $B$ *be any two transcendental basis of an extension field* $K/F$. *If* $A$ *is finite then* $|A| = |B|$.

*Proof.* The proof depends on the fact of the exchange principle that for the two transcendental bases $A$ and $B$, if we take any element $\{a\}$ in $A$ then there is an element $\{b\}$ in $B$ with the property that $(A \setminus \{a\}) \cup \{b\}$ is again a transcendental basis of $K$.

Let $A = \{a_1, \ldots, a_n\}$ and we take $A' = \{a_2, \ldots, a_n\}$. By claiming that there is an element $b$ in $B$, say $b = b_1$ such that $\{b_1, a_2, \ldots, a_n\}$ is a transcendental basis. To check that, if every element of $B$ is algebraic over $F(A')$ then $K$ is algebraic over $F(B)$ and hence algebraic over $F(A')$ which is contradiction.

Thus, there is an element $b$ in $B$, say $b = b_1$ so that we have $b_1$ is transcendental over $F(A')$. Hence $B' = \{b_1, a_2, \ldots, a_n\}$ is algebraically independent but since $A$ is maximal algebraically independent then $a_1$ is algebraic over $F(B')$. It follows that $K$ is algebraic over $F(b_1, a_1, \ldots, a_n)$ and hence is algebraic over $F(B')$. We can continue in this process until we obtain a transcendental basis $\{b_1, \ldots, b_n\} \subset B$ thus $|B| = |A|$. □

**2.5.5 Definition.** Let $K/F$ be an extension field. The transcendence degree of $K$ over $F$ denoted by $tr.deg(K/F)$ is the cardinality of any transcendence basis of $K$ over $F$.

**2.5.6 Example.** We have that $tr.deg(\mathbb{Q}(\sqrt{2}, e)/\mathbb{Q}) = 1$ since $\sqrt{2}$ is algebraic while $e$ is transcendental.

**2.5.7 Example.** We have that $tr.deg(\mathbb{Q}(\pi, e)/\mathbb{Q})$ is either $1$ or $2$, it is still not precise since it is not clear yet whether $e$ and $\pi$ are algebraically dependent or not.

**2.5.8 Theorem.** *Hungerford (1980) If $K_1$ and $K_2$ are two ACF extensions of the fields $F_1$ and $F_2$ respectively where*

$$tr.deg(K_1/F_1) = tr.deg(K_2/F_2).$$

*Then every isomorphism of fields $\sigma : F_1 \to F_2$ extends to an isomorphism $\tau : K_1 \to K_2$.*

*Proof.* The proof of this theorem is in [Hungerford] Theorem 1.12. □

# 3. Model Theory

In this chapter, we study the basic notation of model theory, we study the concepts of language, structures, theory and so on. A language is a set of relations, functions, and constant symbols, it is a new way of looking at mathematical objects abstractly by some tools such as formulas, variables, and terms, then we associate an interpretation to the language to describe any element of the structure mathematically using logic especially first-order logic. We move on to study the properties of a theory such as quantifier elimination and completeness. The main results in this chapter are mainly from Marker (2002), Deloro (2013) and Boxall (2017).

## 3.1 Basic Notation of Model Theory

In this section, we introduce the basic concepts for model theory.

**3.1.1 Definition.** Deloro (2013) A first-order language $\mathcal{L}_M$ is a set consists of the three following mutually disjoint subsets:

1. The collection of all relation symbols $R_{\mathcal{L}}$.
2. The collection of all constant symbols $C_{\mathcal{L}}$.
3. The collection of all function symbols $F_{\mathcal{L}}$.

with the function $p_{\mathcal{L}} : R_{\mathcal{L}} \cup F_{\mathcal{L}} \to \mathbb{Z}_{>0}$ which called the arity function, for every function and relation symbol it gives the number of arguments it takes. Note that any set of $R_{\mathcal{L}}, F_{\mathcal{L}}$, and $C_{\mathcal{L}}$ can be empty.

**3.1.2 Example.** Boxall (2017) Consider $\mathcal{L}_{\mathbb{R}} = \{+, -, \cdot, 1, 0, <\}$ to be the language of real numbers where $1, 0$ are constant symbols, $+, \cdot$ are function symbols with arity $2$ while $-$ is function symbol with arity $1$ and $<$ is relation symbol with arity $2$.



**3.1.3 Definition.** Boxall (2017) Suppose $\mathcal{L}$ be a first-order language, we define an $\mathcal{L}$-structure $\mathcal{M}$ as a pair $(M, I)$ where $M$ is a nonempty set called the underlying set and $I$ is a function which assigns every element of $\mathcal{L}$ to an appropriate structural feature of $M$ called the interpretation of $\mathcal{L}$ in $M$ as follows:

1. For each constant symbol $c$, $I(c)$ is in $M$.
2. For each n-ary relation symbol $R$, $I(R)$ is a subset of $M^n$.
3. For each n-ary function symbol $f$, $I(f) : M^n \to M$ is a function.

**3.1.4 Example.** Boxall (2017) Suppose that $M = \mathbb{R}$ and $\mathcal{L} = \mathcal{L}_{\mathbb{R}}$, we define the interpretation $I$ of $\mathcal{L}_{\mathbb{R}}$ in $M = \mathbb{R}$ as follows:

$I(0)$ in $\mathbb{R}$ is the number zero.
$I(1)$ in $\mathbb{R}$ is the number one.
$I(+) : \mathbb{R}^2 \to \mathbb{R}$ is the standard addition operation
$I(\cdot) : \mathbb{R}^2 \to \mathbb{R}$ is the standard multiplication operation.
$I(-) : \mathbb{R} \to \mathbb{R}$ is the standard unary minus operation.
$I(<) \subseteq \mathbb{R}^2$ is the set of all tuples $(a, b)$ where $a$ is less than $b$ by the usual ordering.

**3.1.5 Definition.** Boxall (2017) Let $\mathcal{M} = (M, I_M)$ and $\mathcal{N} = (N, I_N)$ be any two $\mathcal{L}$-structures, $f : \mathcal{M} \to \mathcal{N}$ be a function and define for $T \subseteq M^n$, $f(T) = \{(f(t_1), \ldots, f(t_n)) : (t_1, \ldots, t_n) \text{ in } T\}$. We call $f$ to be an $\mathcal{L}$-structure isomorphism if the following holds:

1. The function $f$ is bijective.
2. For $R$ in $R_{\mathcal{L}}$, we have $f(I_M(R)) = I_N(R)$.
3. For $S$ in $F_{\mathcal{L}}$ with k-arity, we have $f(I_M(S)(\bar{m})) = I_N(S)(f(\bar{m}))$ for all $\bar{m}$ in $M^k$.
4. We have $f(I_M(c)) = I_N(c)$ for all $c$ in $C_{\mathcal{L}}$.

**3.1.6 Definition.** Deloro (2013) The collection of $\mathcal{L}$-terms of a first-order language $\mathcal{L}$ is defined as follows:

1. Every constant symbol $c$ is a term.
2. Every variable symbol $x, y, z, \ldots$ is a term.
3. For every function symbol $f$ with $n$-ary and $x_1, \ldots x_n$ are terms, we have $f(x_1, \ldots, x_n)$ is a term.



**3.1.7 Definition.** Marker (2002) We define an atomic $\mathcal{L}$-formula to be one of the following forms:

1. If $t_1$ and $t_2$ are terms then $t_1 = t_2$ is an atomic formula.
2. If $R$ is an $n$-ary relation symbol and $t_1, \ldots, t_n$ are terms, then $R(t_1, \ldots, t_n)$ is a formula called the atomic formula.

Note that we use the word formula to mean a first-order formula.

**3.1.8 Definition.** Marker (2002) The collection of $\mathcal{L}$-formulas is defined to be one of the following:

1. If $\phi$ is an atomic $\mathcal{L}$-formula then $\neg\phi$ is a formula.
2. If $\phi$ and $\psi$ are two atomic formulas then $\phi \wedge \psi$, $\phi \vee \psi$, $\phi \to \psi$ and $\phi \leftrightarrow \psi$ are formulas.
3. If $\phi$ is a formula and $x$ is a variable symbol, then using quantifiers as follows $\forall x\phi$ and $\exists\phi$ produces formula again.

**3.1.9 Definition.** Boxall (2017) A formula is called quantifier-free formula if it has no quantifier.

**3.1.10 Definition.** Boxall (2017) For a language $\mathcal{L}$ and a formula $\phi$, a subformula of $\phi$ is a formula which occurs within $\phi$. An appearance of a variable $x$ in a formula $\phi$ is called bound if it belongs to a subformula $\psi$ of the form $\exists x\psi$ or $\forall x\psi$. An appearance of $x$ in $\phi$ is free if it is not bound. A variable $x$ is called a free variable of a formula $\phi$ if it appears in $\phi$ at least one time as a free variable. If $\phi$ is a formula with free variables $t_1, \ldots, t_n$, we write $\phi$ as $\phi(t_1, \ldots, t_n)$.

**3.1.11 Definition.** Deloro (2013) A formula that has no free variable is called a sentence.

**3.1.12 Example.** Consider the formula $\phi$ which is given by $x + y = 0$, then $x, y$ are free variables and we write $\phi(x, y)$ while in the formula $\psi$ which is given by $\forall x \exists y(x + y = 0)$ there is no free variable and hence $\psi$ is a sentence.

**3.1.13 Definition.** Deloro (2013) Let $\mathcal{M}$ be an $\mathcal{L}$-structure. If $\phi(x_1, \ldots, x_n)$ be an $\mathcal{L}$-formula and $a_1, \ldots, a_n$ in $M$ such that the property of $\phi$ is true for $a_1, \ldots, a_n$ in $M$, we say that $\mathcal{M}$ satisfies $\phi(a_1, \ldots, a_n)$ and we write $\mathcal{M} \models \phi(a_1, \ldots, a_n)$.

Any sentence in an $\mathcal{L}$-structure $\mathcal{M}$ is either true or false, if a sentence $\phi$ is true in $\mathcal{L}$-structure $\mathcal{M}$ we say that $\mathcal{M}$ models $\phi$ and write it as $\mathcal{M} \models \phi$.

**3.1.14 Example.** Deloro (2013) Let $\mathcal{M} = (\mathbb{R}, I)$ where $I$ is the standard interpretation so we have $\mathcal{M} \models \forall x \exists y(x + y = 0)$ while $\mathcal{M} \not\models \exists x(x \cdot x = -1)$.

**3.1.15 Definition.** Marker (2002) Let $\mathcal{M} = (M, I_M)$ and $\mathcal{N} = (N, I_N)$ be two $\mathcal{L}$-structures. An $\mathcal{L}$-embedding $f : \mathcal{M} \to \mathcal{N}$ is a one-to-one map $f : M \to N$ such that the interpretation of $\mathcal{L}$ in $M$ coincides with the interpretation of $\mathcal{L}$ in $N$. If $M \subseteq N$ then we call either $\mathcal{M}$ a substructure of $\mathcal{N}$ or $\mathcal{N}$ is an extension of $\mathcal{M}$, written as $\mathcal{M} \subseteq \mathcal{N}$.

**3.1.16 Definition.** Marker (2002) Let $\mathcal{M} = (M, I_M)$ and $\mathcal{N} = (N, I_N)$ be two $\mathcal{L}$-structures, we call an $\mathcal{L}$-embedding $f : \mathcal{M} \to \mathcal{N}$ to be elementary embedding if

$$\mathcal{M} \models \phi(a_1, \ldots, a_n) \text{ if and only if } \mathcal{N} \models \phi(f(a_1), \ldots, f(a_n))$$

for any $\mathcal{L}$-formulas $\phi$ and all $a_1, \ldots, a_n$ in $M$.

If $\mathcal{M}$ is a substructure of $\mathcal{N}$, then $\mathcal{M}$ is an elementary substructure of $\mathcal{N}$, written as $\mathcal{M} \preceq \mathcal{N}$.

**3.1.17 Definition.** Deloro (2013) We define a set of sentences in a language $\mathcal{L}$ to be an $\mathcal{L}$-theory.

The following is mainly from Marker (2002), if $T$ be an $\mathcal{L}$-theory and $\phi$ be an $\mathcal{L}$-sentence. A proof of $\phi$ from $T$ is a finite sequence of $\mathcal{L}$-formulas $\psi_1, \ldots, \psi_n$ such that $\psi_i$ follows from $\psi_1, \ldots, \psi_{i-1}$ by logical rules for each $i$, we write $T \vdash \phi$ if there exists a proof of $\phi$ from $T$. For example of a simple logical rules is that from the two $\mathcal{L}$-sentences $\phi$ and $\psi$, we may conclude $\phi \wedge \psi$. A set of sentences is said to be consistent if there is no proof of a contradiction.

**3.1.18 Definition.** Marker (2002) An $\mathcal{L}$-theory $T$ is satisfiable if there exists an $\mathcal{L}$-structure $\mathcal{M}$ such that $\mathcal{M} \models \phi$ for all $\phi$ in $T$.

**3.1.19 Theorem.** *Marker (2002)(Completeness and soundness) A set of sentences is consistent if and only if it is satisfiable.*

*Proof.* The proof of this theorem is given in [Marker] Corollary 2.1.3. □

**3.1.20 Theorem.** *Marker (2002)(compactness theorem) An $\mathcal{L}$-theory $T$ is consistent if and only if every finite subset of $T$ is consistent.*

*Proof.* The proof of this theorem is in [Marker] Theorem 2.1.4. □

**3.1.21 Definition.** The deductive closure of an $\mathcal{L}$-theory $T$ is the set of all sentences which are true in every model of $T$.

**3.1.22 Lemma.** Marker (2002) Let $T$ be an $\mathcal{L}$-theory and $\phi$ be an $\mathcal{L}$-sentence. If $T \models \phi$, then $A \models \phi$ for some finite $A \subseteq T$.

*Proof.* Suppose that $A$ be a finite subset of $T$ with $A \not\models \phi$, thus $A \cup \{\neg\phi\}$ is satisfiable. Therefore $T \cup \{\neg\phi\}$ is finitely satisfiable. Hence by using the Compactness Theorem (3.1.20), $T \not\models \phi$. □

**3.1.23 Definition.** Marker (2002) Let $\mathcal{M}$ be an $\mathcal{L}$-structure. A set $X \subseteq M^n$ is definable if and only if there exists an $\mathcal{L}$-formula $\phi(x_1, \ldots, x_n, y_1, \ldots, y_m)$ and $\bar{b} = (b_1, \ldots, b_m)$ in $M^m$ such that $X = \{\bar{a} = (a_1, \ldots, a_n) \in M^n : \mathcal{M} \models \phi(a_1, \ldots, a_n, b_1, \ldots, b_m)\}$.

## 3.2 Quantifier Elimination

Quantifier elimination is a very important tool in mathematical logic because it is a concept of simplification. In model theory, it is used to characterize many theories such as completeness, completeness in model theory is a nice property for any $\mathcal{L}$-theory which states that an $\mathcal{L}$-theory is complete if any two $\mathcal{L}$-structures satisfy the same sentences.

**3.2.1 Definition.** Marker (2002) An $\mathcal{L}$-theory $T$ has quantifier elimination if for every formula $\phi(\overline{x})$ there exists a formula without quantifiers $\psi(\overline{x})$ with the property that $T \models \forall x[\phi(\overline{x}) \leftrightarrow \psi(\overline{x})]$.



**3.2.2 Example.** Marker (2002) Let $\psi(a, b, c, d)$ be the formula

$$\exists x \exists y \exists z \exists w(x \cdot a + y \cdot c = 1 \wedge x \cdot b + y \cdot d = 0 \wedge z \cdot a + w \cdot c = 0 \wedge z \cdot b + w \cdot d = 1)$$

This formula is exactly expressing the existence of a matrix $\begin{pmatrix} x & y \\ z & w \end{pmatrix}$ which is inverse of the matrix $\begin{pmatrix} a & b \\ b & d \end{pmatrix}$ so this formula can be written as a quantifier-free formula for any field $F$ as follows:

$$F \models \psi(a, b, c, d) \leftrightarrow ad - bc \neq 0$$

**3.2.3 Proposition.** Marker (2002) If $\mathcal{M}$ is a substructure of $\mathcal{N}$ where $\bar{a}$ in $M$ and $\phi(\overline{x})$ is a quantifier-free formula, then $\mathcal{M} \models \phi(\bar{a})$ if and only if $\mathcal{N} \models \phi(\bar{a})$. This means that quantifier-free formulas are preserved under substructure and extension also.

*Proof.* The proof of this proposition is in [Marker] Proposition 1.18. □

**3.2.4 Theorem.** *Marker (2002) Let $\mathcal{L}$ be a language with a constant symbol $c$, $T$ be an $\mathcal{L}$-theory with the property that any two models of $T$ have a common substructure and $\phi(\overline{x})$ be an $\mathcal{L}$-formula. Then the following are equivalent:*

*(1) There is a quantifier-free formula $\psi(\overline{x})$ with the property that $T \models \forall \overline{x}[\phi(\overline{x}) \leftrightarrow \psi(\overline{x})]$.*

*(2) If $\mathcal{M}$ and $\mathcal{N}$ are two models of $T$ with common substructure $\mathcal{A}$ with $\overline{a}$ in $\mathcal{A}$, then $\mathcal{M} \models \phi(\overline{a})$ if and only if $\mathcal{N} \models \phi(\overline{a})$.*

*Proof.* Marker (2002) Firstly, we prove that (1) implies (2) as follows:

Let $\mathcal{M}$ and $\mathcal{N}$ are two models of $T$ and $\overline{a}$ in $\mathcal{A}$ such that $\mathcal{A}$ is a common substructure of $\mathcal{M}$ and $\mathcal{N}$. By (1), we have a quantifier-free formula $\psi(\overline{a})$ such that

$$\mathcal{M} \models \phi(\overline{a}) \text{ if and only if } \mathcal{M} \models \psi(\overline{a}). \tag{3.2.1}$$

We have quantifier-free formulas are preserved under substructure as stated in Proposition (3.2.3) then $\mathcal{A} \models \psi(\overline{a})$, similarly since quantifier-free formulas are preserved under extension as stated in Proposition (3.2.3) then $\mathcal{N} \models \psi(\overline{a})$ so by property (1), we have

$$\mathcal{N} \models \psi(\overline{a}) \text{ if and only if } \mathcal{N} \models \phi(\overline{a}). \tag{3.2.2}$$

Now, from equations (3.2.1) and (3.2.2), we obtain that

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

Secondly, we prove that (2) implies (1) as follows: Assume that If $\mathcal{M}$ and $\mathcal{N}$ are two models of $T$ with common substructure $\mathcal{A}$ with $\overline{a}$ in $\mathcal{A}$, then $\mathcal{M} \models \phi(\overline{a})$ if and only if $\mathcal{N} \models \phi(\overline{a})$.

If we suppose that $T \models \forall \overline{x}\phi(\overline{x})$ then we can expresses it as follows $T \models \forall \overline{x}[\phi(\overline{x}) \leftrightarrow c = c]$. Similarly, if $T \models \forall \overline{x}\neg\phi(\overline{x})$ then we can expresses it as follows $T \models \forall \overline{x}[\phi(\overline{x}) \leftrightarrow c \neq c]$, thus we can assume that both $T + \{\phi(\overline{x})\}$ and $T + \{\neg\phi(\overline{x})\}$ are satisfiable (consistent).

Let

$$\Gamma(\overline{x}) = \{\psi(\overline{x}) : \psi \text{ is quantifier-free formula and } T \models \forall \overline{x}[\phi(\overline{x}) \rightarrow \psi(\overline{x})]\} \tag{3.2.3}$$

We can add some constant symbols $d_1, \ldots, d_m$ to the language $\mathcal{L}$ where $\overline{d} = d_1, \ldots, d_m$ has the same length as $\overline{x}$. Our goal is to show that $T + \Gamma(\overline{d}) \models \phi(\overline{d})$.

**Claim that T+$\Gamma(\overline{d}) \models \phi(\overline{d})$**

We prove the claim by contradiction as follows, assume contrarily that $T + \Gamma(\overline{d}) + \{\neg\phi(\overline{d})\}$ is consistent. Let $\mathcal{M} \models T + \Gamma(\overline{d}) + \{\neg\phi(\overline{d})\}$. Suppose that $\mathcal{A}$ is a substructure of $\mathcal{M}$ generated by the constant $\overline{d}$. The atomic diagram of $\mathcal{A}$ is given as follows:

$$Diag(\mathcal{A}) = \{\psi(\overline{d}) : \ \psi \text{ is either an atomic } \mathcal{L}\text{-formula or its negation is an atomic } \mathcal{L}\text{-formula and } \mathcal{A} \models \psi(\overline{d})\} \tag{3.2.4}$$

Let

$$\sum = T + Diag(\mathcal{A}) + \{\phi(\overline{d})\},$$

if $\sum$ is not satisfiable then by the Compactness Theorem there exists a finite subset of $T$, say $\psi_1(\overline{d}), \ldots, \psi_n(\overline{d})$ in $Diag(\mathcal{A})$ with the property that

$$T \models \forall \overline{x}[\bigwedge_{i=1}^{n} \psi_i(\overline{x}) \rightarrow \neg\phi(\overline{x})], \text{ this implies that } T \models \forall \overline{x}[\phi(\overline{x}) \rightarrow \bigvee_{i=1}^{n} \neg\psi_i(\overline{x})].$$

Therefore, by Proposition (3.2.3), we obtain that $\bigvee_{i=1}^{n} \neg\psi_i(\overline{x})$ in $\Gamma(\overline{x})$.

Since $\mathcal{M} \models T$, then $\mathcal{M} \models \bigvee_{i=1}^{n} \neg\psi_i(\overline{d})$ and since as we know that quantifier-free formulas are preserved under substructure, thus $\mathcal{A} \models \neg\psi_i(\overline{d})$ for some $i$, hence we obtain a contradiction with the definition of $Diag(\mathcal{A})$. Consequently, $\sum$ is satisfiable.

Moreover, if we assume that $\mathcal{N} \models \sum$ then $\mathcal{N} \models \phi(\overline{d})$. Since $Diag(\mathcal{A}) \subseteq \sum$ so we may assume that $\mathcal{A} \subseteq \mathcal{N}$. Also, since we have $\mathcal{M} \models \neg\phi(\overline{d})$ and by using (2), we obtain that $\mathcal{N} \models \neg\phi(\overline{d})$ which is a contradiction. Therefore $T + \Gamma(\overline{d}) \models \phi(\overline{d})$.

Finally, by the Compactness Theorem there is a finite subset of $T$ , $\psi_1(\overline{x}), \ldots, \psi_n(\overline{x})$ in $\Gamma(\overline{x})$ where

$$T \models \forall\overline{x}[\bigwedge_{i=1}^{n} \psi_i(\overline{x}) \rightarrow \phi(\overline{x})].$$

This implies that

$$T \models \forall\overline{x}[\bigwedge_{i=1}^{n} \psi_i(\overline{x}) \leftrightarrow \phi(\overline{x})] \text{ where } \bigwedge_{i=1}^{n} \psi_i(\overline{x}) \text{ is a quantifier free formula.}$$

Now, we have shown the existence of a formula without quantifiers $\psi(\overline{x})$ with the property that

$$T \models \forall x[\phi(\overline{x}) \leftrightarrow \psi(\overline{x})] \text{ which is exactly (1).}$$

□

The following shows that one can prove quantifier elimination by removing one existential quantifier at a time.

**3.2.5 Theorem.** *Marker (2002) Let $\mathcal{L}$ be a language, $T$ be an $\mathcal{L}$-theory such that for every quantifier-free $\mathcal{L}$-formula $\theta(\overline{x}, w)$, there is a quantifier-free formula $\psi(\overline{x})$ where $T \models \forall\overline{x}[\exists w\theta(\overline{x}, w) \leftrightarrow \psi(\overline{x})]$. Then, $T$ has the property of quantifier elimination.*



*Proof.* Marker (2002) Our goal is to show that every $\mathcal{L}$-formula $\phi(\overline{x})$ is equivalent to a quantifier-free formula, we will do that by induction on the complexity of $\phi(\overline{x})$. If $\phi(\overline{x})$ is a quantifier-free formula, then it is clear that there is nothing to show.

The base step of the induction is the case that, if the formula $\phi(\overline{x})$ has only one quantifier, so the quantifier is either existential as $\phi(\overline{x}) \equiv \exists w\theta(\overline{x}, w)$ or universal as $\phi(\overline{x}) \equiv \forall w\theta(\overline{x}, w)$ where $\theta(\overline{x}, w)$ is a quantifier-free formula. In the case of the existential quantifier, by our assumption property, there exists a quantifier-free formula $\psi(\overline{x})$ with the property that

$$T \models \forall\overline{x}[\exists w\theta(\overline{x}, w) \leftrightarrow \psi(\overline{x})] \text{ then } T \models \forall\overline{x}[\phi(\overline{x}) \leftrightarrow \psi(\overline{x})].$$

In the case of the universal quantifier, we may rewrite the formula as $\phi(\overline{x}) \equiv \neg[\exists w\neg\theta(\overline{x}, w)]$. So we have$\neg\phi(\overline{x}) \equiv \exists w\neg\theta(\overline{x}, w)$, here similarly by our assumption, there exists a quantifier-free formula $\psi_1(\overline{x})$ with the property that

$$T \models \forall\overline{x}[\exists w\neg\theta(\overline{x}, w) \leftrightarrow \psi_1(\overline{x})]$$
$$T \models \forall\overline{x}[\neg\phi(\overline{x}) \leftrightarrow \psi_1(\overline{x})]$$
$$T \models \forall\overline{x}[\phi(\overline{x}) \leftrightarrow \neg\psi_1(\overline{x})].$$

The induction hypothesis: assume that every $\mathcal{L}$-formula with $n$ quantifier is equivalent to a formula without quantifiers where $n > 1$.

The induction step: our goal is to prove that every formula $\phi(\overline{x})$ with $n+1$ quantifier then we can rewrite $\phi(\overline{x})$ either existential as $\phi(\overline{x}) \equiv \exists w\theta(\overline{x}, w)$ or universal as $\phi(\overline{x}) \equiv \forall w\theta(\overline{x}, w)$ where $\theta(\overline{x}, w)$ is any formula with $n$ quantifier. By the induction assumption, we have that $\theta(\overline{x}, w)$ is equivalent to a quantifier-free formula and by the base step of our induction we have $\phi(\overline{x})$ is equivalent to a quantifier-free formula. □

We use Theorems (3.2.4) and (3.2.5) to have the following quantifier elimination test.

**3.2.6 Corollary.** Marker (2002) Let $\mathcal{L}$ be a language with at least one constant symbol $d$ and $T$ be an $\mathcal{L}$-theory such that any two models $\mathcal{M}$ and $\mathcal{N}$ of $T$ have a common substructure $\mathcal{A}$. Suppose that for every quantifier free formula $\phi(\overline{x}, w)$, if $\overline{a}$ in $A$ and $b$ in $M$ such that $\mathcal{M} \models \phi(\overline{a}, b)$ , then there exists $c$ in $N$ such that $\mathcal{N} \models \phi(\overline{a}, c)$. Then $T$ has the quantifier elimination property.

*Proof.* Assume that if $\overline{a}$ in $A$ and $b$ in $M$ such that $\mathcal{M} \models \phi(\overline{a}, b)$, then there exists $c$ in $\mathcal{N}$ satisfying $\mathcal{N} \models \phi(\overline{a}, c)$. This is just property (2) of Theorem (3.2.4) for the formula $\exists w\phi(\overline{x}, w)$. By the equivalence between property (1) and property (2) of Theorem (3.2.4), then there is a quantifier-free formula $\psi(\overline{x})$ with the property that

$$T \models \forall \overline{x}[\exists w\theta(\overline{x}, w) \leftrightarrow \psi(\overline{x})].$$

Hence, by using Theorem (3.2.5), we show that $T$ has the property of quantifier elimination. □

## 3.3 Completeness

The main results in this section are mainly from Marker (2002).

**3.3.1 Definition.** Deloro (2013) Any two $\mathcal{L}$-structures $\mathcal{M}$ and $\mathcal{N}$ are called elementarily equivalent if they satisfy the same sentences, that means

$$\mathcal{M} \models \phi \text{ if and only if } \mathcal{N} \models \phi \text{ for any } \mathcal{L}\text{-sentence } \phi$$

and we write $\mathcal{M} \equiv \mathcal{N}$.

**3.3.2 Example.** Deloro (2013) We have the complex field structure $(\mathbb{C}, +, -, \cdot, 0, 1)$ and the real field structure $(\mathbb{R}, +, -, \cdot, 0, 1)$ are not elementarily equivalent since the sentence $\exists x(x \cdot x + 1 = 0)$ which is true in the complex structure but false in the real structure.

The two structures $(\mathbb{Q}, <)$ and $(\mathbb{R}, <)$ are elementarily equivalent since they satisfy the same sentences.

**3.3.3 Theorem.** *Any two isomorphic $\mathcal{L}$-structures are elementarily equivalent.*

*Proof.* The proof of this theorem is in [Marker] Theorem 1.1.10. □

**3.3.4 Definition.** Marker (2002) Let $\mathcal{L}$ be a language, an $\mathcal{L}$-theory $T$ is called complete theory if for any sentence $\psi$, either $T \models \psi$ or $T \models \neg\psi$.

**3.3.5 Proposition.** Marker (2002) An $\mathcal{L}$-theory $T$ is complete if and only if for any two models $\mathcal{M}$ and $\mathcal{N}$ of $T$ and any $\mathcal{L}$-sentence $\psi$, we have $\mathcal{M} \models \psi$ if and only if $\mathcal{N} \models \psi$. This means that an $\mathcal{L}$-theory $T$ is complete if and only if any two models are elementarily equivalent.

*Proof.* Firstly, we assume that $T$ be a complete $\mathcal{L}$-theory and $\mathcal{M}$ be a model of $T$ with $\mathcal{M} \models \psi$ for some $\mathcal{L}$-sentence $\psi$. If we assume that $T \models \neg\psi$, then $\mathcal{M} \models \neg\psi$ but this contradicts that $T$ is complete so $T \models \psi$, and hence $\mathcal{N} \models \psi$ for any other model $\mathcal{M}$ of $T$. This shows that any two models $\mathcal{M}$ and $\mathcal{N}$ of a complete theory $T$ are elementarily equivalent.

Conversely, assume that any two models $\mathcal{M}$ and $\mathcal{N}$ of an $\mathcal{L}$-theory $T$ are elementarily equivalent and let $\psi$ be an $\mathcal{L}$-sentence. If $\mathcal{M} \models \psi$, then for every model $\mathcal{N} \models T$, we obtain that $\mathcal{N} \models \psi$, therefore

$$T \models \psi. \tag{3.3.1}$$

Otherwise, if $\mathcal{M} \not\models \psi$, then $\mathcal{M} \models \neg\psi$, and hence

$$T \models \neg\psi. \tag{3.3.2}$$

Now, from (3.3.1) and (3.3.2), we showed that if for any two models of an $\mathcal{L}$-theory $T$ are elementarily equivalent, then the theory $T$ is complete. □

**3.3.6 Theorem.** *Marker (2002) Let $\mathcal{L}$ be a language with at least one constant symbol $c$, if $T$ is an $\mathcal{L}$-theory satisfying the quantifier elimination property and any two models of $T$ have a common substructure, then $T$ is a complete theory.*

*Proof.* Suppose $\mathcal{M}$ and $\mathcal{N}$ are two models of $T$ with a common substructure $\mathcal{A}$, let $\phi$ be any $\mathcal{L}$-sentence in $T$. Because of the quantifier elimination property, there exists a quantifier free sentence $\psi$ where

$$\mathcal{M} \models (\phi \leftrightarrow \psi), \text{ also } \mathcal{N} \models (\phi \leftrightarrow \psi).$$

So if we assume that

$$\mathcal{M} \models \phi \text{ then } \mathcal{M} \models \psi.$$



Because quantifier-free formulas are preserved under substructure and we have that $\mathcal{A}$ is a substructure of $\mathcal{M}$ then

$$\mathcal{A} \models \psi.$$

Similarly, because $\mathcal{A}$ is a substructure of $\mathcal{N}$ and quantifier free formulas are preserved under extension, so

$$\mathcal{N} \models \psi.$$

Now, for any sentence $\phi$ and any two models $\mathcal{M}$ and $\mathcal{N}$ with a common substructure $\mathcal{A}$, we have that

$$\mathcal{M} \models \phi \text{ implies that } \mathcal{N} \models \phi.$$

Finally $\mathcal{M}$ and $\mathcal{N}$ satisfy the same sentences and hence $T$ is complete. □

In the following, we give an example of an incomplete $\mathcal{L}$-theory that can be modified to be complete.

**3.3.7 Example.** Consider the theory of groups whose axioms are exactly the group axioms so that a model of this theory is just any group. The theory of groups is not complete because of the existence of commutative and non-commutative groups, so the sentence

$$\psi \equiv \forall x \forall y (x * y = y * x)$$

is a sentence for which the theory of groups $T$ has the property that neither $T \models \psi$ nor $T \not\models \psi$.

We can modify this theory to be complete as follows:

If we add the following axioms to the theory:

1. The first axiom is $\exists x \exists y (x \neq y \wedge x \neq 1 \wedge y \neq 1)$ which shows the existence of two different elements with the identity.
2. The second axiom is $\forall x \forall y (x = 1 \vee y = 1 \vee x * y = 1)$ which shows that each of the two elements different from the identity is inverse of the other.

Now, the only model of this modified theory is the cyclic group of order $3$, thus for any sentence $\psi$ in the language of groups, we have either $T \models \psi$ or $T \not\models \psi$ and hence the modified theory is now complete theory.

## 3.4 Model-Completeness

In this section. we introduce the concept of model-completeness which is one of the immediate consequences of the quantifier elimination property.

**3.4.1 Definition.** Marker (2002) An $\mathcal{L}$-theory $T$ is model-complete if all the embeddings are elementary embeddings, this means that if $\mathcal{M}$ and $\mathcal{N}$ are any two models of $T$ such that $\mathcal{M} \subseteq \mathcal{N}$, then $\mathcal{M} \preceq \mathcal{N}$.



**3.4.2 Theorem.** *Marker (2002) If an $\mathcal{L}$-theory $T$ admits the quantifier elimination property, then $T$ is model-complete.*

*Proof.* To show that $T$ is a model-complete theory, we need to show that if $\mathcal{M}$ and $\mathcal{N}$ are two models of $T$ such that $\mathcal{M} \subseteq \mathcal{N}$, then $\mathcal{M} \preceq \mathcal{N}$ which means that $\mathcal{M}$ is an elementary substructure of $\mathcal{N}$.

Let $\mathcal{M}$ and $\mathcal{N}$ are two models of the theory $T$ which has quantifier elimination where $\mathcal{M} \subseteq \mathcal{N}$ and $\phi(\bar{x})$ be any $\mathcal{L}$-formula with $\bar{a}$ in $M$. Because of quantifier elimination, there exists a quantifier-free formula $\psi(\bar{x})$ with the property that

$$\mathcal{M} \models \phi(\bar{a}) \text{ if and only if } \mathcal{M} \models \psi(\bar{a}). \tag{3.4.1}$$

Since quantifier-free formula are preserved under extension, we have

$$\mathcal{M} \models \psi(\bar{a}) \text{ if and only if } \mathcal{N} \models \psi(\bar{a}). \tag{3.4.2}$$

Therefore, from (3.4.1) and (3.4.2), we obtain that

$$\mathcal{M} \models \phi(\bar{a}) \text{ if and only if } \mathcal{N} \models \phi(\bar{a}) \tag{3.4.3}$$

which shows that $\mathcal{M} \preceq \mathcal{N}$ and hence $T$ is model-complete. □

**3.4.3 Remark.** Marker (2002) The converse of Theorem (3.4.2) is not necessarily true, so there is an $\mathcal{L}$-theory which is model-complete and does not have the quantifier elimination, we can consider the theory of ACFA as an example. We give the definition of ACFA in the following

**3.4.4 Definition.** Kamensky (2009) A difference field is the pair $(K, \sigma)$ where $K$ is a field and $\sigma$ is an endomorphism of $K$. A difference field $(K, \sigma) \models$ACFA if and only if the following conditions hold:

1. The field $K$ is an ACF.
2. The endomorphism $\sigma$ is an automorphism.
3. If $V$ is an irreducible variety over $K$, and if $V^\sigma$ is the image of $V$ under $\sigma$, and if $S$ is an irreducible closed subvariety of $V \times V^\sigma$ such that the projection maps $S \to V$ and $S \to V^\sigma$ are dominate, and if $T$ is a proper closed subvariety of $S$, then there exists some $v$ in $V$ with $(v, \sigma(v))$ in $S \setminus T$.

**3.4.5 Example.** The theory of DLO (discrete linear orders) with a bottom but no top is not model-complete since we can find two models $\mathcal{M}$ and $\mathcal{N}$ such that $\mathcal{M} \subseteq \mathcal{N}$ but $\mathcal{M} \not\preceq \mathcal{N}$ as follows:

Consider the two models $\mathbb{Z}_{\geq 1}$ and $\mathbb{Z}_{\geq 0}$ where $\mathbb{Z}_{\geq 1} \subseteq \mathbb{Z}_{\geq 0}$, if we take the sentence $\phi(y) \equiv \exists x(x < y)$, then $\mathbb{Z}_{\geq 0} \models \phi(1)$ while $\mathbb{Z}_{\geq 1} \not\models \phi(1)$. Therefore $\mathbb{Z}_{\geq 1} \not\preceq \mathbb{Z}_{\geq 0}$, this means that there exists substructure which is not elementary, and hence the theory is not model-complete.

Note that for the language $\mathcal{L} = \{<, f, =\}$ where $<$ and $=$ are 2-arity relation symbols with a single unary successor function symbol $f$, we define the theory of DLO (discrete linear orders) by the following axioms:

1. $\forall x(x \not< x)$.
2. $\forall x \forall y(x < y \vee x = y \vee y < x)$.
3. $\forall x \forall y \forall z(x < y \wedge y < z \to x < z)$.
4. $\forall x \forall y(x < y) \leftrightarrow s(x) = y \vee s(x) < y$ (Every non-maximal element has a successor).
5. $\forall x \exists y(x = s(y))$ (Every non-minimal element has a predecessor).

# 4. Model Theory of ACF

In this chapter, our goal is to introduce a suitable language $\mathcal{L}$ for the algebraically closed fields to discuss some properties of the algebraically closed fields such as quantifier elimination, completeness and model-completeness. The main results in this chapter can be found in Marker (2002).

## 4.1 ACF Language

In this section, we introduce a suitable language to the theory of algebraically closed fields.

**4.1.1 Definition.** Let $\mathcal{L}_r = \{+, \cdot, 0, 1\}$ be the language of rings, where $+$ and $\cdot$ are function symbols with arity equal 2 and $0$ and $1$ are two constant symbols. The ring axioms are given by the following:

1. Addition is associative

   $\forall x \forall y \forall z((x + y) + z = x + (y + z))$.

2. Multiplication is associative

   $\forall x \forall y \forall z((x \cdot y) \cdot z = x \cdot (y \cdot z))$.

3. Addition is commutative

   $\forall x \forall y(x + y = y + x)$.

4. Distributive law

   $\forall x \forall y \forall z(x \cdot (y + z) = x \cdot y + x \cdot z)$.

5. Additive inverse

   $\forall x \exists y(x + y = 0)$.

6. Additive identity

   $\forall x(x + 0 = x)$.

7. Multiplicative identity

   $\forall x(x \cdot 1 = x)$.

8. Integral domain property

   $\forall x \forall y(x \cdot y = 0 \implies x = 0 \vee y = 0)$.

   If we add the following two axioms we obtain the theory of fields.

9. Multiplication is commutative

   $\forall x \forall y(x \cdot y = y \cdot x)$.

10. Multiplicative inverse property

    $\forall x \exists y(x = 0 \vee x \cdot y = 1)$

So any set $K$ satisfying the previous axioms is a field and we say it models a field, written as $K \models$field.

**4.1.2 Definition.** If we add the following algebraically closed property that every non-constant polynomial has a zero to the axioms of fields, we obtain the algebraically closed field axioms

$$\forall x_1 \ldots \forall x_n \exists y(y^n + x_1 y^{n-1} + \cdots + x_n = 0) \text{ where } y^n = \underbrace{y \cdot y \cdot \cdots \cdot y}_{n\text{-times}}.$$

**4.1.3 Definition.** Any set $K$ satisfying the axioms of algebraically closed fields is called a model of ACF and we write $K \models ACF$.

**4.1.4 Remark.** The algebraically closed field theory ACF does not give any information about the characteristic of the ACF models. Let $\phi_n$ be the sentence

$$\forall x[\underbrace{x + x + \cdots + x}_{n\text{-times}} = 0].$$

So let $\text{ACF}_p$ be ACF$\cup\{\phi_p\}$ where $p$ is a prime number and $\text{ACF}_0$ is ACF$\cup\{\neg\phi_n\}$ where $n = 1, 2, 3, \ldots$.

We use $\text{ACF}_p$ to give the theory of algebraically closed fields of characteristic $p$, where $p$ is either a prime number or zero.

## 4.2 Quantifier Elimination for ACF

In the following, we study the quantifier elimination property for $\text{ACF}_p$.

**4.2.1 Example.** The theory of fields does not have the quantifier elimination property.

We prove that by giving the following counter example, let the real field $\mathbb{R}$ and the rational field $\mathbb{Q}$ with the rational field $\mathbb{Q}$ as a common substructure, consider the formula $\psi(b)$ which is $\exists a(a \cdot a = b)$. It is clear that

$$\mathbb{R} \models \psi(3) \text{ while } \mathbb{Q} \not\models \psi(3)$$

Thus from Theorem (3.2.4), $\psi$ has no equivalent quantifier-free formula $\phi$.

**4.2.2 Theorem.** *Marker (2002) The theory of $\text{ACF}_p$ has quantifier elimination property.*

*Proof.* Let $K$ and $L$ be two algebraically closed fields containing $F$ as a common subfield which is the prime subfield of $K$ and $L$.

We will use Corollary (3.2.6) as follows, we will take $\bar{a}$ in $F$, $b$ in $K$ and $\phi(\bar{x}, y)$ is a quantifier free formula such that $K \models \phi(\bar{a}, b)$. If we are able to show the existence of $c$ in $L$ such that $L \models \phi(\bar{a}, c)$ then we are sure that $\text{ACF}_p$ admits quantifier elimination.

Since $\phi(\bar{a}, b)$ is a quantifier free formula, we can rewrite it for simplicity as a disjunctions of conjunctions of atomic formulas, we can write any atomic formula $\theta(x_1, \ldots, x_n)$ in the language of rings $\mathcal{L}_r$ as the polynomial $f(x_1, \ldots, x_n) = 0$ and the negated atomic formulas are of the form $f(x_1, \ldots, x_n) \neq 0$ where $f$ in $\mathbb{Z}[X_1, \ldots, X_n]$ so we can consider $f(\bar{a}, y)$ as a polynomial in the polynomial ring $F[Y]$.

Now, we can express $\phi(\bar{a}, y)$ as follows

$$\phi(\bar{a}, y) \leftrightarrow \bigvee_{j=1}^{k} (\bigwedge_{i=1}^{n} f_i(y) = 0 \wedge \bigwedge_{i=1}^{m} g_i(y) \neq 0).$$

Since we have $K \models \phi(\bar{a}, b)$ then

$$K \models \bigwedge_{i=1}^{n} f_i(b) = 0 \wedge \bigwedge_{i=1}^{m} g_i(b) \neq 0.$$

Now, we have the following two possible cases:

(1) If some of the polynomials $f_i(b)$ are nonzero for some $i \leq m$ then b is algebraic element in $F$, thus $b$ in $\bar{F}$ so which is subset of $L$, thus we can conclude that $b$ in $L$. Hence $L \models \phi(\bar{a}, b)$ and we are done.

(2) If all the polynomials $f_i(b)$ are zero polynomials, we examine $\bigwedge_{i=1}^{m} g_i(b) \neq 0$ so that we can find finitely many zeros because non of the polynomials $g_i(b)$ is zero for every $i$, we call the set of the possible zeros as $A = \{a : g_i(a) = 0\}$. Now, we have $L \setminus A$ is non-empty since $L$ is ACF and by Proposition (2.2.8) ACF are infinite, then there exists an element $c$ in $L \setminus A$ such that $L \models \phi(\bar{a}, c)$ and hence we are done.

□

**4.2.3 Example.** Marker (2002)The following two formulas show how quantifier elimination is useful to transform a quantifier formula into a quantifier-free formula as a disjunction.

1. The formula

$$\psi(b_0, \ldots, b_n) \equiv \exists x(b_0 + \sum_{i=1}^{n} b_i x^i = 0)$$

shows the existence of a zero for the polynomial of $n$ degree with $b_0, \ldots, b_n$ as coefficients, we know that this formula is true in $\mathrm{ACF}_p$ for any non-constant polynomial.

Since $\mathrm{ACF}_p$ has quantifier elimination so we can find a quantifier free formula $\phi$ such that

$$\phi \equiv b_0 = 0 \vee \bigvee_{i=1}^{n} b_i \neq 0 \text{ where } \phi \leftrightarrow \psi.$$

2. The formula

$$\phi(b_0, b_1, b_2) \equiv \exists x \exists y(b_2 x^2 + b_1 x + b_0 = 0 \wedge b_2 y^2 + b_1 y + b_0 = 0) \wedge \neg(x = y)$$

shows the existence of two distinct zeros for the quadratic polynomial with $b_0, b_1, b_2$ as coefficients.

Since $\mathrm{ACF}_p$ has quantifier elimination and the quadratic polynomial has two distinct zeros in $\mathrm{ACF}_p$ if and only if the leading coefficient and the discriminant are not zero. Thus there exists a quantifier-free formula $\psi$ such that

$$\psi \equiv b_2 \neq 0 \wedge {b_1}^2 - 4b_2 b_0 \neq 0 \text{ where } \phi \leftrightarrow \psi.$$

## 4.3 Completeness for ACF

In the following, we study the completeness property for $\mathrm{ACF}_p$.

**4.3.1 Remark.** The theory of algebraically closed fields is not complete because it does not decide the characteristic.

**4.3.2 Theorem.** *Marker (2002) The theory of $\mathrm{ACF}_p$ is a complete theory.*

*Proof.* To prove the completeness of $\mathrm{ACF}_p$, we will try to prove that any two models for $\mathrm{ACF}_p$ are elementarily equivalent which means that if $K$ and $L$ are two $\mathrm{ACF}_p$ models and $\phi$ be any sentence then $K \models \phi$ if and only if $L \models \phi$.

Now, if we suppose that $K \models \mathrm{ACF}_p$ and $L \models \mathrm{ACF}_p$, let $\phi$ be any sentence in the language $\mathcal{L}_r$. Since $\mathrm{ACF}_p$ has quantifier elimination property so there exists a quantifier free formula $\psi$ with the property that

$$\mathrm{ACF}_p \models \phi \leftrightarrow \psi. \tag{4.3.1}$$

By Proposition (2.2.8) we know that $\mathrm{ACF}_p$ must be infinite field, also by Theorem (2.1.4) we have that both $K$ and $L$ have a prime subfield $F$ which is either isomorphic to the field of rationals $\mathbb{Q}$ or the field $\mathbb{Z}_p$ so we can take the field $F$ as a common subfield of $K$ and $L$.

Since quantifier-free formula are preserved under substructure, so

$$K \models \psi \text{ if and only if } F \models \psi. \tag{4.3.2}$$

Because quantifier-free formula are preserved under extension and we have that $L$ is an extension of $F$, so

$$F \models \psi \text{ if and only if } L \models \psi. \tag{4.3.3}$$

From (4.3.2) and (4.3.3), we observe that

$$K \models \psi \text{ if and only if } L \models \psi. \tag{4.3.4}$$

Finally, from (4.3.1) and (4.3.4) we obtain that

$$K \models \phi \text{ if and only if } L \models \phi \tag{4.3.5}$$

which means that any two $\mathrm{ACF}_p$ models are elementarily equivalent $K \equiv L$ and hence $\mathrm{ACF}_p$ is complete. □

**4.3.3 Theorem.** *The theory of $\mathrm{ACF}_p$ is model-complete.*

*Proof.* The model-completeness of $\mathrm{ACF}_p$ is just a consequence of Theorem (3.4.2) and (4.2.2). □

# 5. Ax-Grothendieck Theorem

In this Chapter, we introduce the Ax-Grothendieck theorem which gives a relation between injectivity and surjectivity of the polynomial map in a finite dimensional complex space. It was proved independently by James Ax and Alexander Grothendieck in the middle of the 19th century, Rudin also gave a proof of this theorem using the topological structure. The main results in this chapter are mainly from [Magner], [Hils and Loeser], and [Marker et al.].

## 5.1 Algebraic Ax-Grothendieck

**5.1.1 Definition.** Magner Let $K$ be a field and $n$ be a natural number, a map $f : K^n \to K^n$ is a polynomial map if there exist polynomials $f_1, \ldots, f_n$ in $K[x_1, \ldots, x_n]$ such that

$$f(x_1, \ldots, x_n) = (f_1(x_1, \ldots, x_n), \ldots, f_n(x_1, \ldots, x_n)).$$

This means that the individual map in one coordinate consists of polynomials in $n$ variables, so that $f$ is a collection of $n$ polynomials in $K[x_1, \ldots, x_n]$.

**5.1.2 Theorem.** *Hils and Loeser (2019) If $f : \mathbb{C}^n \to \mathbb{C}^n$ is an injective polynomial map, then $f$ is bijective.*

In the case of $n = 1$, the theorem can be easily proved as follows.

**5.1.3 Proposition.** Magner If $f : \mathbb{C} \to \mathbb{C}$ is an injective polynomial map, then $f$ is bijective.

*Proof.* Assume that $f$ is injective, then it is non constant polynomial. Therefore, for any number $a$ in $\mathbb{C}$, we have $f(z) - a$ is a non-constant polynomial. By using the fundamental theorem of algebra [2.2.9], the polynomial $f(z) - a$ has a zero in $\mathbb{C}$ which means that $f(z) - a = 0$ for some $z$ in $\mathbb{C}$ and hence $f$ is surjective map. □



We can study the Ax-Grothendieck theorem as an extension of the fundamental theorem of algebra, so we will start with the algebraic version of Ax-Grothendieck as follows:

The following shows that Ax-Grothendieck is true within any finite field.

**5.1.4 Proposition.** Magner If $f : K^n \to K^n$ is an injective polynomial map where $K$ is a finite field and $n$ is a natural number, then $f$ is bijective.

*Proof.* The proof of this theorem is clear and it depends on the set-theoretic fact which states that any injective map from a finite set to itself is necessarily bijective. □

**5.1.5 Remark.** We use $f(\vec{x})$ to express the polynomial map $f(x_1, \ldots, x_n)$ in $K[x_1, \ldots, x_n]$, similarly we use $f(\vec{x}, \vec{y})$ to express the polynomial map $f(x_1, \ldots, x_n, y_1, \ldots, y_n)$ in $K[x_1, \ldots, x_n, y_1, \ldots, y_n]$.

We use Hilbert's Nullstellenstaz theorem to check the injectivity and surjectivity properties of polynomials as algebraic statements as follows:

**5.1.6 Theorem.** *Hils and Loeser (2019) Let $K$ be an ACF. If $f_1, \ldots, f_n$ in $K[x_1, \ldots, x_n]$ vanishes at all the points for which $\{g_i\}$ in $K[x_1, \ldots, x_n]$ vanish, then there exist a polynomial $Q_i$ and $r \geq 1$ such that $\sum_{i=1}^{n} g_i Q_i = f^r$*

*Proof.* The proof of this theorem is in [Hils and Loeser] Theorem 3.5.5.

□

**5.1.7 Lemma.** Magner If $K$ is an ACF, a polynomial map $f : K^n \to K^n$ with $f = (f_1, \ldots, f_n)$ is injective if and only if there exists a polynomial $Q_{i,j}$ in $K[x_1, \ldots, x_n, y_1, \ldots, y_n]$ and natural number $r_j$ such that

$$\sum_{i=1}^{n} (f_i(\vec{x}) - f_i(\vec{y}))Q_{i,j}(\vec{x}, \vec{y}) = (x_j - y_j)^{r_j} \quad \text{for all } 1 \leq j \leq n.$$

*Proof.* Firstly, suppose that $f$ is injective, this means that if $f_i(\vec{x}) - f_i(\vec{y}) = 0$ for all $i$, then $\vec{x} - \vec{y} = 0$ which means that $x_j - y_j = 0$ for all $j$. If we fix $j$ and by using the hypothesis of Nullstellensatz (5.1.6), we conclude that the polynomial $x_j - y_j$ vanishes in the same points at which the collection of polynomials $f_i(\vec{x}) - f_i(\vec{y})$ in $K[x_1, \ldots, x_n, y_1, \ldots, y_n]$ vanishes because of injectivity. Hence, by Theorem (5.1.6), we obtain the polynomials $Q_{i,j}$ in

$$\sum_{i=1}^{n} (f_i(\vec{x}) - f_i(\vec{y}))Q_{i,j}(\vec{x}, \vec{y}) = (x_j - y_j)^{r_j}.$$

Conversely,

$$\text{if } \sum_{i=1}^{n} (f_i(\vec{x}) - f_i(\vec{y}))Q_{i,j}(\vec{x}, \vec{y}) = (x_j - y_j)^{r_j},$$

and $f_i(\vec{x}) - f_i(\vec{y}) = 0$ for all $i$.

Thus $x_j - y_j = 0$ for all $j$, this implies that $\vec{x} - \vec{y} = 0$ and hence $f$ is injective. □



**5.1.8 Lemma.** Magner Let $K$ be an ACF. A polynomial map $f : K^n \to K^n$ with $f = (f_1, \ldots, f_n)$ is not surjective if and only if there exists $z$ in $K^n$ and a polynomial $R(\vec{x})$ in $K[x_1, \ldots, x_n]$ such that $(f(\vec{x}) - z)R(\vec{x}) = 1$. We use $1$ as a notation to express $(1, \ldots, 1)$.

*Proof.* Firstly, suppose that $f$ is not surjective, so there exists $z$ in $K^n$ such that $f(\vec{x}) - z \neq 0$ for any $\vec{x}$ in $K^n$. Now, by using the Nullstellensatz Theorem (5.1.6) for the constant polynomial $1$, we can obtain a polynomial $R(\vec{x})$ in $K[x_1, \ldots, x_n]$ such that $(f(\vec{x}) - z)R(\vec{x}) = 1$.

Conversely, if there is an element $z$ in $K^n$ and a polynomial $R$ in $K$ such that $(f(\vec{x}) - z)R(\vec{x}) = 1$, then $f(\vec{x}) \neq z$ for all $\vec{x}$ in $K^n$, therefore $f$ is not surjective. □

The following show that the Ax-Grothendieck theorem is true within the algebraic closure $\bar{K}$ of a finite field $K$.

**5.1.9 Theorem.** *Magner Let $K$ be a finite field with $\bar{K}$ as its algebraic closure. If $f : \bar{K}^n \to \bar{K}^n$ is an injective polynomial map, then $f$ is bijective.*

*Proof.* Suppose contrarily that $f : \bar{K}^n \to \bar{K}^n$ is a polynomial map which is injective and not surjective. Since $f$ is injective, we can use Lemma (5.1.7) as follows. The system $f(\vec{x}) = f(\vec{y})$ where $\vec{x} \neq \vec{y}$ has no solution over the ACF $\bar{K}$ so by Lemma (5.1.7), there is a natural number $r$ and a polynomial $Q : \bar{K}^n \times \bar{K}^n \to \bar{K}^n$ such that

$$(f(\vec{x}) - f(\vec{y}))Q(\vec{x}, \vec{y}) = (\vec{x} - \vec{y})^r. \tag{5.1.1}$$

Similarly, because of non surjectivity of $f$, compared to Lemma (5.1.8), there exists an element $z$ in $\bar{K}^n$ such that $f(x) = z$ has no solution over the ACF $\bar{K}$. So there exists a polynomial $R : \bar{K}^n \to \bar{K}^n$ such that

$$(f(\vec{x}) - z)R(\vec{x}) = 1. \tag{5.1.2}$$

If we fix $Q$, $z$, and $R$ as above and let $k$ be the field generated by $K$ and the coefficients of all the polynomials $f$, $Q$, $R$, and $z$ where $k$ is a subfield of $\bar{K}$. Now by Lemma (5.1.7) and Lemma (5.1.8), we observe that $f$ is descended from $\bar{K}$ to $k$, thus $f : k^n \to k^n$ is an injective polynomial map which is not surjective. Since $k$ is finitely generated and all the elements of $k$ are algebraic over the field $k$, hence $k$ is finite and this is a contradiction with Proposition (5.1.4). □

## 5.2 Ax-Grothendieck in Model Theory

In this section, we introduce a proof of the Ax-Grothendieck theorem in model theory using first-order logic, the results of this section are mainly from Marker et al. (2017) and Hils and Loeser (2019).

The following theorem is called Lefschetz's principle.

**5.2.1 Theorem.** *Marker et al. (2017) If $\phi$ be any sentence in the language of rings, then the following are equivalent:*

1. $\mathbb{C} \models \phi$ *which means that $\phi$ is true in the complex field $\mathbb{C}$.*
2. $ACF_0 \models \phi$ *which means that $\phi$ is true in every ACF with characteristic $0$.*
3. $ACF_0 \models \phi$ *which means that $\phi$ is true in some ACF with characteristic $0$.*
4. $ACF_p \models \phi$ *for arbitrary large primes $p$ which means that there exists $n$ such that for all $p > n$ such that $\phi$ is true is some ACF with characteristic $p$.*
5. $ACF_p \models \phi$ *for sufficiently large primes $p$ which means that there exists arbitrary large prime $p$ where $\phi$ is true in some ACF with characteristic $p$.*

*Proof.* It is clear that $(1)$, $(2)$ and $(3)$ are equivalent by the completeness of $\mathrm{ACF}_0$ as proved in Theorem (4.3.2).

The two statements $(4)$ and $(5)$ are clearly equivalent because of the completeness of $\mathrm{ACF}_p$. For $(2)$ to $(5)$, if we suppose that $\mathrm{ACF}_0 \models \phi$ so by Lemma (3.1.22), there is a finite subset $A$ of $\mathrm{ACF}_0$ such that $A \models \phi$, if we choose $p$ large enough, then $\mathrm{ACF}_p \models A$. Hence, $\mathrm{ACF}_p \models \phi$ for sufficiently large prime $p$.

Finally, for $(4)$ to $(2)$, suppose that $\mathrm{ACF}_0 \not\models \phi$. Since $\mathrm{ACF}_0$ is complete, then $\mathrm{ACF}_0 \models \neg\phi$ and by Lemma (3.1.22), there is a finite subset $A$ of $\mathrm{ACF}_0$ such that $A \models \neg\phi$. So if we choose $p$ large enough, we obtain that $\mathrm{ACF}_p \models A$ and hence $\mathrm{ACF}_p \models \neg\phi$ which means that $\mathrm{ACF}_p \not\models \phi$ by completeness theorem. □

**5.2.2 Theorem.** *Hils and Loeser (2019) Let $K$ be an ACF$_0$ and $n > 0$ is a natural number. If $f : K^n \to K^n$ is an injective polynomial map, then $f$ is bijective.*

*Proof.* Let $f : K^n \to K^n$ be a polynomial map and the coefficients of $f$ be in the algebraic closure of $K$ which is $K$, so there exists a formula $\phi(x_1, \ldots, x_n, y_1, \ldots, y_n)$ such that for all $a_1, \ldots, a_n, b_1, \ldots, b_n$ in $K$ where

$$K \models \phi(a_1, \ldots, a_n, b_1, \ldots, b_n) \text{ if and only if } f(a_1, \ldots, a_n) = (b_1, \ldots, b_n).$$

We can express the injectivity $\phi_{\text{inj}}$ as the following formula:

$$(\forall x_1, \ldots, x_n \forall x'_1, \ldots, x'_n \forall y_1, \ldots, y_n)(\phi(x_1, \ldots, x_n, y_1, \ldots, y_n) \wedge \phi(x'_1, \ldots, x'_n, y_1, \ldots, y_n) \to \bigwedge_{i=1}^{n} (x_i = x'_i)).$$

Similarly, we can express surjectivity $\phi_{\text{surj}}$ as the following formula:

$$(\forall y_1, \ldots, y_n \exists x_1, \ldots, x_n)\phi(x_1, \ldots, x_n, y_1, \ldots, y_n).$$

Now, our goal is to show that

$$\text{ACF}_0 \models (\phi_{\text{inj}} \to \phi_{\text{surj}}).$$

By using Lefchetz's principle, it is sufficient to show that ACF$_p \models (\phi_{\text{inj}} \to \phi_{\text{surj}})$.

If we fix a prime $p$ and a field $F \models$ACF$_p$. Consider $L = acl(\emptyset)$, since $L$ generated by the empty set $\emptyset$ so it is an isomorphic copy of $\mathbb{F}_p$, then $L \models$ACF$_p$. Since ACF$_p$ is complete theory as stated in Theorem (4.3.2), it is enough to show that $L \models (\phi_{\text{inj}} \to \phi_{\text{surj}})$.

Assume that $L \models \phi_{\text{inj}}$ and let $b_1, \ldots, b_n$ in $L$ are parameters, we need to find $a_1, \ldots, a_n$ such that $L \models \phi(a_1, \ldots, a_n, b_1, \ldots, b_n)$ to prove surjectivity. We have that each $b_i$ is algebraic over the empty set $\emptyset$, since the field generated by $\emptyset$ is an isomorphic copy of $\mathbb{F}_p$ which is finite, so iterating by Corollary (2.1.24), there is a finite field $L_0$ which is subfield of $L$ and contains $b_1, \ldots, b_n$. Therefore the restriction $g$ of the map defined by $\phi$ is a map from $L_0^n$ to $L_0^n$ where $g$ is injective and $L_0^n$ is finite, hence by Proposition (5.1.4), $f$ is bijective. □



**5.2.3 Theorem.** *Marker et al. (2017) If $f : \mathbb{C}^n \to \mathbb{C}^n$ is an injective polynomial map, then $f$ is bijective where $n$ is a positive natural number.*

*Proof.* The proof of this theorem is an instant consequence of Theorems (5.2.1) and (5.2.2). □

## 5.3 Application

The results of this section are mainly from Adamatzky (2018). One of the interesting applications of the Ax-Grothendieck theorem is studying the cellular automaton concept.

Cellular automaton provided a potential solution and is a popular technique to model the dynamics of many processes, since they can predict complex space pattern dynamic evolution using some simple rules. Cellular automaton has been used in different areas of science, for example physics, theoretical biology, and microstructure modeling.

**5.3.1 Definition.** A cellular automaton is a non-linear dynamical system in which space and time are discrete, it consists of a regular grid in which every cell occupied a specific state, and there are some rules for the configuration to pass between different states.

**5.3.2 Definition.** An initial state of the grid is stated at time 0 by assigning a state for each cell.

**5.3.3 Remark.** Note that the rule of configurations is the same for all the cells and does not change by time, and a sequence of configurations is called pattern.

**5.3.4 Definition.** For a given cell, we call all the cells that can be reached from this cell by the rules of configuration as its neighbors.

**5.3.5 Example.** An example of cellular automaton is Conway's Game of Life.

**5.3.6 Definition.** A state in a cellular automaton is called a "Garden of Eden" if this state can not be reached from a previous state following the rules, in other words it is a state that can only occur in generation 0.

**5.3.7 Definition.** A two finite patterns are twins if one can be substituted for the other whenever it appears in any sequence of applications of the rules without changing in the future states.

**5.3.8 Theorem.** *(Garden of Eden theorem)*

1. *A cellular automaton is injective if every pair of distinct configurations of the automaton remain different after a step of the automaton.*
2. *A cellular automaton is surjective if it has no Garden of Eden configuration, in other words, if every configuration has a predecessor.*

*Proof.* The proof of this theorem is in [Adamatzky]. □

**5.3.9 Corollary.** Every injective cellular automaton is bijective

*Proof.* The proof of this theorem is in [Adamatzky]. □



The Ax-Grothendieck theorem can be used to verify important results in cellular automaton such as the Garden of Eden theorem, a result which is similar to the Ax-Grothendieck theorem that gives a relation between injectivity and surjectivity but in cellular automaton. The direct proof of these results is already known but the proof by the Ax-Grothendieck theorem can be extended to automaton acting on amenable groups which is important mathematical objects inside the concept of cellular automaton.

## 5.4 Conclusion

In summary, the theory of algebraically closed fields has various important model-theoretic results such as quantifier elimination, and model-completeness as an instant consequence of the quantifier elimination property. Also, the theory of algebraically closed fields is not complete but once we decide the characteristic we obtain the theory of $\mathrm{ACF}_p$ which is complete theory. Every injective polynomial map within an n-dimensional complex space is bijective.

## 5.5 Future Work

There is much work to investigate the field of complex numbers from the model-theoretic aspect. As a future work, we are going to study the field of complex numbers with an additional predicate added to the language to define the subfield of algebraic numbers. This more complicated structure does not have quantifier elimination. However, every formula is equivalent to a finite boolean combination of existential formulas. We are going to prove this with a version of the back and forth argument.

# Acknowledgements

I would like to thank my supervisors Dr. Gareth Boxall and Dr. Charlotte Kestner for their continuous support, encouragement and most helpful comments. Their guidance showed me the right way in all the time during my work under their supervision.

A sincere gratitude goes to the whole family at AIMS as lecturers, tutors and staff for this fruitful period of my life, indeed I have learned a lot in this place, I would like to come back again of course. A special thank goes to Prof. Barry Green, Prof. Jeff Sanders, the academic director Dr. Simukai Utete, she is doing a great job at AIMS regarding all the students and to Jan Groenewald the brain of technology at AIMS.

I would also like to thank Dr. Prudence Djagba for his great effort, he is not just a tutor he is a helpful person, I appreciate his effort for me during my stay at AIMS.

I am grateful for my father Prof. Salah El-Din Hussein, I appreciate all what he is doing for me. My words could never express my gratitude to you.

It is my pleasure to thank my friend Dr. Mohamed Anwar who suggested me to study at AIMS, he always guide me and helped me a lot.

A special thanks goes to my beautiful friend Fameno Rakotoniaina for her continuous support.

Finally, I am especially grateful to my family, my parents, Omnia, Mahmoud and Yossif whom have loved me unconditionally and always support me. To my mother, there is no enough words to express how you are making my life better, everything without you would be tough.

# References


Adamatzky, A. *Cellular Automata: A Volume in the Encyclopedia of Complexity and Systems Science*. Springer, 2018.

Boxall, G. *Model Theory Lecture Notes*. University of Stellenbosch, 2017. Unpublished manuscript.

Deloro, A. *Basic Model Theory of Algebraically Closed Fields*. Moscow Higher School of Economics, 2013.

Fraleigh, J. B. *A first course in abstract algebra*. Pearson Education India, 2003.

Hils, M. and Loeser, F. *A First Journey Through Logic*, volume 89. American Mathematical Soc., 2019.

Hungerford, T. *Algebra*. Texts in Math. 73. Springer, New York, 1980.

Kamensky, M. *Model Theory of Difference Fields*. Notre-Dame University, USA, 2009.

Lang, S. *Algebra*. Graduate texts in mathematics. Springer, 2002.

Magner, R. *What is the Ax-Grothendieck Theorem?* Eastern Connecticut State University.

Marker, D. *Model theory: an introduction*, volume 217. Springer Science & Business Media, 2002.

Marker, D., Messmer, M., and Pillay, A. *Model theory of fields*, volume 5. Cambridge University Press, 2017.

Stewart, I. N. *Galois theory*. CRC Press, 2015.

Tent, K. and Ziegler, M. *A course in model theory*, volume 40. Cambridge University Press, 2012.