國立交通大學

應用數學系

碩士論文

On Decidable Fragments of Theories in Field Arithmetic

體算術理論中的可判定句型

研究生 ： 林俊佑

指導教授 ： 董世平 教授 / 翁志文 教授

中華民國一百零七年六月

On Decidable Fragments

# of Theories in Field Arithmetic

體算術理論中的可判定句型

Student: Chun-Yu Lin Advisor: Shih-Ping Tung
Chih-Wen Weng

研究生: 林俊佑 指導教授：董世平 教授
翁志文 教授

國立交通大學

應用數學系

碩士論文

A Thesis
Submitted to Department of Applied Mathematics
College of Science
National Chiao Tung University
in Partial Fulfillment of Requirements
for the Degree of Master
in Applied Mathematics

June 2018
Hsinchu, Taiwan, Republic of China

中華民國一百零七年六月

體算術理論中的可判定句型

研究生：林俊佑　　　　指導教授：董世平 教授
翁志文 教授

國立交通大學

應用數學系

摘 要

在本論文中，我們給出在存在封閉的條件下於數體中為真的 $\forall^n\exists$ 句型的保持定理之證明，我們證明在特徵數零與完美希爾伯特體中的 $\exists\forall$ 理論皆是可判定的，我們也證明了在特徵數零中的希爾伯特體、擬代數封閉域、一般希爾伯特體及一般擬代數封閉域中的 $\forall\exists$ 理論皆為可判定的。

關鍵詞：可判定句型、希爾伯特體、擬代數封閉域。

On Decidable Fragments of Theories in Field Arithmetic

Student: Chun-Yu Lin   Advisor: Shih-Ping Tung / Chih-Wen Weng

Department of Applied Mathematics

National Chiao Tung University

Abstract

In this thesis, we prove the preservation theorem of $\forall^n\exists$ sentences over number fields under existentially closedness. We show that the $\exists\forall$ theories of Hilbertian fields with characteristic 0 and perfect Hilbertian fields are both decidable. We also prove that the $\forall\exists$ theories of Hilbertian fields with characteristic 0, Hilbertian fields, PAC fields with characteristic 0, and PAC fields are all decidable.

Keywords: Decidable Fragments, Hilbertian fields, PAC fields.

Acknowledgement

Many people have helped toward the writing of this thesis. I would first like to thank my thesis advisors, Professor Shih-Ping Tung and Professor Chih-Wen Weng. Professor Tung taught me logic and bring me to the research of decision problems. This thesis would not be complete without his patient guidance. Professor Weng gives me many valuable suggestions and supports me during my graduate studies. Also, I would like to thank Professor Ming-Hsuan Kang for his constantly answering my questions and fruitful discussions about algebraic number theory and field theory. I have greatly appreciated the crucial suggestions provided by Professor Moshe Jarden who is the expert in Field Arithmetic.

I would also like to thank my friends: Mr. Yung-Jie Hsieh, Jing-Jia Kao, and Der-Ming Dung. Without them, the time throughout my years of study would be dull. Finally, I would like to express my gratitude to my parents and my elder sisters for theircontinuous encouragements. Thank you.

Chun-Yu Lin, Hsinchu, Taiwan
June, 2018

Contents

Chapter 1

Introduction

In mathematics, we often face problems take the form: find an effective procedure by means of which it can be determined in finitely many steps for each element of our interested set, whether or not the element satisfied the defining property. The solution of such problem usually consists of exhibiting algorithmic-like arguments or proofs to demonstrate that procedure. The problems of this kind are called decision problem or decidability of theories which depends on the set we considered. To be more precise, we give the definition of decision problem as following.

Definition 1.1. Given a mathematical theory $\mathcal{T}$ or a problem $\mathbf{P}$, the decision problem or theory is the about search for the existence of a decision algorithm **AL** which will accomplish the following works:

1. For a sentence ϕ expressed in the language $\mathcal{L}$ of $\mathcal{T}$, **AL** will determine whether ϕ is true in $\mathcal{T}$,i.e. whether $\phi \in \mathcal{T}$.

2. For a instance $\mathcal{I}$ of a problem $\mathbf{P}$, **AL** will produce the correct answer for this instance $\mathcal{I}$, which may be ”YES”,”NO”,an integer,etc.

Example 1.2. We give some examples about decision problems or theories.

1. Word Problems for groups and semigroups (find algorithms to decide whether two words in the generator represent the identical element),

2. Hilbert’s Tenth Problem over commutative ring R (find algorithms to decide whether a given polynomial $f(\overline{x}) \in R[x_1, \ldots, x_n]$ of n-variables has solutions $\overline{a} \in R^n$),

3. Decidability of first order theory of $\mathbb{R}$ (find algorithms to decide whether a given sentence is true in $\mathbb{R}$),

4. Decidability of first order theory of number fields (find algorithms to decide whether a given sentence is true in all number fields).

As in Definition 1.1, if such an algorithm does exist, we shall say that the decision problem of $\mathcal{T}$ or **P** is solvable, or that the theory $\mathcal{T}$ is **decidable**. If no decision algorithm **AL** exists, we call the decision problem of $\mathcal{T}$ or **P unsolvable**, or the theory $\mathcal{T}$ is **undecidable**. The **AL** is called a decision(or effective) procedure for $\mathcal{T}$ or **P**. Since there are computational (or algorithmic) aspect of many mathematical subjects (e.g. numerical analysis[31], computational algebraic geometry[9] and computational algebraic number theory[8], etc.), most of the decision problems in mathematics are solvable. However, there are still some decision problems that are unsolvable. For example, the word problem is unsolvable [5]. Hilbert's tenth problem over $\mathbb{Z}$ and $\mathbb{N}$ are both unsolvable [11]. For the first order theories, the cases are different. In 1931, K. Gödel announced his famous incompleteness theorem which implies that the elementary theory of $\langle \mathbb{N}, +, \cdot, 0, 1\rangle$ and $\langle \mathbb{Z}, +. \cdot, 0, 1\rangle$ are undecidable [17]. On the other hand, C. H. Langford proved in 1927 that the elementary theory of $\langle \mathbb{N}, \leq\rangle$ is decidable [22]. Also, the elementary theory of abelian groups is decidable [37]. There are many elementary theories of various mathematical structure have been proved to be decidable or undecidable since then. We list some theories of fields that will be discussed in this thesis and refer to [12] and [26, Chapter 13 and 16] for exhaustive lists of decidable and undecidable theories.

Theorem 1.3. *The following elementary theories in the language $\mathcal{L}$ are all decidable.*

1. *The elementary theory of $\mathbb{R}$ [40],*
2. *The elementary theory of $\mathbb{Q}_p$, the p-adic field [40],*
3. *The elementary theory of algebraically closed fields of characteristic p for some prime number p or p=0 [1].*

Theorem 1.4. *The following elementary theories in the language $\mathcal{L}$ are all undecidable.*

1. *The elementary theory of fields [34],*
2. *The elementary theory of fields of characteristic 0 [34],*
3. *The elementary theory of algebraic number fields [35],*
4. *The elementary theory of Hilbertian fields [15],*
5. *The elementary theory of PAC fields [7].*

Notice that even if we consider the same domain, different structures may have different decidability of the elementary theories. The results proposed by Gödel and Langford mentioned above are good examples. But for those structures whose elementary theories are undecidable, we may ask the following problem:

Question 1.5. What subsets of undecidable theories are decidable or undecidable ? We try to find the decidable fragments(i.e. dividing line) of decidability of different theories.

Since this thesis mainly focus on decidable fragments of field theories, we only list decidability results about rings and fields in the following paragraphs and in other chapters. For the question 1.5, there are two different approaches: different numbers of quantifier, different kinds of quantifier ($\forall$ or $\exists$). To discuss these two approaches, we need some definition of terminology.

Definition 1.6. Let Q deote the quantifier $\forall$ or $\exists$. We call φ a $Q_1^m Q_2^n$ sentence for $m, n \in \mathbb{N}$ if and only if φ is logically equivalent to a sentence of the form $Q_1 x_1 \cdots Q_1 x_m Q_2 y_1 \cdots Q_2 y_n \varphi'(x_1, \ldots, x_m, y_1, \ldots, y_n)$ where φ' is a quantifier-free formula. We call ψ a $Q_1^m Q_2^n$ equation if and only if ψ is of the form

$$Q_1 x_1 \cdots Q_1 x_m Q_2 y_1 \cdots Q_2 y_n f(x_1, \ldots, x_m, y_1, \ldots, y_n) = 0$$

where f is a polynomial.

For example, Hilbert's Tenth Problem can be formulated in the form of question as: Decide whether or not the set of $\exists^n$ equations for all $n \geq 0$ over $\mathbb{N}$ and $\mathbb{Z}$ are decidable. For sets of $Q_1^m Q_2^n$ sentences, we formulate following definition.

Remark 1.7. In this thesis, we often use the logically equivalent form of $Q_1^m Q_2^n$ sentences for $m, n \in \mathbb{N}$ in the proofs of theorems. Note that logically equivalence of two sentences are **not** decidable in general. But this does not affect the proofs since we only use the model-theoretic properties of $Q_1^m Q_2^n$ sentences rather than the computability of logically equivalent form of $Q_1^m Q_2^n$ sentences in our proofs.

Definition 1.8. Let Q denote the quantifier $\forall$ or $\exists$. We call a subset of elementary theory $Th(K)$ (resp. $Th(\mathbf{K})$) of an mathematical structure K (resp. a class of mathematical structure $\mathbf{K}$) a $Q_1^m Q_2^n$ theory if it consists of $Q_1^m Q_2^n$ sentences which is true in K (resp. true in all mathematical structures in $\mathbf{K}$).

Of course, we can extend the definition for $Q_1^m Q_2^n$ equation and theory to $Q_1^{m_1} \cdots Q_n^{m_n}$ for $m_1, \ldots, m_n \in \mathbb{N}$ and $Q_1, \ldots, Q_n \in \{\forall, \exists\}$ like arithmetical hierarchy in recursion theory. But the there are few results in three or more alternative quantifiers of $Q_1^{m_1} \cdots Q_n m_n$ theory over other algebraic structures than $\mathbb{N}$ and $\mathbb{Z}$. So we mainly consider $Q_1^m Q_2^n$ equation and theory. Notice that if we know that a $Q_1^m Q_2^n$ theory of some mathematical structures (or a class of mathematical structures) is decidable, then so is the set of $Q_1^m Q_2^n$ equations. But if a $Q_1^m Q_2^n$ theory of some mathematical structures (or a class of mathematical structures) is undecidable, it may still happens that the set of $Q_1^m Q_2^n$ equations is decidable. Since Hilbert's tenth problem over $\mathbb{N}$ and $\mathbb{Z}$ are unsolvable, we may ask what is the least n such that the set of $\exists^n$ equations for all $n \geq 0$ over $\mathbb{N}$ and $\mathbb{Z}$ are **undecidable** ? This is the first approach of our question 1.5.

Theorem 1.9. *1. The set of $\exists^n$ equations over $\mathbb{N}$ is undecidable for all $n \geq$ **9** [19].*

*2. The set of $\exists^n$ equations over $\mathbb{Z}$ is undecidable for all $n \geq$ **11** [39].*

Note that the set of $\exists$ equations over $\mathbb{N}$ and $\mathbb{Z}$ are decidable as [23] indicates. Since the decidability of $\exists^2$ equations over $\mathbb{N}$ and $\mathbb{Z}$ are still unknown [11], we still have no answer for $2 \leq n \leq 8$ in the case of $\mathbb{N}$ and for $2 \leq n \leq 10$ in the case of $\mathbb{Z}$. For the second approach, we can separate it into global and local directions.

Definition 1.10. The global and local approach of different quantifier of decidable fragments are defined as following:

1. The global direction: Consider the $Q_1^m Q_2^n$ sentences with m or n (or both) to be ranged over all natural numbers,

2. The local direction: Consider the $Q_1^m Q_2^n$ sentences with m,n to be some fixed natural numbers.

Note that the Π_1^0, Σ_1^0, Π_2^0, and Σ_2^0 sentences in recursion theory are all special cases of above definition.

Theorem 1.11. *We have following results about decidability of the set of $Q_1^m Q_2^n$ equations and in global direction.*

1. *The set of $\exists^n$ equations for all $n \in \mathbb{N}$ over $\mathbb{N}$ and $\mathbb{Z}$ are both undecidable [11]. (For the decidability $\exists^n$ equations with all $n \in \mathbb{N}$ over other commutative rings, see [29]),*

2. *The set of $\forall^n \exists$ equations for all $n \geq 0$ over $\mathbb{Z}$ is decidable but the set of $\forall^n \exists$ equations for all $n \geq 0$ over $\mathbb{N}$ is undecidable. Also, the set of $\forall^n \exists^2$ equations for all $n \geq 0$ over $\mathbb{Z}$ is undecidable [41].*

If we consider the global direction in $Q_1^m Q_2^n$ theory, the results are slightly different.

Theorem 1.12. *For all $m, n \in \mathbb{N}$, we have following results:*

1. *The $\forall^m \exists^n$ theories of $\mathbb{N}$ and $\mathbb{Z}$ are undecidable, respectively [41],*
2. *The $\forall^m \exists^n$ theory of $\mathbb{Q}$ is undecidable [21],*
3. *The $\forall^m \exists^n$ theory of a number field are undecidable [28],*
4. *The $\forall^m$ theories of fields and integral domains are both decidable [27],*
5. *The $\exists^m$ theory of PAC fields is decidable [15].*

Now, for the local direction, we often consider the case in $\forall^m \exists^n$ theories so that the decidability of $\forall^m \exists^n$ equations are determined automatically.

Theorem 1.13. *We have the following results about decidability of $Q_1^m Q_2^n$ theory in global direction.*

1. *The set of $\forall\exists$ equations over $\mathbb{N}$ and $\mathbb{Z}$ are both decidable [20],*
2. *The $\forall\exists$ and $\exists\forall$ theory of $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ and an algebraic number field K are decidable, respectively [42, 43],*
3. *The $\forall\exists$ theory of algebraic number fields, fields of characteristic 0, and fields are decidable, respectively [43],*
4. *The $\forall\exists$ theory of integral domains is decidable [44],*
5. *The $\forall\exists$ theory of algebraic integer rings is decidable [45].*

In this thesis, we first prove the preservation theorem for $\forall^n \exists$ sentence with arbitrary n over an algebraic number field and discuss the possible implication for Hilbert's tenth problem over number fields. Then we show that the $\exists\forall$ theories of Hilbertian fields of characteristic 0 and perfect Hilbertian fields are both decidable. In the last section, we prove that the $\forall\exists$ theories of Hilbertian fields of characteristic 0, Hilbertian fields, PAC fields of characteristic 0, and PAC fields are all decidable.

Chapter 2

Preliminaries and Notations

In this chapter, we introduce the necessary background in model theory, computability theory and field arithmetic to understand to theorems and proofs in this thesis.

2.1 Notation

By $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ we denote the field of rational numbers, the field of real numbers, and the field of complex numbers, respectively. By $\mathbb{N}$,$\mathbb{Z}$ we denote the set of natural numbers, and the ring of integers, respectively. If K is a field, we denote by $\bar{K}$ a fixed algebraic closure of K, by K_s the separable closure of K in $\bar{K}$, and by Gal(K)=Gal(K_s/K) the absolute Galois group of K.

A set is countable if and only if it is countably infinite or finite. We denote $\aleph_0$ by the first infinite cardinal number and ω by the smallest infinite ordinal number.

2.2 Model theory

The basic objects in model theory are formulas, models, and languages. A language is a collection of symbols we use in "everyday" mathematics like analysis, geometry, or algebra. A formula is a string of symbols formulated under some syntactic rules. A structure is a set with an assignment that assign the respective rules of three categories of symbols(function, relation, and constant symbols) under the set. After giving intended meaning of symbols in formulas, we can find structures where these formulas are true. Then we get models. Models are generalization of groups, rings, ordered sets, and other objects in universal algebra. For formal definitions of language, structure, formula, sentence, satisfaction, and proof, see [4] or [13].

In this thesis, we mainly use the **language of rings** is $\mathcal{L} = \mathcal{L}_{ring}$, is a collection of symbols which consists of logical symbols $\langle\neg$(not),$\wedge$(and),$\vee$(or), $\rightarrow$(implies),$\leftrightarrow$(if and only if),$\forall$(for every), $\exists$(there exists),$x_0, x_1, \dots, y, z$(variables) $\rangle$ and $\langle +, -, \cdot, 0, 1\rangle$ as non-logical symbols. If K is an $\mathcal{L}$-structure, and A is a subset of domain of K, denote by $\mathcal{L}_A = \mathcal{L} \cup \{c_a : a \in A\}$ the language $\mathcal{L}$ adding a new constant symbol c_a for each element $a \in A$. It is understood that if $a \neq b$, then c_a, c_b are different symbols. We may then expand the $\mathcal{L}$-structure K to the $\mathcal{L}_A$ structure $K_A = (K, a)_{a \in A}$ by interpreting each new constant symbol c_a by $a \in A$. We give the definitions of two important objects in model theory.

Definition 2.1. An $\mathcal{L}$-theory (or simply, a theory), is a set of sentences of the language $\mathcal{L}$. A **model** of a theory $\mathcal{T}$ is an $\mathcal{L}$-structure M which satisfies all sentences in $\mathcal{T}$, denoted by $M \models \mathcal{T}$. A sentence φ is a **consequence** of a theory $\mathcal{T}$ if every model of $\mathcal{T}$ is a model of φ, denoted by $\mathcal{T} \models \varphi$.

For example, a ring and a field are models of the set of ring or field axioms commonly described in algebra text, respectively. If $\mathcal{K}$ is a class of $\mathcal{L}$-structures, then $Th(\mathcal{K})$ denotes the set of all sentences true in all $\mathcal{L}$-structures of $\mathcal{K}$, and $Th(\{K\})$ is denoted by $Th(K)$. Usually, we called $Th(\mathcal{K})$ the **(elementary) theory** of $\mathcal{K}$.

A class $\mathcal{K}$ of $\mathcal{L}$-structures is said to be an **elementary class** if there exists a theory $\mathcal{T}$ in $\mathcal{L}$ such that $\mathcal{K}$ is exactly the class of all models of $\mathcal{T}$. The class of commutative rings and fields are examples of elementary class.

A theory $\mathcal{T}$ is **inconsistent** if every formula of $\mathcal{L}$ can be deduced from $\mathcal{T}$,i.e. there is a proof for every formula of $\mathcal{L}$ from $\mathcal{T}$. Otherwise $\mathcal{T}$ is **consistent**. If $\mathcal{T}$ is consistent and no set of sentences of $\mathcal{L}$ properly containing $\mathcal{T}$ is consistent, we say $\mathcal{T}$ is **maximal consistent**.

Definition 2.2. An $\mathcal{L}$-theory $\mathcal{T}$ is **complete** if the set of consequences of $\mathcal{T}$ is maximal consistent. In other words, given an $\mathcal{L}$-sentence φ, either $\mathcal{T} \models \varphi$ or $\mathcal{T} \models \neg\varphi$.

If K is an $\mathcal{L}$-structure, then $Th(K)$ is complete. But if $\mathcal{K}$ is a class of $\mathcal{L}$-structures, then $Th(\mathcal{K})$ is not necessarily complete. The theory of class of all fields is not complete. The theory of class of algebraic closed fields of characteristic 0 is complete [10, Example 3.4.3].

Definition 2.3. An $\mathcal{L}$-theory $\mathcal{T}$ is **axiomatizable** if there exists a decidable set of $\mathcal{L}$-sentence $\mathcal{S}$ such that $\mathcal{S}$ and $\mathcal{T}$ have the same consequences. We call $\mathcal{S}$ a set of axioms of $\mathcal{T}$.

The theory of class of all fields is axiomatizable by axioms of fields. However, the theory of class of algebraic number fields is not axiomatizable [35]. Like in abstract algebra, we are also interested in the relation between two structures.

Definition 2.4. Let $\mathcal{A}$ and $\mathcal{B}$ be $\mathcal{L}$-structures. A map $s : \mathcal{A} \to \mathcal{B}$ is an $\mathcal{L}$-**morphism** if for all relation symbols $R \in \mathcal{L}$, function symbols $f \in \mathcal{L}$, and all tuples $\bar{a}, \bar{b} \in \mathcal{A}$, we have: if $\bar{a} \in R^{\mathcal{A}}$, then $s(\bar{a}) \in R^{\mathcal{B}}$; $s(f^{\mathcal{A}}(\bar{b})) = f^{\mathcal{B}}(s(\bar{b}))$.

If the morphism $s : \mathcal{A} \to \mathcal{B}$ is injective and further satisfy the condition that for all relation symbols $R \in \mathcal{L}$ and all tuple $\bar{a} \in \mathcal{A}$, $\bar{a} \in R^{\mathcal{A}} \iff s(\bar{a}) \in R^{\mathcal{B}}$, we say s is an **embedding**. An **isomorphism** between two $\mathcal{L}$-structures $\mathcal{A}$ and $\mathcal{B}$ is a bijective morphism, whose inverse is also a morphism. Also, the concept of embedding in algebra can be generalized to the following concept.

Definition 2.5. Let $\mathcal{A}$ and $\mathcal{B}$ be $\mathcal{L}$-structures. We say that $\mathcal{A}$ is isomorphically embedded in $\mathcal{B}$ if there is a substructure $\mathcal{D}$ of $\mathcal{B}$ such that $\mathcal{A}$ is isomorphic to $\mathcal{D}$.

Definition 2.6. Let $\mathcal{A}$ and $\mathcal{B}$ be $\mathcal{L}$-structures. $\mathcal{A}$ and $\mathcal{B}$ are **elementary equivalent** if every sentence that is true in $\mathcal{A}$ is true in $\mathcal{B}$, and vice versa.

The structure $\langle \bar{\mathbb{Q}}, 0, 1, +, -, \cdot \rangle$ is elementary equivalent to $\langle \mathbb{C}, 0, 1, +, -, \cdot \rangle$ [10, P.139]. If the $\mathcal{L}$-structure $\mathcal{A} \subseteq \mathcal{B}$, then we can give following definition.

Definition 2.7. Let $\mathcal{A}$ and $\mathcal{B}$ be $\mathcal{L}$-structures. We say $\mathcal{B}$ is an **elementary extension** of $\mathcal{A}$ if

1. $\mathcal{A} \subseteq \mathcal{B}$ (i.e. $\mathcal{A}$ is a substructure of $\mathcal{B}$)
2. For any $\mathcal{L}$-formula $\varphi(\bar{x})$ and tuples of elements $\bar{a}$ of domain of $\mathcal{A}$, $\mathcal{A} \models \varphi(\bar{a}) \iff \mathcal{B} \models \varphi(\bar{a})$.

Note that even two $\mathcal{L}$-structures $\mathcal{A}, \mathcal{B}$ are elementary equivalent and $\mathcal{A}$ is a substructure of $\mathcal{B}$, then $\mathcal{B}$ is not necessarily elementary extension of $\mathcal{A}$ (Take $\langle \omega \setminus \{0\}, \leq \rangle$ and $\langle \omega, \leq \rangle$ for example). A consistent theory whose maps between all models are elementary is exceptionally nice theory.

Definition 2.8. A consistent theory $\mathcal{T}$ is said to be **model complete** if for all models $\mathcal{A}$, $\mathcal{B}$ of $\mathcal{T}$, if $\mathcal{A} \subset \mathcal{B}$ then $\mathcal{B}$ is an elementary extension of $\mathcal{A}$.

For example, the theory of algebraically closed fields and real closed fields are both model complete [10, Example 3.5.2]. The concept of prime field in field theory can be generalized to the following concept.

Definition 2.9. A model $\mathcal{A}$ of an $\mathcal{L}$-theory is said to be **algebraically prime** if $\mathcal{A}$ is isomorphically embeddable in every model of $\mathcal{T}$.

For example, $\mathbb{Q}$ and $\mathbb{F}_p$ are algebraically prime model of theory of fields of characteristic 0 and p, respectively. With this concept, we can characterize the complete theory through model complete theory.

Proposition 2.10. *[10, Proposition 3.5.11] Let $\mathcal{T}$ be a model complete theory. If $\mathcal{T}$ has an algebraically prime model then $\mathcal{T}$ is complete.*

For examples about how to use this proposition, see P.197 in [10]. Then we define the model theoretic concept that generalizes the concept of algebraically closed in field theory. This concept will be frequently used in this thesis.

Definition 2.11. Let $\mathcal{A}$ and $\mathcal{B}$ be $\mathcal{L}$-structures. Then $\mathcal{A}$ is **existentially closed** in $\mathcal{B}$ if each existential sentence φ of $\mathcal{L}_A$ which is true in $\mathcal{B}$ is also true in $\mathcal{A}$.

If $\mathcal{A}$ is existentially closed in $\mathcal{B}$, then we have following two important properties which guarantee the existence of structure which is elementary extension of $\mathcal{A}$.

Proposition 2.12. *[30, Lemma 6.27] Let $\mathcal{A} \subseteq \mathcal{B}$ be $\mathcal{L}$-structures. Then $\mathcal{A}$ is existentially closed in $\mathcal{B}$ if and only if $\mathcal{B}$ can be embedded in a structure $\mathcal{A}^*$ for $\mathcal{L}$ which is elementary extension of $\mathcal{A}$.*

Proposition 2.13. *[30, Lemma 6.28] Let $\mathcal{A} \subseteq \mathcal{B}$ be $\mathcal{L}$-structures. Suppose that $\mathcal{A}$ is existentially closed in $\mathcal{B}$ and $\mathcal{A}^*$ is elementarily equivalent to $\mathcal{A}$. Then there exists an existentially closed embedding of $\mathcal{A}^*$ into an $\mathcal{L}$-structure $\mathcal{B}^*$ which is elementarily equivalent to $\mathcal{B}$.*

In the following paragraphs, we investigate the relation of two models under some relations of two theories.

Definition 2.14. Let $\mathcal{T}$ and $\mathcal{U}$ be two theories. If the universal consequences (consequences that are universal sentences) of $\mathcal{T}$ and $\mathcal{U}$ are identical, then we said $\mathcal{T}$ and $\mathcal{U}$ are **cotheories**.

For example, the theory of algebraically closed fields, fields, and integral domains are cotheories of each other. If $\mathcal{T}$ and $\mathcal{U}$ are cotheories, we have following property about models lying above.

Proposition 2.15. *[10, Remark 3.5.6] $\mathcal{T}$ and $\mathcal{U}$ are cotheories if and only if every model of $\mathcal{T}$ can be extended to a model of $\mathcal{U}$, and vice versa.*

If one of the theory $\mathcal{T}$ is model complete, we get following definition.

Definition 2.16. Let $\mathcal{T}$ and $\mathcal{U}$ be two theories. We said $\mathcal{T}$ is a **model companion** of $\mathcal{U}$ if $\mathcal{T}$ is a cotheory of $\mathcal{U}$ and $\mathcal{T}$ is model complete.

For example, the theory of algebraically closed fields and real closed fields are model companions of the theory of fields and ordered fields, respectively. In the last part, we introduce preservation theorem that will be frequently used in this thesis.

Definition 2.17. Let $\mathcal{A}$ be an $\mathcal{L}$-structures. A theory $\mathcal{T}$ is preserved under submodels (resp. extension) if any submodels (resp. extension) of $\mathcal{A}$ is a models of $\mathcal{T}$.

Proposition 2.18. *[10, Corollary 3.2.5] Let $\mathcal{A}$ and $\mathcal{B}$ be $\mathcal{L}$-structures. An $\mathcal{L}$-sentence is preserved under (a) substructures, (b)extensions if and only if it is logically equivalent to a sentence which is (a) universal, (b) existential, respectively.*

2.3 Computability theory

As in the introduction, we have given the informal definition of decision problem in Definition 1.1. However, there is a significant methodological difference between the study of decidability and the study of undecidability of a theory $\mathcal{T}$. The decision problem of a theory $\mathcal{T}$ can be solved by demonstrating a decision algorithm **AL** which is directly recognized and accepted by mathematician as being an effective computational procedure. On the other hand, to establish the undecidability of a theory $\mathcal{T}$, we need formal or precise mathematical meaning of decidability so that we can show that the theory $\mathcal{T}$ is undecidable. With this motivation in mind, the assignment of a rigorous mathematical meaning on decidability involves the notion of recursive function. Let $\mathcal{F}_n$ be the class of all functions from $\mathbb{N}^n$ to $\mathbb{N}$. Denote $\mathcal{F}$ as $\bigcup_{n=1}^{\infty} \mathcal{F}_n$. Among the functions of $\mathcal{F}$, those that suit recursive operation of ”elementary” mathematics are called primitive recursive functions. If we include less ”computable” functions, then we get recursive functions.

Definition 2.19. The set of **primitive recursive functions** is the smallest subset of $\mathcal{F}$ which contain the following functions (called **initial function**):

1. The identical zero function: $f(x) = 0$.
2. The successor function: $S(x) = x + 1$.
3. The projection function: $U_i^n(x_1, \ldots, x_n) = x_i$, for $n \in \mathbb{N}$ and $1 \leq i \leq n$.

and closed under the following operations:

1. Composition: If $g \in \mathcal{F}_m$ and $h_1, \ldots, h_m \in \mathcal{F}_n$ are primitive recursive functions, then the function

$$f(x_1, \ldots, x_n) = g(h_1(x_1, \ldots, x_n), \ldots, h_m(x_1, \ldots, x_n))$$

is also primitive recursive.

2. Primitive recursion: If $f_0 \in \mathcal{F}_n$ and $g \in \mathcal{F}_{n+2}$ are primitive recursive functions, then the function $f \in \mathcal{F}_{n+1}$, which is defined by the following induction,

$$f(x_1, \ldots, x_n, 0) = f_0(x_1, \ldots, x_n)$$

$$f(x_1, \ldots, x_n, y+1) = g(x_1, \ldots, x_n, y, f(x_1, \ldots, x_n, y))$$

is also primitive recursive.

Remark 2.20. *A function is primitive recursive if there is a **derivation**, namely a sequence $f_1, f_2, \ldots, f_k = f$ such that each f_i, $i \leq k$, is either an initial function, or f_i is obtained from $\{f_j : j < i\}$, by an application of Composition or Primitive recursion.*

For example, the constant function, additive function, multiplicative function, and exponential function are all primitive recursive functions. The minimum operator separate recursive and primitive recursive function apart.

Definition 2.21. Let $R(\mathbf{x}, y)$ be an (n+1)-ary relation on $\mathbb{N}$ such that for each $\mathbf{x}$ there exists y for which $R(\mathbf{x}, y)$ is true. Then the **minimum operator** $(\mu y)R(\mathbf{x}, y)$ is the smallest y for which $R(\mathbf{x}, y)$ is true.

Definition 2.22. The family of **recursive functions** is the smallest subset of $\mathcal{F}$ which contains all primitive recursive functions and is closed under composition, primitive recursion, and minimum operator.

For an n-ary relation $R(x_1, \ldots, x_n)$, if the characteristic function of R is primitive recursive (resp. recursive), then we say this relation is primitive recursive (resp. recursive). The definition for a set to be primitive recursive is identical.

Remark 2.23. *If we can decide for each $(\boldsymbol{x}, y)$ whether or not $R(\boldsymbol{x}, y)$ is true, then we can also compute $(\mu y)R(\boldsymbol{x}, y)$ through checking the validity of $R(\boldsymbol{x}, 0)$, $R(\boldsymbol{x}, 0)$,... in order. We can find the smallest y for which $R(\boldsymbol{x}, y)$ is true in finite steps. However, there is no bound for the steps in terms of R and $\boldsymbol{x}$.*

Since our definitions of recursive and primitive recursive function are only valid in $\mathbb{N}$, we need a way to label other symbols with natural numbers so that we can also utilize the concepts to other algorithms. Gödel numbering gives such a numbering. The numbering is an injective map ν from the set of all terms and formulas in a given language $\mathcal{L}$ to $\mathbb{N}$.

Definition 2.24. For an $\mathcal{L}$-theory $\mathcal{T}$, if $\nu(\mathcal{T})$ is recursive (resp. primitive recursive) set, then we said $\mathcal{T}$ is **recursive** (resp. primitive recursive).

We also give the corresponding definition of recursive and primitive recursive functions for computable algebra which will be used in this thesis. Consider a sequence $(\xi_1, \xi_2, \ldots)$ of symbols. We define **polynomial words** inductively: Each elements of $\mathbb{Z}$ and each ξ_i is a polynomial word. If t_1 and t_2 are polynomial words and $n \in \mathbb{Z}$, then $n \cdot t_1$,$(t_1 + t_2)$, and $(t_1 \cdot t_2)$ are polynomial words. We denote the set of formal quotients of polynomial words by Ξ. For example $((3 \cdot \xi_1) + (\xi_2 \cdot \xi_2))/(\xi_2 + (-2 \cdot \xi_2))$ is an element of Ξ. Writing each $n \in \mathbb{N}$ in its decimal form and xi_i as $\xi[i]$, we can view Ξ as a subset of the set Ξ' of all finite strings in the following alphabet

$$\langle \zeta_1, \zeta_2, \ldots, \zeta_{19} \rangle = \langle 0, 1, \ldots, 9, \xi, /, +, \cdot, -, (,), [,] \rangle.$$

Then the Gödel numbering on Ξ' is given by the injective map $\nu : \Xi' \to \mathbb{N}$ defined by

$$\nu(\zeta_{m(1)}\zeta_{m(2)} \cdots \zeta_{m(i)}) = p_1^{m(1)} p_2^{m(2)} \cdots p_i^{m(i)},$$

where $2 < p_1 < p_2 < \cdots$ is the sequence of prime numbers. Restrict ν to Ξ and denote as v, we have $v(\Xi)$ is a primitive recursive subset of $\mathbb{N}$. For each $n \in \mathbb{N}$, let $v^{(n)} : \Xi^n \to \mathbb{N}^n$ be the coordinate function which is n-th power of v. To each function $\rho : \Xi^n \to \Xi$ there corresponds a unique function $\rho' : \mathbb{N}^n \to \mathbb{N}$ such that $\rho' \circ v^{(n)} = v \circ \rho$ and ρ' is identically to 1 on $\mathbb{N}^n \setminus v^{(n)}(\Xi^n)$. We call ρ a primitive recursive function if the corresponding ρ' is primitive recursive function. Similarly, a subset Δ of Ξ^n is primitive recursive if $v^{(n)}(\Delta)$ is primitive recursive. For example, the set $\mathbb{N}$, $\mathbb{Z}$, all sets $\{\xi_i : i \in S\}$ with S a primitive recursive subset of $\mathbb{N}$, and the set Θ of all polynomial words are all primitive recursive (see [15, P.402]).

Definition 2.25. A field K is said to be **presented** if there exists an injective map : $\mu : K \to \Xi$ such that $\mu(K)$ is a primitive recursive subset of Ξ and the following functions over K are all primitive recursive (via μ):

1. additive operation,
2. multiplicative operation,
3. inverse function on $K^\times$,
4. characteristic of K.

For example, $\mathbb{Q}$ and $\mathbb{F}_p$ are presented. Now, let $S = K[X_1, X_2, \ldots]$ with presented field K and Γ be the set of all polynomial words in $X_1, X_2, X_3, \ldots$ with coefficients in Ξ. We can define primitive recursive functions on Γ as above. Since K is presented, we can extend $\mu : K \to \Xi$ to an embedding of S into Γ by mapping each polynomial in S to its canonical form in Γ.

Definition 2.26. An **effective algorithm** over a presented field K is a primitive recursive map $\lambda : A \to B$ where A and B are explicitly given primitive recursive subset of S^n and S^m, respectively.

Definition 2.27. A presented field K is said to have the **splitting algorithm** if K has an effective algorithm for factoring each elements of K[X] into a product of irreducible factors.

Proposition 2.28. *[15, Lemma 19.1.3] The following algorithms are effective:*

1. *Factoring an element of* $\mathbb{Q}[x]$ *into a product of irreducible polynomials,*

2. *Factoring an element of* $K[x_1, \ldots, x_n]$ *in to a product of irreducible factors with K a presented field with a splitting algorithm.*

A presented field K is said to have an **elimination theory** if every finitely generated presented extension F of K has a splitting algorithm. The following proposition tell us which field has elimination theory.

Proposition 2.29. *[15, Corollary 19.2.10] Every presented perfect field K with a splitting algorithm has an elimination theory.*

Given an $\mathcal{L}$-theory $\mathcal{T}$, if we know the characteristic function $\chi_{\nu(\mathcal{T})}$ with given Gödel numbering is primitive recursive, then there must exists a derivation of $\chi_{\nu(\mathcal{T})}$ by Remark 2.20. From this, we obtain a finite set of instructions through translate back each function in the derivation. This set of instructions can decide whether a given sentence θ belongs to $\mathcal{T}$ or not. This is what we call a **decision procedure** (or a decision algorithm **AL** as in Definition 1.1), recursive or primitive as $\mathcal{T}$ is recursive or primitive recursive. This definition also holds for recursive relation or primitive recursive subset δ of Ξ^n as above. The distinction of recursive and primitive recursive procedures lies in the use of minimum operator. Procedures that use only minimum operator which y is bounded by two numbers is primitive recursive.

To decide whether an $\mathcal{L}$-sentence θ belongs to $\mathcal{L}$-theory $\mathcal{T}$ or not, we usually apply a set of instructions for $\mathcal{L}$ to θ to help us. These instructions arise from certain operations by compositions, primitive recursions, and minimizations. The Gödel numbering can translate these operations into recursive operations on $\mathbb{N}$. Theoretically, we inspect these operations on $\mathbb{N}$ to prove the recursiveness of functions, theories or sets. In practice, as P.160 in [15] indicates, we often avoid details steps that show our procedures to be recursive or primitive recursive. Therefore, we rely on a direct analysis of the origin set of instructions on given language $\mathcal{L}$ in this thesis through informal description of decision algorithms **AL**. This is the approach we use to prove primitive recursiveness in this thesis.

2.4 Hilbertian Fields

For basic field theory, we refer to [25]. The polynomial $x^4 + 1 \in \mathbb{Z}[X]$ is irreducible over $\mathbb{Q}$, but it's reducible over $\mathbb{F}_p$. A polynomial $f \in K[X_1, \ldots, X_n]$ over a field K is called **absolutely irreducible** if f is irreducible over $\bar{K}$. Absolute irreducible polynomials behave differently, as the following proposition shows.

Proposition 2.30. *[15, Proposition 9.4.3] Let R be an integral domain and $f \in R[X_1, \ldots, X_n]$ be an absolutely irreducible polynomial. Then for almost all (in the sense of Zariski topology) prime ideals $\mathfrak{p} \in Spec(R)$ the following holds where $\kappa(\mathfrak{p}) = Frac(R/\mathfrak{p})$ denote the quotient field of $R/\mathfrak{p}$: The polynomial f (mod $\mathfrak{p}$) is absolutely irreducible in $\kappa(\mathfrak{p})[X_1, \ldots, X_n]$.*

The Proposition above tell us that the reduction of coefficients conserve absolute irreducibility. However, this is in general no more true for specializing coefficient in the field : An absolutely irreducible polynomial $f \in \mathbb{C}[X, Y]$, monic in Y with $deg_Y(f) > 1$ become reducible polynomial $f(X, \eta) \in \mathbb{C}[X]$ for all $\eta \in \mathbb{C}$. There are fields where this phenomenon does not appear. This is the Hilbertian field named after Hilbert for his work on irreducibility theorem in 1892.

Definition 2.31. Let K be a field. Consider irreducible polynomials $f_1, \ldots, f_m \in K(T_1, \ldots, T_r)[X_1, \ldots, X_n]$ and $0 \neq g \in K[T_1, \ldots, T_r]$. Define a Hilbert subset of K^r as

$$H_K(f_1, \ldots, f_m; g) = \{\mathbf{a} \in K^r : f_i(\mathbf{a}) \text{ is defined and irreducible in } K[\mathbf{X}] \text{ for } i = 1, \ldots, m, \text{and } g(\mathbf{a}) \neq 0\}$$

K is **Hilbertian** if all its Hilbert subsets are nonempty.

This is modern definition of Hilbertian fields. The reason why we need g($\mathbf{a}$) $\neq$ 0 is that we will use this property in the proof of 4.14. People who do research in inverse Galois theory usually use the classical definition which is the three equivalent conditions in the following Theorem. These two definitions are actually equivalent.

Theorem 2.32. *[47, Corollary 1.8] The following conditions on K are equivalent:*

1. *For each irreducible polynomial $f(X, Y)$ in two variables over K, of degree ≥ 1 in Y, there are infinitely many $b \in K$ such that the specialized polynomial $f(b, Y)$(in one variable) is irreducible.*

2. *Given a finite extension F of K, and $h_1(X, Y), \ldots, h_m(X, Y) \in F[X][Y]$ that are irreducible as polynomials in Y over the field $F(X)$, there are infinitely many $b \in K$ such that the specialized polynomials $h_1(b, Y), \ldots, h_m(b, Y)$ are irreducible in $F(Y)$.*

3. *For any $p_1(X,Y),\dots,p_t(X,Y) \in K[X][Y]$ that are irreducible and of degree > 1 when viewed as polynomial in Y over $K(X)$, there are infinitely many $b \in K$ such that none of the specialized polynomials $p_1(b,Y),\dots,p_t(b,Y)$ has a root in K.*

The Hilbertian fields have following properties

Proposition 2.33. *[47, Lemma 1.10] Suppose K is Hilbertian, and $f(X_1,\dots,X_s)$ is an irreducible polynomial in $s \geq 2$ variables over K, of degree ≥ 1 in X_s.*

1. *Then there are infinitely many $b \in K$ such that the polynomial $f(b,X_2,\dots,X_s)$ (in s-1 variables) is irreducible over K.*

2. *For any nonzero $p \in K[X_1,\dots,X_{s-1}]$ there are $b_1,\dots,b_{s-1} \in K$ such that $p(b_1,\dots,b_{s-1}) \neq 0$ and $f(b_1,\dots,b_{s-1},X_s)$ is irreducible (as polynomial in one variable) in X_s.*

The Hilbert irreducibility theorem gives some examples of Hilbertian fields.

Theorem 2.34. *[47, Theorem 1.23] The rational number field $\mathbb{Q}$ is Hilbertian.*

The following crucial theorem tells us how to construct Hilbertian field from any given fields.

Theorem 2.35. *[15, Theorem 13.4.2] Suppose K is a global field or finitely generated transcendental extension of an arbitrary field. Then K is Hilbertian.*

Therefore, number fields and function fields $\mathbb{F}_p(t)$ are all Hilbertian. With the following Proposition, we can also characterize some non-Hilbertian fields.

Proposition 2.36. *[15, Lemma 16.11.5] Let K be a Hilbertian field. Then $Gal(K)$ is not finitely generated.*

Since $Gal(\mathbb{C})$ is trivial, we know that $\mathbb{C}$ is not Hilbertian. $Gal(\mathbb{R})$ is a cyclic group of two elements and hence $\mathbb{R}$ is not Hilbertian. Also, $Gal(\mathbb{F}_p)$ where p is a prime power is the Pr*ü*fer group $\hat{\mathbb{Z}}$. Note that $\hat{\mathbb{Z}}$ is generated by 1. Thus, none of the finite fields is Hilbertian.

2.5 PAC Fields

In field arithmetic, there are two main fields that are under research-Hilbertian fields and PAC fields. In last section, we have introduced Hilbertian fields. Then we will introduce the remaining one. The concept of pseudo algebraically closed field (**PAC**) field was seen by J. Ax in 1967 (see [2]). This concept generalize the property of algebraically closed field that every polynomial has a solution over it.

Definition 2.37. A field F is **pseudo algebraically closed field (PAC)** if every (absolutely irreducible) variety V defined over F has an F-rational point, i.e., a point with all coordinates in F.

For example, separably closed fields, algebraically closed fields are PAC fields [15, Corollay 11.2.4]. We give the following examples of PAC fields constructed from finite fields which is not algebraically closed.

Proposition 2.38. *[14] Infinite algebraic extension of finite fields are PAC fields*

Example 2.39. Let $E = \bigcup_{n=1}^{\infty} \mathbb{F}_{3^{3^n}}$. From P.29 in [6], E is an infinite algebraic extension of $\mathbb{F}_3$ and a splitting field of $\{f(x) \in \mathbb{F}_3[x] :$ deg(f) divides 3^{3^n} with $n \in \mathbb{N}$ and p is irreducible over $\mathbb{F}_3$ $\}$. $x^2 + 1$ is irreducible over $\mathbb{F}_3$ by Gauss Lemma. If $X^2 + 1$ has solutions i on E, i must falls in some finite fields K such that $[K : \mathbb{F}_3] = 2$. But K must be $\mathbb{F}_9$ and there's no such finite subfield in E. Thus, $E \subset \bar{\mathbb{F}_3}$ and E is a PAC field from above Proposition.

Example 2.40. Every nonprincipal ultraproduct of distinct finite fields is a PAC field [3].

Also every algebraic extension of PAC fields are also PAC [15, Corollary 11.2.5]. To characterize PAC field (also Hilbertian field), we need to analysis the corresponding absolute Galois group. For the definitions of inverse system and related topology, see [15, Chapter 1].

Definition 2.41. Consider an inverse system of finite groups $(G_i, \pi_{ji})_{i,j \in I}$ for some directed partially ordered set I, each equipped with the discrete topology and maps $\pi_{ji} : G_j \to G_i$ are continuous homomorphism for all $i, j \in I$. We call the inverse limit $G = \varprojlim G_i$ a profinite group with projection $\pi_i : G \to G_i$ to be continuous homomorphism.

Usually, the Galois groups of infinite Galois extensions are profinite groups as following.

Proposition 2.42. *[15, Corollary 1.3.4] Every profinite group is isomorphic to a Galois group of some Galois extensions.*

Definition 2.43. Let A,B be finite groups and G is a group(not necessarily finite). If for each epimorphisms $\rho : G \to A$ and $\tau : B \to A$ there exists a homomorphism $\gamma : G \to B$ such that $\rho = \tau \circ \gamma$, then we say G is **projective**.

The projective profinite groups are used in the proofs of this thesis. The following theorem gives an example of projective group

Theorem 2.44. *[15, Theorem 11.6.2] The absolute Galois group $Gal(K)$ of a PAC field K is projective.*

Also, we have the converse to theorem above. This Theorem is useful for constructing PAC fields through groups.

Theorem 2.45. *[15, Corollary 23.1.2] Given a projective group G and a field K, there is an extension F of K which is perfect and PAC with $Gal(F) \cong G$.*

Let S be a subset of a profinite group G. Denote the closed subgroup generated by S as $\langle S \rangle$. If $\langle S \rangle = G$,we say S generates G. If it has a finite set of generators, G is said to be **finitely generated**. The minimal number of generators of G is called the **rank** of G.

Notation 2.46. Given a profinite group G, we denote the set of all finite quotients (up to an isomorphism) of G by Im(G).

Now, if a profinite group G is NOT finitely generated, we need to find topological condition on the minimal set of generators of G in order to define the rank of G.

Definition 2.47. A subset X of a profinite group G is said to converge to 1 if $X \setminus N$ is a finite set for every open normal subgroup N of G.

Proposition 2.48. *[15, Proposition 17.1.1] Every profinite group G has a set of generators that converges to 1.*

Definition 2.49. The rank of a non-finitely generated profinite group G is defined as the cardinality of a set of generators of G that converges to 1.

The following proposition shows that this definition is independent of the particular set of generators.

Proposition 2.50. *[15, Proposition 17.1.2] Let G be a non-finitely generated profinite group. Denote the family of all open (resp. open normal) subgroup of G by $\mathcal{M}$ (resp. $\mathcal{N}$). Suppose X is a set of generator of G that converges to 1. Then $|X| = |\mathcal{M}| = |\mathcal{N}|$.*

Remark 2.51. *If G is an infinite finitely generated profinite group, then G has infinitely many open normal subgroups. For example, $\{2, 3\}$ is a minimal subset of generators of the Prüfer group $\hat{\mathbb{Z}}$ but rank$(\hat{\mathbb{Z}}) = 1$. So Proposition 2.50 does not hold in this case.*

The definition of the rank of finitely and non-finitely generated profinite groups differ from each other. A unified definition of rank(G) in both cases could be taken as the minimal cardinality of a set of generators that converges to 1.

Notation 2.52. We denote $\mathcal{C}$ as a family of finite groups containing the trivial group. Each group in $\mathcal{C}$ is called $\mathcal{C}$-group.

Definition 2.53. The family $\mathcal{C}$ of finite groups is called a formation if $\mathcal{C}$ satisfies the following conditions:

1. (closed under taking quotients) If $G \in \mathcal{C}$ and $\bar{G}$ is a homomorphic image of G, then $\bar{G} \in \mathcal{C}$.
2. (closed under fiber products) Let G be an arbitrary finite group and N_1, N_2 are normal subgroups of G. If $G/N_1, G/N_2 \in \mathcal{C}$ and $N_1 \cap N_2 = 1$, then $G \in \mathcal{C}$.

The family $\mathcal{C}$ of finite groups is called a full formation if it is closed under taking quotients, subgroups, and extensions.

We show that the full formation $\mathcal{C}$ is indeed a formation. Under the assumption of Definition 2.53(2), N_2 is isomorphic to N_1N_2/N_1 by isomorphism theorem. Note that N_1N_2/N_1 is a subgroup of G/N_1. Then $N_2 \in \mathcal{C}$. Since also $G/N_2 \in \mathcal{C}$, the exact sequence $1 \to N_2 \to G \to G/N_2 \to 1$ implies $G \in \mathcal{C}$. This satisfies the conclusion of Definition 2.53(2).

Definition 2.54. A pro-$\mathcal{C}$ group is an inverse limit $G = \varprojlim G_i$ of $\mathcal{C}$-groups for which the connecting homomorphism $G_j \to G_i$ are epimorphisms for all i,j.

Remark 2.55. *If the formation $\mathcal{C}$ contains all finite groups, the pro-$\mathcal{C}$ groups are just profinite groups. Also, the formation which contains all finite groups is clearly a full formation.*

Now, we introduce free pro-$\mathcal{C}$ groups arising as completion of free abstract groups. Let X be a set and G a profinite group. A map $\varphi : X \to G$ is said to be **convergent to 1** if $X \setminus \varphi^{-1}(H)$ is a finite set for each open normal subgroup H of G.

Definition 2.56. Let G be a group and $\mathcal{N}$ be the directed family of normal subgroups of finite index in G so that N_i is subgroup of $\bigcap_{j \in J} N_j$ with $i \in I$ and finite subset J of I. The direct limit $\hat{G} = \varprojlim G/N_i$ for all $N_i \in \mathcal{N}$ with map $\pi_i : \hat{G} \to G/N_i$ defined by restriction of $pr_i : \prod_{i \in I} G/N_i \to N_i$ to $\hat{G}$ is called the **profinite completion** of G with respect to $\mathcal{N}$.

Definition 2.57. Let $\mathcal{C}$ be a formation of finite groups and X be a subset of $\hat{F}$ which does not contain 1. A free pro-$\mathcal{C}$ group with basis X is a pro-$\mathcal{C}$ group $\hat{F}$ with a map $\tau : X \to \hat{F}$ satisfying :

1. X generates $\hat{F}$, and converges to 1

2. For each map φ of X into a pro-$\mathcal{C}$ group G which is convergent to 1 and satisfies $G = \langle \varphi(X) \rangle$ there exists a unique epimorphism $\hat{\varphi} : \hat{F} \to G$ with $\hat{\varphi} \circ \tau = \varphi$.

We refer to Proposition 17.4.2 and Lemma 17.4.3 in [15] for the construction of free pro-$\mathcal{C}$ group from free group uniquely through profinite completion. With these constructions, we have the following proposition.

Proposition 2.58. *Let $\mathcal{C}$ be a formation of finite groups and $\hat{F}$ a free pro-$\mathcal{C}$ group with basis X. Suppose $\mathcal{C}$ contains a nontrivial group of rank at most $|X|$. Then*

1. *$rank(\hat{F}) = |X|$,*
2. *Suppose $e = |X| < \infty$, then every set of generator of $\hat{F}$ of e elements is a basis of $\hat{F}$,*
3. *Let F be the free abstract group on X and $\mathcal{N}(X)$ the set of all normal subgroups N of F with $F/N \in \mathcal{C}$ and $X \setminus N$ finite. Then $\hat{F}$ is the profinite completion with respect to $\mathcal{N}(X)$ and the canonical map $\theta : F \to \hat{F}$ maps each $x \in X$ to itself.*

Notation 2.59. We denote the unique free pro-$\mathcal{C}$ group with basis X by $\hat{F}_X(\mathcal{C})$. If $X = \varnothing$, then $\hat{F}_X(\mathcal{C}) = 1$. If |X|= m for some cardinal m, we denote $\hat{F}_m(\mathcal{C})$ to be the free pro-$\mathcal{C}$ group with basis X. If the formation $\mathcal{C}$ is the family of all finite groups, we simplify $\hat{F}_m(\mathcal{C})$ to $\hat{F}_m$ (e.g. $\hat{F}_1 = \hat{\mathbb{Z}}$).

Therefore, if the basis is of cardinality $\aleph_0$ and the formation $\mathcal{C}$ is the family of all finite groups, then we denote $\hat{F}_\omega$ be the free pro-$\mathcal{C}$ group of rank $\aleph_0$ which is also a profinite group. This group will be used in the proofs of main theorems in this thesis.

Definition 2.60. An **embedding problem** for a profinite group G is a pair $(\varphi : G \to A, \alpha : B \to A)$ in which φ and α are continuous epimorphisms of groups. If B is finite, we call the problem **finite**. The embedding problem is said to be **solvable** (resp. **weakly solvable**) if there exists a continuous epimorphism (resp. homomorphism) $\gamma : G \to B$ with $\alpha \circ \gamma = \varphi$. The map γ is called a **solution** (resp. **weak solution**) to the embedding problem.

Now, if G is a pro-$\mathcal{C}$ group. Then we call the pair $(\varphi : G \to A, \alpha : B \to A)$ in which φ and α are epimorphisms of profinite groups a **$\mathcal{C}$-embedding problem** (resp. **pro-$\mathcal{C}$ embedding problem**), if B is a $\mathcal{C}$-group (resp. pro-$\mathcal{C}$ group). From above definition, a profinite group G is projective if every embedding problem for G is weakly solvable.

Definition 2.61. A field K is called ω**-free** if each finite embedding problem for Gal(K) is solvable.

From P.652 in [15], we know that a field is ω-free if and only if it has a countable elementary substructure F_0 with $Gal(F_0) \cong \hat{F}_\omega$. Therefore, given a countable Hilbertian field, we can make an ω-free PAC field by taking large algebraic extension as follows.

Proposition 2.62. *[15, Theorem 18.6.1] Let K be a countable Hilbertian field and K_s is separable closure of K. Let $\sigma \in Gal(K)^e$ for some $e \in \mathbb{N}$. Then the fix field of all elements of σ over K_s, denote by $K_s(\sigma)$ is a PAC field for almost all $\sigma \in Gal(K)^e$.*

Take the maximal Galois extension of K in $K_s(\sigma)$ and denote it by $K_s[\sigma]$. Then we have following Theorem which gives the examples of ω-free PAC fields.

Theorem 2.63. *[15, Theorem 27.4.8] For almost all $\sigma \in Gal(K)^e$ for some $e \in \mathbb{N}$, the field $K_s[\sigma]$ is an ω-free PAC field.*

Definition 2.64. A profinite group G **has the embedding property** if each embedding problem $(\varphi : G \to A, \alpha : B \to A)$ where φ and α are epimorphisms and $B \in$ Im(G) (i.e. B is a finite quotient of G) is solvable. That is, there exists an epimorphism $\gamma : G \to B$ with $\alpha \circ \gamma = \varphi$.

Now we are ready to introduce the Frobenius field which is of the main object in PAC field.

Definition 2.65. A field K is called a **Frobenius** field if K is PAC and Gal(K) has the embedding property.

Example 2.66.

1. From Theorem 24.8.1 in [15], we know that $K_s[\sigma]$ is a Frobenius field since $Gal(K_s[\sigma]) \cong \hat{F}_\omega$.

2. The absolute Galois group of E in Example 2.39 is isomorphic to $\prod_{p\neq 3} \mathbb{Z}_p$ where $\mathbb{Z}_p$ is p-adic group [15, P.900]. From Proposition 2.2.1 in [**?**], $\prod_{p\neq 3} \mathbb{Z}_p$ is a profinite group. With Theorem 4.3.3 in [**?**], we conclude that $\prod_{p\neq 3} \mathbb{Z}_p$ is a free profinite abelian group. From [15, Theorem 24.3.3], E is a Frobenius field.

3. The absolute Galois group of K in Example 2.40 is isomorphic to $\hat{\mathbb{Z}}$ [3]. Since $\hat{\mathbb{Z}}$ is free profinite group of rank 1 [**?**, Example 3.3.8], $\hat{\mathbb{Z}}$ has embedding property by Theorem 24.3.3 in [15]. Then K is also a Frobenius field.

The problem of finding PAC field which is not Frobenius is raised in [16, Problem 1.9]. We refer to Example 24.6.7 in [15] for field which is PAC but not Frobenius. For general profinite groups, neither the projective property nor the embedding property imply each other. See Example 24.6.1 and 24.6.7 in [15].

Definition 2.67. A profinite group is called **superprojective** if it is both projective and has the embedding property.

Actually, the absolute Galois group of Frobenius field is superprojective [15, Proposition 24.1.5]. Since a profinite group is projective if and only if it is isomorphic to the absolute Galois group of a PAC field [15, Corollary 23.1.3], the key to construct PAC field but not Frobenius is to find a projective profinite group which is not superprojecitve. The following class of Frobenius fields is the main object in this thesis.

Notation 2.68. Consider a fixed superprojective group G and a field K, we denote Frob(K,G) as the class of all perfect Frobenius fields M that contain K with Im(Gal(M))=Im(G)

We will show that the theory of Frob($\mathbb{Q}$,$\hat{F}_\omega$) is decidable in next chapter.

Chapter 3

Decidability of $\forall^n\exists$ theory

In this chapter, we prove the preservation theorem about $\forall^n\exists$ theory for arbitrary n over algebraic number field and discuss the possible development about Hilbert's tenth problem. First, we fix the first order language $\mathcal{L} = \mathcal{L}_{ring}$, the language of ring theory introduced in the preliminary. Using Proposition 2.12 and Proposition 2.13 introduced in the preliminary, we have the following preservation theorem about $\forall^n\exists$ sentence:

Theorem 3.1. *Let K be an algebraic number field contained in a field F. Then F satisfies all $\forall^n\exists$ sentence true in K with all $n \in \mathbb{N}$ if and only if K is existentially closed in F.*

Proof. For the only if part, suppose that K is not existentially closed in F. Then there are some existential sentences, say $\exists^n\bar{x}\varphi(\bar{x})$ with $\varphi(\bar{x})$ quantifier-free and some $n \in \mathbb{N}$, which is true in F but false in K. So K$\models \forall\bar{x}\neg\varphi(\bar{x})$. Since F satisfies all $\forall^n\exists$ sentence true in K, F must satisfies $\forall\bar{x}\neg\varphi(\bar{x})$ which contradicts to our assumption.

Conversely, suppose that there exists a $\forall^n\exists$ sentence, say $\forall^n\bar{x}\exists y\varphi(\bar{x}, y)$, which is true in K but false in F. Since K is existentially closed in F, there exist a field $\hat{K}$ such that $\hat{K}$ is elementary extension of K and F is embedded in $\hat{K}$ by Proposition 2.12. We claim that F is algebraically closed in $\hat{K}$. Since K is a number field, $\hat{K}$ cannot be algebraically closed (algebraically closed property are elementary statements). So $\hat{K} \neq \bar{F}$. Choose $a \in \hat{K} \cap \bar{F}$. Consider the irreducible polynomial Irr(a,F) of degree n for some positive integer n and write Irr(a,F) as $p(\bar{u}, x)$ where $\bar{u} \in F^n$ is the sequence of coefficients of Irr(a,F). Apply Proposition 2.13, there exists a field $\hat{F}$ so that $\hat{K}$ is embedded in $\hat{F}$ and $\hat{F}$ is an elementary extension of F. Suppose that F $\models \forall x p(\bar{u}, x) \neq 0$. From the choice of a,$\hat{K} \models \exists x p(\bar{u}, x) = 0$. Through elementarily equivalence, we have $\hat{F} \models \forall x p(\bar{u}, x) \neq 0$. However, the preservation theorem shows that $\hat{K} \models \forall x p(\bar{u}, x) \neq 0$ which is a contradiction. Therefore, F$\models \exists x p(\bar{u}, x) = 0$. Since $\bar{K}$ is non-standard number field, the irreducibility of $p(\bar{u}, x)$ can also be preserved. The irreducibility of f shows that $deg(f) = 1$. Therefore, $a \in$ F and we have F is algebraically closed in $\hat{K}$ which proves our claim. From Disjunctive normal form ,$\varphi(\bar{x}, y) \iff \bigvee_{i=1}^{s}[\bigwedge_{j=1}^{m_i} f_{i,j}(\bar{x}, y) = 0 \wedge \bigwedge_{k=1}^{n_i} g_{i,k}(\bar{x}, y) \neq 0]$ for some $s, m_i, n_i \in \mathbb{N}$. For any $\bar{a} \in F^n$, we have to find $b \in F$ such that $F \models \varphi(\bar{a}, b)$. From the K-embedding of F to $\hat{K}$, we may assume that F is a subfield of $\hat{K}$. Then $F^n \subset \hat{K}^n$ for all $n \in \mathbb{N}$. Given any $\bar{a} \in F^n$, we can find $b \in \hat{K}$ such that $\hat{K} \models \varphi(\bar{a}, b)$ since $\hat{K} \models \forall^n \bar{x} \exists y \varphi(\bar{x}, y)$. Then for some $i = 1, \ldots, s$,$\hat{K} \models \bigwedge_{j=1}^{m_i} f_{i,j}(\bar{a}, b) = 0 \wedge \bigwedge_{k=1}^{n_i} g_{i,k}(\bar{a}, b) \neq 0$. We have following two cases:

1. If some of $f_{i,j}(\bar{a}, y)$ has positive degree for some j, $b \in F$ since F is algebraically closed in $\hat{K}$. Also $b \in F \subset \hat{K}$ implies $g_{i,k}(\bar{a}, b) \neq 0$ for all $k = 1, \ldots, n_i$. Then $F \models \varphi(\bar{a}, b)$.

2. If $f_{i,j}(\bar{a}, y) \equiv 0$ for all $j = 1, \ldots, m_i$, but $g_{i,k}(\bar{a}, b) \neq 0$ for all $k = 1, \ldots, n_i$, we know $g_{i,k}(\bar{a}, y)$ are not identically zero. Since F is infinite and of characteristic 0, we can find $c \in F$ so that $g_{i,k}(\bar{a}, c) \neq 0$ for all k. Note that $f_{i,j}(\bar{a}, c) = 0$ for all $j = 1, \ldots, m_i$. Then $F \models \varphi(\bar{a}, c)$.

From above argument 1 and 2, we have $F \models \forall^n x \exists y \varphi(\bar{x}, y)$ since $\bar{a} \in F^n$ is arbitrary. Note that we do not fix the value of n in our proof. Therefore, this contradiction shows that F preserves all $\forall^n \exists$ sentences true in K. □

On the other hand, we show the following general proposition for models which is the "counterpart" of preservation theorem of the existentially closed property.

Proposition 3.2. *Let $\mathcal{A}, \mathcal{B}$ be $\mathcal{L}$-structure. If $\mathcal{A}$ is existentially closed in $\mathcal{B}$. then every $\forall^n \exists^m$ sentence for all $m, n \in \mathbb{N}$ true in $\mathcal{B}$ is also true in $\mathcal{A}$.*

Proof. Let $\psi = \forall^n \bar{x} \exists^m \bar{y} \varphi(\bar{x}, \bar{y})$ for some fix $m, n \in \mathbb{N}$ and suppose $\mathcal{B} \models \psi$. Then given any n-tuples $\bar{a}$ of elements of $dom(\mathcal{A}) \subseteq dom(\mathcal{B})$, we have $\mathcal{B} \models \exists^m \bar{y} \varphi(\bar{a}, \bar{y})$. Since $\mathcal{A}$ is existentially closed in $\mathcal{B}$, $\mathcal{A} \models \varphi(\bar{a}, \bar{y})$. Therefore, $\mathcal{A} \models \forall^n \bar{x} \exists^m \bar{y} \varphi(\bar{x}, \bar{y})$ and hence $\mathcal{A} \models \psi$. □

Corollary 3.3. *If K is an algebraic number fields contained in some fields F such that K is existentially closed in F, then the $\forall^n \exists$ theory of K is the same as the $\forall^n \exists$ theory of F for all $n \in \mathbb{N}$.*

Proof. We denote $\forall^n \exists$ theory of K as $Th_{\forall^n \exists}(K)$ and use the same notation for $\forall^n \exists$ theory of F. So Theorem 3.1 shows that $Th_{\forall^n \exists}(K) \subseteq Th_{\forall^n \exists}(F)$. The Proposition 2.12 implies $Th_{\forall^n \exists}(F) \subseteq Th_{\forall^n \exists}(K)$. Then we have $Th_{\forall^n \exists}(K) = Th_{\forall^n \exists}(F)$ for all $n \in \mathbb{N}$ □

If we find some fields F as in Corollary 3.3 and F belongs to some elementary class, we know that the $\forall^n\exists$ theory of an algebraic number field is axiomatizable. From Corollary 2.5 in [43], we know that the $\exists^n\forall$ theory for arbitrary n of an algebraic number field is axiomatizable. Take the union of sets of axioms in these two set, we may say that the union axioms are $\forall^n\exists$-complete. This means that, for any $\forall^n\exists$ sentence φ, φ or $\neg\varphi$(which is an $\exists^n\forall$ sentence) is deducible from these two axioms. From Theorem 1 in [32], if a theory T is axiomatizable and complete then T is decidable. Therefore, we can show that the $\forall^n\exists$ theory for arbitrary n of an algebraic number field is decidable.

A set S is $\forall^n\exists$-Diophantine definable if there exists a polynomial

$$f(a, x, t_1, \ldots, t_n) \in \mathbb{Z}[a, x, t_1, \ldots, t_n]$$

such that $a \in S \iff \forall t_1 \cdots \forall t_n \exists x f(a, x, t_1, \ldots, t_n) = 0$, where the quantified variables may range over some algebraic number fields. Given a polynomial $f(x_1, \ldots, x_n)$ the decidability of $\exists x_1 \cdots \exists x_n f(x_1, \ldots, x_n) = 0$ is equivalent to the decidability of $\forall x_1 \cdots \forall x_n f(x_1, \ldots, x_n) \neq 0$. Over a ring if the set of nonzero elements is $\forall^n\exists$-Diophantine definable then the decidability of $\forall^{m+n}\exists$ equations will imply the decidability of $\exists^m$ equations. So if we have he $\forall^n\exists$ theory for arbitrary n of an algebraic number field is decidable, then the $\forall^{m+n}\exists$ equations over an algebraic number field is decidable and hence the $\exists^m$ equations over an algebraic number field is decidable. Since Hilbert's tenth problem over number fields is still open, this provides another approach to prove Hilbert's tenth problem over number fields.

Chapter 4

Decidability of $\exists\forall$ and $\forall\exists$ theory

4.1 Decidable $\exists\forall$ theory

In this chapter, we investigate the decidability of $\exists\forall$ theory of class of Hilbertian fields of characteristic 0 and perfect Hilbertian fields. From [43, P.1017], we know that the decidability of $\exists\forall$ theory of fields for characteristic 0 is still open. Therefore, we give some counter-example to understand the relation between fields of characteristic 0 and its related models. In model theory, we know that for all fields of characteristic 0, there exist a ”small” and a ”big” model of field so that each small model can be embedded in all fields of characteristic 0 and each big model contains some fields of characteristic 0. This is what the following theorem tells us.

Theorem 4.1. *[10, Example 3.5.9 and 3.5.10]*

1. *The theory of algebraically closed fields of characteristic 0 is a model companion of the theory of fields of characteristic 0.*

2. *The field of rational number is an algebraically prime model of the theory of fields of characteristic 0.*

Therefore, for each field F of characteristic 0, we can embed $\mathbb{Q}$ in to F and extend F to its algebraic closure $\bar{F}$. Note that $\bar{\mathbb{Q}}$ is elementary submodel of each algebraically closed field. Then we may ask whether it's possible to characterize the $\exists\forall$ theory of fields of characteristic 0 through Theorem 4.1. But we will give a counterexample to show that the $\exists\forall$ theory of class of fields with characteristic 0 is strictly contained in the set of $\exists\forall$ sentences true in $\mathbb{Q}$,$\bar{\mathbb{Q}}$, and the class of number fields.

Example 4.2. Let L be the Euclidean closure of $\mathbb{Q}$,i.e. field obtained from $\mathbb{Q}$ by iteratively adding square roots of all elements as following: Let $F_0 = \mathbb{Q}$, $F_{i+1} =$

$F_i(\{\sqrt{a}|a \in F_i\})$. Then $L = \bigcup_{i=1}^{\infty} F_i$. By field theory, there exist an increasing sequence of finite-degree extension of $\mathbb{Q}$, denote as $\{K_j|K_j \subset K_{j+1}$ for all j and $K_0 = \mathbb{Q}\}$ since L is an infinite algebraic extension of $\mathbb{Q}$. So each K_j contains only finitely many square roots of K_{j-1}. Let $\varphi(x, y) = \exists x \forall y(y^2 \neq x) \vee (x^3 = 2)$. Since $\sqrt{2} \notin \mathbb{Q}$, $\mathbb{Q} \models \varphi(x, y)$. Also, not every element in K_j has square root. Then $K_j \models \varphi(x, y)$ for all j. But $L \not\models \varphi(x, y)$ because everything in L has square root and $\sqrt[3]{2} \notin L$. And $\sqrt[3]{2} \in \bar{\mathbb{Q}}$ shows that $\bar{\mathbb{Q}} \models \varphi(x, y)$.

The example above tells us that we need to seek more sophisticated field to prove the decidability of $\exists\forall$ theory of fields of characteristic 0.

From Theorem 1.4 in the Introduction, we know that the elementary theory of Hilbertian fields and PAC fields are both undecidable. Also, from [36, P. 304-305], we know that the elementary theory of any class of fields which contains $\mathbb{Q}$ is undecidable. Then the elementary theories of Hilbertian fields of characteristic 0 and perfect Hilbertian fields are both undecidable too.

With undecidable theories above, we want to investigate what fragments of theory Hilbertian fields and PAC fields are decidable ? In the following paragraphs, we show that the elementary theory of Hilbertian PAC fields of characteristic 0 is decidable first. Then we use this result to prove that the $\exists\forall$ theory of Hilbertian fields of characteristic 0 and perfect Hilbertian fields are both decidable. We need to introduce more facts about free pro-$\mathcal{C}$ groups which will be used in the proof of decidability of the elementary theory of Hilbertian PAC fields with characteristic 0.

Proposition 4.3. *[15, Corollary 22.4.5] Let $\mathcal{C}$ be a full formation of finite groups and F a free pro-$\mathcal{C}$ group. Then F is projective.*

Proposition 4.4. *[15, Lemma 24.3.3] Let $\mathcal{C}$ be a formations of finite groups and F is a free pro-$\mathcal{C}$ group. Then F has the embedding property.*

These two propositions above give us some criterion to check the property of superprojective in profinite group with the formation $\mathcal{C}$ to be all finite groups.

Theorem 4.5. *[15, Theorem 24.8.1] Let $\mathcal{C}$ be a formation of finite groups and F a pro-$\mathcal{C}$ group of at most countable rank. Then F is isomorphic to $\hat{F}_\omega(\mathcal{C})$ if and only if Im(F)= $\mathcal{C}$ and F has the embedding property.*

Proposition 4.6. *[15, Corollary 24.8.3] Let F be a profinite group at most countable rank. Suppose every finite embedding problem for F is solvable. Then F is isomorphic to $\hat{F}_\omega$.*

The following important theorem shows that the elementary theory of the class Frob(K,G) is decidable.

Theorem 4.7. *[15, Theorem 30.6.2] Let K be a presented field with elimination theory and G a superprojective group such that Im(G) is primitive recursive. Then there exists a primitive recursive decision procedure for the theory of Frob(K,G).*

In order to use Theorem 4.7, we need to prove that the family of finite groups is primitive recursive.

Proposition 4.8. *The family of all finite groups is a primitive recursive set.*

Proof. Denote the family of all finite groups as FGrps. Let X be the set of all matrices $\mathbf{x} = (x_{ij})_{1\leq i,j\leq n}$ with entries x_{ij} such that $x_{11}, x_{12}, \ldots, x_{1n}$ are distinct symbols and for each i between 1 and n, the i'th row is a permutation of the first one such that $x_{1j} = x_{j1}$ for $j = 1, \ldots, n$. Since for each set $x_{11}, x_{12}, \ldots, x_{1n}$, there are $(n-1)\cdot(n-1)!$ matrices in X, we can effectively produce X through permutation in finite steps. Therefore, we view $\mathbf{x}$ as a multiplication table for the set $\{x_{11}, x_{12}, \ldots, x_{1n}\}$ under the rule $x_{ij} = x_{i1}x_{1j}$. Since each matrix is of finite order, we can effective check whether this rule makes $\mathbf{x}$ a group. Also, we order X in a sequence such that a matrix of order $n \times n$ precedes each matrix of order $n' \times n'$ if $n < n'$. Then we can effectively produce a set FGrps(X) as a subset of X with each elements of FGrps(X) uniquely corresponding to a finite group in FGrps. From the preliminary, we know that FGrps is primitive recursive. □

We use the propositions above to prove that the decidability of $\omega-$free PAC fields of characteristic 0.

Theorem 4.9. *The elementary theory of ω-free PAC fields of characteristic 0 is decidable.*

Proof. Denote the elementary theory of ω-free PAC fields of characteristic 0 as Th(ω -PAC0) We know $\mathbb{Q}$ is a presented field with splitting algorithm through Proposition 2.28 and has elimination theory by Proposition 2.29. From Proposition 4.3 and Proposition 4.4, the free pro-$\mathcal{C}$ group of rank $\aleph_0$ with formation $\mathcal{C}$ of all finite groups, $\hat{F}_\omega$, is superprojective. Apply Theorem 4.5, we have Im($\hat{F}_\omega$)=$\mathcal{C}$. This set is primitive recursive by Proposition 4.8. We conclude that the elementary theory of Frob($\mathbb{Q}, \hat{F}_\omega$), denoted as Th(Frob($\mathbb{Q}, \hat{F}_\omega$)), is decidable through Theorem 4.7. Now we need to show Th(ω -PAC0) = Th(Frob($\mathbb{Q}, \hat{F}_\omega$)). It sufficient to show that the class of ω-free PAC fields of characteristic 0 is the same class as $Frob(\mathbb{Q}, \hat{F}_\omega)$. Let K be an ω-free PAC fields of characteristic 0. By definition, every finite embedding problem for the absolute Galois group Gal(K) is solvable. From Proposition 4.6, Gal(K) is isomorphic to $\hat{F}_\omega$. Then Theorem 4.5 shows that Im(Gal(K))=$\mathcal{C}$ = Im($\hat{F}_\omega$) where $\mathcal{C}$ is the family of all finite groups and Gal(K) has the embedding property.

Since K is of characteristic 0,K contains $\mathbb{Q}$ by Theorem 4.1. Therefore, we have $K \in Frob(\mathbb{Q}, \hat{F_\omega})$. Conversely, suppose that M is a perfect Frobenius field containing $\mathbb{Q}$ with Im(Gal(M)) = Im($\hat{F_\omega}$). So M is of characteristic 0. By the definition of Frobenius field, we know that Gal(M) has the embedding property and M is a PAC field. Using Theorem 4.5, Gal(K) is isomorphic to $\hat{F_\omega}$. Note that Im(Gal(M)) consists of all finite groups through the equality setting above. Then every finite embedding problem for Gal(M) is solvable. Therefore, M is an ω-free PAC field of characteristic 0 and we finish our proof. □

However, the following deep theorem connects the properties of ω-free and Hilbertian together.

Theorem 4.10. *[18, Theorem 5.10.3] Let K be a PAC field. Then K is ω-free if and only if K is Hilbertian.*

Now we have the corollary as we claim before.

Corollary 4.11. *The elementary theory of Hilbertian PAC fields of characteristic 0 is decidable.*

Proof. From Theorem 4.10, we know that the class of ω-free PAC fields of characteristic 0 is the same as the class of Hilbertian PAC fields of characteristic 0. Theorem 4.9 shows that Th(ω -PAC0) is decidable. Then we have the elementary theory of Hilbertian PAC fields of characteristic 0 is also decidable. □

We quote another Theorem which will be used to prove some techniques.

Theorem 4.12. *[46, Theorem 3.2] Let K be a Hilbertian fied and $\varphi(\bar{x}, y)$ be quantifier free $\mathcal{L}$-formula over K. If $\forall \bar{x} \exists y \varphi(\bar{x}, y)$ is true in K, then $\exists y \bar{\varphi}(y)$ is true in $K(\bar{X})$.*

Corollary 4.13. *Let K be a Hilbertian field and $\varphi(\bar{x}, y)$ be a formula in disjunctive normal form, i.e. $\varphi = \varphi_1 \vee \cdots \vee \varphi_s$ for some $s \in \mathbb{N}$ and $\varphi_i = \bigwedge_{j=1}^{m_i} f_{i,j}(\bar{x}, y) = 0 \wedge \bigwedge_{k=1}^{n_i} g_{i,k}(\bar{x}, y) \neq 0$, where $f_{i,j}(\bar{x}, y)$ and $g_{i,k}(\bar{x}, y)$ are polynomials over K. If $\forall \bar{x} \exists y \varphi(\bar{x}, y)$ is true in K, then there exists an i and polynomial $F(\bar{x})$ and $G(\bar{x}) \not\equiv 0$ over K such that in $K[\bar{x}, y]$, $G(\bar{x})y - F(\bar{x})$ are irreducible common factor of each $f_{i,j}(\bar{x}, y)$, $1 \leq j \leq m_i$, but not a factor of any $g_{i,k}(\bar{x}, y)$, $1 \leq k \leq n_i$.*

Proof. From Theorem 4.12, we can find $p(\bar{x})$ ∈K($\bar{X}$) such that $\varphi(\bar{x}, p(\bar{x}))$ is true in K($\bar{X}$) since $\bar{\varphi}(y) \equiv \varphi(\bar{x}, y)$ over K($\bar{X}$). Then there exists an $1 \leq i \leq s$ so that $\bigwedge_{j=1}^{m_i} f_{i,j}(\bar{x}, p(\bar{x})) = 0 \wedge \bigwedge_{k=1}^{n_i} g_{i,k}(\bar{x}, p(\bar{x})) \neq 0$ is true in K($\bar{X}$). Write $p(\bar{x}) = \frac{F(\bar{x})}{G(\bar{x})}$ where F($\bar{x}$) and G($\bar{x}$) are relatively prime and F($\bar{x}$),G($\bar{x}$)∈ K[$\bar{x}$] with G($\bar{x}$)$\not\equiv$ 0. By Factor Theorem, $y - \frac{F(\bar{x})}{G(\bar{x})}$ is an irreducible common factor of each $f_{i,j}(\bar{x}, y)$, but not a factor of any $g_{i,k}(\bar{x}, y)$ for $1 \leq k \leq n_i$. Then Gauss lemma shows that G($\bar{x}$)y-F($\bar{x}$)

is an irreducible common factor of each $f_{i,j}(\bar{x}, y)$ but not a factor of any $g_{i,k}(\bar{x}, y)$ for $1 \leq k \leq n_i$. This finishes our proof. □

Then we use this corollary to prove the preservation theorem of ∀∃ sentences over Hilbertian field which is mentioned in [46, P.800].

Proposition 4.14. *Let K be a Hilbertian field contained in a field F. If K is algebraically closed in F, then F satisfies all ∀∃ sentences true in K.*

Proof. Suppose that there exists an ∀∃ sentence which is true in K but false in F. Reduce $\varphi(x, y)$ to disjunctive normal form. Thus, $\varphi(x, y)$ is logically equivalent to $\bigvee_{i=1}^{s}[\bigwedge_{j=1}^{m_i} f_{i,j}(x, y) = 0 \wedge \bigwedge_{k=1}^{n_i} g_{i,k}(x, y) \neq 0]$ where $f_{i,j}(x, y)$ and $g_{i,k}(x, y)$ are polynomials over $\mathbb{Z}$. By Corollary 4.13, there exists an i and polynomials F(x),G(x)∈K[x], with G(x)$\not\equiv$ 0, such that G(x)y-F(x) is an irreducible common factor of the polynomials $f_{i,j}(x, y)$ for $1 \leq j \leq m_i$, but not a factor of $g_{i,k}(x, y)$ for $1 \leq k \leq n_i$. Since F$\models \exists x \forall y \neg\varphi(x, y)$, choose $x' \in$F so that F$\models \forall y \neg\varphi(x', y)$. Because K$\models \forall x \exists y \varphi(x, y)$, $x' \in$F$-$K by preservation theorem of universal sentence. Since K is algebraically closed in F, G(x')$\neq$ 0. Then $f_{i,j}(x, \frac{F(x)}{G(x)}) = 0$ for every $1 \leq j \leq m_i$ shows that F$\models \bigwedge_j f_{i,j}(x', \frac{F(x')}{G(x')}) = 0$. Note that G(x)y-F(x) is not a factor of $g_{i,k}(x, y)$ in K(X)[y] for any $1 \leq k \leq n_i$, so $g_{i,k}(x, \frac{F(x)}{G(x)}) \neq 0$ in K(X). Since x' is transcendental over K, we have $g_{i,k}(x', \frac{F(x')}{G(x')}) \neq 0$. Thus F$\models \bigwedge_j f_{i,j}(x', \frac{F(x')}{G(x')}) = 0 \wedge \bigwedge_k g_{i,k}(x', \frac{F(x')}{G(x')}) \neq 0$ for some i. Therefore, F$\models \exists y \varphi(x', y)$ with $y = \frac{F(x)}{G(x)}$ which contradicts to the assumption. This finishes our proof. □

The following key theorem connects general fields and Hilbertian PAC fields together.

Theorem 4.15. *[15, Proposition 13.4.6] Every field K has a regular extension F which is PAC and Hilbertian.*

Using Proposition 4.14, Theorem 4.15, and Corollary 4.11, we can get following series of decidable results about ∀∃ and ∃∀ theories of Hilbertian fields and PAC fields.

Theorem 4.16. *The ∃∀ theory of Hilbertian field of characteristic 0 is the same as the ∃∀ theory of Hilbertian PAC fields of characteristic 0.*

Proof. Since every Hilbertian PAC field of characteristic 0 is a Hilbertian field of characteristic 0, the ∃∀ theory of Hilbertian fields of characteristic 0 is contained in the ∃∀ theory of Hilbertian PAC fields of characteristic 0. We want to show that these two sets are in fact the same. Suppose that there is an ∃∀ sentence $\exists x \forall y \varphi(x, y)$ with $\varphi(x, y)$ quantifier-free which is true in every Hilbertian PAC fields of characteristic 0 but false in a Hilbertian field K of characteristic 0. According to Theorem 4.15, we can find a Hilbetian PAC field F of characteristic 0 which is regular extension of K. Using Proposition 4.14, we have $F \models \forall x \exists y \neg \varphi(x, y)$ which contradicts to the assumption. □

Corollary 4.17. *The $\exists\forall$ theory of Hilbertian fields of characteristic 0 is decidable*

Proof. From Corollary 4.11, the $\exists\forall$ theory of Hilbertian PAC fields of characteristic 0 is decidable. Then the Theorem 4.16 tell us the result we want. □

Actually, we can extend the result above to perfect Hilbertian fields. We quote one theorem about decidability of elementary theory of perfect Frobenius fields.

Theorem 4.18. *[15, Theorem 31.1.4] Let $\mathcal{C}$ be a primitive recursive full family of finite groups. Then the theory of perfect Frobenius fields M such that each Gal(M) is a pro-$\mathcal{C}$ group is primitive recursive.*

We need another proposition about pro-$\mathcal{C}$ groups.

Lemma 4.19. *[15, Corollary 24.8.2] Let $\mathcal{C}$ be a formation of finite groups and G is a pro-$\mathcal{C}$ group of at most countable rank. Then G is isomorphic to $\hat{F}_\omega(\mathcal{C})$ if and only if every $\mathcal{C}$-embedding problem for G is solvable.*

Then we have the following theorem about decidability of perfect ω-free PAC fields.

Theorem 4.20. *The elementary theory of perfect ω-free PAC fields is decidable.*

Proof. K is a perfect ω-free PAC fields $\iff$ K is a perfect PAC field and every finite embedding problem of Gal(K) is solvable $\iff$ K is a perfect PAC field where Gal(K) is isomorphic to $\hat{F}_\omega$ by taking $\mathcal{C}$ as the formation of all finite groups in Lemma 4.19 $\iff$ K is a perfect Frobenius field where Gal(K) is isomorphic to $\hat{F}_\omega$. Proposition 4.8 has shown $\mathcal{C}$ is primitive recursive. From Theorem 4.18, we have the desired result. □

Theorem 4.21. *The $\exists\forall$ theory of perfect Hilbertian fields is decidable.*

Proof. From Theorem 4.10, we know that the perfect Hilbertian PAC field is the same as the perfect ω-free PAC field. We claim that the $\exists\forall$ theory of perfect Hilbertian fields and the $\exists\forall$ theory of perfect Hilbertian PAC fields are identical. Then the result follows from Theorem 4.20.

Since every perfect Hilbertian PAC fields is a perfect Hilbertian field, the $\exists\forall$ theory of perfect Hilbertian fields is contained in the $\exists\forall$ theory of perfect Hilbertian PAC fields. Suppose that there is an $\exists\forall$ sentence $\exists x \forall y \varphi(x, y)$ with $\varphi(x, y)$

quantifier-free which is true in all perfect Hilbertian PAC fields of but false in a perfect Hilbertian field K. According to Theorem 4.15, there exists a regular extension F which is Hilbertain and PAC. Since K is perfect, F is also perfect. But Proposition 4.14 tells us that $F \models \forall x \exists y \neg \varphi(x, y)$ which contradicts to our assumption, This finishes our proof. □

Notice that the elementary theories of most local fields are decidable according to the Theorem 1.3. Therefore, the ∃∀ theory of real number(and real closed fields), algebraically closed fields, and p-adic fields are all decidable.

Proposition 4.22. *[38, Corollary 2.3] The recursive sets are closed under union, intersection and complementation.*

We ended by proving the following corollary which use all the results we proved in this chapter.

Corollary 4.23. *The ∃∀ theory of local fields and Hilbertian fields of characteristic 0 is decidable*

Proof. Apply Proposition 4.22 to 1.3 and Corollary 4.17, we get the corollary. □

With interest in algebraic number theroy, the corollary above tells us that the ∃∀ theory of local and global fields is decidable.

4.2 Decidable ∀∃ theory

Using the theorems proved in previous section, we can give a proof of the decidability of ∀∃ theory of Hilbertian fields of characteristic 0. First, we need the following lemma about preservation of $\exists^n \forall$ sentences over Hilbertian fields.

Lemma 4.24. *Let K be a Hilbertian field and F is a regular extension of K. Then F satisfies all the $\exists^n \forall$ sentences true in K for arbitrary n.*

Proof. The proof of this lemma is essentially the same as the proof of Proposition 2.4 in [43]. □

Theorem 4.25. *The ∀∃ theory of Hilbertian fields of characteristic 0 is decidable.*

Proof. From Corollary 4.11, the ∀∃ theory of Hilbertian PAC fields of characteristic 0 is decidable. If we shows that the ∀∃ theory of Hilbertian fields of characteristic 0 and the ∀∃ theory of Hilbertian PAC fields of characteristic 0 are identical, then we get the desired result.

Since every Hilbertian PAC fields of characteristic 0 is a Hilbertian field of characteristic 0, the $\forall\exists$ theory of Hilbertian fields of characteristic 0 is contained in the $\forall\exists$ theory of Hilbertian PAC fields of characteristic 0. To show that these two sets are in fact the same, suppose that there exists an $\forall\exists$ sentence $\forall x\exists y\varphi(x, y)$ with $\varphi(x, y)$ quantifier-free which is true in every Hilbertian PAC fields of characteristic 0 but false in a Hilbertian field K of characteristic 0. From Theorem 4.15, we can find a Hilbertian PAC field F which is regular extension of K. Then Lemma 4.24 tell us that $F \models \exists x\forall y\neg\varphi(x, y)$ which contradicts to our assumption. □

Remark 4.26. The $\forall\exists$ theory of Hilbertian fields of characteristic 0 is contained in the $\forall\exists$ theory of number fields and containing the $\forall\exists$ theory of fields of characteristic 0. From Theorem 3.1 in [43], we know that the $\forall\exists$ theory of number fields and the $\forall\exists$ theory of fields of characteristic 0 are equal. So these three $\forall\exists$ theories above are all equal and we get the decidability result through Theorem 3.3 in [43].

Corollary 4.27. *The $\forall^n\exists$ theory of Hilbertian fields of characteristic 0 is decidable for arbitrary positive integer n.*

Proof. From Corollary 4.11, the $\forall^n\exists$ theory of Hilbertian PAC fields of characteristic 0 is decidable for arbitrary positive integer n. Since Lemma 4.24 shows the preservation of $\exists^n\forall$ sentences over Hilbertian fields, we can modify the same proof in Theorem 4.25 to get the $\forall^n\exists$ theory of Hilbertian fields of characteristic 0 and the $\forall^n\exists$ theory of Hilbertian PAC fields of characteristic 0 are identical for arbitrary positive integer n. This proves the result we want. □

Next, we prove the decidability of $\forall\exists$ theory of Hilbertian fields. From Proposition 3.2, we can easily get the following preservation theorem of $\exists^n\forall^m$ sentences for all $m, n \in \mathbb{N}$.

Proposition 4.28. *Let $\mathcal{A}, \mathcal{B}$ be $\mathcal{L}$-structure. If $\mathcal{A}$ is existentially closed in $\mathcal{B}$. then every $\exists^n\forall^m$ sentence for all $m, n \in \mathbb{N}$ true in $\mathcal{A}$ is also true in $\mathcal{B}$.*

Proof. If there exist an $\exists^n\forall^m$ sentence which is true in $\mathcal{A}$ but false in $\mathcal{B}$ for some $m, n \in \mathbb{N}$, then we can find that the negation of $\exists^n\forall^m$ sentence (i.e. $\forall^n\exists^m$ sentence) is also true in $\mathcal{A}$ by Proposition 3.2 and leads to a contradiction. □

But in field theories, the existentially closed property can be characterized by transcendental extension.

Theorem 4.29. *[33, Proposition 1] Let K be an infinite field and F is an extension field of K. If F is purely transcendental extension of K, then K is existentially closed in F.*

Note that the Theorem above require the fields to be infinite. So we need to guarantee all the Hilbertian fields and PAC fields are infinite.

Proposition 4.30. *[15, P.218] If K is a Hilbertian field, then K must be infinite.*

Proposition 4.31. *[15, Proposition 11.1.1] If K is a PAC field, then K must be infinite.*

Also, we need the decidability of $\forall\exists$ theory of infinite fields.

Proposition 4.32. *The $\forall\exists$ theory of infinite fields is decidable*

Proof. Let $\forall x \exists y \varphi(x, y)$ be an $\forall\exists$ sentence. Reduce $\varphi(x, y)$ to disjunctive normal form: $\varphi(x, y) \iff \bigvee_{i=1}^{s}[\bigwedge_{j=1}^{m_i} f_{i,j}(x, y) = 0 \wedge \bigwedge_{k=1}^{n_i} g_{i,k}(x, y) \neq 0]$. Suppose that $\forall x \exists y \varphi(x, y)$ is true in all fields of characteristic 0. Then $\forall x \exists y \varphi(x, y)$ in true in the rational number. Notice that $\mathbb{Q}$ is a Hilbertian field by Hilbert's irreducibility theorem. From Corollary 4.13, there exist an i and polynomials $F(x), G(x) \in \mathbb{Q}[x]$, with $G(x) \not\equiv 0$, such that $G(x)y - F(x)$ is an irreducible common factor of $f_{i,j}(x, y)$ in $\mathbb{Q}[x, y]$ for $1 \leq j \leq m_i$ but not a factor of $g_{i,k}(x, y)$ for $1 \leq k \leq n_i$. As Proposition 2.28 says, we have a splitting algorithm to factor $f_{i,j}(x, y)$ and $g_{i,k}(x, y)$ for every i, j, k over $\mathbb{Q}$ and looking for the polynomial $G(x)y - F(x)$ which satisfies our requirement. From Gauss' lemme, we may assume that F(x) and G(x) are polynomials over $\mathbb{Z}$. Let m be the maximal degree of y in $g_{i,k}(x, y)$ such that $g_{i,k}(x, \frac{F(x)}{G(x)}) \cdot G(x)^m$ are over $\mathbb{Z}$ for all $1 \leq k \leq n_i$. Then consider the greatest common divisor of the contents of G(x) and $g_{i,k}(x, \frac{F(x)}{G(x)}) \cdot G(x)^m$ for $1 \leq k \leq n_i$, and denote it by b. From the proof of Theorem 3.7 in [43], we know that $\forall x \exists y \varphi(x, y)$ is true in all infinite fields iff $\forall x \exists y \varphi(x, y)$ holds in all fields of characteristic 0 and $\exists y \varphi(t, y)$ holds in every rational function field $\mathbb{F}_p(t)$, where p is a prime divisor of b. Corollary 3.4 and final paragraphs of proof of Theorem 3.7 in [43] implies $\forall x \exists y \varphi(x, y)$ is true in all infinite fields is decidable. □

From Theorem 2.35 in the preliminary, we know that every finitely generated transcendental extension of an arbitrary field is Hilbertian. This gives us a way to connect infinite fields and Hilbertian fields.

Theorem 4.33. *The $\forall\exists$ theory of Hilbertian fields is decidable.*

Proof. We claim that the $\forall\exists$ theory of Hilbertian fields and $\forall\exists$ theory of infinite fields are identical. Then Proposition 4.32 implies the result we want. Proposition 4.30 tells us that all the Hilbertian fields are infinite fields. So the $\forall\exists$ theory of infinite fields is contained in the $\forall\exists$ theory of Hilbertian fields. Conversely, suppose that there exists an $\forall\exists$ sentence $\forall x \exists y \varphi(x, y)$ with $\varphi(x, y)$ quantifier-free which is true in every Hilbertian fields but false in a infinite field K. Consider the function field K(t). According to Theorem 2.35, K(t) is a Hilbertian field. Note that K is existentially closed in K(t) by Theorem 4.29. Takes $m, n = 1$ in Proposition 4.28 and we get $K(t) \models \exists x \forall y \neg \varphi(x, y)$ which contradicts to our assumption. This proves our claim. □

In the following paragraphs, we prove the decidability of the $\forall\exists$ theory of PAC fields. The proof is similar to the proof of the decidability of the $\forall\exists$ theory of Hilbertian fields. First we demonstrate the case in characteristic 0. For PAC fields, the algebraically closed property implies the existentially closed property as following theorem shows. This gives us a way to use regular extension condition in Theorem 4.15 and preservation theorem of $\exists^n\forall^m$ sentences for arbitrary m,n under existential closedness.

Theorem 4.34. *[15, Proposition 11.3.5] A field K is PAC if and only if K is existentially closed in every regular extension.*

Theorem 4.35. *The $\forall\exists$ theory of PAC fields of characteristic 0 is decidable.*

Proof. From Corollary 4.11, the $\forall\exists$ theory of Hilbertian PAC fields of characteristic 0 is decidable. If we shows that the $\forall\exists$ theory of PAC fields of characteristic 0 and the $\forall\exists$ theory of Hilbertian PAC fields of characteristic 0 are identical, then we get the desired result.

Since every Hilbertian PAC field of characteristic 0 is a PAC field of characteristic 0, the $\forall\exists$ theory of PAC fields of characteristic 0 is contained in the $\forall\exists$ theory of Hilbertian PAC fields of characteristic 0. On the other hand, let's assume that there exists an $\forall\exists$ sentence $\forall x \exists y \varphi(x, y)$ with $\varphi(x, y)$ quantifier-free which is true in every Hilbertian PAC field of characteristic 0 but false in a PAC field P of characteristic 0. From Theorem 4.15 we can find a Hilbertian PAC field K of characteristic 0 which is regular extension of P. Then Theorem 4.34 shows that P is existentially closed in K. Take $m, n = 1$ in Proposition 4.28 and conclude that $K \models \exists x \forall y \neg \varphi(x, y)$ which contradicts to our assumption. □

Corollary 4.36. *The $\forall^m\exists^n$ theory of PAC fields of characteristic 0 is decidable for arbitrary integers m,n.*

Proof. From Corollary 4.11, the $\forall^m\exists^n$ theory of Hilbertian PAC fields of characteristic 0 is decidable for arbitrary integers m,n. Notice that Proposition 4.28 shows the preservation of $\exists^n\forall^m$ sentences for all $m, n \in \mathbb{N}$ over any $\mathcal{L}$-structures under existential closedness. Then we can modify the proof in Theorem 4.35 to show that the $\forall^m\exists^n$ theory of PAC fields of characteristic 0 and the $\forall^m\exists^n$ theory of Hilbertian PAC fields of characteristic 0 are identical. This proves the desired result. □

Notice that the Corollary 4.11 does not show the decidability of Hilbertian PAC field. So we need to seek other $\forall\exists$ theory of some structures to prove the decidability of $\forall\exists$ theory of PAC fields. Observe that from Theorem 4.25 and Theorem 4.34 that the $\forall\exists$ theory of Hilbertian fields of characteristic 0 and the $\forall\exists$ theory of PAC fields of characteristic 0 are identical. Also, the following theorem connects general fields and PAC fields through totally transcendental extension.

Theorem 4.37. *[48, P.209] Every field K has a totally transcendental extension F which is a PAC field.*

Therefore, we may prove the decidability of $\forall\exists$ theory of PAC fields through Hilbertian fields.

Theorem 4.38. *The $\forall\exists$ theory of PAC fields is decidable.*

Proof. We claim the the $\forall\exists$ theory of PAC fields and the $\forall\exists$ theory of Hilbertian fields are identical. Then Theorem 4.33 implies the theorem.

Suppose that there exists an $\forall\exists$ sentence $\forall x \exists y \varphi(x, y)$ with $\varphi(x, y)$ quantifier-free which is true in every PAC fields but false in a Hilbertian field H. By Theorem 4.37, we can find a PAC field P which is totally transcendental extension of H. Using Lemma 4.24, we have $P \models \exists x \forall y \neg\varphi(x, y)$ which contradicts to our assumption. Conversely, assume that there exists an $\forall\exists$ sentence $\forall x \exists y \varphi(x, y)$ with $\varphi(x, y)$ quantifier-free which is true in every Hilbertian fields but false in a PAC field P. Consider the function field P(t) which is a Hilbertian field by Theorem 2.35. According to Theorem 4.29, P is existentially closed in P(t). Then take $m, n = 1$ in Proposition 4.28 $P(t) \models \exists x \forall y \neg\varphi(x, y)$ which contradicts to the assumption. Therefore, we have proved our claim. □

Chapter 5

Conclusion

In this thesis, we have proved the following results:

1. The $\forall^n \exists$ sentence over number field is preserved under the existentially closedness,

2. The $\exists\forall$ theory of Hilbertian fields of characteristic 0 and perfect Hilbertian fields are decidable,

3. The $\forall\exists$ theory of Hilbertian fields of characteristic 0 and Hilberitan fields are all decidable,

4. The $\forall\exists$ theory of PAC fields of characteristic 0 and PAC field are decidable.

From [43], we know that there are still no effective methods to solve the decidability of $\exists\forall$ theory of different fields. Also, since Hilbert's tenth problem over $\mathbb{Q}$ and number fields are still open, we propose the following problems for the future developments.

Problem 5.1. Are these following theories decidable ?

1. $\forall^n \exists$ theory of number fields for arbitrary n,

2. $\exists\forall$ theory of PAC fields,

3. $\exists\forall$ theory of number fields,

4. $\exists\forall$ theory of fields of characteristic 0,

5. $\exists\forall$ theory of fields.

Bibliography

[1] J. Ax, S. Kochen, Diophantine problems over local fields III: Decidable fields, *Ann. of Math.*, Vol. 83 (1966), No. 3, 437-456.

[2] J. Ax, Solving diophantine problems modulo every prime, *Ann. of Math.*, Vol. 85 (1967), No. 2, 161-183.

[3] J. Ax, The Elementary Theory of Finite Fields *Anna. of Math.*, Vol. 88 (1968), No. 2, 239-271.

[4] J. Barwise, *An Introduction to First-Order Logic*, In *Handbook of mathematical logic*, J. Barwise (ed.), North-Holland, Amsterdam, 1977, pp. 5-46.

[5] W. W. Boone, F. B. Cannonito and R. C. Lyndon, *Word Problems*, North-Holland, Amsterdam, 1973.

[6] J. V. Brawley and G. E. Schnibben, *Infinite Algebraic Extensions of Finite Fields*, contemporary Mathematics, Vol. 95, American Mathematical Society, New York, 1989.

[7] G. Cherlin, L, v. d. Dries, A. MacIntyre, Decidability and Undecidability theorem for PAC-fields, *Bull. Amer. Math. Soc.(N.S.)*, Vol. 4 (1981), No. 1, 101-104.

[8] H. Cohen, *A course in Computational Algebraic Number Theory*, Graduate Text in Mathematics, Vol. 183, Springer-Verlag, Berlin, 2000.

[9] D. A. Cox, J. Little and D. O'Shea, *Ideals, Varieties, and Algorithms (Second Edition)*, Undergraduate Text in Mathematics, Springer-Verlag, New York, 1998.

[10] C. C. Chang and H. J. Keisler, *Model theory*, Dover Publications, New York, 2012.

[11] M. Davis, Yu. Matijacevič and J. Robinson, Hilbert's Tenth Problem. Diophantine equations: positive aspects of a negative solution, *Proc. Symposia Pure Math.* Vol. 28, 1976, pp. 223-378.

[12] Yu. L. Ershov, I. A. Lavrov, A. D. Taimanov and M. A. Taitslin, Elementary Theories, *Russian Math. Surveys*, Vol.20 (1965), No.4, 35-105.

[13] H. B. Enderton, *A Mathematical Introduction to Logic (Second Edition)*, Academic Press, New York, 2001.

[14] Y. Ershov, Fields with a solvable theory, *Soviet Math. Dokl.*, Vol. 8 (1967), No. 3, 575-576.

[15] M. D. Fried and M. Jarden, *Field Arithmetic, revised and enlarged by M. Jarden*, Ergebnisse der Mathematik und ihrer Grenzgebiete, vol. 11 (Second Edition), Springer-Verlag, Berlin, 2005.

[16] M. D. Fried, D. Haran, M. Jarden, Galois stratification over Frobenius fields, *Advance in Mathematics*, Vol. 51 (1984), No. 1, 1-35.

[17] K. Gödel, *Ü*ber formal unentscheidbare Sätz der Principia Mathematica und verwandter Systeme, I. *Monatsh. Math. Phys.,* No. 38 (1931), 173-198.

[18] M. Jarden, *Algebraic Patching*, Springer Monograph in Mathematics, Springer, Heidelberg, 2011.

[19] J. P. Jones, Universal Diophantine equation, *The Journal of Symbolic Logic*, Vol. 47 (1982), No. 3, 549-571.

[20] J. P. Jones, Classification of quantifier prefixes over Diophantine equations, *Zeitschrift fur mathematische Logik und Grundlagen der Mathematik*, Vol. 27 (1981), 403-410.

[21] J. Koenigsmann, Defining $\mathbb{Z}$ in $\mathbb{Q}$, *Ann. of Math.*, Vol. 183 (2016), No. 1, 73-93.

[22] C. H. Langford, Theorems on deducibility, *Ann. of Math.*, (Ser. 2) Vol .28 (1927), 459-471.

[23] Yu. Matijacevič and J. Robinson, Reduction of an arbitrary Diophantine equation to one in 13 unknowns, *Acta Arith.*, Vol. 27 (1975), 521-553.

[24] D. Marker, *Introduction to the Model theory of Fields*, In *Model Theory of Fields*, D. Marker, M. Messmer and A. Pillay, Springer-Verlag, Berlin, 1997, pp. 1-37.

[25] P. Morandi, *Field and Galois Theory*, Graduate Text in Mathematics, Vol. 167, Springer-Verlag, New York, 1996.

[26] J. D. Monk, *Mathematical logic*, Graduate Text in Mathematics, Vol. 37, Springer-Verlag, New York, 1976.

[27] H. Ono, Equational theories and universal theories of fields, *J. Math. Soc. Japan*, Vol. 35 (1983), N0.2, 289-306.

[28] J. Park, A universal first order formula defining the ring of integers in a number field, *Mathematical Research Letters*, Vol. 20 (2013), No.5, 961-980.

[29] B. Poonen, Undecidability in number theory, *Notice Amer. Math. Soc.*, Vol 55 (2008), No. 3, 344-350.

[30] B. Poizat, *A course in model theory: an introduction to contemporary mathematical logic*, Springer-Verlag, New York, 2000.

[31] A. Quarteroni, R. Sacco and F. Saleri, *Numerical Mathematics (Second Edition)*, Texts in Applied Mathematics, Springer-Verlag, Berlin, 2007.

[32] M. O. Rabin, *Decidable theories*, In *Handbook of mathematical logic*, J. Barwise (ed.), North-Holland, Amsterdam, 1977, pp. 595-630.

[33] P. Ribenboim, Remarks on existentially closed fields and diophantine equations, *Rend. Sem. Mat. Univ. Padova*, vol. 71 (1984), 229-237.

[34] J. B. Robinson, Definability and decision problems in arithmetic, *The Journal of Symbolic Logic*, Vol. 14 (1949), No. 2, 98-114.

[35] J. B. Robinson, The undecidability of algebraic rings and fields, *Proceedings of the American Mathematical Society*, Vol. 10 (1959), 279-284.

[36] J. B. Robinson, The decision problem for fields, In *The theory of Models*, C. Karp, et al., North-Holland, Amsterdam, 1965, pp. 299-311.

[37] W. Szmielew, Elementary properties of Abelian groups, *Fund. Math.*, Vol. 41 (1954), No. 2, 203-271.

[38] R. I. Soare, *Recursively Enumerable Set and Degrees: A study of computable functions and computably generated sets*, Springer-Verlag, Berlin Heidelberg, 1987.

[39] Z. W. Sun, Further Results on Hilbert's Tenth Problem, (2017), arXiv: 1704.03504.

[40] A. Tarski, *A Decision Method for Elementary Algebra and Geometry,* Prepared for publication with the assistance of J. C. C. McKinsey, 2nd revised ed., University of California Press, Berkeley and Los Angeles, 1951.

[41] S. P. Tung, On weak number theories, *Japan. J. Math. (N.S.)*, Vol. 11 (1985), No. 2, 203-232.

[42] S. P. Tung, Provability and Decidability of Arithmetical Universal-Existential Sentences, *Bulletin of the London Mathematical Society*, vol. 18 (1986), No. 3, 241-247.

[43] S. P. Tung, Decidable fragments of field theories, *The Journal of Symbolic Logic*, vol. 55 (1990), No. 3, 1007-1018.

[44] S. P. Tung, Algorithms for sentences over integral domains, *Annals of Pure and Applied Logic*, Vol. 47 (1990), No. 2, 189-197.

[45] S. P. Tung, Sentences over Integral Domains and Their Computational Complexities *Information and Computation*, Vol. 149 (1999), No. 2, 99-133.

[46] S. P. Tung, Computational complexity of sentences over fields, *Information and Computation*, vol. 206 (2008), No. 7, 791-805.

[47] H. Völklein, *Groups as Galois Groups : An introduction*, Cambridge University Press, 1996.

[48] W. H. Wheeler, Model-complete theories of pseudo-algebraically closed fields, *Annals of Mathematical Logic*, vol. 17 (1979), No. 3, 205-226.