ABSTRACT

DIOPHANTINE GENERATION, GALOIS THEORY, AND HILBERT'S TENTH PROBLEM

by

Kendra Kennedy

April, 2012

Chair: Dr. Alexandra Shlapentokh

Major Department: Mathematics

Hilbert's Tenth Problem was a question concerning existence of an algorithm to determine if there were integer solutions to arbitrary polynomial equations over $\mathbb{Z}$. Building on the work by Martin Davis, Hilary Putnam, and Julia Robinson, in 1970 Yuri Matiyasevich showed that such an algorithm does not exist. One can ask a similar question about polynomial equations with coefficients and solutions in the rings of algebraic integers. In this thesis, we survey some recent developments concerning this extension of Hilbert's Tenth Problem. In particular we discuss how properties of Diophantine generation and Galois Theory combined with recent results of Bjorn Poonen, Barry Mazur, and Karl Rubin show that the Shafarevich-Tate conjecture implies that there is a negative answer to the extension of Hilbert's Tenth Problem to the rings of integers of number fields.

DIOPHANTINE GENERATION, GALOIS THEORY, AND HILBERT'S TENTH PROBLEM

A Thesis

Presented to

The Faculty of the Department of Mathematics

East Carolina University

In Partial Fulfillment

of the Requirements for the Degree

Master of Arts in Mathematics

by

Kendra Kennedy

April, 2012

DIOPHANTINE GENERATION, GALOIS THEORY, AND HILBERT'S TENTH PROBLEM

by

Kendra Kennedy

APPROVED BY:

DIRECTOR OF THESIS:

Dr. Alexandra Shlapentokh

COMMITTEE MEMBER:

Dr. M.S. Ravi

COMMITTEE MEMBER:

Dr. Chris Jantzen

COMMITTEE MEMBER:

Dr. Richard Ericson

CHAIR OF THE DEPARTMENT
OF MATHEMATICS:

Dr. Johannes Hattingh

DEAN OF THE
GRADUATE SCHOOL:

Dr. Paul Gemperline

ACKNOWLEDGEMENTS

I would first like to express my deepest gratitude to my thesis advisor, Dr. Shlapentokh. It was not only a great pleasure, but an honor for me to work with her. I am thankful for her guidance, encouragement, and faith in me throughout the thesis process. Also, I appreciate the amount of time she spent making sure I understood the material fully, prompting its success.

Next, I want to give a special thanks to Dr. Benson for his guidance, time, and support during my graduate studies at East Carolina University. I would like to recognize my teaching mentor, Dr. Ries, who has always provided excellent advice and words of encouragement. Additionally, I want to thank my undergraduate advisor, Dr. Poliakova, who inspired me to pursue mathematics.

For encouraging me to pursue my dreams and believing that I am capable, I want to thank my family, especially my parents, for their unending support. I dedicate this thesis to them.

TABLE OF CONTENTS

CHAPTER 1: Introduction

In the 1900s, David Hilbert proposed a list of 23 problems that would greatly influence mathematics in the twentieth century. His tenth problem, known as Hilbert's Tenth Problem (HTP), dealt with the solvability of Diophantine equations. In particular, he wanted to know whether it was possible to create an algorithm that could tell whether a polynomial equation in many variables had solutions in the integers.

After many years, it was discovered that no such algorithm existed. Yuri Matiyasevich proved that Diophantine subsets of $\mathbb{Z}$ were the same as computably enumerable sets. His proof was based on the earlier work of Martin Davis, Hilary Putnam, and Julia Robinson. (See [4] for the details of the solution of the original problem.) The fact that Diophantine and recursively enumerable sets were the same implied that Hilbert's Tenth Problem was unsolvable. The solution to Hilbert's Problem gave rise to new questions; in particular, whether HTP was solvable over rings of integers of number fields. In this thesis, we consider some of the developments which led to a partial answer to this question.

This thesis is divided into the following sections: the first chapter presents the necessary background from Recursion Theory and explains the exact nature of the result by Yuri Matiyasevich, Martin Davis, Hilary Putnam, and Julia Robinson; the second chapter introduces the necessary material from Algebra and more specifically, Galois Theory; the third section introduces the notion of Diophantine generation and explains the main results concerning rings of integers of number fields.

CHAPTER 2: Computability

This chapter contains some basic information on computable functions, sets, rings, and fields. In this chapter and throughout, we will use the terms "computable," "decidable," and "recursive" interchangeably.

In addition, throughout this thesis we will use $\mathbb{Z}_{\geq 0}$ to mean non-negative integers and $\mathbb{Z}_{>0}$ to mean positive integers.

2.1 Computable Sets and Functions

First we want to define computable sets. In order to do this, we must define the characteristic function of a set.

Definition 2.1 (Characteristic Function)**.** For $A \subset \mathbb{Z}_{\geq 0}^m$, the characteristic function is defined in the following way:

$$\chi_A : \mathbb{Z}_{\geq 0}^m \to \{0, 1\}$$

$$\chi_A(x_1, ..., x_m) = \begin{cases} 1 \text{ if } (x_1, ..., x_m) \in A \\ 0 \text{ if } (x_1, ..., x_m) \notin A. \end{cases}$$

We now define computable functions, computable sets, and computably enumerable sets.

Definition 2.2.

- If $f : \mathbb{Z}_{\geq 0}^m \longrightarrow \mathbb{Z}_{\geq 0}^k$ for some positive integers m and k, then f is called computable if there exists a computer program or an algorithm to compute f.
- If $A \subseteq \mathbb{Z}_{\geq 0}^m$ and χ_A is computable, then we say the set is computable.

- If there is an algorithm or a computer program that can list the elements of a set, we say the set is computably enumerable.

The following classical theorem laid the ground work for solving HTP. (See [7] for more details.)

Theorem 2.3. *There are computably enumerable sets that are not computable.*

In particular, the following famous set is computably enumerable but not computable.

Example 2.4. Let φ_n be the n^{th} program in the listing of all possible programs and define the Halting Set as follows:

$$K = \{n|\varphi_n(n) \text{ terminates on input n}\}.$$

Before we can state the main theorem that led to the solution of Hilbert's Tenth Problem, we need to introduce the notion of Diophantine sets.

Definition 2.5. Let R be an integral domain. Let m and n be positive integers. Let $A \subset R^n$. We say A has a Diophantine definition over R if there exists a polynomial

$$f(y_1, ..., y_n, x_1, ..., x_m) \in R[y_1, .., y_n, x_1, ..., x_m]$$

such that for all $(t_1, ..., t_n) \in R^n$, we have

$$(t_1, ..., t_n) \in A \Leftrightarrow \exists x_1, ..., x_m \in R, f(t_1, ..., t_n, x_1, ..., x_m) = 0.$$

This set A is called Diophantine over R.

Now we state an example of a Diophantine set over $\mathbb{Z}$.

Example 2.6. The set of even integers

$$\{y \in \mathbb{Z} | \exists x \in \mathbb{Z} : y = 2x\}$$

is a Diophantine set over $\mathbb{Z}$.

Yuri Matiyasevich, Martin Davis, Hilary Putnam, and Julia Robinson proved the following theorem that we will refer to as the MDPR Theorem.

Theorem 2.7. *Diophantine sets of tuples of nonnegative integers are the same as computably enumerable sets.*

There are two immediate corollaries of the MDPR Theorem.

Corollary 2.8. *There are Diophantine sets which are undecidable.*

Corollary 2.9. *HTP is unsolvable.*

Proof. Indeed, suppose $A \subset \mathbb{Z}$ is a non-recursive Diophantine set with a Diophantine definition $P(T, X_1, \ldots, X_k)$. Assume also that we have an algorithm to determine the existence of integer solutions for polynomials. Now, let $a \in \mathbb{Z}$ and observe that $a \in A$ if and only if $P(a, X_1, \ldots, X_K) = 0$ has solutions in $\mathbb{Z}^k$. So if we can answer Hilbert's question algorithmically, we can determine the membership in A algorithmically. □

2.2 Some Examples of Computable and Non-computable Sets

An example of a decidable set is the set of all primes. The set of all primes is decidable because we can test algorithmically for primality. Now we consider whether a subset of all the primes is decidable or not.

Claim 2.10. *Let $P = \{2, 3, 5, ...\} = \{P_1, P_2, P_3, ...\}$ be the set of all primes. Let $A = \{P_{i_1}, ..., P_{i_k}, ..\}$ be a subset of primes. Let $I = \{i_1, ..., i_k, ...\}$ be the indexes of the primes in A. In this case, A is decidable if and only if I is decidable.*

Proof. Suppose I is decidable. Let $n \in \mathbb{Z}_{\geq 0}$ and consider the following procedure for determining whether $n \in A$.

Procedure:

1. Determine if n is a prime. If not, then $n \notin A$. If yes, proceed to step 2.
2. Find i such that $n = P_i$. List P until n occurs.
3. Check whether $i \in I$. If yes, $n \in A$. If no, $n \notin A$.

Conversely, assume A is decidable. We will show I is decidable. Let $i \in \mathbb{Z}_{>0}$ be given. Consider the procedure below to determine whether $i \in I$.

Procedure:

1. Find P_i. That is, list $P_1, P_2, ..., P_i$ until we reach P_i.
2. Check whether $P_i \in A$. If yes, $i \in I$. If not, $i \notin I$.

□

2.3 Computable and Non-computable Rings and Fields

Definition 2.11. A ring R is recursive (computable) if there exists an injective map $j : R \to \mathbb{Z}_{\geq 0}$ such that

1. $j(R)$ is computable
2. $\{(j(a), j(b), j(c)) | c = a + b\}$ is computable.
3. $\{(j(a), j(b), j(c)) | c = ab\}$ is computable.

We observe that $\mathbb{Z}$ and $\mathbb{Q}$ are recursive, since the set of all integers can be represented as a pair of non-negative integers (a, b), where $a = 0$ if the integer is non-negative and $a = 1$ otherwise, and b is the absolute value of the integer. Similarly, $\mathbb{Q}$

can be represented by a triple of non-negative integers. Further, it is easy to describe addition, multiplication, and division using these codes.

We continue with two examples which show that it is not hard to construct rings and fields that are not computable.

Example 2.12. Let I be an undecidable set and let $A = \{P_i | i \in I\}$ be an undecidable set of primes. Then we have that $F = \mathbb{Q}(\sqrt{P_i}, i \in I)$ is an undecidable field.

Example 2.13. Let I be an undecidable set of primes and let $S = \{P_i | i \in I\}$. Then we have that $O_{\mathbb{Q},S} = \{\frac{m}{n} | m \in \mathbb{Z},\ n \in \mathbb{Z}_{\neq 0},\ n \text{ is divisible by primes in } S \text{ only}\}$ is an undecidable ring.

In general we have the following result whose proof can be found in [8][Appendix A].

Theorem 2.14. *If R is a recursive integral domain and there is an algorithm to determine if an element of R has an inverse, then*

1. *the fraction field of R is recursive,*
2. *any finite extension of the fraction field is recursive, and*
3. *the integral closure of R in a finite extension is recursive.*

CHAPTER 3: Galois Theory

Our goal in this chapter is to survey the results from Galois Theory that will be used to show the undecidability of Hilbert's Tenth Problem over number fields. As a general reference for this material we recommend [1] and [2]. All the fields we consider below will be of characteristic zero. We start with the notion of field homomorphism.

Definition 3.1 (Field Homomorphism)**.** Let K and L be fields and let $\sigma : K \longrightarrow L$ be such that $\sigma(0_K) = 0_L$ and $\sigma(1_K) = 1_L$, and for any two elements $x, y \in K$ we have that $\sigma(x + y) = \sigma(x) + \sigma(y)$ and $\sigma(xy) = \sigma(x)\sigma(y)$. In this case, σ is called a field homomorphism. If σ is a bijection, then σ is called an isomorphism. If $K = L$ and σ is a bijection, then σ is called an automorphism.

Remark 3.2. It is not hard to show that a field homomorphism sends multiplicative and additive inverses to multiplicative and additive inverses.

We will now discuss several important properties of fields and homomorphisms.

Proposition 3.3. *If $\sigma : \mathbb{Q} \to \mathbb{Q}$ is a homomorphism, then σ is the identity map.*

Proof. Since σ is a homomorphism for both addition and multiplication, we have that $\sigma(0) = 0$ and $\sigma(1) = 1$. By induction, for $n \in \mathbb{Z}_{>0}$ we have

$$\sigma(n) = \sigma(\underbrace{1 + 1 + ... + 1}_{\text{n times}}) = \underbrace{\sigma(1) + \sigma(1) + ... + \sigma(1)}_{\text{n times}} = \underbrace{1 + 1 + ... + 1}_{\text{n times}} = n.$$

Since $\sigma(-x) = -\sigma(x)$ for all $x \in \mathbb{Q}$, we have that $\sigma(-n) = -\sigma(n) = -n$ for all $n \in \mathbb{Z}_{>0}$. Similarly, for any $x \in \mathbb{Q}^*$, $\sigma\left(\frac{1}{x}\right) = \frac{1}{\sigma(x)}$, and therefore for any $m \in \mathbb{Z}_{\neq 0}$ we have $\sigma\left(\frac{1}{m}\right) = \frac{1}{\sigma(m)} = \frac{1}{m}$. Finally, let $x = \frac{P}{Q}$ be any non-zero element of $\mathbb{Q}$ with $Q \neq 0$, and observe that $\sigma(x) = \sigma\left(\frac{P}{Q}\right) = \frac{\sigma(P)}{\sigma(Q)} = \frac{P}{Q}$. □

Corollary 3.4. *The only automorphism of* $\mathbb{Q}$ *is the identity map.*

Definition 3.5. A field G is algebraically closed if every polynomial over G has a root in G.

Definition 3.6. If F is a field, then the algebraic closure of F is the smallest algebraically closed field containing F.

Definition 3.7. Let E be an algebraic extension of a field F. In this case, $\alpha \in E$ and $\beta \in E$ are called conjugate over F if $\text{irr}(\alpha, F) = \text{irr}(\beta, F)$, where $\text{irr}(\alpha, F)$ is the monic irreducible polynomial for α over F and $\text{irr}(\beta, F)$ is the monic irreducible polynomial for β over F. In particular, α and β are zeros of the same irreducible monic polynomial over F.

Proposition 3.8. *Let* G/F *be a finite extension generated by* $\alpha \in G$. *Let* $1, \alpha, ..., \alpha^{n-1}$ *be the basis of* G/F *generated by powers of* α. *In this case,* $\alpha^j = \sum_{i=1}^{n-1} A_{i,j}\alpha^i$, *where* $A_{i,j}$ *depend only on* i *and* j *and the irreducible polynomial of* α. *More specifically,* $A_{i,j}$ *is a fixed polynomial in the coefficients of* $irr(\alpha, F)$. *In other words,* $A_{i,j} = P_{i,j}(B_0, \ldots, B_{n-1})$, *where* $B_0, \ldots, B_{n-1}$ *are the coefficients of the irreducible polynomial of* α *over* F *and each* $P_{i,j}(x_0, \ldots, x_{n-1}) \in F[x_o, ..., x_{n-1}]$ *is fixed.*

Proof. We proceed by induction.

Base Case:

For $j = 0, ..., n-1$, we have $P_{i,i} = 1$ for $i = j$ and $P_{i,j} = 0$ for $i \neq j$.

Induction Step:

Assume for $j \leq k$, we have $\alpha^j = \sum_{i=0}^{n-1} A_{i,j}\alpha^i$. We want to show $\alpha^{k+1} = \sum_{i=0}^{n-1} A_{i,k+1}\alpha^i$.

We have $\alpha^n + B_{n-1}\alpha^{n-1} + ... + B_0 = 0$. Multiplying by α^m, we obtain

$$\alpha^{n+m} + B_{n-1}\alpha^{n-1+m} + ... + B_0\alpha^m = 0.$$

Now assuming $k+1 \geq n$ and $k+1-n = m$, we obtain

$$\alpha^{k+1} + B_{n-1}\alpha^k + ... + B_0\alpha^m = 0.$$

Thus,

$$\alpha^{k+1} = -\sum_{r=1}^{n-1} B_{n-r}\alpha^{k-r+1}.$$

By the induction hypothesis, we have

$$\alpha^{k+1} = -\sum_{r=1}^{n-1} B_{n-r} \sum_{i=0}^{n-1} A_{i,k-r+1}\alpha^i.$$

Thus,

$$\begin{aligned} \alpha^{k+1} &= \sum_{i=0}^{n-1}\sum_{r=1}^{n-1} A_{i,k-r+1}B_{n-r}\alpha^i \\ &= \sum_{i=0}^{n-1} \alpha^i \left(\sum_{r=1}^{n-1} A_{i,k-r+1}B_{n-r} \right), \end{aligned}$$

where $\sum_{r=1}^{n-1} A_{i,k-r+1}B_{n-r}$ is a polynomial in $B_0, \ldots, B_{n-1}$ depending only on i, k, and n. □

Theorem 3.9. *Let F be a field and let α and β be conjugate over F with*

$$\deg(\alpha, F) = \deg(\beta, F) = n,$$

where $\deg(\alpha, F)$ is the degree of α over F and $\deg(\beta, F)$ is the degree of β over F. In this case,

$$\Psi_{\alpha,\beta} : F(\alpha) \to F(\beta)$$

defined by

$$\Psi_{\alpha,\beta}(a_0 + a_1\alpha + ... + a_{n-1}\alpha^{n-1}) = a_0 + a_1\beta + ... + a_{n-1}\beta^{n-1}$$

is an isomorphism of fields.

Proof. By definition, we have

$$\Psi_{\alpha,\beta}(a_0 + a_1\alpha + ... + a_{n-1}\alpha^{n-1}) = a_0 + a_1\beta + ... + a_{n-1}\beta^{n-1} \in F(\beta).$$

Thus, we have a well-defined map whose domain is all of $F(\alpha)$.

We now show that $\Psi_{\alpha,\beta}$ is a homomorphism of fields. For addition, we have

$$\begin{aligned}
\Psi_{\alpha,\beta}\left(\sum_{i=0}^{n-1} a_i\alpha^i + \sum_{i=0}^{n-1} b_i\alpha^i\right) &= \Psi_{\alpha,\beta}\left(\sum_{i=0}^{n-1}(a_i + b_i)\alpha^i\right) \text{ (by the distributive law)} \\
&= \sum_{i=0}^{n-1}(a_i + b_i)\beta^i \text{ (by definition)} \\
&= \sum_{i=0}^{n-1} a_i\beta^i + \sum_{i=0}^{n-1} b_i\beta^i \text{ (by distributivity)} \\
&= \Psi_{\alpha,\beta}\left(\sum_{i=0}^{n-1} a_i\alpha^i\right) + \Psi_{\alpha,\beta}\left(\sum_{i=0}^{n-1} b_i\alpha^i\right) \text{ (by definition)}
\end{aligned}$$

For multiplication, we have the following equalities which hold in part by Proposition 3.8 (we are using the same notation as in this proposition)

$$\begin{aligned}
\Psi_{\alpha,\beta}\left(\left(\sum_{i=0}^{n-1} a_i\alpha^i\right)\left(\sum_{j=0}^{n-1} b_j\alpha^j\right)\right) &= \Psi_{\alpha,\beta}\left(\sum_{i,j=0}^{n-1} a_i b_j \alpha^{i+j}\right) \\
&= \Psi_{\alpha,\beta}\left(\left(\sum_{i,j=0}^{n-1} a_i b_j\right)\left(\sum_{k=0}^{n-1} A_{i+j,k}\alpha^k\right)\right) \\
&= \Psi_{\alpha,\beta}\left(\sum_{k=0}^{n-1}\left(\sum_{m=0}^{2n-2}\sum_{i+j=m;i,j=0}^{n-1} A_{m,k}a_i b_j\right)\alpha^k\right)
\end{aligned}$$

$$
\begin{aligned}
&= \sum_{k=0}^{n-1} \left(\sum_{m=0}^{2n-2} \sum_{i+j=m;i,j=0}^{n-1} A_{m,k} a_i b_j \right) \beta^k \\
&= \left(\sum_{i,j=0}^{n-1} a_i b_j \right) \left(\sum_{k=0}^{n-1} A_{i+j,k} \beta^k \right) \\
&= \sum_{i,j=0}^{n-1} a_i b_j \beta^{i+j} (\text{since } \beta \text{ and } \alpha \text{ are conjugates}) \\
&= \left(\sum_{i=0}^{n-1} a_i \beta^i \right) \left(\sum_{j=0}^{n-1} b_j \beta^j \right) \\
&= \Psi_{\alpha,\beta} \left(\sum_{i=0}^{n-1} a_i \alpha^i \right) \Psi_{\alpha,\beta} \left(\sum_{j=0}^{n-1} b_j \alpha^j \right)
\end{aligned}
$$

Now, we must show that $\Psi_{\alpha,\beta}$ is a bijection. First note that $\Psi_{\alpha,\beta}$ is onto since every element of $F(\beta)$ is of the form $\sum_{i=0}^{n-1} a_i \beta^i = \Psi_{\alpha,\beta}(\sum_{i=0}^{n-1} a_i \alpha^i)$. Now, let us show that $\Psi_{\alpha,\beta}$ is one-to-one. Suppose $\Psi_{\alpha,\beta}(\sum_{i=0}^{n-1} a_i \alpha^i) = \Psi_{\alpha,\beta}(\sum_{i=0}^{n-1} b_i \alpha^i)$. In this case, we have $(\sum_{i=0}^{n-1} a_i \beta^i) = (\sum_{i=0}^{n-1} b_i \beta^i)$. Thus, $a_i = b_i$ for $i = 0, 1, ..., n-1$, since $\{1, \ldots, \beta^{n-1}\}$ is a basis of $F(\beta)$ over F. Hence, $\sum_{i=0}^{n-1} a_i \alpha^i = \sum_{i=0}^{n-1} b_i \alpha^i$. □

The following lemma is a generalization of the previous theorem.

Lemma 3.10. *Let F and F' be fields and let α be algebraic over F and β be algebraic over F'. Further, let $p(x) = irr(\alpha, F)$ and $q(x) = irr(\beta, F')$. Let $\sigma : F \longrightarrow F'$ be an isomorphism of fields such that*

$$\sigma(p(x)) = q(x).$$

Now extend

$$\sigma : F(\alpha) \to F'(\beta)$$

by setting

$$\sigma\left(\sum_{i=0}^{n-1=\deg(p(x))-1} a_i\alpha^i\right) = \sum_{i=0}^{n-1=\deg(p(x))-1} \sigma(a_i)\beta^i$$

for any n-tuple $a_0, \ldots, a_{n-1} \in F$. *In this case, the extended* σ *is an isomorphism of fields.*

Proof. First notice that we have $p(x)$ is irreducible if and only if $q(x)$ is irreducible. That is, $\deg(p(x)) = \deg(q(x))$. Thus, we have that the extended σ is a bijection because $\{1, \alpha, .., \alpha^{n-1}\}$ and $\{1, \beta, ..., \beta^{n-1}\}$ are bases of $F(\alpha)$ over F and $F'(\beta)$ over F' respectively and because σ is a bijection.

Now it remains to show that the extended σ is a homomorphism. Here we use the fact that we are working with fields of characteristic zero. For any $i \in \mathbb{Z}_{\geq 0}$, we have that

$$\alpha^i = \sum_{j=0}^{n-1} A_{i,j}\alpha^j = \sum_{j=0}^{n-1} Q_{i,j}(a_0, ..., a_{n-1})\alpha^j,$$

where $A_{i,j} = Q_{i,j}(a_0, ..., a_{n-1})$, $a_0 + a_1x + \ldots + x^n = \text{irr}(\alpha, F)$, and $Q_{i,j}(x_0, ..., x_{n-1}) \in \mathbb{Q}[x_0, ..., x_{n-1}]$ is a fixed polynomial over $\mathbb{Q}$ depending on i, j and n only by Proposition 3.8. First we see that

$$\sigma(A_{i,j}) = \sigma(Q_{i,j}(a_0, ..., a_{n-1})) = Q_{i,j}(\sigma(a_0), ..., \sigma(a_{n-1})),$$

since the coefficients of $Q_{i,j}$ are in $\mathbb{Q}$ and are not be moved by σ by Proposition 3.3. Let $x = \sum_{i=0}^{n-1} c_i\alpha^i$ and $y = \sum_{i=0}^{n-1} b_i\alpha^i$ where $c_i \in F$ and $b_i \in F$. For addition, we have

$$\begin{aligned}\sigma(x+y) &= \sigma\left(\sum_{i=0}^{n-1} c_i\alpha^i + \sum_{i=0}^{n-1} b_i\alpha^i\right) \\ &= \sigma\left(\sum_{i=0}^{n-1}(c_i + b_i)\alpha^i\right)\end{aligned}$$

$$
\begin{aligned}
&= \sum_{i=0}^{n-1} (c_i + b_i)\beta^i \\
&= \sum_{i=0}^{n-1} c_i\beta^i + \sum_{i=0}^{n-1} b_i\beta^i \\
&= \sum_{i=0}^{n-1} \sigma(c_i)\beta^i + \sum_{i=0}^{n-1} \sigma(b_i)\beta^i.
\end{aligned}
$$

For multiplication, we have

$$
\begin{aligned}
\sigma(xy) &= \sigma\left(\left(\sum_{i=0}^{n-1} c_i\alpha^i\right)\left(\sum_{j=0}^{n-1} b_j\alpha^j\right)\right) \\
&= \sigma\left(\sum_{i,j=0}^{n-1} c_i b_j \alpha^{i+j}\right) \\
&= \sigma\left(\sum_{k=0}^{n-2}\left(\sum_{i+j=k} c_i b_j\right)\alpha^k\right) \\
&= \sigma\left(\sum_{k=0}^{n-2}\left(\sum_{r=0}^{k} c_r b_{k-r}\right)\left(\sum_{i=0}^{n-1} Q_{i,k}(a_0, ..., a_{n-1})\alpha^i\right)\right) \\
&= \sigma\left(\sum_{i=0}^{n-1}\left(\sum_{k=0}^{n-2}\sum_{r=0}^{k} c_r b_{k-r} Q_{i,k}(a_0, ..., a_{n-1})\right)\alpha^i\right) \\
&= \sum_{i=0}^{n-1}\left(\sum_{k=0}^{n-2}\sum_{r=0}^{k} \sigma(c_r)\sigma(b_{k-r}) Q_{i,k}\left(\sigma(a_0), ..., \sigma(a_{n-1})\right)\right)\beta^i \\
&= \left(\sum_{i=0}^{n-1}\sigma(c_i)\beta^i\right)\left(\sum_{j=0}^{n-1}\sigma(b_j)\beta^i\right) \\
&= \sigma(x)\sigma(y).
\end{aligned}
$$

Thus, σ is a homomorphism. □

We continue with more properties of field homomorphisms.

Proposition 3.11. *Let F be a field and let α be algebraic over F. Let $\bar{F}$ be the algebraic closure of F. Let $\Psi : F(\alpha) \to \bar{F}$ with $\Psi|_F = id$. In this case, $\Psi(\alpha)$ is a*

conjugate of α over F in the algebraic closure.

Proof. Let $f(T) = a_o + a_1T + ... + T^n$ be the irr(α, F). We have that $f(\alpha) = 0$. Furthermore, for $a_i \in F$, we have $a_0 + a_1\alpha + ... + \alpha^n$. Thus, we have

$$a_0 + a_1\Psi(\alpha) + ... + (\Psi(\alpha))^n = 0.$$

□

Definition 3.12. If σ is an isomorphism of F onto some field, then an element a of E is fixed by σ if $\sigma(a) = a$. Furthermore, a collection S of isomorphisms of E leaves a subfield F of E fixed if each $a \in F$ is fixed by every $\sigma \in S$. In addition, we say that σ leaves F fixed if $S = \{\sigma\}$ leaves F fixed.

Theorem 3.13. *Let $\{\sigma_i, i \in I\}$ be a collection of isomorphisms of a field E. Then $E_{\{\sigma_i\}} = \{a \in E | \sigma_i(a) = a$ for all $i \in I\}$ is a subfield of E.*

Proof. First note that $\{0, 1\} \in E$ by the definition of isomorphism. Let $a \in E_{\{\sigma_i\}}$ and $b \in E_{\{\sigma_i\}}$. Then we have that $\sigma_i(a + b) = \sigma_i(a) + \sigma_i(b) = a + b$ and $\sigma_i(a - b) = \sigma_i(a) - \sigma_i(b) = a - b$. In addition, we have $\sigma_i(ab) = \sigma_i(a)\sigma_i(b) = ab$, and for $b \neq 0$ we have $\sigma_i\left(\frac{a}{b}\right) = \frac{\sigma_i(a)}{\sigma_i(b)} = \frac{a}{b}$. □

Theorem 3.14. *The set of all automorphisms of a field E is a group under composition.*

Proof. Let $\sigma : E \to E$ and $\tau : E \to E$ be automorphisms. That is, σ and τ are bijections and isomorphisms. We must show that $\sigma \circ \tau$ is a bijection and that $\sigma \circ \tau$ is a homomorphism. First we know that a composition of two bijections is a bijection itself. Thus, it remains to show $\sigma \circ \tau$ is a homomorphism. Let $x \in E$ and $y \in E$.

Then we have

$$\begin{aligned}(\sigma \circ \tau)(x+y) &= \sigma(\tau(x+y)) \\ &= \sigma(\tau(x)+\tau(y)) \text{ since } \tau \text{ is a homomorphism} \\ &= \sigma(\tau(x))+\sigma(\tau(y)) \text{ since } \sigma \text{ is a homomorphism} \\ &= (\sigma \circ \tau)(x)+(\sigma \circ \tau)(y)\end{aligned}$$

and

$$\begin{aligned}(\sigma \circ \tau)(xy) &= \sigma(\tau(xy)) \\ &= \sigma(\tau(x)\tau(y)) \text{ since } \tau \text{ is a homomorphism} \\ &= \sigma(\tau(x))\sigma(\tau(y)) \text{ since } \sigma \text{ is a homomorphism} \\ &= ((\sigma \circ \tau)(x))((\sigma \circ \tau)(y)).\end{aligned}$$

Also, we have that the identity map is an automorphism of E and the inverse of an automorphism is also an automorphism of E. Thus, we have that E is a group under function composition. □

Theorem 3.15. *Let E be a field and let F be a subfield of E. Then the set $G(E/F)$ of all automorphisms of E leaving F fixed is a group and $F \subseteq E_{G(E/F)}$.*

Proof. Let σ and τ be automorphisms of E fixing F. We need to show that $\sigma \circ \tau$ also fixes F. If $x \in F$, then we have $(\sigma \circ \tau)(x) = \sigma(\tau(x)) = \sigma(x) = x$. Also, note that the identity automorphism is in $G(E/F)$ and furthermore that $\sigma^{-1} \in G(E/F)$. Therefore, we now have that $G(E/F)$ is a subgroup of the group of all automorphisms of E. □

Definition 3.16. In Theorem 3.15, the group $G(E/F)$ is the group of automorphisms

of E fixing F is also called the group of E over F.

To prove the Isomorphism Extension Theorem, we will need to use Zorn's Lemma (an alternative to Axiom of Choice). The following definition explains the necessary terms.

Definition 3.17. A subset T of a partially ordered set S is a chain if every two elements $a \in T$ and $b \in T$ are comparable.

Lemma 3.18 (Zorn's Lemma)**.** *If a partially ordered set S is such that every chain in S has an upper bound in S, then S has at least one maximal element.*

We now prove the Isomorphism Extension Theorem.

Theorem 3.19 (Isomorphism Extension Theorem)**.** *Let E/F be an algebraic extension of fields. Let $\sigma : F \to F'$ be an isomorphism. Furthermore, let $\bar{F}'$ be the algebraic closure of F'. In this case, σ can be extended to an isomorphism $\tau : E \to E' \subset \bar{F}'$ such that $\tau(a) = \sigma(a)$ for all $a \in F$.*

Proof. Consider the set of all pairs (L, λ) where L is a subfield of E containing F, $F \subseteq L \subseteq E$ and $\lambda : L \to L' \subset \bar{F}'$ is an isomorphism such that $\lambda|_F = \sigma$. Observe that S is not empty since $(F, \sigma) \in S$. So we can also define a partial ordering on S by setting $(L_1, \lambda_1) \leq (L_2, \lambda_2)$ to mean $F \subseteq L_1 \subseteq L_2$ and $\lambda_2|_{L_1} = \lambda_1$.
Let I be any index set. Let $T = \{(H_i, \lambda_i) | i \in I\}$ be a chain in S. Let $H = \cup_{i \in I} H_i$ and note that $H \subseteq E$ is a field. Indeed, let $a \in H$ and $b \in H$. Since $H = \cup_{i \in I} H_i$, then there exists $i_1 \in I$ and $i_2 \in I$ such that $a \in H_{i_1}$ and $b \in H_{i_2}$. Since T is a chain, it is totally ordered, and we must have $H_{i_1} \subseteq H_{i_2}$ or $H_{i_2} \subseteq H_{i_1}$. Without loss of generality, assume $H_{i_1} \subseteq H_{i_2}$ and observe that now $a, b \in H_{i_2}$ and $a+b, a-b, \frac{a}{b}$ for $b \neq 0, \frac{b}{a}$ for $a \neq 0$ are all in $H_{i_2} \subseteq H$.
Next define $\lambda : H \to H' \subset \bar{F}'$ by setting $\lambda(c) = \lambda_i(c)$, where $c_i \in H_i$. We need to

show that $\lambda(c)$ does not depend on the choice of i. If $c \in H_j$ for $j \neq i$, then either $(H_j, \lambda_j) \leq (H_i, \lambda_i)$ or $(H_i, \lambda_i) \leq (H_j, \lambda_j)$. In the first case, we have $\lambda_i|_{H_j} = \lambda_j$ and therefore $\lambda_i(c) = \lambda_j(c) = \lambda(c)$. In the second case, we have $\lambda_j|_{H_i} = \lambda_i$ and therefore $\lambda_j(c) = \lambda_i(c) = \lambda(c)$. Thus, λ is well-defined.

Now we show that λ is an injective homomorphism. First let us show that λ is injective. Let $a, b \in H$ and assume $\lambda(a) = \lambda(b)$. As above, there exists H_i such that $a, b \in H_i$ and $\lambda(a) = \lambda(b) = \lambda_i(a) = \lambda_i(b)$, but $a = b$ since λ_i is injective.

Next, we show that λ is a homomorphism. Let $a, b \in H$ and let H_i be such that $a, b \in H_i$ which implies that $a + b \in H_i$ and $ab \in H_i$. In this case, since λ_i is a homomorphism we have

$$\begin{aligned} \lambda(a+b) &= \lambda_i(a+b) \\ &= \lambda_i(a) + \lambda_i(b) \\ &= \lambda(a) + \lambda(b), \end{aligned}$$

and we also have

$$\begin{aligned} \lambda(ab) &= \lambda_i(ab) \\ &= (\lambda_i(a))(\lambda_i(b)) \\ &= (\lambda(a))(\lambda(b)). \end{aligned}$$

Thus, we have shown that $(H, \lambda) \in S$ and (H, λ) is an upper bound for T, Zorn's Lemma applies, and S contains a maximal element (τ, K). Let $\tau : K \to K' \subset \bar{F}'$. If $K = E$, we are done. If $K \neq E$, then since $(K, \tau) \in S$ and $K \subsetneqq E$, there exists $\alpha \in E \setminus K$. Since α is algebraic over F, α is algebraic over K. Let $p(x) = \text{irr}(\alpha, K)$ and furthermore let $q(x) = \tau(p(x))$. Let $\beta \in \bar{F}'$ be a root of $q(x)$. By Lemma 3.10,

there exists an isomorphism $\tau' : K(\alpha) \to \tau(K(\beta))$, which contradicts the assumption that (K, τ) was a maximal element of S. Thus, $K = E$. □

Definition 3.20. Let F be a field with algebraic closure $\bar{F}$. Let $\{f_i(x)|i \in I\} \subset F[x]$. A field $E \subseteq \bar{F}$ is a splitting field of $\{f_i(x)|i \in I\}$ over F, if it is the smallest field containing F with all the zeros of $f_i(x)$ for each i. A field $K \subseteq \bar{F}$ is a splitting field if it is a splitting field of some collection of polynomials over F and $F \subseteq K$.

Proposition 3.21. *Let I be an index set. Let F be a field with algebraic closure $\bar{F}$. Let $A = \{\alpha_i|i \in I\} \subset \bar{F}$ be the set of all roots of a collection of one-variable polynomials over F. Further, let $B = \{\beta_j|j \in J\}$ where $\beta_j = \prod_{i \in I} \alpha_i^{a_{i,j}}$ and there are only finitely many $a_{i,j}$ that are not zero. Let $G = \{\gamma_k|k \in K\}$ where $\gamma_k = \sum x_{j,k}\beta_j$ is a finite linear combination with $x_{j,k} \in F$. Lastly, let $D = \{\delta_l|l \in L\}$ where δ_l is a ratio of two elements from G with the denominator element not equal to zero. In this case, we have that $D = \{\delta_l|l \in L\}$ is a field and is the smallest field containing F and A, and thus a splitting field of the collection of polynomials corresponding to A.*

Proof. First we see that $0, 1 \in D$ since $0, 1 \in F$. Note also that sums and products of linear combinations in G are linear combinations in G. Thus, the sum and the product of two elements in D is in D. Therefore, $D \subset \bar{F}$ must be a field. □

Theorem 3.22. *A field E with $F \subseteq E \subseteq \bar{F}$ is a splitting field over F if and only if for every $\sigma : \bar{F} \to \bar{F}$ such that $\sigma|_F = id$, we have that $\sigma(E) = E$.*

Proof. Assume E is a splitting field and σ is an automorphism of $\bar{F}$ fixing F. Let $y \in E$. In this case, in the notation of Proposition 3.21, we have

$$y = \frac{\gamma_1}{\gamma_2} = \frac{Q_1(\alpha_1, ..., \alpha_k)}{Q_2(\alpha_1, ..., \alpha_k)}$$

where $Q_1, Q_2 \in F[x_1, ..., x_k]$. Now as σ leaves F fixed, we have

$$\sigma(y) = \frac{Q_1(\sigma(\alpha_1), ..., \sigma(\alpha_k))}{Q_2(\sigma(\alpha_1), ..., \sigma(\alpha_k))} \in E$$

since roots go to roots in $\bar{F}$.

Conversely, suppose $\sigma(E) = E$ for any automorphism σ of $\bar{F}$. We will show E is a splitting field. If $E = F$, this covers the polynomial case where $\deg(p(x)) = 1$ and nothing else. So now assume $E \neq F$. We will show E contains all the roots of any irreducible over F polynomial with roots in E. If $F \subsetneq E$, let $\alpha \in E \setminus F$ and $g(x) = \text{irr}(\alpha, F)$. Let $\sigma : F(\alpha) \to F(\beta)$ where β is conjugate of α over F. We have previously shown

1. σ is an isomorphism (by Theorem 3.9), and
2. we can extend σ to $\bar{F}$ (by Lemma 3.10).

Thus, $\beta \in E$. □

Next, we prove two lemmas and a theorem in order to state and prove the Main Theorem of Galois Theory.

Lemma 3.23. *Let F be a field and let $\bar{F}$ be the algebraic closure. In characteristic zero, if $g(x)$ is irreducible over F, then in $\bar{F}$ all roots of $g(x)$ are distinct.*

Proof. Assusme $g(x)$ has a root a of multiplicity $n > 1$. In $\bar{F}$, factor $g(x) = (x-a)^n h(x)$ and note that $\gcd(h(x), (x-a)) = 1$. Thus, we have that

$$g'(x) = n(x-a)^{n-1}h(x) + h'(x)(x-a)^n \neq 0$$

since $n(x-a)^{n-1}h(x) \neq 0$, and therefore g' is divisible by at most $n-1$-st power of $(x-a)$. At the same time, $\gcd(g(x), g'(x)) = (x-a)^{n-1}f(x) \neq g(x)$ for some

$f(x) \in F[x]$ prime to $(x-a)$. Hence, $h(x)$ would have a non-trivial factor over F, but this cannot be true. Thus, all roots are distinct. □

Definition 3.24. A finite extension E/F is a separable extension if every irreducible polynomial over F does not have multiple roots in E.

Theorem 3.25 (Primitive Element Theorem)**.** *If E/F is a finite separable extension of infinite fields, then $E = F(\alpha)$ for some $\alpha \in E$. In this case, α is called a primitive element and E/F is called a simple extension.*

Proof. Assume $E = F(\beta, \gamma)$. Let $\beta_1 = \beta, ..., \beta_n$ be all the conjugates of β over F and $\gamma = \gamma_1, ..., \gamma_m$ be the conjugates of γ over F. All conjugates are distinct since the extension is separable. Since F is infinite, we can find $a \in F$ such that $a \neq \dfrac{(\beta_i - \beta)}{(\gamma - \gamma_j)}$ for $i = 1, ..., n$ and $j = 2, ...m$. Thus, $a(\gamma - \gamma_j) \neq (\beta_i - \beta)$.

Now let $\alpha = \beta + a\gamma$ and $f(x) = \text{irr}(\beta, F)$. Let $h(x) = f(\alpha - ax) \in (F(\alpha))[x]$. Then we have $h(\gamma) = f(\alpha - a\gamma) = f(\beta) = 0$, but $h(\gamma_j) = f(\alpha - a\gamma_j) \neq f(\beta_i)$ for any i and for $j \neq 1$. Therefore, $h(\gamma_j) \neq 0$ for $j > 1$. Indeed, we have $\alpha = \beta + a\gamma \neq \beta_i \Leftrightarrow \alpha - a\gamma_j = \beta + a\gamma - a\gamma_j \neq \beta_i$ for any i. The last non-equality holds because

$$\beta + a\gamma = a\gamma_j + \beta_i \Rightarrow \beta - \beta_i = a(\gamma_j - \gamma)$$

but this contradicts the fact that $a \neq \dfrac{(\beta_i - \beta)}{(\gamma - \gamma_j)}$. Therefore, $h(x) \neq 0$ for any $\gamma_2, ..., \gamma_m$.

Now let $g(x) = \text{irr}(\gamma, F)$. In this case, $h(x)$ and $g(x)$ have a common root. Hence, $h(x)$ has a linear factor $(x - \gamma) \in (F(\alpha))[x]$. Thus, $\gamma \in F(\alpha)$.

Now since $\gamma \in F(\alpha)$, then for $a \in F$ we have $a\gamma \in F(\alpha)$. Additionally, we have that $\alpha = \beta - a\gamma \in F(\alpha)$. Thus, $(\beta - a\gamma) + (a\gamma) \in F(\alpha)$ and hence $\beta \in F(\alpha)$.

We have shown $F(\beta, \gamma) \subseteq F(\alpha)$. Since $\alpha = \beta - a\gamma$, we have $F(\alpha) \subset F(\beta, \gamma)$. Therefore, $F(\beta, \gamma) = F(\alpha)$. That is, if we have a finite separable extension with two

generators, then we can reduce the number of generators to one. By induction, any number of finite generators can be reduced to one. □

Lemma 3.26. *Let F be a field and $\bar{F}$ be the algebraic closure of F. Further, let M be a field such that $F \subseteq M \subseteq \bar{F}$ and the extension M/F is finite and separable. In this case, we have the number of injective homomorphisms σ such that $\sigma : M \to \bar{F}$ and $\sigma|_F = id$ is the degree of the extension $[M : F]$.*

Proof. Since the extension M/F is finite and separable, by the Primitive Element Theorem we have that it is simple. That is, the extension M/F is generated by a single element α. Any injective homomorphism σ such that $\sigma : M \to \bar{F}$ and $\sigma|_F = \mathrm{id}$ must send α to a conjugate over F by Proposition 3.11, and every conjugate of α over F also generates an injective homomorphism σ with the required properties by Theorem 3.9. Thus, the number of such injective homomorphisms is exactly the number of conjugates of α over F, which is the degree of the extension. □

Remark 3.27. In this thesis, we have assumed that the characteristic of all the fields under consideration is zero. In this case, all the extensions are separable.

We now define the Galois group and proceed to state the Main Theorem of Galois Theory.

Definition 3.28. Let K be a separable splitting field over F and let K be a finite extension of F. In this case, we say that K is a finite normal extension of F.

Definition 3.29. Let K be a finite normal extension over F. In this case, we say $G(K/F)$, as defined above, is the Galois group of K over F. Further, the extension K/F is called a Galois extension.

Theorem 3.30 (Main Theorem of Galois Theory)**.** *Let K be a finite normal extension of a field F with a Galois group $G(K/F)$. For a field E where $F \subseteq E \subseteq K$, let*

$\lambda(E) \subseteq G(K/F)$ be the subgroup containing all the elements of $G(K/F)$ fixing E. In this case,

$$\lambda : \{\textit{intermediate fields between } K \textit{ and } F\} \to \{\textit{subgroups of } G(K/F)\}$$

is one-to-one. Further, λ has the following properties:

1. *$\lambda(E) = G(K/E)$.*
2. *$E = K_{G(K/E)} = K_{\lambda(E)}$, where $K_{G(K/E)}$ is the set of elements fixed by the Galois group of K over E and $K_{\lambda(E)}$ is the set of elements fixed by $\lambda(E)$.*
3. *If $H \subseteq G(K/E)$, then $\lambda(K_H) = H$, where K_H is the set of elements fixed by H.*
4. *$[K : E] = |\lambda(E)|$ and $[E : F] = [G(K/F) : \lambda(E)] =$ the number of left cosets of $\lambda(E)$ in $G(K/F)$.*
5. *E is a normal extension of F if and only if $\lambda(E)$ is a normal subgroup of $G(K/F)$. Also if $\lambda(E)$ is a normal subgroup of $G(K/F)$, then*

$$G(E/F) = \frac{G(K/F)}{G(K/E)}.$$

6. *Subfields of K containing F are in bijection with subgroups of $G(K/F)$.*

Proof. We will prove each property separately.

1. First clearly we have $\lambda(E) \subseteq G(K/E)$ since $\lambda(E)$ is the subgroup of $G(K/F)$ keeping E fixed. Now we must show $G(K/E) \subseteq \lambda(E)$. If $\sigma \in G(K/E)$, then σ is an automorphism of K keeping E fixed and therefore F fixed. Thus, $\sigma \in G(K/F)$. Hence, $G(K/E) \subseteq \lambda(E)$. Therefore, $\lambda(E) = G(K/E)$.

2. Notice that we have $E \subseteq K_{G(K/E)}$ since $K_{G(K/E)}$ is a fixed field of $G(K/E)$. Now we must show $K_{G(K/E)} \subseteq E$. Let $\alpha \in K \setminus E$. Let $f(x) = \text{irr}(\alpha, E)$. There exists $\sigma : E(\alpha) \to E(\beta)$, where β is a conjugate over α over E. By the Isomorphism Extension Theorem, we can extend σ to $\bar{F}$. Note that σ keeps E fixed. Since K/F is normal, σ is an automorphism of K. That is, $\sigma \in \lambda(E) = G(K/E) \subset G(K/F)$, and in particular, $K_{G(K/E)} \subseteq E$. Thus, $K_{G(K/E)} = E$. This shows λ is one to one.

3. We will show that λ is onto. Clearly, $H \subseteq \lambda(K_H)$. We need to show equality. Suppose $H \subsetneqq \lambda(K_H)$. By the Primitive Element Theorem, $K = K_H(\alpha)$. Let

$$n = [K : K_H] = |G(K/K_H)|.$$

If $H \subsetneqq \lambda(K_H) = G(K/K_H)$, then we have $|H| < n$. Let $\sigma_1, .., \sigma_{|H|}$ be all the elements of H, and consider $f(x) = \prod_{i=1}^{|H|}(x - \sigma_i(\alpha))$ where $\deg(f(x)) = |H| < n$. We claim that the coefficients of $f(x)$ are in H. Indeed, since coefficients of f are symmetric functions of $\{\sigma_1(\alpha), ..., \sigma_{|H|}(\alpha)\} = A$, where $\sigma_1(\alpha), ..., \sigma_{|H|}(\alpha) \in K$ and $\sigma(A) = A$ for any $\sigma \in H$, we have $[K : K_H] = [K_H(\alpha) : K] \leq |H| < n$ since $\sigma(\sigma_i(\alpha)) = \sigma \circ \sigma_i(\alpha) = \sigma_j(\alpha)$ because H is a group. Thus, we arrive at a contradiction.

4. We have already shown that for any intermediate field E it is the case that $[K : E] = |\lambda(E)|$. Thus, it remains to show $[E : F] = [G(K/F) : \lambda(E)]$. First notice that we have $[K : E] = G(K/E) \subset G(K/F)$ and $[K : F] = |G(K/F)|$ and $[K : E][E : F] = [K : F]$. Thus,

$$[E : F] = \frac{[K : F]}{[K : E]} = \frac{|G(K/F)|}{|G(K/E)|} =$$

$$\text{index of } G(K/E) \text{ in } G(K/F) = \text{number of left cosets.}$$

5. Assume $G(K/E) \rhd G(K/F)$. To show that E is normal over F, it is enough to show that for any $\sigma : E \to \bar{F}$ such that $\sigma_F = \text{id}$ it is the case that $\sigma(E) = E$. Any such σ can be extended to $\sigma : K \to \bar{F}$ and since K is normal over F, we have $\sigma(K) = K$ so that it is enough to consider $\sigma \in G(K/F)$. We want to show for all $\alpha \in E$ and all $\sigma \in G(K/F)$, we have $\sigma(\alpha) \in E$.

   By property 2, E is the fixed field of $G(K/E)$. Thus, by definition of fixed field,

$$\begin{aligned}
\sigma(\alpha) \in E &\Leftrightarrow \forall \tau \in G(K/E),\, \tau(\sigma(\alpha)) = \sigma(\alpha) \\
&\Leftrightarrow \forall \tau \in G(K/E),\, \sigma^{-1} \circ \tau(\sigma(\alpha)) = \alpha \\
&\Leftrightarrow \forall \tilde{\tau} \in G(K/E),\, \tilde{\tau}(\alpha) = \alpha,
\end{aligned}$$

where the last implication is true because $G(K/E)$ is a normal subgroup in $G(K/F)$ and conjugation is an automorphism of the group.
Suppose now that E/F is a normal extension, let $\sigma \in G(K/F)$, $\tau \in G(K/E)$, $\alpha \in E$ and note that as above, we have $\sigma(\alpha) \in E$ and $\tau(\sigma(\alpha)) = \sigma(\alpha)$ or $\sigma^{-1}(\tau(\sigma(\alpha))) = \alpha$. Thus, $\sigma^{-1} \circ \tau \circ \sigma \in G(K/E)$ or $G(K/E)$ is normal in $G(K/F)$. □

We finish with the definitions of abelian and cyclic extensions and a corollary concerning abelian and cyclic Galois groups we will need later.

Definition 3.31. A finite normal extension K of a field F is abelian over F if $G(K/F)$ is an abelian group.

Definition 3.32. A finite normal extension K of a field F is cyclic over F if $G(K/F)$ is a cyclic group.

Corollary 3.33 (Abelian and Cyclic Extensions)**.**

1. *Any subgroup of an abelian group is normal and the quotient group is defined and is also abelian.*

2. *If F/K is an abelian extension, then if we have an intermediate field E with $K \subseteq E \subseteq F$, then E/K is Galois and abelian. In general, E/K is normal if and only if $G(F/E)$ is normal in $G(F/K)$, the Galois group of F over K. However, if $G(F/K)$ is abelian, this is automatically true.*

3. *If G is a cyclic group, $H \subset G$ a subgroup, then H is cyclic and G/H is cyclic.*

4. *If F/K is a cyclic extension, then if we have an intermediate field E with $K \subseteq E \subseteq F$, then E/K is Galois and abelian.*

CHAPTER 4: Diophantine Generation and Hilbert's Tenth Problem

In this chapter we discuss the main results on extensions of Hilbert's Tenth Problem to the rings of integers of number fields.

4.1 Diophantine Definitions and Field-Diophantine Definitions

In this section, we define the basic notions we need for the main results. First we prove a proposition which will allow us to substitute a single polynomial equation for a finite system of equations.

Proposition 4.1. *Let K be a field which is not algebraically closed and let*

$$h(x) = x^n + a_{n-1}x^{n-1} + ... + a_0$$

be a polynomial without roots in K. Let $f(x) \in K[x]$ and $g(x) \in K[x]$. In this case, for all $x \in K$, we have

$$a_0 g^n(x) + a_1 g^{n-1}(x) f(x) + ... + a_n f^n(x) = 0$$

$$\Updownarrow$$

$$f(x) = 0 \text{ and } g(x) = 0.$$

Proof. Assume $f(x) = g(x) = 0$. Using substitution, we obtain that

$$a_0 g^n(x) + a_1 g^{n-1}(x) f(x) + ... + a_n f^n(x) = 0.$$

Conversely, suppose

$$a_0 g^n(x) + a_1 g^{n-1}(x) f(x) + ... + a_n f^n(x) = 0,$$

and also suppose $g(x) \neq 0$. In this case, dividing

$$a_0 g^n(x) + a_1 g^{n-1}(x) f(x) + ... + a_n f^n(x) = 0$$

by $g^n(x)$, we obtain

$$a_0 + a_1 \left(\frac{f(x)}{g(x)}\right) + a_2 \left(\frac{f(x)}{g(x)}\right)^2 + ... + a_n \left(\frac{f(x)}{g(x)}\right)^n = 0.$$

This implies that $\frac{f(x)}{g(x)}$ is a root of h in K.

Now let

$$\bar{h}(y) = a_o y^n + a_1 y^{n-1} + ... + a_n.$$

We claim that $\bar{h}(y)$ has no roots in K. Suppose $\bar{h}(y) = 0$ for some $y \in K$. Since $a_n \neq 0$, we conclude that $y \neq 0$, and we can set $x = \dfrac{1}{y} \neq 0 \in K$. Now we have that

$$\bar{h}\left(\frac{1}{x}\right) = a_o \left(\frac{1}{x}\right)^n + a_1 \left(\frac{1}{x}\right)^{n-1} + ... + a_n = 0.$$

Multiplying both sides by x^n, we obtain $a_0 + a_1 x + ... + a_n x^n = 0$, which is a contradiction of our assumption on h.

Now assume

$$a_0 g^n(x) + a_1 g^{n-1}(x) f(x) + ... + a_n f^n(x) = 0,$$

but $f(x) \neq 0$. Dividing the left side by $f^n(x)$, we obtain

$$a_0 \left(\frac{g^n(x)}{f^n(x)} \right) + a_1 \left(\frac{g^{n-1}(x)}{f^{n-1}(x)} \right) + ... + a_n = 0.$$

This implies that $\bar{h} \left(\frac{g(x)}{f(x)} \right) = 0$, which is a contradiction to the fact that $\bar{h}(y)$ has no roots in K.

Thus, if $a_0 g^n(x) + a_1 g^{n-1}(x) f(x) + ... + a_n f^n(x) = 0$, then $f(x) = g(x) = 0$. □

From this proposition we immediately conclude the following corollary.

Corollary 4.2. *If R is a recursive integral domain with a fraction field which is not integrally closed, then there exists an algorithm for determining if a single arbitrary polynomial equation has solutions in R if and only if there exists an algorithm to determine whether an arbitrary finite system of polynomial equations has solutions in R.*

We now review the notions of Diophantine sets and Diophantine definitions first discussed in the introduction.

Definition 4.3. Let R be an integral domain. Let m and n be positive integers. Let $A \subset R^n$. We say A has a Diophantine definition over R if there exists a polynomial

$$f(y_1, ..., y_n, x_1, ..., x_m) \in R[y_1, .., y_n, x_1, ..., x_m]$$

such that for all $(t_1, ..., t_n) \in R^n$, we have

$$(t_1, ..., t_n) \in A \Leftrightarrow \exists x_1, ..., x_m \in R, f(t_1, ..., t_n, x_1, ..., x_m) = 0.$$

This set A is called Diophantine over R.

Now we will modify the notion of Diophantine definition to establish the notion of field-Diophantine definition.

Definition 4.4. Let R be an integral domain with a quotient field F. Let k and m be positive integers. Let $A \subset F^k$. Assume that there exists a polynomial

$$f(a_1, ..., a_k, b, x_1, ..., x_m)$$

with coefficents in R such that

$$\forall a_1, ..., a_k, b, x_1, ..., x_m \in R,$$

$$f(a_1, ..., a_k, b, x_1, ..., x_m) = 0 \Rightarrow b \neq 0$$

and

$$A = \{(t_1, ..., t_k) \in F^k \mid \exists a_1, ..., a_k, b, x_1, ..., x_m \in R,$$
$$bt_1 = a_1, ..., bt_k = a_k, f(a_1, ..., a_k, b, x_1, ..., x_m) = 0\}.$$

In this case, we say that A is field-Diophantine over R and will call f a field-Diophantine definition of A over R.

Remark 4.5. It is not hard to see that if R is an integral domain with a quotient field F, then a subset A of R^k has a Diophantine definition over R if and only if A has a field-Diophantine definition over R. Indeed, a Diophantine definition is a field-Diophantine definition with b as above set to 1. Conversely, if $f(y_1, ..., y_k, z, x_1, ..., x_m)$ is a field-Diophantine of a set $A \subset R^k$, then

$$g(y_1, \ldots, y_k, z, x_1, \ldots, x_m) = f(zy_1, ..., zy_k, z, x_1, ..., x_m)$$

is a Diophantine definition of A over R^k.

4.2 Coordinate Polynomials

We will now introduce coordinate polynomials in order to extend the notion of Diophantine definition and the notion of field-Diophantine definition to the notion of Diophantine generation.

Lemma 4.6. *Let F/G be a finite field extension. Let $\Omega = \{\omega_1, ..., \omega_n\}$ be a basis of F over G. Then for $l = 1, 2..., n$ there exist*

$$P_l(x_1, ..., x_n, y_1, ..., y_n) \in G[x_1, ..., x_n, y_1, ..., y_n]$$

depending on Ω only such that for all $a_1, .., a_n, b_1, ...b_n$ we have that

$$\sum_{i=1}^{n} a_i\omega_i \sum_{j=1}^{n} b_j\omega_j = \sum_{l=1}^{n} P_l(a_1, .., a_n, b_1, ...b_n)\omega_l.$$

Proof. Let $\{A_{i,j,l} \in G \mid i, j, l = 1, ..., n\}$ be a set of elements of G such that $\omega_i\omega_j = \sum_{l=1}^{n} A_{i,j,l}\omega_l$. First note this set exists because F is a field. By associativity, distributivity, commutativity, and reordering, we have

$$\begin{aligned}
\sum_{i=1}^{n} a_i\omega_i \sum_{j=1}^{n} b_j\omega_j &= \sum_{i=1}^{n}\sum_{j=1}^{n} a_i\omega_i b_j\omega_j \\
&= \sum_{i=1}^{n}\sum_{j=1}^{n} a_i b_j\omega_i\omega_j \\
&= \sum_{i,j=1}^{n} a_i b_j\omega_i\omega_j \\
&= \sum_{i,j=1}^{n} a_i b_j \sum_{l=1}^{n} A_{i,j,l}\omega_l
\end{aligned}$$

$$
\begin{aligned}
&= \sum_{i,j=1}^{n} \sum_{l=1}^{n} a_i b_j A_{i,j,l} \omega_l \\
&= \sum_{l=1}^{n} \sum_{i,j=1}^{n} a_i b_j A_{i,j,l} \omega_l \\
&= \sum_{l=1}^{n} \left(\sum_{i,j=1}^{n} a_i b_j A_{i,j,l} \right) \omega_l \\
&= \sum_{l=1}^{n} P_l(a_1, .., a_n, b_1, ...b_n) \omega_l
\end{aligned}
$$

where $P_l(a_1, ..., a_n, b_1, ..., b_n) = \sum_{i,j=1}^{n} a_i b_j A_{i,j,l}$. □

In a similar manner, we can also prove the following lemma.

Lemma 4.7. *Let F/G be a finite field extension and let $\Omega = \{\omega_1, ..., \omega_n\}$ be a basis of F over G. Let $a_1, ..., a_n \in G$. In this case, there exist*

$$P_1, ..., P_n, Q \ \in \ G[x_1, ..., x_n]$$

depending only on $F, G,$ and Ω such that

$$\sum_{i=1}^{n} a_i \omega_i \neq 0 \Leftrightarrow \sum_{i=1}^{n} \frac{P_i(a_1, ..., a_n)}{Q(a_1, ..., a_n)} \omega_i = \left(\sum_{i=1}^{n} a_i \omega_i \right)^{-1}$$

where $Q(a_1, ..., a_n) \neq 0$. That is,

$$\left(\sum_{i=1}^{n} \frac{P_i(a_1, ..., a_n)}{Q(a_1, ..., a_n)} \omega_i \right) \left(\sum_{i=1}^{n} a_i \omega_i \right) = 1$$

where $Q(a_1, ..., a_n) \neq 0$.

Proof. Let $1 = \sum_{i=1}^{n} B_i \omega_i, B_i \in G$. Let $\sum_{i=1}^{n} b_i \omega_i, b_i \in G$ be the inverse of the given

element and consider the following sequence of equalities:

$$\sum_{i=1}^{n} a_i\omega_i \sum_{i=1}^{n} b_i\omega_i = 1,$$

$$\sum_{l=1}^{n} P_l(a_1,..,a_n,b_1,...b_n)\omega_l = \sum_{l=1}^{n}\left(\sum_{i,j=1}^{n} a_i b_j A_{i,j,l}\right)\omega_l = \sum_{l=1}^{n} B_l\omega_l,$$

$$\sum_{i,j=1}^{n} a_i b_j A_{i,j,l} = B_l, l = 1,\ldots,n, \text{ and}$$

$$\sum_{j=1}^{n}\left(\sum_{i=1}^{n} a_i A_{i,j,l}\right) b_j = B_l, l = 1,\ldots,n.$$

Thus, we have a linear system in $b_1,\ldots,b_n$ with a unique solution. The matrix $C = (c_{l,j})$ corresponding to this system has an entry $\sum_{i=1}^{n} a_i A_{i,j,l}$ in the position corresponding to l-th row and j-th column, and each entry is a polynomial in the coordinates of the original element and the elements of the set $\{A_{i,j,l}\}$, and this polynomial depends on indexes j, l, and n only. Now the conclusion follows from Cramer's Rule and the fact that the determinant of a matrix is a fixed polynomial in its entries which depends on the matrix size only.

□

Next we observe a formal property of sums.

Remark 4.8. If $A, a_{i,j}$ are elements of a field, then

$$A(a_{1,1}+...+a_{1,k})\cdots(a_{b,1}+...+a_{b,k}) = \sum Aa_{1,s_1}a_{2,s_2}...a_{b,s_b}$$

where $1 \le s_i \le k$.

Lemma 4.9. *Let M/F be a finite field extension of degree k. Let $\Omega = \{\omega_1,...,\omega_k\}$*

be a basis of M over F. If $P(T_1, ..., T_m) \in F[T_1, ..., T_m]$ then there exist polynomials $P_1^{\Omega}(t_{1,1}..., t_{m,k}), ..., P_k^{\Omega}(t_{1,1}..., t_{m,k})$ such that

1. *$P_1^{\Omega}, ..., P_k^{\Omega}$ depend only on Ω and*
2. *$P\left(\sum_{j=1}^k t_{1,j}\omega_j, ..., \sum_{j=1}^k t_{m,j}\omega_j\right) = \sum_{j=1}^k P_j{}^{\Omega}(t_{1,1}, ..., t_{m,k})\omega_j$.*

Proof. First by Lemma 4.6, we have

$$\omega_i\omega_j = \sum_{r=1}^{k} A_{i,j,r}\omega_r$$

where $A_{i,j,r} \in F$ depend only on Ω. Thus by induction, for $c_1, \ldots, c_k \in \mathbb{Z}_{\geq 0}$, we obtain

$$\prod_{i=1}^{k} \omega_i^{c_i} = \sum_{r=1}^{k} A_{c_1,...,c_k,r}\omega_r. \tag{4.1}$$

Let $\deg(P) = d$ and let

$$\begin{aligned} P(T_1, ..., T_m) &= \sum_{j_1+...+j_m \leq d,\ j_i \geq 0} B_{j_1,...,j_m} {T_1}^{j_1} {T_2}^{j_2} \cdots {T_m}^{j_m} \\ &= \sum_{j_1+...+j_m \leq d, j_i \geq 0} B_{j_1,...,j_m} \left(\sum_{r=1}^{k} t_{1,r}\omega_r\right)^{j_1} \cdots \left(\sum_{r=1}^{k} t_{m,r}\omega_r\right)^{j_m}. \end{aligned}$$

To expand $\left(\sum_{r=1}^k t_{1,r}\omega_r\right)^{j_1} \cdots \left(\sum_{r=1}^k t_{m,r}\omega_r\right)^{j_m}$, we note that we have a product of

the form $\prod_{u=1}^{e}\sum_{r=1}^{k} a_{u_r}$ where $e \leq d$ and

$$\begin{cases} a_{u,r} = t_{1,r}w_r & \text{for } u = 1, ..., j_1 \\ a_{u,r} = t_{2,r}w_r & \text{for } u = j_1 + 1, ..., j_1 + j_2 \\ \vdots & \\ a_{u,r} = t_{m,r}w_r & \text{for } u = j_1 + j_2 + ... + j_{m-1} + 1, ..., j_1 + j_2 + ... + j_m = e. \end{cases}$$

Now for $e = j_1 + ... + j_m$, we have

$B_{j_1,...,j_m}\left(\sum_{r=1}^{k} t_{1,r}\omega_r\right)^{j_1} \cdots \left(\sum_{r=1}^{k} t_{m,r}\omega_r\right)^{j_m}$

$= B_{j_1,...,j_m}\prod_{u=1}^{e}\sum_{r=1}^{k} a_{u,r}$

$= B_{j_1,...,j_m}\sum_{s_1,...,s_e} a_{1,s_1}\ldots a_{e,s_e}, 1 \leq s_i \leq k$ (by Remark 4.8)

$= B_{j_1,...,j_m}\sum_{r_{1,1},...,r_{m,j_m}}(t_{1,r_{1,1}}\ldots t_{1,r_{1,j_1}}\ldots t_{m,r_{m,1}}\ldots t_{m,r_{m,j_m}})(\omega_{r_{1,1}}\ldots\omega_{r_{1,j_1}}\ldots\omega_{r_{m,1}}\ldots\omega_{r_{m,j_m}})$

$= B_{j_1,...,j_m}\sum_{i=1,...,m,j=1,...,k,a_{i,j}=1,...,j_i} C_{a_{1,1},...,a_{m,k},j_1,...,j_m}\prod_{i=1,...,m,j=1,...,k} t_{i,j}^{a_{i,j}}\prod_{e=1}^{k}\omega_e^{b_e}$

$= B_{j_1,...,j_m}\prod_{i=1,...,d,j=1,...,k} t_{i,j}^{a_{i,j,j_1,...,j_m}}\sum_{r=1}^{k} A_{b_1,...,b_k,r}\omega_r$ (from (4.1)),

where $1 \leq r_{i,j} \leq k, 1 \leq e \leq k, 0 \leq a_{i,j} \leq j_i, b_e = \sum_{i=1}^{m} a_{i,e}$. □

4.3 Diophantine Generation

We are now ready to address the central notion of this chapter – the Diophantine generation. First we need a preliminary lemma.

Lemma 4.10. *Let R be an integral domain with quotient field F. For some positive integer k, let $A \subset F^k$. Let m be a positive integer such that $m \leq k$. Assume that A has a field-Diophantine definition over R. Let*

$$B = \{(x_1, ..., x_r) \in F^r | x_i = P_i(y_1, ..., y_m),$$
$$(y_1, ..., y_m, H_{m+1}(y_1, ..., y_m), ..., H_k(y_1, ..., y_m)) \in A\},$$

where $P_1, ..., P_r, H_{m+1}, ..., H_k \in F[y_1, ..., y_m]$. *Then* B *also has a field-Diophantine definition over* R.

Proof. Let $f(u_1, ..., u_k, u, z_1, ..., z_s)$ be a field-Diophantine definition of A over R. Now if we let $y_i = \frac{u_i}{u}$ for $i = 1, ..., m$ we have

$$\begin{aligned} B = \{(x_1, ..., x_r) \in F^r | \exists u_1, ..., u_k, u, z_1, ..., z_s \in R, \\ x_i = P_i\left(\frac{u_1}{u}, ..., \frac{u_m}{u}\right), i = 1, ..., r, \\ H_{m+1}\left(\frac{u_1}{u}, ..., \frac{u_m}{u}\right), ..., H_k\left(\frac{u_1}{u}, ..., \frac{u_m}{u}\right), f(u_1, ..., u_k, u, z_1, ..., z_s) = 0\}. \end{aligned}$$

Next if we let $y_j = H_j\left(\frac{u_1}{u}, ..., \frac{u_m}{u}\right)$ for $j = m+1, ..., k$ and use $y_j = \frac{u_j}{u}$ for $j = m+1, ..., k$, we can substitute and see that

$$y_j = \frac{u_j}{u} = H_j\left(\frac{u_1}{u}, ..., \frac{u_m}{u}\right) \Rightarrow u_j = uH_j\left(\frac{u_1}{u}, ..., \frac{u_m}{u}\right)$$

for $j = m+1, ..., k$. Now we obtain

$$\begin{aligned} B = \{(x_1, ..., x_r) \in F^r | \exists u_1, ..., u_k, u, z_1, ..., z_s \in R, \\ x_i = P_i\left(\frac{u_1}{u}, ..., \frac{u_m}{u}\right), i = 1, ..., r, \\ u_j = uH_j\left(\frac{u_1}{u}, ..., \frac{u_m}{u}\right), j = m+1, ..., k, f(u_1, ..., u_k, u, z_1, ..., z_s) = 0\}. \end{aligned}$$

Let d_H be the highest degree of $H_{m+1}, ..., H_k$. Let D_H be a common denominator of all the coefficients of $H_{m+1}, ..., H_k$. Let

$$\bar{H}_j(u_1, ..., u_m, u) = D_H u^{d_H} H_j\left(\frac{u_1}{u}, ..., \frac{u_m}{u}\right)$$

for $j = m+1, ..., k$. Here we used the fact that R is an integral domain with quotient

field F to eliminate our denominators. Also, note that u^{d_H} eliminates the u's in the denominators. Similarly, we let d be the highest degree of $P_1, ..., P_r$, and let D be a common denominator of all the coefficients of $P_1, ..., P_r$ in R. Let

$$\bar{P}_i(u_1, ..., u_m, u) = u^d D P_i\left(\frac{u_1}{u}, ..., \frac{u_m}{u}\right) \in R[u_1, ..., u_m, u]$$

for $i = 1, ..., r$. Thus, we now obtain

$$\begin{aligned} B = \{(x_1, ..., x_r) \in F^r | \exists u_1, ..., u_k, u, z_1, ..., z_s \in R, \\ u\bar{H}_j(u_1, ..., u_m, u) = D_H u^{d_H} u_j, j = m+1, ..., k, \\ u^d D x_i = \bar{P}_i(u_1, ..., u_m, u), i = 1, ..., r, f(u_1, ..., u_k, u, z_1, ..., z_s) = 0\}, \end{aligned}$$

and further obtain

$$\begin{aligned} B = \{(x_1, ..., x_r) \in F^r | \exists u_1, ..., u_k, u, z_1, ..., z_s \in R, \\ ux_i = u_i, u = Du^d, u_i = \bar{P}_i(u_1, ..., u_m, u), i = 1, ..., r, \\ \bar{H}_j(u_1, ..., u_m, u) = D_H u^{d_H - 1} u_j, j = m+1, ..., k, f(u_1, ..., u_k, u, z_1, ..., z_s) = 0\}. \end{aligned}$$

Thus, B has a field-Diophantine definition over R. □

Next, we define the notion of Diophantine generation, generalizing further the notion of Diophantine definition.

Definition 4.11 (Diophantine Generation)**.** Let R_1 and R_2 be two rings with quotient fields F_1 and F_2 respectively. Assume that neither F_1 nor F_2 is algebraically closed. Let F be a finite extension of F_1 such that $F_2 \subset F$. Also, assume that for some basis $\Omega = \{\omega_1, ..., \omega_k\}$ of F over F_1, there exists a polynomial $f(a_1, ..., a_k, b, x_1, ..., x_m)$ with

coefficients in R_1 such that

$$f(a_1, ..., a_k, b, x_1, ..., x_m) = 0 \Rightarrow b \neq 0$$

and

$$R_2 = \{ \sum_{i=1}^{k} t_i \omega_i \mid \exists a_1, ..., a_k, b, x_1, ..., x_m \in R_1,$$
$$bt_1 = a_1, ..., bt_k = a_k, f(a_1, ..., a_k, b, x_1, ..., x_m) = 0\}.$$

In this case, we say that R_2 is Dioph-generated over R_1 and denote this as

$$R_2 \leq_{Dioph} R_1.$$

Further, we say $f(a_1, ..., a_k, b, x_1, ..., x_m)$ is a defining polynomial of R_2 over R_1. Additionally, we say $\Omega = \{\omega_1, ..., \omega_k\}$ is a Diophantine basis of R_2 over R_1 and F is the defining field for the basis Ω.

We now state an example of Diophantine generation.

Example 4.12. Let F/G be a finite extension of degree k with basis Ω of F over G. Then we have that $F \leq_{Dioph} G$ since for each $z \in F$ we can write $z = \sum_{i=1}^{k} a_i \omega_i$.

We now consider properties of Diophantine generation and prove that it is transitive. First we state a lemma which follows directly from the definition of Diophantine generation.

Lemma 4.13. *Let R_1 and R_2 be integral domains with quotient fields F_1 and F_2 respectively. Let F be a finite extension of F_1 such that $F_2 \subset F$. In this case, we can conclude that $R_2 \leq_{Dioph} R_1$ if there exists a basis $\Omega = \{\omega_1, .., \omega_k\}$ of F over F_1 and a*

set $A_\Omega \subset {F_1}^k$ *with a field-Diophantine definition over* R_1 *such that*

$$R_2 = \left\{ \sum_{i=1}^{k} z_i \omega_i | (z_1, ..., z_k) \in A_\Omega \right\}. \tag{4.2}$$

Conversely, if F *is a defining field and* Ω *is a corresponding Diophantine basis of* R_2 *over* R_1*, then* R_2 *has a representation of the form 4.2, where* $A_\Omega \subset {F_1}^k$ *is field-Diophantine over* R_1*.*

Notation 4.14. A_Ω will be called a defining set for the basis Ω.

Notation 4.15. Let G/F be a finite field extension. Let $\Omega = \{\omega_1, ..., \omega_k\}$ be a basis of G over F. For some positive integer n, let $B \subset G^n$. Then define $B^\Omega \subset F^{kn}$ to be the set such that

$$(a_{1,1}, ..., a_{k.n}) \in B^\Omega \Leftrightarrow \left(\sum_{i=1}^{k} a_{i,1}\omega_i, ..., \sum_{i=1}^{k} a_{i,n}\omega_i \right) \in B.$$

Using this notation for rings R_1 and R_2 such that $R_2 \leq_{Dioph} R_1$ with a Diophantine basis Ω as above, we can conclude by Lemma 4.13 that $R_2^\Omega \subset F_1^n$ is field Diophantine over R_1, where F_1 is the fraction field of R_1.

We now show that the notion of Diophantine generations is a proper extension of both the notion of field-Diophantine definition and the notion of Diophantine definition.

Proposition 4.16. *Let* R_1 *and* R_2 *be integral domains with quotient fields* F_1 *and* F_2 *respectively such that* $R_2 \leq_{Dioph} R_1$*. Let* F *be a defining field and let* $\Omega = \{\omega_1, ..., \omega_k\}$ *be a Diophantine basis of* R_2 *over* R_1*. Let* $B \subset F_2^n$ *have a field-Diophantine definition over* R_2*. Then* $B^\Omega \subset F_1^{kn}$ *has a field-Diophantine definition over* R_1*.*

Proof. Let $f(z_1, ..., z_n, y, x_1, ..., x_r)$ be a field-Diophantine definition of B over R_2. In this case, we have that

$$B = \{(t_1, ..., t_n) \in F_2^n \mid \exists z_1, ..., z_n, y, x_1, ..., x_r \in R_2,$$
$$yt_1 = z_1, ..., yt_n = z_n, f(z_1, ..., z_n, y, x_1, ..., x_r) = 0\}$$

and $f(z_1, ..., z_n, y, x_1, ..., x_r) = 0$ implies $y \neq 0$. As $y, z_i \in R_2$ and $R_2 \leq_{Dioph} R_1$, we have that

$$y = \sum_{i=1}^{k} \frac{u_i}{v}\omega_i \text{ and } z_i = \sum_{j=1}^{k} \frac{u_{i,j}}{v_i}\omega_j$$

where $u_i, u_{i,j}, v \in R_1$, and for some $\bar{a} \in R_1^l$ and $\bar{b_i} \in R_1^l, i = 1, \ldots, n$ we have that

$$g(u_1, ..., u_k, v, a_1, ..., a_l) = 0 \text{ and } g(u_{i,1}, ..., u_{i,k}, v_i, b_{i,1}, ..., b_{i,l}) = 0$$

with $g(x_1, \ldots, x_k, y, z_1, \ldots, z_l)$ being the defining polynomial of R_2 over R_1.
Now let $r \in \{1, ..., n\}$. By substitution, we have that

$$\left(\sum_{i=1}^{k} \frac{u_i}{v}\omega_i\right) t_r = \sum_{j=1}^{k} \frac{u_{r,j}}{v_r}\omega_j.$$

By Lemma 4.7, we have that

$$t_r = \left(\sum_{j=1}^{k} \frac{u_{r,j}}{v_r}\omega_j\right)\left(\sum_{i=1}^{k} \frac{P_i\left(\frac{u_1}{v}, ..., \frac{u_k}{v}\right)}{Q\left(\frac{u_1}{v}, ..., \frac{u_k}{v}\right)}\omega_i\right),$$

where $Q\left(\frac{u_1}{v}, ..., \frac{u_k}{v}\right) \neq 0$, $P_i\left(\frac{u_1}{v}, ..., \frac{u_k}{v}\right)$, and $Q\left(\frac{u_1}{v}, ..., \frac{u_k}{v}\right)$ depend only on Ω.

Further, by Lemma 4.6, we have

$$t_r = \sum_{i=1}^{k} B_i \left(\frac{u_{r,1}}{v_r}, ..., \frac{u_{r,k}}{v_r}, \frac{P_1\left(\frac{u_1}{v}, ..., \frac{u_k}{v}\right)}{Q\left(\frac{u_1}{v}, ..., \frac{u_k}{v}\right)}, ..., \frac{P_k\left(\frac{u_1}{v}, ..., \frac{u_k}{v}\right)}{Q\left(\frac{u_1}{v}, ..., \frac{u_k}{v}\right)} \right) \omega_i,$$

where B_i is a fixed polynomial depending only on Ω. Now we will proceed to clear out our denominators. Let

$$D_{1,r} = \left[v_r Q\left(\frac{u_1}{v}, ..., \frac{u_n}{v}\right) \right]^{d_1}$$

where d_1 is the maximum of the degrees of $B_1, ..., B_k$. Then let

$$\bar{B}_{i,r} = D_{1,r} B_i = \bar{B}_i \left(u_{r,1}, ..., u_{r,k}, v_r, P_1\left(\frac{u_1}{v}, ..., \frac{u_k}{v}\right), ..., P_k\left(\frac{u_1}{v}, ..., \frac{u_k}{v}\right), Q\left(\frac{u_1}{v}, ..., \frac{u_k}{v}\right) \right).$$

Let

$$D_2 = v^{d_2}$$

where d_2 is the maximum of the degrees of $\bar{B}_1, ..., \bar{B}_k$. Then let

$$\bar{\bar{B}}_{i,r} = D_2 \bar{B}_{i,r} = \bar{\bar{B}}_{i,r} \left(u_{r,1}, .., u_{r,k}, v_r, u_1, .., u_k, v \right).$$

Let $D_r(u_1, \ldots, u_n, v, v_r) = D_{1,r} D_2$ and note that it is a fixed polynomial depending on the basis and the maximum values of the indexes only and for values of the variable satisfying the equations above, it is non-zero. Now we have

$$D_r t_r = \sum_{i=1}^{k} \bar{\bar{B}}_{i,r}(u_{r,1}, ..., u_{r,k}, v_r, u_1, ..., u_k, v)\omega_i.$$

We now rewrite $f(z_1, ..., z_n, y, x_1, ..., x_l) = 0$. We can rewrite this equation as follows:

$$f\left(\sum_{j=1}^{k} \frac{u_{1,j}}{v_1}\omega_j, ..., \sum_{j=1}^{k} \frac{u_{n,j}}{v_n}\omega_j, \sum_{j=1}^{k} \frac{u_j}{v}\omega_j, \sum_{j=1}^{k} \frac{x_{1,j}}{X_1}\omega_j, .., \sum_{j=1}^{k} \frac{x_{l,j}}{X_l}\omega_j\right) = 0,$$

where each $u_{i,j}, v_i, u_j, v, x_{i,j}, X_i \in R_1$. Now as g is the defining polynomial of R_2 over R_1, for some $\bar{a}_1, \ldots, \bar{a}_n \in R_1^m$, we have that

$$\begin{cases} g(u_{1,1}, ..., u_{1,k}, v_1, a_{1,1}, ..., a_{1,m}) = 0 \\ \vdots \\ g(u_{n,1}, ..., u_{n,k}, v_n, a_{n,1}, ..., a_{n,m}) = 0 \end{cases}$$

ensures that $\sum_{j=1}^{k} \frac{u_{r,j}}{v_r}\omega_j \in R_2$ for $r \in \{1, ..., n\}$, and also implies $v_r \neq 0$.
Additionally, if for some $b_{1,1}, \ldots, b_{l,m}, X_1, \ldots, X_l \in R_1$ we have

$$\begin{cases} g(x_{1,1}, ..., x_{1,k}, X_1, b_{1,1}, ..., b_{1,m}) = 0 \\ \vdots \\ g(x_{l,1}, ..., x_{l,k}, X_l, b_{l,1}, ..., b_{l,m}) = 0 \end{cases}$$

then $\sum_{j=1}^{k} \frac{x_{s,j}}{X_s}\omega_j \in R_2$ for $s \in \{1, ..., l\}$, and also $X_s \neq 0$. Lastly, if for some $a_1, \ldots, a_m \in R_1$ we have

$$g(u_1, ..., u_k, v, a_1, ..., a_m) = 0,$$

then $\sum_{j=1}^{k} \frac{u_j}{v}\omega_j \in R_2$ and $v \neq 0$.

Finally we work with coordinate polynomials to rewrite

$$f(z_1, ..., z_n, y, x_1, ..., x_l) = 0$$

for $z_1, ..., z_n, y, x_1, ..., x_l \in R_2 \subset F$ in terms of $\Omega = \{\omega_1, ..., \omega_n\}$, which is a basis of F over F_1 and also a Diophantine basis of R_2 over R_1. We have

$$f(z_1, ..., z_n, y, x_1, ..., x_l) = 0$$

$$\Updownarrow$$

$$f\left(\sum_{j=1}^{k} \frac{u_{1,j}}{v_1}\omega_j, ..., \sum_{j=1}^{k} \frac{u_{n,j}}{v_n}\omega_j, \sum_{j=1}^{k} \frac{u_j}{v}\omega_j, \sum_{j=1}^{k} \frac{x_{1,j}}{X_1}\omega_j, .., \sum_{j=1}^{k} \frac{x_{l,j}}{X_l}\omega_j\right) = 0$$

$$\Updownarrow$$

$$\sum_{j=1}^{k} {f_j}^{\Omega}\left(\frac{u_{1,1}}{v_1}, ..., \frac{u_{1,k}}{v_1}, ..., \frac{u_{n,1}}{v_n}, ..., \frac{u_{n,k}}{v_n}, \frac{u_1}{v}, ..., \frac{u_k}{v}, \frac{x_{1,1}}{X_1}, .., \frac{x_{1,k}}{X_1}, ..., \frac{x_{l,1}}{X_l}, ..., \frac{x_{l,k}}{X_l}\right)\omega_j = 0,$$

where we have k polynomials from F that have ratios in R_1 and depend only on Ω. Let $E = \max(\deg({f_j}^{\Omega}))$ and in addition let $C = (v_1 \cdots v_n v X_1 \cdots X_l)^E$. Now let

$$\begin{aligned}\bar{f}_j^{\Omega} &= C f_j^{\Omega}\left(\frac{u_{1,1}}{v_1}, ..., \frac{u_{1,k}}{v_1}, ..., \frac{u_{n,1}}{v_n}, ..., \frac{u_{n,k}}{v_n}, \frac{u_1}{v}, ..., \frac{u_k}{v}, \frac{x_{1,1}}{X_1}, .., \frac{x_{1,k}}{X_1}, ..., \frac{x_{l,1}}{X_l}, ..., \frac{x_{l,k}}{X_l}\right) \\ &= \bar{f}_j^{\Omega}\left(u_{1,1}, ..., u_{1,k}, ..., u_{n,1}, ..., u_{n,k}, u_1, ..., u_k, x_{1,1}, .., x_{1,k}, ..., x_{l,1}, ..., x_{l,k}\right).\end{aligned}$$

In this case, we have

$$\begin{aligned}B = \{(t_1, ..., t_n) \ \in \ F_2^n \mid \exists \bar{a}_r \in R_1^m, u_{1,1}, \ldots, u_{n,k}, \\ u_1, \ldots, u_k, v_1, \ldots, v_n, v, x_{1,1}, \ldots, x_{l,k}, X_1, \ldots, X_l \in R_1\end{aligned}$$

$$D_r t_r = \sum_{i=1}^{k} \bar{\bar{B}}_{i,r}(u_{r,1}, ..., u_{r,k}, v_r, u_1, ..., u_k, v)\omega_i, r = 1, ..., n,$$

$$g(u_{r,1}, ..., u_{r,k}, v_r, \bar{a}_r) = 0, r = 1, ..., k,$$

$$\bar{f}_j^{\Omega}(u_{1,1}, ..., u_{n,k}, v_1, ..., v_n, u_1, ..., u_k, v, x_{1,1}, ..., x_{l,k}, X_1, ..., X_l) = 0, j = 1, ..., k\}.$$

Then we have

$$B^{\Omega} = \{(w_{1,1}, ..., w_{k,n}) \in F_1^{kn} \mid \exists \bar{a}_r \in R_1^m, u_{1,1}, \ldots, u_{n,k},$$

$$u_1, \ldots, u_k, v_1, \ldots, v_n, v, x_{1,1}, \ldots, x_{l,k}, X_1, \ldots, X_l \in R_1$$

$$D_r w_{i,r} = \bar{\bar{B}}_i(u_{r,1}, ..., u_{r,k}, v_r, u_1, ..., u_k, v), r = 1, ..., k, i = 1, \ldots, n$$

$$g(u_{r,1}, ..., u_{r,k}, v_r, \bar{a_r}) = 0, r = 1, ..., k,$$

$$\bar{f}_j^{\Omega}(u_{1,1}, ..., u_{n,k}, v_1, ..., v_n, u_1, ..., u_k, v, x_{1,1}, ..., x_{l,k}, X_1, ..., X_l) = 0, j = 1, ..., k\}.$$

Thus, $B^{\Omega} \subset F_1^{kn}$ has a field-Diophantine definition over R_1. □

We now state without proof a property of Diophantine generation. The proof can be found in Lemma 2.1.11 of [8].

Proposition 4.17. *Let R_1, R_2 be integral domains with fraction fields F_1, F_2 respectively and $R_2 \leq_{Dioph} R_1$. Let F be any field containing both F_1 and F_2 and of finite degree over F_1 (by definition of Diophantine generation, at least one such field exists), and let Ω be any basis of F over F_1. In this case, F is a defining field and Ω is a defining basis.*

In view of Proposition 4.17, we can make the following observation.

Remark 4.18. If $R_2 \subset F_1$, and R_2 is field-Diophantine over R_1, then clearly $R_2 \leq_{Dioph} R_1$ with basis consisting of $\{1\}$. Also of $R_2 \leq_{Dioph} R_1$, then we can choose a power

basis as a Diophantine basis for the defining field over F_1. Since R_2 is a subset of F_1, this is equivalent to using a basis consisting of $\{1\}$ and the defining polynomial for Diophantine generation becomes a field-Diophantine definition.

We now connect Diophantine generation to Hilbert's Tenth Problem.

Proposition 4.19. *If R_1 and R_2 are recursive rings with $R_1 \leq_{Dioph} R_2$ and HTP is not solvable over R_1, then it is not solvable over R_2.*

Proof. If $R_1 \leq_{Dioph} R_2$, then given a polynomial equation over R_1, we can algorithmically construct a system of polynomial equations over R_2 such that the system has solutions in R_2 if and only if the original polynomial equation had solutions in R_1. In view of the Corollary 4.2, we conclude that if there is no algorithm to tell whether a polynomial equation over R_1 has solutions in R_1, then there is no such algorithm over R_2. □

Now we will prove transitivity of Dioph-generation.

Theorem 4.20. *Let R_1, R_2, and R_3 be integral domains with quotient fields F_1, F_2, and F_3 respectively. Assume that F_1, F_2, and F_3 are all subfields of a field F, which is not algebraically closed. Further assume that all the extensions F/F_i for $i = 1, 2, 3$ are finite. Lastly assume that $R_2 \leq_{Dioph} R_1$ and $R_3 \leq_{Dioph} R_2$. In this case, we have $R_3 \leq_{Dioph} R_1$.*

Proof. Let F be the defining field for both (R_1, R_2) and (R_2, R_3). We can make such a choice by Proposition 4.17. Let $\Omega = \{\omega_1, ..., \omega_k\}$ be a Diophantine basis for R_2 over R_1 such that F is the corresponding defining field. Further, let $\Lambda = \{\lambda_1, ..., \lambda_n\}$ be a Diophantine basis for R_3 over R_2 such that F is the corresponding defining field as

well. By Lemma 4.13, we can write

$$R_3 = \left\{ \sum_{i=1}^{n} z_i \lambda_i | (z_1, ..., z_n) \in A_\Lambda \subseteq F_2^n \right\},$$

where A_Λ has a field-Diophantine definition over R_2. Further, by Proposition 4.16, A_Λ^Ω has a field-Diophantine definition over R_1. Thus, we obtain

$$\begin{aligned} R_3 &= \left\{ \sum_{i=1}^{n} z_i \lambda_i | (z_1, ..., z_n) \in A_\Lambda \subseteq F_2^n \right\} \\ &= \left\{ \sum_{i=1}^{n} \sum_{j=1}^{k} y_{i,j} \omega_j \lambda_i | (y_{1,1}, ..., y_{n,k}) \in A_\Lambda^\Omega \subseteq F_1^{nk} \right\} \\ &= \left\{ \sum_{i=1}^{n} \sum_{j=1}^{k} y_{i,j} \lambda_i \omega_j | (y_{1,1}, ..., y_{n,k}) \in A_\Lambda^\Omega \subseteq F_1^{nk} \right\} \\ &= \left\{ \sum_{s=1}^{k} \sum_{j=1}^{k} \sum_{i=1}^{n} \left(y_{i,j} A_{i,j,s} \right) \omega_s | (y_{1,1}, ..., y_{n,k}) \in A_\Lambda^\Omega \right\}, \end{aligned}$$

where

$$z_i = \sum_{j=1}^{k} y_{i,j} \omega_j, \ \sum_{s=1}^{k} A_{i,j,s} \omega_s = \lambda_i \omega_j, \ A_{i,j,s} \in F_1.$$

Let

$$B_\Omega = \left\{ (t_1, ..., t_k) \in F_1^k | t_s = \sum_{j=1}^{k} \sum_{i=1}^{n} \left(y_{i,j} A_{i,j,s} \right), (y_{1,1}, ..., y_{n,k}) \in A_\Lambda^\Omega \right\}.$$

By Lemma 4.10, we know that B_Ω has a field-Diophantine definition over R_1 and since we have

$$R_3 = \left\{ \sum_{s=1}^{k} t_s \omega_s | (t_1, ..., t_k) \in B_\Omega \right\},$$

by Lemma 4.13, $R_3 \leq_{Dioph} R_1$. □

We will now state and prove the finite intersection property.

Theorem 4.21. *Let $R_i \subset R$ for $i = 1, ..., m$ be rings such that the quotient field of*

R is not algebraically closed and for all $i = 1, ..., m$ we have that $R_i \leq_{Dioph} R$. Then $\cap_{i=1}^{m} R_i \leq_{Dioph} R$.

Proof. We have that R_i has a Diophantine definition $f_i(t, x_1, ..., x_{n_i})$ over R since $R_i \subset R$ and $R_i \leq_{Dioph} R$. Thus, for all $x \in R$ we have that there exist $x_{1,1}, ..., x_{m,n_m} \in R$ with $f_i(x, x_{i,1}, ..., x_{i,n_i}) = 0$ for $i = 1, ..., m$ if and only if $x \in \cap_{i=1}^{m} R_i$. □

4.4 Rings of Integers of Number Fields

First, we need to define the rings of integers of number fields and discuss some of their properties.

Definition 4.22 (Number Fields and Rings of Integers)**.** If K is a finite extension of $\mathbb{Q}$, then K is called a number field. If $x \in K$ satisfies a monic irreducible polynomial over $\mathbb{Z}$, then x is called an algebraic integer.

The following propositions are standard results from Number Theory. See [3] for more details.

Proposition 4.23 (Properties of Integers of Number Fields)**.**

- *The set of all integers of a number field K is a ring. In the future we will denote this ring by O_K.*
- *For any number field K there exists a basis Ω of K over $\mathbb{Q}$ such that $O_K = \{x \in K | x = \sum a_i \omega_i, a_i \in \mathbb{Z}\}$. (Such a basis is called an integral basis of K over $\mathbb{Q}$.)*

In this section, we will use the following theorem due to Mazur, Poonen, and Rubin which could be stated as follows:

Theorem 4.24. *If F/K is a cyclic extension of prime degree p and if the Shafarevich-Tate conjecture is true for K, then $O_K \leq_{Dioph} O_F$ where O_K and O_F are the rings of integers over the number fields K and F respectively.*

Our main goal to show $\mathbb{Z} \leq_{Dioph} O_E$ for any number field E, assuming a certain number-theoretic conjecture is true, can now be achieved. We will do this through a series of reductions. We will first show that if

(1) **for any cyclic extension F/K of a number field of prime degree p, we have that $O_K \leq_{Dioph} O_F$,**

then it follows that $\mathbb{Z} \leq_{Dioph} O_E$, for any number field E. Then

(2) we will apply Mazur, Rubin, and Poonen's results to conclude if the Shafarevich-Tate conjecture holds then the previous statement holds.

Before we proceed, we need to discuss more properties of the rings of integers of number fields. As an immediate corollary to Proposition 4.23 we have the following fact.

Corollary 4.25. *For any number field K, we have $O_K \leq_{Dioph} \mathbb{Z}$.*

One can also show the following proposition is true. (The proof can be found in Chapter 2 of [8].)

Proposition 4.26. *If M/K is a finite extension of number fields, then $O_M \leq_{Dioph} O_K$.*

Proposition 4.27. *Let L/M be a cyclic extension and assume statement (1) holds. In this case, we have $O_M \leq_{Dioph} O_L$.*

Proof. We will do this by induction on $[L : M] = n$. For the case, $n = 1$ is trivial because everything is $\leq_{Dioph}$ than itself. Assume for any cyclic extension of degree $k < n$ the proposition holds. We will show it holds for n. Let τ be a generator of

$G(L/M)$. Since $n > 1$, there exists a prime p dividing n. Let $\sigma = \tau^{\frac{n}{p}}$ and note $\text{ord}(\sigma) = p$. Let $H = L_{<\sigma>}$. Then we have the following $M \subset H \subset L$, $[H : M] = \frac{n}{p} < n$, and $[L : H] = p$. Further by Corollary 3.33, all the extensions are cyclic. Thus, $O_H \leq_{Dioph} O_L$ by (1). By the induction hypothesis, we have $O_M \leq_{Dioph} O_H$. Lastly, by transitivity of Dioph-generations, we have $O_M \leq_{Dioph} O_L$. □

Proposition 4.28. *Let L/M be Galois and assume (1) holds, then $O_M \leq_{Dioph} O_L$.*

Proof. Let $\{\sigma_1, ..., \sigma_n\} = G(L/M)$. For each $i \in \{1, ..., n\}$ consider $L_{<\sigma>}$ and note that

1. $L/L_{<\sigma_i>}$ is cyclic and
2. $\bigcap_{i=1}^{n} L_{<\sigma_i>} = M$.

By Proposition 4.27, we have $O_{L_{<\sigma_i>}} \leq_{Dioph} O_L$. By the intersection property of Dioph-generations, we have $O_M = \bigcap_{i=1}^{n} O_{L_{<\sigma_i>}} \leq_{Dioph} O_L$. □

Proposition 4.29. *If (1) holds and L/M is any finite extension of number fields of degree n, then $O_L \leq_{Dioph} O_M$.*

Proof. Let M^G be any field Galois over O_L and containing M. (In particular, if $M = L(\alpha)$, M^G can be $M(\alpha = \alpha_1, ..., \alpha_n)$ where $\alpha_1, \ldots, \alpha_n$ are are all conjugates of α over L.) By Proposition 4.26, we have $O_{M^G} \leq_{Dioph} O_M$. By the previous proposition, we have $O_L \leq_{Dioph} O_{M^G}$. Lastly, by transitivity of Dioph-generations, we have $O_L \leq_{Dioph} O_M$. □

We now state the main theorem of this section.

Theorem 4.30. *If the Shafarevich-Tate conjecture on elliptic curves is true, then $\mathbb{Z} \leq_{Dioph} O_K$ for any number field K, and thus Hilbert's Tenth Problem is not decidable over the ring of integers of any number field K.*

Proof. From a result of Poonen (see [6]) and a result of Mazur and Rubin (see [5]), it follows that assuming the Shafarevich-Tate conjecture for elliptic curves, for any prime degree cyclic extension of number fields M/K we have $O_K \leq_{Dioph} O_M$. Thus by Proposition 4.29, we have that $\mathbb{Z} \leq_{Dioph} O_K$ for any number field K. $\square$

REFERENCES

[1] Fraleigh, J. B. (2003). *A first course in abstract algebra*. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont.

[2] Herstein, I. N. (1996). *Abstract algebra*. Prentice Hall Inc., Upper Saddle River, NJ, third edition. With a preface by Barbara Cortzen and David J. Winter.

[3] Janusz, G. J. (1996). *Algebraic number fields*, volume 7 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, second edition.

[4] Matiyasevich, Y. V. (1993). *Hilbert's tenth problem*. Foundations of Computing Series. MIT Press, Cambridge, MA. Translated from the 1993 Russian original by the author, With a foreword by Martin Davis.

[5] Mazur, B. and Rubin, K. (2010). Ranks of twists of elliptic curves and Hilbert's tenth problem. *Invent. Math.*, 181(3):541–575.

[6] Poonen, B. (2002). Using elliptic curves of rank one towards the undecidability of Hilbert's tenth problem over rings of algebraic integers. In *Algorithmic number theory (Sydney, 2002)*, volume 2369 of *Lecture Notes in Comput. Sci.*, pages 33–42. Springer, Berlin.

[7] Rogers, Jr., H. (1987). *Theory of recursive functions and effective computability*. MIT Press, Cambridge, MA, second edition.

[8] Shlapentokh, A. (2007). *Hilbert's tenth problem*, volume 7 of *New Mathematical Monographs*. Cambridge University Press, Cambridge. Diophantine classes and extensions to global fields.