Hilbert’s Tenth Problem: Diophantine Classes and Other Extensions to Global Fields.

Alexandra Shlapentokh
Department of Mathematics
East Carolina University
Greenville, NC 27858
shlapentokha@mail.ecu.edu

October 26, 2005
To my thesis adviser Harold N. Shapiro, who taught me not to be scared.

Acknowledgements

The author would like to thank the following people for helpful suggestions and corrections: Gunther Cornelissen, Martin Davis, Jospeh Flenner, Dino Lorenzini, Laurent Moret-Bailly and Bjorn Poonen.

The author also acknowledges support from the National Science Foundation (DMS-0354907).
# Contents

1 **Introduction.**
   1.1 In the Beginning. ........................................ 1
   1.2 Diophantine Definitions and Diophantine Sets. ......... 4

2 **Diophantine Classes: Definition and Basic Facts.** .... 9
   2.1 Diophantine Generation. .................................. 9
   2.2 Diophantine Generation of Integral Closure and Dioph-regularity. 24
   2.3 Big Picture: Diophantine Family of a Ring. ............ 26

3 **Diophantine Equivalence and Diophantine Decidability.** 31
   3.1 Weak Presentations. ..................................... 31
   3.2 Some Properties of Weak Presentations. ................. 33
   3.3 How Many Diophantine Classes Are There? ............... 39
   3.4 Diophantine Generation and Hilbert’s Tenth Problem .... 40

4 **Integrality at Finitely Many Primes and Divisibility of Order at Infinitely Many Primes.** 48
   4.1 The Main Ideas. ........................................... 49
   4.2 Integrality at Finitely Many Primes in Number Fields. 51
   4.3 Integrality at Finitely Many Primes over Function Fields. 57
   4.4 Divisibility of Order at Infinitely Many Primes Over Number Fields. 63
   4.5 Divisibility of Order at Infinitely Many Primes Over Function Fields. 70

5 **Bound Equations for Number Fields and Their Consequences.** 73
   5.1 Real Embeddings. ......................................... 73
   5.2 Using Divisibility in the Rings of Algebraic Integers. 74
   5.3 Using Divisibility in Bigger Rings. ...................... 77
6 Units of Rings of $\mathcal{O}$-integers of Norm 1. 82
6.1 What Are the Units of the Rings of $\mathcal{O}$-integers? 82
6.2 Norm Equations of Units. 85
6.3 Pell Equation. 88
6.4 Non-integral Solutions of Some Unit Norm Equations. 100

7 Diophantine Classes over Number Fields. 106
7.1 Vertical Methods of Denef and Lipshitz. 106
7.2 Integers of Totally Real Number Fields
and Fields with Exactly One Pair of Non-real Embeddings. 108
7.3 Integers of Extensions of Degree 2 of Totally Real Number Fields. 111
7.4 The Main Results for the Rings of $\mathcal{O}$-integers and an Overview
of the Proof. 114
7.5 The Main Vertical Definability Results for Rings of $\mathcal{O}$-integers
in Totally Real Number Fields. 116
7.6 Consequences for Vertical Definability over Totally Real Fields. 123
7.7 Horizontal Definability for the Rings of $\mathcal{O}$-integers of Totally
Real Number Fields and Diophantine Undecidability for These
Rings. 126
7.8 Vertical Definability Results for Rings of $\mathcal{O}$-integers of the To-
tally Complex Extensions of Degree 2 of Totally Real Number Fields. 127
7.9 Some Consequences. 134
7.10 Big Picture for Number Fields Revisited. 138
7.11 Further results. 140

8 Diophantine Undecidability of Function Fields. 143
8.1 Defining Multiplication Through Localized Divisibility. 143
8.2 $p$-th Power Equations over Function Fields I: Overview and
Preliminary Results. 149
8.3 $p$-th Power Equations over Function Fields II: $p$-th Powers of
a Special Element. 161
8.4 $p$-th Power Equations over Function Fields III: $p$-th Powers of
Arbitrary Functions. 167
8.5 Diophantine Model of $\mathbb{Z}$ over Function Fields over Finite Fields
of Constants. 177

9 Bounds for Function Fields. 180
9.1 Height Bounds. 180
9.2 Using $p$-th Powers to Bound the Height. 182
10 Diophantine Classes over Function Fields. 184
10.1 The Weak Vertical Method Revisited. 184
10.2 The Weak Vertical Method Applied to Non-Constant Cyclic Extensions. 186
10.3 The Weak Vertical Method Applied to Constant Field Extensions. 189
10.4 Vertical Definability for Large Subrings of Global Function Fields. 191
10.5 Integrality at Infinitely Many Primes over Global Function Fields. 194
10.6 The Big Picture for Function Fields Revisited. 196

11 Mazur’s Conjectures and Their Consequences. 200
11.2 A Ring Version of Mazur’s Conjecture. 201
11.3 First Counterexamples. 204
11.4 Consequences for Diophantine Models. 207

12 Results of Poonen. 210
12.1 A Statement of the Main Theorem and an Overview of the Proof. 210
12.2 Properties of Elliptic Curves I: Factors of Denominators of Points. 213
12.3 Properties of Elliptic Curves II: The Density of the Set of “Largest” Primes. 215
12.4 Properties of Elliptic Curves III: Finite Sets Looking Big. 220
12.5 Properties of Elliptic Curves IV: Consequences of a Result of Vinogradov. 221
12.6 Construction of Sets $T_1(P)$ and $T_2(P)$ and Their Properties. 222
12.7 Proof of Poonen’s Theorem. 228

13 Beyond Global Fields. 231
13.1 Function Fields of Positive Characteristic of Higher Transcendence Degree or over Infinite Fields of Constants. 231
13.2 Algebraic Extensions of Global Fields of Infinite Degree. 233
13.3 Function Fields of Characteristic 0. 235

A Recursion Theory. 237
A.1 Computable Functions. 237
A.2 Recursively Enumerable Sets. 245
A.3 Turing and Partial Degrees. 247
A.4 Degrees of Sets of Indices, Primes and Products. 248
A.5 Computable Algebra. 250
A.6 Recursive Presentation of $\mathbb{Q}$. 250
### A.7 Recursive Presentation of Other Fields

#### 256

### A.8 Representing Sets of Primes and Rings of \( \mathcal{O} \)-integers in Number Fields

#### 262

### B Number Theory

#### B.1 Global Fields, Valuations and Rings of \( \mathcal{O} \)-integers

- 268

#### B.2 Existence Through Approximation Theorems

- 280

#### B.3 Linearly Disjoint Fields

- 283

#### B.4 Divisors, Prime and Composite, under Extensions

- 288

#### B.5 Density of Prime Sets

- 311

#### B.6 Elliptic Curves

- 323

#### B.7 Coordinate Polynomials

- 331

#### B.8 Basic Facts about Local Fields

- 336

#### B.9 Derivations

- 337

#### B.10 Some Calculations

- 339

---

### Bibliography

- 348

### Index

- 358
Chapter 1

Introduction.

1.1 In the Beginning.

The subject of this book dates back to the beginning of the XX century. In 1900, at the International Congress of Mathematicians, David Hilbert presented a list of problems which exerted great influence on the development of Mathematics in the twentieth century. The tenth problem on the list had to do with solving Diophantine equations. Hilbert was interested in a construction of an algorithm which could determine whether or not an arbitrary polynomial equation in several variables had solutions in integers. If we translate Hilbert’s question into modern terms, we can say that he wanted a program taking coefficients of a polynomial equation as input and producing “yes” or “no” answer to the question “Are there integer solutions?”. This problem became known as Hilbert’s Tenth Problem.

It took some time to prove that the algorithm requested by Hilbert did not exist. At the end of the sixties, building on the work of Martin Davis, Hilary Putnam, and Julia Robinson, Yuri Matiyasevich proved that Diophantine sets over \( \mathbb{Z} \) were the same as recursively enumerable sets, and, thus, Hilbert’s Tenth Problem was unsolvable. The original proof and its immediate implications have been described in detail. An interested reader can, for example, be referred to a book by Matiyasevich (see [52] – the original Russian edition or [53] – an English translation), an article by Davis (see [12]) and an article by Davis, Robinson and Matiyasevich (see [13]). The solution of the original Hilbert’s Tenth Problem gave rise to a whole new class of problems some of which are the subject of this book.

The question posed by Hilbert can of course be asked of any recursive ring. In other words, given a recursive ring \( R \), we can ask whether there exists an algorithm capable of determining when an arbitrary polynomial equation over \( R \) has solutions in \( R \). Since the time when the solution of Hilbert’s
Tenth Problem was obtained, this question has been answered for many rings. In this book we will describe the developments in the subject pertaining to subrings of global fields: number fields and algebraic function fields over finite fields of constants. While there has been significant progress in the subject, many interesting questions are still unanswered. Chief among them are the questions of solvability of the analog of Hilbert’s Tenth Problem over $\mathbb{Q}$ and the ring of algebraic integers of an arbitrary number field. Recent results of Poonen brought us “arbitrarily close” to solving the problem for $\mathbb{Q}$ but formidable obstacles still remain.

A question which is closely related to the analogs of Hilbert’s Tenth Problem over number fields is the question of Diophantine definability of $\mathbb{Z}$. As we will see in this book, Diophantine definability of $\mathbb{Z}$ over a ring of characteristic zero contained in a field which is not algebraically closed, implies the unsolvability of Hilbert’s Tenth Problem for this ring. In general, questions of Diophantine definability are of independent number theoretic and model theoretic interest. In particular, the question of Diophantine definability of $\mathbb{Z}$ over $\mathbb{Q}$ has generated a lot of interest. Barry Mazur has made several conjectures which imply that such a definition does not exist. In this book we will discuss some of these conjectures and their consequences for generalizations of Hilbert’s Tenth Problem to other domains.

For various technical reasons which we will endeavor to make clear in this book, greater progress has been made over the function fields over finite fields of constants. In particular, we do know that the analog of Hilbert’s Tenth Problem is unsolvable over all function fields of positive characteristic over finite field of constants. The main unanswered questions here have to do with Diophantine definability. In particular, we still do not know if $\mathcal{S}$-integers have a Diophantine definition over a function field though in some sense we have come “arbitrarily close” to such a definition.

We would also like to address our main motivation in writing this book. We wanted to put together a single coherent account of various methods employed so far in generalizing Hilbert’s Tenth Problem to domains other than $\mathbb{Z}$ contained in global fields. In particular, we wanted to highlight the expected similarities and differences in the way various problems were solved over number fields and function fields of positive characteristic. In our opinion the relative comparison of these two cases brings to light the nature of the difficulties encountered over the number fields: existence of archimedean valuations.

The material contained in the book will require some familiarity on the part of the reader with Number Theory and Recursion Theory. We have
collected the required background information with references in Appendix A (Recursion Theory) and Appendix B (Number Theory). As a general reference for Recursion Theory we suggest *Theory of Recursive Functions and Effective Computability* by H. Rogers, McGraw-Hill, 1967. Unfortunately, there is no single reference for the number theoretic material used in the book. However, the reader can find most of the necessary material in *Field Arithmetic* by M. Jarden and M. Fried, Second Edition, Springer Verlag, 2005 (this book also contains material pertaining to Recursion Theory), *Algebraic Number Fields* by J. Janusz, Academic Press, 1973, and *Introduction to Theory of Algebraic Functions of One Variable* by C. Chevalley, Mathematical Surveys #6, AMS, Providence, 1951, and *An Invitation to Arithmetic Geometry*, by D. Lorenzini, Graduate Studies in Mathematics, Volume 9, AMS, 1997. Understanding Poonen’s results in Chapter 12 will require some familiarity with elliptic curves. For this material the reader can consult *The Arithmetic of Elliptic Curves* by Joseph Silverman, Springer Verlag, 1986.

Before proceeding further we should also settle on the future use of some terms. Given a ring $R$, we will call the analog of Hilbert’s Tenth Problem over $R$, the “Diophantine problem of $R$”. The expression “Diophantine (un)solvability of a ring $R$” will refer to the (un)solvability of the Diophantine problem of $R$. All the rings in the book will be assumed to be integral domains with identity. We will also settle on a fixed algebraic closure of $\mathbb{Q}$ contained in the field of complex numbers and assume that all the number fields occurring in the book are subfields of this algebraic closure. Similarly, for each prime $p$, we will fix an algebraic closure of a rational function field over a $p$-element field of constants, and assume that any global function field of characteristic $p$ occurring in this book is a subfield of this algebraic closure. On occasion we will also talk about the compositum of abstract fields. For these cases we will also maintain an implicit assumption throughout the book that all the fields in question are subfields of the same algebraically closed field.

Finally we would like to say a few words about the structure of this book and and its possible uses as a text for a class. Chapters 1 – 3 contain the introductory material necessary to familiarize the reader with the terminology and to establish a connection between algebraic and logical concepts presented in this book. Chapters 4 – 12 are the technical core of the book: Chapter 4 discusses definability of order at a prime of global fields; Chapters 5 – 7 cover Diophantine classes of number fields; Chapters 8 – 10 go over the analogous material for function fields; Chapter 11 addresses Mazur’s conjectures and their relation to the issues of Diophantine definability; Chapter 12 describes Poonen’s results on undecidability and Mazur’s conjectures for “large”
subrings of $\mathbb{Q}$. The ideas described in Chapters 4–10 are essentially number-theoretic in nature, while Chapters 11 and 12 add geometric flavor to the mix. Finally, Chapter 13 briefly surveys some issues related to the problems discussed in the book but not covered by the book.

An experienced reader can probably skip most of Chapters 1–3 except for the definition of Diophantine generation (Definition 2.1.5) and the relation between Diophantine generation and HTP (Section 3.4). Chapters on definition of order at a prime in number fields and function fields, and Mazur’s conjectures are fairly self-contained and can be read independently. Understanding Poonen’s results does require knowing the statement of the modified Mazur’s conjectures (Section 11.2) and material on Diophantine models (Section 3.4).

Parts of the book can be used as a text for an undergraduate course. Assuming just an undergraduate course in Algebra, one can cover the following chapters and sections: Chapters 1–3, Sections 6.3, and 7.1.1–7.3. Such a course will include some general ideas on Diophantine definability and discuss in detail HTP over the rings of integers of number fields.

There are several options for a semester long graduate course which would assume some background in algebraic Number Theory. One option is to cover the Diophantine classes of number fields: Chapters 1–3, Sections 4.1 and 4.2, and Chapters 5–7. Another option is to cover the analogous material for function fields: Chapters 1–3, Sections 4.1 and 4.3, and Chapters 8–10. The third possibility is to cover Mazur’s conjectures and Poonen’s results: Chapters 1–3, Sections 11.2 and 11.4, and Chapter 12. Such a course would also require a background in elliptic curves. Appendices should be used “as needed” for all the course versions.

The key to the whole subject lies in the notions of Diophantine definition and Diophantine set which we describe and discuss in the next section.

### 1.2 Diophantine Definitions and Diophantine Sets.

#### 1.2.1 Definition.

Let $R$ be an integral domain. Let $m, n$ be positive integers and let $\mathcal{A} \subset R^n$. Then we will say that $\mathcal{A}$ has a Diophantine definition over $R$ if there exists a polynomial

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

such that for all \((t_1, \ldots, t_n) \in \mathbb{R}^n\),
\[(t_1, \ldots, t_n) \in \mathcal{A} \iff \exists x_1, \ldots, x_m, f(t_1, \ldots, t_n, x_1, \ldots, x_m) = 0.\]
The set \(\mathcal{A}\) is called \textit{Diophantine over} \(\mathbb{R}\).

We can now state the precise result obtained by Matiyasevich.

\textbf{1.2.2 Theorem.}

The Diophantine sets over \(\mathbb{Z}\) coincide with the recursively enumerable sets.

The negative answer to Hilbert’s problem is an immediate corollary of this theorem since not all the recursively enumerable sets are recursive. (For the definition of recursive and recursively enumerable sets and their relationship to each other, see Appendix A: Definition A.1.2, Definition A.1.3, Definition A.2.1, Lemma A.2.2 and Proposition A.2.3.)

Indeed, suppose we had an algorithm taking the coefficients of a polynomial equation as inputs and determining whether the polynomial equation has a solution. Let \(A \subset \mathbb{N}\) be a recursively enumerable but not recursive set. By the theorem above, there exists a polynomial \(f(y, x_1, \ldots, x_m)\) with integer coefficients such that \(f(t, x_1, \ldots, x_m) = 0\) has integer solutions if and only if \(t \in A\). Given a specific \(t \in \mathbb{N}\), we can use \(t\) and other coefficients of \(f\) as the required input for our algorithm, and determine whether \(f(t, x_1, \ldots, x_m) = 0\) has solutions \((x_1, \ldots, x_m)\) in \(\mathbb{Z}\). But this will also determine whether or not \(t \in A\). Since, by assumption, there is no algorithm to determine membership in \(A\), we must conclude that Hilbert’s Tenth Problem is unsolvable.

Having seen how Matiyasevich’s Theorem implied the unsolvability of Hilbert’s Tenth Problem via its characterization of the Diophantine sets, we would like to consider some alternative descriptions of Diophantine sets which will shed some light on the nature of our subject. The definition of Diophantine sets which we used above naturally identifies these sets as number-theoretic objects. Matiyasevich’s Theorem tells us that these sets also belong in Recursion Theory. On the other hand, as we will see from the lemma below, one could also consider Diophantine sets as the sets definable in the language of rings by positive existential formulas, and thus a subject of Model Theory. Finally, Diophantine sets are also projections of algebraic sets, and consequently belong in Algebraic Geometry. Thus, the reader can imagine that the flavor of the discussion can vary widely depending on how we view the Diophantine sets. In this book we display a pronounced bias towards the number-theoretic
of the matter at hand, though we will make some forays into geometry in our discussion of Mazur’s conjectures and Poonen’s results.

As we have mentioned in the previous section, Diophantine definitions can be used to establish unsolvability of Diophantine problem of other rings. Before we can explain in more detail how this is done, we have to make the following observation.

### 1.2.3 Lemma.

Let $R$ be a ring whose quotient field $K$ is not algebraically closed. (Here we remind the reader that by our assumption all the rings in this book are integral domains.) Let

$$\{f_i(x_1, \ldots, x_r), i = 1, \ldots, m\}$$

be a finite collection of polynomials over $R$. Then there exists a polynomial $H(x_1, \ldots, x_r) \in R[x_1, \ldots, x_r]$ such that the system

$$\begin{cases} f_1(x_1, \ldots, x_r) = 0; \\ \cdots \\ f_m(x_1, \ldots, x_r) = 0. \end{cases}$$

has solutions in $R$ if and only if $H(x_1, \ldots, x_r) = 0$ has solutions in $R$.

**Proof.**

It is enough to prove the lemma for the case $m = 2$. Let $h(x)$ be a polynomial with no roots in $K$. Assume $h(x) = a_0 + a_1 x + \ldots + a_n x^n$, where $a_0, \ldots, a_n \in R$ and $a_n \neq 0$. Further, note that

$$g(x) = x^n h(\frac{1}{x}) = a_0 x^n + a_1 x^{n-1} + \ldots + a_n,$$

is also a polynomial without roots in $K$. Indeed, if for some $b \neq 0$, we have that $g(b) = 0$, then $b^n h(\frac{1}{b}) = 0$ and consequently $h(\frac{1}{b}) = 0$. Finally, since $a_n \neq 0$, we know that $g(0) \neq 0$. Next consider

$$H(x_1, \ldots, x_r) = \sum_{i=0}^n a_i f_1^{n-i}(x_1, \ldots, x_r) f_2^i(x_1, \ldots, x_r).$$

It is clear that if for some $r$-tuple $(b_1, \ldots, b_r) \in R^r$,

$$f_1(b_1, \ldots, b_r) = f_2(b_1, \ldots, b_n) = 0,$$
then $H(b_1, \ldots, b_r) = 0$. Conversely, suppose for some $r$-tuple $(b_1, \ldots, b_r) \in R'$ we have that $H(b_1, \ldots, b_r) = 0$ and $f_1(b_1, \ldots, b_r) \neq 0$. Then

$$h \left( \frac{f_2(b_1, \ldots, b_r)}{f_1(b_1, \ldots, b_r)} \right) = 0.$$

On the other hand, if $f_2(b_1, \ldots, b_r) \neq 0$, then

$$g \left( \frac{f_1(b_1, \ldots, b_r)}{f_2(b_1, \ldots, b_r)} \right) = 0.$$

We can derive two consequences from this lemma. First, we note that over fields which are not algebraically closed having an algorithm for solving an arbitrary single polynomial equation is equivalent to having an algorithm for solving a finite system of polynomial equations. Second, we note that we can allow a Diophantine definition to consist of several polynomial equations without changing the nature of the relation.

We should also note here that for some algebraic geometers the restriction of Diophantine definitions to exactly one polynomial, as opposed to finitely many, might seem unnatural. In our defence we offer two arguments. As demonstrated by the lemma above, this distinction makes no difference for global fields which are the main subjects of this book, and historically questions related to Hilbert’s Tenth Problem have been phrased as questions about a single polynomial.

Equipped with the preceding lemma, we can now show the following.

### 1.2.4 Proposition.

Let $R_1 \subset R_2$ be two recursive rings. Suppose the fraction field of $R_2$ is not algebraically closed. Assume the Diophantine problem of $R_1$ is undecidable and $R_1$ has a Diophantine definition over $R_2$. Then the Diophantine problem of $R_2$ is also undecidable.

**Proof.**

Let $f(t, x_1, \ldots, x_r)$ be a Diophantine definition of $R_1$ over $R_2$. Let $g(t_1, \ldots, t_k)$ be a polynomial over $R_1$, and consider the following system:

$$
\begin{align*}
g(t_1, \ldots, t_k) &= 0; \\
f(t_1, x_1, \ldots, x_r) &= 0; \\
& \quad \cdots \\
f(t_k, x_1, \ldots, x_r) &= 0.
\end{align*}
$$

(1.2.1)
Clearly the equation $g(t_1, \ldots, t_k) = 0$ will have solutions in $R_1$ if and only if system in (1.2.1) above has solutions in $R_2$. Further, by the preceding lemma, since both rings are recursive, given coefficients of $g$ there is an algorithm to construct a polynomial $T(g)(t_1, \ldots, t_k, x_1, \ldots, x_r) \in R_2[t_1, \ldots, t_k, x_1, \ldots, x_r]$ such that the corresponding polynomial equation $T(g)(t_1, \ldots, t_k, x_1, \ldots, x_r) = 0$ has solutions over $R_2$ if and only if (1.2.1) has solutions in $R_2$.

Suppose now that Diophantine problem of $R_2$ is decidable. Then for each polynomial $g$ over $R_1$ we can effectively decide whether $g(t_1, \ldots, t_r) = 0$ has solutions in $R_1$ by first algorithmically constructing $T(g)$, and then algorithmically determining whether $T(g) = 0$ has solutions in $R_2$. Thus the Diophantine problem of $R_1$ is decidable in contradiction of our assumption, and we must conclude that the Diophantine problem of $R_2$ is not decidable.

1.2.5 Remark.

In this proof we used the notions of “algorithm” and ”recursive ring” rather informally. We will formalize this discussion in the chapter on weak presentations.

Almost all the known results (except for Poonen’s Theorem) concerning unsolvability of the Diophantine problem of rings of algebraic numbers have been obtained by constructing a Diophantine definition of $\mathbb{Z}$ over these rings. Before we present details of these and other constructions we would like to enlarge somewhat the context of our discussion by introducing the notions of Diophantine generation, Diophantine Equivalence and Diophantine Classes. These concepts will serve several purposes. They will provide a uniform language for the discussion of “Diophantine relations” between rings with the same and different quotient fields. They will allow us to view the existing results within a unified framework. Finally these concepts will point to some natural directions of possible investigation of more general questions of Diophantine definability.
Chapter 2

Diophantine Classes: Definition and Basic Facts.

In this chapter we will introduce the notion of Diophantine generation which will eventually lead us to the notion of Diophantine classes. We will also obtain the first relatively easy results on Diophantine generation and develop some methods applicable to all global fields: number fields and function fields. Most of the material for this chapter has been derived from [98].

2.1 Diophantine Generation.

We will start with a first modification of the notion of Diophantine definition.

2.1.1 Definition.

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

$$f(a_1, \ldots, a_k, b, x_1, \ldots, x_m)$$

with coefficients in $R$ such that

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

$$f(a_1, \ldots, a_k, b, x_1, \ldots, x_m) = 0 \Rightarrow b \neq 0,$$  \hspace{1cm} (2.1.1)

and

$$A = \{(t_1, \ldots, t_k) \in F^k | \exists a_1, \ldots, a_k, b, x_1, \ldots, x_m \in R,$$

$$bt_1 = a_1, \ldots, bt_k = a_k, f(a_1, \ldots, a_k, b, x_1, \ldots, x_m) = 0\}.$$  \hspace{1cm} (2.1.2)
Then we will say that \( A \) is \textit{field-Diophantine over} \( R \) and we will call \( f \) a \textit{field-Diophantine definition of} \( A \) over \( R \).

Next we will see that the notion of field-Diophantine definition is a proper extension of the notion of Diophantine definition that we discussed in the introduction.

\textbf{2.1.2 Lemma.}

Suppose \( R, A, F, k, m \) are as in Definition 2.1.1. Assume further \( A \subseteq R^k \) and \( F \) is not algebraically closed. Then \( A \) has a Diophantine definition over \( R \) if and only if it has a field-Diophantine definition over \( R \).

\textbf{Proof.}

First we assume that \( A \) has a field-Diophantine definition over \( R \) and show that \( A \) also has a Diophantine definition over \( R \). Let

\[ g = (a_1, \ldots, a_k, b, x_1, \ldots, x_m) \]

be a field-Diophantine definition of \( A \) over \( R \). Then

\[ f(t_1, \ldots, t_k, b, x_1, \ldots, x_m) = g(t_1b, \ldots, t_kb, b, x_1, \ldots, x_m) \]

is a Diophantine definition of \( A \) over \( R \) in the sense that for all \( t_1, \ldots, t_k \in R \),

\[ \exists b, x_1, \ldots, x_m \in R, f(t_1, \ldots, t_k, b, x_1, \ldots, x_m) = 0 \]

\[ \iff (t_1, \ldots, t_k) \in A. \]

Indeed, suppose for some \( t_1, \ldots, t_k, b, x_1, \ldots, x_m \in R \),

\[ f(t_1, \ldots, t_k, b, x_1, \ldots, x_m) = 0. \]

Then

\[ g(t_1b, \ldots, t_kb, b, x_1, \ldots, x_m) = 0 \]

and consequently,

\[ b \neq 0, \]

while

\[ (t_1b/b, \ldots, t_kb/b) = (t_1, \ldots, t_k) \in A. \]

Conversely, suppose \( (t_1, \ldots, t_k) \in A \). Then by assumption on \( g \),

\[ \exists x_1, \ldots, x_m, b \in R, g(bt_1, \ldots, bt_k, b, x_1, \ldots, x_m) = 0. \]
Thus, there exist $x_1, \ldots, x_m, b \in R$ such that
\[ f(t_1, \ldots, t_k, b, x_1, \ldots, x_m) = 0. \]

Suppose now that $f(t_1, \ldots, t_k, x_1, \ldots, x_m)$ is a Diophantine definition of $A$ over $R$. Then consider the following system of equations
\[
\begin{cases}
   f(a_1, \ldots, a_k, x_1, \ldots, x_m) = 0; \\
   b = 1.
\end{cases}
\] (2.1.3)

Let $g(a_1, \ldots, a_k, b, x_1, \ldots, x_m)$ be a polynomial over $R$ such that for all $(a_1, \ldots, a_k, b, x_1, \ldots, x_m) \in F$,
\[ g(a_1, \ldots, a_k, b, x_1, \ldots, x_m) = 0 \] (2.1.4)
is equivalent to $(a_1, \ldots, a_k, b, x_1, \ldots, x_m)$ being a solution to the system (2.1.3). Then $g$ is a field Diophantine definition of $A$. Indeed, suppose equation (2.1.4) holds with all the variables taking values in $R$. Then $b = 1 \neq 0$, and
\[ f(a_1, \ldots, a_k, x_1, \ldots, x_m) = 0. \]

This means, of course, that $(a_1, \ldots, a_k) = (a_1/b, \ldots, a_k/b) \in A$.

Now suppose that $(a_1, \ldots, a_k) \in A$. Then there exists $(x_1, \ldots, x_k) \in R$ such that $g(a_1, \ldots, a_k, 1, x_1, \ldots, x_m) = 0$. Thus the lemma is true.

We will next establish a couple of easy but useful properties of field-Diophantine definitions and sets.

### 2.1.3 Lemma.

Let $R$ be a ring whose fraction field is not algebraically closed. Then the intersections, unions and cartesian products of (field)-Diophantine sets of $R$ are (field)-Diophantine over $R$.

**Proof.**

First we observe that we can obtain a (field-)Diophantine definition of the union by multiplying the (field)-Diophantine definitions of the constituent sets. Secondly, we can consider a cartesian product as an intersection. Indeed, let $A \subseteq R^m$, $B \subseteq R^n$ be two (field-) Diophantine sets. Then
\[ A \times B = \{ (\bar{x}, \bar{y}) \in R^{m+n} : \bar{x} \in A \} \cap \{ (\bar{x}, \bar{y}) \in R^{m+n} : \bar{y} \in B \}, \]
where both sets in the intersection are clearly (field)-Diophantine assuming $A$ and $B$ are. Finally to deal with intersection we can use the same method as in Lemma 1.2.3.
2.1.4 Lemma.

Let $R$ be an integral domain with a quotient field $F$. Let $A \subset F^k$ for some positive integer $k$. Let $m$ be a positive integer less than or equal to $k$. Assume $A$ has a field-Diophantine definition over $R$. Let

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

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

Proof.

Let $f(u_1, \ldots, u_k, u, z_1, \ldots, z_s)$ be a field-Diophantine definition of $A$ over $R$. Then

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

Let $d_H$ be the maximum of the degrees of $H_{m+1}, \ldots, H_k$ and let $D_H$ be a common denominator with respect to $R$ of all the coefficients of $H_{m+1}, \ldots, H_k$. Let

$$\bar{H}_j(u_1, \ldots, u_m, u) = D_H u^{d_H} H_j(u_1/u, \ldots, u_m/u), j = m+1, \ldots, k.$$

Let $d$ be the maximum of the degrees of $P_1, \ldots, P_r$, let $D$ be a common denominator of the coefficients of $P_1, \ldots, P_r$ with respect to $R$, and let

$$\bar{P}_i(u_1, \ldots, u_m, u) = u^d D P_i(u_1/u, \ldots, u_m/u) \in R[u_1, \ldots, u_m, u], i = 1, \ldots, r.$$

Then

$$B = \{ (x_1, \ldots, x_r) \in F^r | \exists u_1, \ldots, u_k, u, z_1, \ldots, z_s \in R, u\bar{H}_j(u_1, \ldots, u_m, u) = D_H u^{d_H} u_j, j = m+1, \ldots, k, u^d D x_i = \bar{P}_i(u_1, \ldots, u_m, u), i = 1, \ldots, r, f(u_1, \ldots, u_k, u, z_1, \ldots, z_s) = 0 \} = \{ (x_1, \ldots, x_r) \in F^r | \exists U, U_1, \ldots, U_r, u_1, \ldots, u_k, u, z_1, \ldots, z_s \in R, U x_i = U_i, U = D u^d, U_i = \bar{P}_i(u_1, \ldots, u_m, u), i = 1, \ldots, r, \bar{H}_j(u_1, \ldots, u_m, u) = D_H u^{d_H-1} u_j, j = m+1, \ldots, k, \}.$$
Given a ring $R$, we can now consider constructing polynomial definitions over $R$ for any subset of the quotient field of $R$. It will turn out that it is also useful to be able to do this not just for the subsets of the quotient field but also for the subsets of finite extensions of the quotient field. To accomplish this goal we extend the notion of Diophantine definition further. The new extended notion is called \textit{Diophantine Generation} and it will allow us to form Diophantine classes.

\subsection*{2.1.5 Definition.}

Let $R_1, R_2$ be two rings with quotient fields $F_1$ and $F_2$ respectively. Assume neither $F_1$ nor $F_2$ is algebraically closed. Let $F$ be a finite extension of $F_1$ such that $F_2 \subset F$. Further, assume that for some basis $\{\omega_1, \ldots, \omega_k\}$ of $F$ over $F_1$ there exists a polynomial $f(a_1, \ldots, a_k, b, x_1, \ldots, x_m)$ with coefficients in $R_1$ such that
\begin{equation}
  f(a_1, \ldots, a_k, b, x_1, \ldots, x_m) = 0 \Rightarrow b \neq 0,
\end{equation}
and
\begin{equation}
  R_2 = \{ \sum_{i=1}^{k} t_i \omega_i | \exists a_1, \ldots, a_k, b, x_1, \ldots, x_m \in R_1, \\
  bt_1 = a_1, \ldots, bt_k = a_k, \\
  f(a_1, \ldots, a_k, b, x_1, \ldots, x_m) = 0 \}.
\end{equation}

Then we will say that $R_2$ is \textit{Dioph-generated over} $R_1$ and denote this fact by
\[ R_2 \leq_{Dioph} R_1. \]

We will also call $f(a_1, \ldots, a_k, b, x_1, \ldots, x_m)$ a \textit{defining polynomial} of $R_2$ over $R_1$, we will call $\Omega = \{\omega_1, \ldots, \omega_k\}$ a \textit{Diophantine basis} of $R_2$ over $R_1$ and we will call $F$ the \textit{defining field} for the basis $\Omega$.

Our next project is to answer some natural questions about Diophantine generation.

1. Is the notion of Diophantine generation a proper extension of the notion of Diophantine and field-Diophantine definitions? In other words we want to answer the following question. Suppose $R_1 \subset F_2$. Then is saying that $R_1 \leq_{Dioph} R_2$ equivalent to saying that $R_1$ is field-Diophantine over $R_2$? (Answer: Yes.)
2. Is Diophantine generation dependent on a particular Diophantine basis? (In other words, what happens if we change the basis of the field $F$ over $F_1$? Will the relationship be preserved?) (Answer: Diophantine generation is not dependent on any specific basis of $F$ over $F_1$. If one basis of $F$ over $F_1$ is a Diophantine basis of $R_2$ over $R_1$, then any basis of $F$ over $F_1$ is a Diophantine basis of $R_2$ over $R_1$.)

3. Is the defining field unique? Can we use a bigger field? Can we use a smaller field? (Defining fields are not unique. Any field containing $F_1F_2$ can be a defining field.)

4. Is this relationship transitive? (In other words, is the use of the symbol "$\leq_{Dioph}$" justified?) (Yes, the relationship is transitive.)

In the following sequence of lemmas we will tackle the questions of the basis and the field first. We start with an easy lemma which follows directly from the definition of Dioph-generation.

### 2.1.6 Lemma.

Let $R_1, R_2$ be integral domains with quotient fields $F_1$ and $F_2$ respectively. Let $F$ be a finite extension of $F_1$ such that $F_2 \subset F$. Then, if there exists a basis $\Omega = \{\omega_1, \ldots, \omega_k\}$ of $F$ over $F_1$ and a set $A_\Omega \subset F_1^k$ with a field-Diophantine definition over $R_1$ such that

$$R_2 = \{ \sum_{i=1}^{k} z_i \omega_i | (z_1, \ldots, z_k) \in A_\Omega \},$$

we can conclude that $R_2 \leq_{Dioph} R_1$. Conversely, if $F$ and $\Omega$ are a defining field and a corresponding Diophantine basis of $R_2$ over $R_1$ respectively, then $R_2$ has a representation of the form (2.1.8), where $A_\Omega \subset F_1^k$ is field-Diophantine over $R_1$.

### 2.1.7 Notation.

$A_\Omega$ will be called a defining set for the basis $\Omega$.

The next lemma will tell us that if $R_2 \leq_{Dioph} R_1$, then we can always use $F_1F_2$ as a defining field and any basis of $F_1F_2$ over $F_1$ as a Diophantine basis.
2.1.8 Lemma.

Let $R_1, R_2$ be integral domains with quotient fields $F_1, F_2$ respectively. Assume $R_2 \leq_{\text{Dioph}} R_1$. (Here we should remind the reader that $R_2 \leq_{\text{Dioph}} R_1$ implies that $F_1 F_2$ is of finite degree over $F_1$ and $F_1$ is not algebraically closed.) Let $\Omega = \{\omega_1, \ldots, \omega_k\}$ be a Diophantine basis of $R_2$ over $R_1$ with $F_\Omega$ being the corresponding defining field. Let $\Lambda = \{\lambda_1, \ldots, \lambda_m\}$ with $m \leq k$ be a basis of a field $F_\Lambda$ over $F_1$, with $F_\Lambda \subseteq F_\Omega$. Then the ring $R_\Lambda = R_2 \cap F_\Lambda \leq_{\text{Dioph}} R_1$ and $\Lambda$ is a Diophantine basis of $R_\Lambda$ over $R_1$.

Proof.

Since $F_\Lambda \subseteq F_\Omega$, for $i = 1, \ldots, m$,

$$\lambda_i = \sum_{j=1}^{k} c_{i,j} \omega_j,$$

where for all $i,j$, we have that $c_{i,j} \in F_1$. Further, we can reorder $\Omega$ if necessary so that the matrix $(c_{i,j})$, $i,j = 1, \ldots, m$ is non-singular. Next note the following.

$$R_\Lambda = \{ \sum_{i=1}^{m} z_i \lambda_i | z_i \in F_1 \text{ and } \exists (t_1, \ldots, t_k) \in A_\Omega, \sum_{i=1}^{m} z_i \lambda_i = \sum_{j=1}^{k} t_j \omega_j \},$$

where $A_\Omega$, the defining set for the basis $\Omega$, is field-Diophantine over $R_1$. Given our ordering of $\Omega$, by Lemma 2.1.4, the equality $\sum_{i=1}^{m} z_i \lambda_i = \sum_{j=1}^{k} t_j \omega_j$ is equivalent to the system,

$$z_i = P_i(t_1, \ldots, t_m), i = 1, \ldots, m,$$

$$t_{m+j} = T_j(t_1, \ldots, t_m), j = 1, \ldots, k - m,$$

where for each $i$ and each $j$ we have that $P_i$ and $T_j$ are fixed polynomials over $F_1$ depending on the choice and ordering of $\Omega$ and $\Lambda$ only. Thus,

$$R_\Lambda = \{ \sum_{i=1}^{m} z_i \lambda_i | (t_1, \ldots, t_m, T_1(t_1, \ldots, t_m), \ldots, T_{k-m}(t_1, \ldots, t_m)) \in A_\Omega \}.$$

Therefore, by Lemma 2.1.4

$$R_\Lambda = \{ \sum_{i=1}^{m} z_i \lambda_i | (z_1, \ldots, z_m) \in A_\Lambda \},$$

where $A_\Lambda$ is field-Diophantine over $R_1$. Hence, $R_\Lambda \leq_{\text{Dioph}} R_1$ by Lemma 2.1.6.

We are now able to prove that defining fields have the desired property.
2.1.9 Corollary.

Let $R_1, R_2$ be integral domains with fraction fields $F_1, F_2$ respectively. Assume that $R_2 \leq \text{Dioph} R_1$. Then we can choose $F_1 F_2$ as a defining field and any basis of $F_1 F_2$ over $F_1$ as a Diophantine basis of $R_2$ over $R_1$.

Proof.

Let $F$ be a defining field from the definition of Diophantine generation. Then as $F_1 F_2 \subseteq F$, from Lemma 2.1.8 it follows that $R_2 \cap F_1 F_2 = R_2 \leq \text{Dioph} R_1$ with $F_1 F_2$ being a defining field and any basis of $F_1 F_2$ a defining basis of $R_2$ over $R_1$.

Lemma 2.1.8 has another consequence answering one of the questions posed above.

2.1.10 Corollary.

Let $R_1, R_2$ be integral domains with the quotient fields $F_1$ and $F_2$ respectively. Assume $F_2 \subseteq F_1$ and $R_2 \leq \text{Dioph} R_1$. Then $R_2$ has a field-Diophantine definition over $R_1$.

Proof.

By Corollary 2.1.9 we can select $F_1 F_2 = F_1$ as our defining field and let the basis of $F_1$ over $F_1$ consist of $\{1\}$. By Lemma 2.1.6 we have that $R_2$ satisfies the equation in (2.1.8) with $k = 1$ and $\omega_1 = 1$. Thus, we have

$$R_2 = \{z_1 \cdot 1 | z_1 \in A_\Omega\},$$

where $A_\Omega$ has a field-Diophantine definition over $R_1$. Thus, $R_2 = A_\Omega$, and $R_2$ has a field-Diophantine definition over $R_1$.

The next lemma will demonstrate that we can always make a defining field larger. This fact will be important for the proof of transitivity of Dioph generation.

2.1.11 Lemma.

Let $R_1, R_2$ be integral domains with quotient fields $F_1$ and $F_2$ respectively. Assume that $R_2 \leq \text{Dioph} R_1$. Let $F$ be any finite extension of $F_1$ containing $F_1 F_2$, and let $\Gamma = \{\gamma_1, \ldots, \gamma_m\}$ be any basis of $F$ over $F_1$. Then $F$ is a defining field and $\Gamma$ is a Diophantine basis of $R_2$ over $R_1$. 

16
Proof.

By Lemma 2.1.8, we know that $F_1 F_2$ is a defining field and any basis $\Omega = \{\omega_1, \ldots, \omega_k\}, k \leq m$ of $F_1 F_2$ over $F_1$ is a Diophantine basis of $R_2$ over $R_1$. Thus, for some polynomial $f(u_1, \ldots, u_k, u, x_1, \ldots, x_r)$ over $R_1$,

$$R_2 = \{ \sum_{i=1}^k t_i \omega_i | \exists u, u_1, \ldots, u_k, x_1, \ldots, x_r,$$

$$ut_1 = u_1, \ldots, ut_k = u_k, f(u_1, \ldots, u_k, u, x_1, \ldots, x_r) = 0 \}$$

and $f(u_1, \ldots, u_k, u, x_1, \ldots, x_r) = 0 \Rightarrow u \neq 0$. Since $F_1 F_2 \subset F$, for $i = 1, \ldots, k$,

$$\omega_i = \sum_{j=1}^m y_{i,j} w \gamma_j,$$

where for all $i, j$, we have that $y_{i,j}, w \in R_1$ and $w \neq 0$. Thus,

$$R_2 = \{ \sum_{i=1}^k \sum_{j=1}^m y_{i,j} \gamma_j t_i | \exists u, u_1, \ldots, u_k, x_1, \ldots, x_r,$$

$$ut_1 = u_1, \ldots, ut_k = u_k, f(u_1, \ldots, u_k, u, x_1, \ldots, x_r) = 0 \}.$$

Let

$$T_j = \sum_{i=1}^k y_{i,j} w t_i.$$

Then

$$wuT_j = \sum_{i=1}^k y_{i,j} u_i \in R_1.$$

Let $U_j = \sum_{i=1}^k y_{i,j} u_i$, and let $U = wu$. Then

$$R_2 = \{ \sum_{j=1}^m T_j \gamma_j |$$

$$\exists U_1, \ldots, U_m, U, u_1, \ldots, u_k, u, x_1, \ldots, x_r \in R_1,$$

$$UT_1 = U_1, \ldots, UT_m = U_m, U = wu.$$
\[ U_j = \sum_{i=1}^{k} y_{ij} u_i, j = 1, \ldots, m, f(u_1, \ldots, u_k, u, x_1, \ldots, x_r) = 0 \}. \]

Note that \( f(u_1, \ldots, u_k, u, x_1, \ldots, x_r) = 0 \) guarantees that \( U \neq 0 \).

The next lemma will consider interaction between Diophantine and field-Diophantine definitions.

### 2.1.12 Lemma.

Let \( R \) be an integral domain with a fraction field \( F \) not algebraically closed. Let \( m, n \in \mathbb{Z}_{>0} \). Let \( A, B \subset F^n, C \subset F^m \), where \( B, C \) are field-Diophantine over \( R \). Suppose for some \( f(\bar{X}, \bar{V}) \in R[\bar{X}, \bar{V}] \), where \( \bar{X} = (X_1, \ldots, X_n) \) and \( \bar{V} = (V_1, \ldots, V_m) \), we have that \( A = \{(a_1, \ldots, a_n) \in B | \exists c_1, \ldots, c_m \in C : f(\bar{a}, \bar{c}) = 0 \} \). Then \( A \) is field Diophantine over \( R \).

**Proof.**

Let \( f_B(\bar{X}, Y, Z) \in R[\bar{X}, Y, Z] \), where \( \bar{X} = (X_1, \ldots, X_n), \bar{Z} = (Z_1, \ldots, Z_r) \), be a field Diophantine definition of \( B \) over \( R \). Let \( f_C(\bar{U}, W, \bar{V}) \in R[\bar{U}, W, \bar{V}] \), where \( \bar{U} = (U_1, \ldots, U_m) \) and \( \bar{V} = (V_1, \ldots, V_l) \), be a field-Diophantine definition of \( C \) over \( R \). Next let

\[ g(\bar{X}, Y, \bar{U}, W) = (YW)^{\deg(f)} f(X_1/Y, \ldots, X_n/Y, U_1/W, \ldots, U_m/W). \]

Let \( D \subset F^n \) be such that

\[ D = \{ \bar{a} \in F^n : \exists \bar{x} \in R^n, \bar{v} \in R^l, w, y \in R, z \in R^r, \bar{u} \in R^m : y \bar{a} = \bar{x} \land g(\bar{x}, y, \bar{u}, w) = 0 \land f_B(\bar{y}, \bar{z}) = 0 \land f_C(\bar{u}, w, \bar{v}) = 0 \}. \]

Then \( D = A \). Indeed suppose \( \bar{a} \in D \). Then \( f_B(\bar{x}, y, \bar{z}) = 0 \land f_C(\bar{u}, w, \bar{v}) = 0 \) imply that \( y \neq 0 \) and \( w \neq 0 \). Thus, \( g(\bar{x}, y, \bar{u}, w) = 0 \) implies

\[ f(x_1/y, \ldots, x_n/y, u_1/w, \ldots, u_k/w) = 0. \]

Since \( f_B(\bar{x}, y, \bar{z}) = 0 \land f_C(\bar{u}, w, \bar{v}) = 0 \), we also have that \( \bar{a} = \bar{x}/y \in B, \bar{c} = \bar{u}/w \in C \) and \( f(\bar{a}, \bar{c}) = 0 \). Thus, \( \bar{a} \in A \).

Suppose now \( \bar{a} \in A \). Then for some \( \bar{c} \in C \) we have that \( f(\bar{a}, \bar{c}) = 0 \). Since \( A \subset B \), for some \( \bar{x} \in R^n, y \in R \setminus \{0\}, z \in R^r \) we have that \( y \bar{a} = \bar{x} \) and \( f_B(\bar{x}, y, \bar{z}) = 0 \). Similarly, since \( \bar{c} \in C \), for some \( \bar{u} \in R^m, w \in R \setminus \{0\} \), and \( \bar{v} \in R^l \) we have that \( w \bar{c} = \bar{u} \) and \( f_C(\bar{u}, w, \bar{v}) = 0 \). Finally, since \( f(\bar{a}, \bar{c}) = 0, w \bar{c} = \bar{u}, y \bar{a} = \bar{x}, y \neq 0, w \neq 0 \), we have that \( g(\bar{x}, y, \bar{u}, w) = 0 \). Thus, \( \bar{a} \in D \).
Since $D$ is clearly field-Diophantine over $F$, the lemma holds.

Our next step is to introduce a new notation designed to simplify the discussion of transitivity of Dioph-generation.

2.1.13 Notation.

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

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

Using this notational scheme for rings $R_1, R_2$ such that $R_2 \leq_{Dioph} R_1$ with a Diophantine basis $\Omega$ as above, we can now conclude by Lemma 2.1.6 that $R_2^\Omega \subset F^n_1$ is field Diophantine over $R_1$, where $F_1$ is the fraction field of $R_1$.

The following proposition is a generalization of Lemma 2.1.6.

2.1.14 Proposition.

Let $R_1, R_2$ 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 $\Omega = \{\omega_1, \ldots, \omega_k\}$ be a Diophantine basis of $R_2$ over $R_1$. Let $B \subset F^n_2$ have a field-Diophantine definition over $R_2$. Then $B^\Omega$ has a field-Diophantine definition over $R_1$.

Proof.

Let $f(a_1, \ldots, a_n, a, x_1, \ldots, x_r)$ be a field-Diophantine definition of $B$ over $R_2$. Then

$$B^\Omega = \{(c_{1,1}, \ldots, c_{k,n}) \in (R_2^\Omega)^n | \left( \sum_{i=1}^{k} c_{i,1}\omega_i, \ldots, \sum_{i=1}^{k} c_{i,n}\omega_i \right) \in B \} =$$

$$\{(c_{1,1}, \ldots, c_{k,n}) \in (R_2^\Omega)^n | \exists Y, Z_1, \ldots, Z_n, X_1, \ldots, X_r \in R_2$$

$$\sum_{i=1}^{k} c_{i,1}\omega_i = Z_1, \ldots, \sum_{i=1}^{k} c_{i,n}\omega_i = Z_n, \quad f(Z_1, \ldots, Z_n, Y, X_1, \ldots, X_r) = 0 \}.$$  (2.1.9)
(Here we remind the reader that (2.1.9) implies $Y \neq 0$). Using our new notational scheme and remembering that $R_2^\Omega \subset F^k$, we now have

$$B^\Omega = \{(c_{1,1}, \ldots, c_{k,n}) \in (R_2^\Omega)^n \mid \exists \bar{y}, \bar{z}_1, \ldots, \bar{z}_n, \bar{x}_1, \ldots, \bar{x}_r \in R_2^\Omega,$$

$$\sum_{i=1}^k y_i \omega_i \sum_{i=1}^k c_{i,j} \omega_i = \sum_{i=1}^k z_{i,j} \omega_i, j = 1, \ldots, n$$

$$f(\sum_{i=1}^k z_{i,1} \omega_i, \ldots, \sum_{i=1}^k z_{i,n} \omega_i, \sum_{i=1}^k y_i \omega_i, \sum_{i=1}^k x_{i,1} \omega_i, \ldots, \sum_{i=1}^k x_{i,r} \omega_i) = 0\}. \hspace{1cm} (2.1.10)$$

Let $h(U, V, W) = UV - W$. Then using coordinate polynomials with respect to basis $\Omega$ (see Section B.7), we have that

$$B^\Omega = \{(c_{1,1}, \ldots, c_{k,n}) \in (R_2^\Omega)^n \mid \exists \bar{y}, \bar{z}_1, \ldots, \bar{z}_n, \bar{x}_1, \ldots, \bar{x}_r \in R_2^\Omega :$$

$$h_i(\bar{y}, \bar{c}_j, \bar{z}_j) = 0, i = 1, \ldots, k, j = 1, \ldots, n,$$

$$f_i(\bar{z}_1, \ldots, \bar{z}_n, \bar{y}, \bar{x}_1, \ldots, \bar{x}_r) = 0, i = 1, \ldots, n\}$$

Now the lemma follows by Lemmas 2.1.3 and 2.1.12.

We are now ready to prove the main theorem of this section: the transitivity of Dioph-generation.

2.1.15 Theorem.

Let $R_1, R_2, R_3$ be integral domains with quotient fields $F_1, F_2, F_3$ respectively. Assume that $F_1, F_2, F_3$ are all subfields of a field $F$ which is not algebraically closed. Assume also that all the extensions $F/F_i, i = 1, 2, 3$ are finite. Finally, assume $R_2 \leq_{\text{Dioph}} R_1$ and $R_3 \leq_{\text{Dioph}} R_2$. Then $R_3 \leq_{\text{Dioph}} R_1$.

Proof.

From the previous discussion we know that we can select $F$ as a defining field for both pairs: $(R_1, R_2)$ and $(R_2, R_3)$. Let $\Omega = \{\omega_1, \ldots, \omega_k\}$ be a Diophantine basis for $R_2$ over $R_1$ such that $F$ is the corresponding defining field, and likewise let $\Lambda = \{\lambda_1, \ldots, \lambda_n\}$ be a Diophantine basis of $R_3$ over $R_2$ with corresponding defining field $F$. Further, by Lemma 2.1.6 we can write

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

20
where $A$ has a field-Diophantine definition over $R$. By Proposition 2.1.14, $A^{\Omega}_A$ has a field-Diophantine definition over $R$. Thus,

$$R_3 = \left\{ \sum_{i=1}^{n} \sum_{j=1}^{k} y_{i,j} \lambda_j \omega_j \mid (y_{1,1}, \ldots, y_{n,k}) \in A^{\Omega}_A \subseteq F_{1}^{nk} \right\} =$$

$$\left\{ \sum_{s=1}^{k} \sum_{i,j} y_{i,j} A_{i,j,s} \omega_s \mid (y_{1,1}, \ldots, y_{n,k}) \in A^{\Omega}_A \right\},$$

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

$$B_{\Omega} = \{(t_1, \ldots, t_k) \in F_1^k \mid t_s = \sum_{i,j} y_{i,j} A_{i,j,s}, (y_{1,1}, \ldots, y_{n,k}) \in A^{\Omega}_A \}.$$

Then by Lemma 2.1.4, $B_{\Omega}$ has a field-Diophantine definition over $R$. Next we note that

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

Finally we conclude that $R_3 \leq_{\text{Dioph}} R_1$ by Lemma 2.1.6.

We will now exploit the transitivity of Dioph-generation to obtain more general properties of this relation. We will start with a very common application of transitivity of Diophantine generation.

2.1.16 Going all the way down.
Suppose $R_3 \subset R_2 \subset R_1$ are integral domains whose fraction fields are not algebraically closed. Assume further that $R_2 \leq \text{Dioph} R_1$ and $R_3 \leq \text{Dioph} R_2$. Then $R_3 \leq \text{Dioph} R_1$.

2.1.17 Going up and then down.

Let $R_2 \subseteq R_1$ be integral domains with quotient fields $F_1, F_2$ respectively. Assume that $F_1/F_2$ is a finite extension and $F_1$ is not algebraically closed. Assume further that $R_1 \leq \text{Dioph} R_2$. Then for any $A \subset R_1$ Diophantine over $R_1$, $A \cap R_2$ is Diophantine over $R_2$.

Proof.

Let $f(t, \overline{y}) = f(t, y_1, \ldots, y_l)$ be a Diophantine definition of $A$ over $R_1$ and let $\Omega = \{\omega_1, \ldots, \omega_n\}$ be a Diophantine basis of $R_1$ over $R_2$ with

$$P(Z_1, \ldots, Z_n, B, X_1, \ldots, X_m) = P(\bar{Z}, B, \bar{X})$$

being the corresponding defining polynomial. Then $t \in A \cap R_2$ if and only if $t \in R_2$ and

$$\exists y_1, \ldots, y_l \in R_1, f(t, y_1, \ldots, y_l) = 0. \quad (2.1.11)$$

On the other hand, $(2.1.11)$ is true if and only if

$$\left\{ \begin{array}{l}
\exists \bar{a}_1, \ldots, \bar{a}_l \in R_2^n, b_1, \ldots, b_l \in R_2, \\
\exists \bar{x}_1, \ldots, \bar{x}_m \in R_2^n, \\
P(\bar{a}_1, b_1, \bar{x}_1) = 0, \\
\vdots \\
P(\bar{a}_l, b_l, \bar{x}_l) = 0, \\
f(t, \sum_{j=1}^n \frac{a_{i,j}}{b_i} \omega_j, \ldots, \sum_{j=1}^n \frac{a_{i,j}}{b_i} \omega_j) = 0, \end{array} \right. \quad (2.1.12)$$

where $\bar{a}_i = (a_{i,1}, \ldots, a_{i,n}), \bar{x}_i = (x_{i,1}, \ldots, x_{i,m})$.

Now, let $f_i^\Omega(u, \bar{v}_1, \ldots, \bar{v}_l), i = 1, \ldots, n$, where $\bar{v}_j = (v_{j,1}, \ldots, v_{j,n})$, be the coordinate polynomials of $f(t, \overline{y})$ with respect to basis $\Omega$ and variables
\( y_1, \ldots, y_l \). (We remind the reader again to see Section B.7 for a discussion of coordinate polynomials.) Then we can rewrite the system above as

\[
\exists \bar{a}_1, \ldots, \bar{a}_l \in \mathbb{R}^n, b_1, \ldots, b_l \in \mathbb{R}^2,
\exists \bar{x}_1, \ldots, \bar{x}_m \in \mathbb{R}^n,
P(\bar{a}_1, b_1, \bar{x}_1) = 0,
\vdots
P(\bar{a}_l, b_l, \bar{x}_l) = 0,
f^\Omega_1(t, \bar{a}_1/b_1, \ldots, \bar{a}_l/b_l) = 0,
\vdots
f^\Omega_n(t, \bar{a}_1/b_1, \ldots, \bar{a}_l/b_l) = 0,
\]

(2.1.13)

where \( \bar{a}_j/b_j = (a_{j,1}/b_j, \ldots, a_{j,n}/b_j) \). The final step is to note that since “\( P \)”-equations guarantee that \( b_1, \ldots, b_l \) are not zero, we can multiply “\( f \)” equations by \( \prod_{j=1}^l b_{\deg(f)} \) without changing the solution set of the system. The last step will produce a system of polynomial equations over \( \mathbb{R}^2 \) which will be the Diophantine definition of \( A \cap \mathbb{R}^2 \).

Using transitivity again can also produce a "Going down and then up" method.

### 2.1.18 Going down and then up.

Let \( R_1 \subset R_2 \subset R_3 \) be integral domains with quotient fields \( F_1, F_2 \) and \( F_3 \) respectively. Assume that \( F_3 \) is not algebraically closed and \( F_3/F_1 \) is a finite extension. Suppose also that \( R_1 \leq_{\text{Dioph}} R_3 \) and \( R_2 \leq_{\text{Dioph}} R_1 \). Then \( R_2 \leq_{\text{Dioph}} R_3 \).

The next property is a restatement of Lemma 2.1.3 using new terminology.

### 2.1.19 The Finite Intersection Property.

Let \( R_i \subset R, i = 1, \ldots, m \) be rings such that the quotient field of \( R \) is not algebraically closed and for all \( i = 1, \ldots, m \) we have that \( R_i \leq_{\text{Dioph}} R \). Then \( \bigcap_{i=1}^m R_i \leq_{\text{Dioph}} R \).
Proof.

Since $R_i \subset R$ and $R_i \leq_{Dioph} R$, we can conclude that $R_i$ has a Diophantine
definition $f_i(t, x_1, \ldots, x_{n_i})$ over $R$. Then for all $x \in R$ we have that there exist$x_{1,1}, \ldots, x_{m,n_m} \in R$ with $f_i(x, x_{i,1}, \ldots, x_{i,n_i}) = 0, i = 1, \ldots, m$ if and only if$x \in \bigcap_{i=1}^m R_i$.

2.2 Diophantine Generation of Integral Closure
and Dioph-regularity.

In this section we would like to discuss two important properties of Diophantine
 generation over integrally closed subrings of global fields: Dioph-generation of
 integral closure and fraction field of a ring. We will start with integral closure
 for rings of $\mathcal{O}$-integers. The description of these rings can be found in Section
 B.1 of the Number Theory Appendix.

2.2.1 Proposition.

Let $K$ be a global field, let $R$ be a ring with quotient field $K$, let $G$
 be a
 finite extension of $K$ and let $R_G$ be the integral closure of $R$ in $G$. Then
$R_G \leq_{Dioph} R$.

Proof.

Let $n = [G : K]$, and let $\Omega = \{\omega_1, \ldots, \omega_n\} \subset O_K$ be a basis of $G$ over $K$.
Then by Lemma B.4.12, every element of $R_G$ can be written as $\sum_{i=1}^n a_i \omega_i$,
where $a_i \in R$ and $D$ is the discriminant of the basis – a fixed (non-zero)
constant of $R$. Hence $R_G \leq_{Dioph} R$.

We will now discuss the following question. When can the quotient field of
an integral domain be Dioph-generated over an integral domain? The answer
to this question is contained in the following lemma.

2.2.2 Lemma.

Let $R$ be an integral domain and let $F$ be its quotient field. Then $F \leq_{Dioph} R$
if and only if the set of non-zero elements of $R$ has a Diophantine definition
over $R$. 

24
Proof.

First assume that the set of non-zero elements of $R$ has a Diophantine definition over $R$. Let $f(y, x_1, \ldots, x_n)$ be a Diophantine definition of the set of non-zero elements of $R$. Then clearly

$$F = \{t \mid \exists b, a, x_1, \ldots, x_n \in R, bt = a, f(b, x_1, \ldots, x_n) = 0\}.$$  

Conversely, suppose that $F \leq_{\text{Dioph}} R$ and let $g(z, y, x_1, \ldots, x_n)$ be a defining polynomial, i.e.

$$F = \{w \mid \exists y, z, x_1, \ldots, x_n : yw = z \land g(z, y, x_1, \ldots, x_n) = 0\}.$$  

Then $g(1, y, x_1, \ldots, x_n)$ will be a Diophantine definition of the set of the non-zero elements of $R$.

We now give the property discussed above a name.

2.2.3 Definition.

Let $R$ be an integral domain such that the set of its non-zero elements has a Diophantine definition over the ring. Then $R$ will be called $\text{Dioph-regular}$.

Our next task is to show that all the rings we will consider in this book are Dioph-regular. The proof below is a generalization of the proof by Denef for rings of algebraic integers from [18].

2.2.4 Proposition.

Let $K$ be a global field, and let $\mathcal{W}$ be any collection of non-archimedean primes of $K$. Then $O_{K,\mathcal{W}}$ is Dioph-regular.

Proof.

First, assume that the complement of $\mathcal{W}$ contains at least two primes $p_1$ and $p_2$. Let $a_i \equiv 0 \mod p_i, a_i \in O_K$ for $i = 1, 2$ and $(a_1, a_2) = 1$. Such $a_1, a_2 \in O_K$ exist by the Strong Approximation Theorem (Theorem B.2.1). Let $x \in O_{K, \mathcal{W}}$.

Then $x \neq 0$ if and only if the following equation has solutions in $O_{K, \mathcal{W}}$:

$$xw = (u_1a_1 - 1)(u_2a_2 - 1).$$

Indeed, suppose that $x = 0$, then either $a_1$ or $a_2$ is invertible in $O_{K, \mathcal{W}}$. This is not true by the choice of $p_1$ or $p_2$. Suppose now $x \neq 0$. Then let $\frac{x}{a_1a_2}$ be the
divisor of $x$, where $\mathfrak{A}_1, \mathfrak{A}_2, \mathfrak{B}$ are integral divisors, $\mathfrak{A}_i$ and the divisor of $a_i$ are relatively prime. (See Definition B.1.23 for the definition of the divisor of an element.) By the Strong Approximation Theorem, there exists $u_i \in O_K$ such that $u_i \equiv a_i^{-1} \mod \mathfrak{A}_i$. Thus, the divisor of $(u_1a_1 - 1)(u_2a_2 - 1)$ is of the form $\mathfrak{A}_1\mathfrak{A}_2\mathfrak{C}$, where $\mathfrak{C}$ is an integral divisor. Hence, the divisor of $w$ is of the form $\mathfrak{B}\mathfrak{C}$ and consequently, $w \in O_K \subset O_{K,W}$.

We now remove the assumption that the complement of $\mathcal{W}$ has at least two primes. First of all, if $\mathcal{W}$ contains all the primes, then $O_{K,W} = K$ and the proposition is trivially true. Secondly, if the complement of $\mathcal{W}$ contains only one prime $p$, then let $M$ be a finite extension of $K$ where $p$ splits into distinct factors. (Such an extension exists by Lemma B.4.14.) Let $O_{M,\mathcal{W}_M}$ be the integral closure of $O_{K,W}$ in $M$. By Proposition B.1.22, we have that $O_{M,\mathcal{W}_M}$ is a ring of $\mathcal{W}_M$-integers and $\mathcal{W}_M$ contains at least two primes of $M$. By the argument above, the set of non-zero elements of $O_{M,\mathcal{W}_M}$ has a Diophantine definition over $O_{M,\mathcal{W}_M}$. At the same time by Lemma 2.2.2, it is the case that $O_{M,\mathcal{W}_M} \leq_{Dioph} O_{K,W}$. Thus we can use the “Going Up and Then Down Method” (see Subsection 2.1.17) to complete the proof.

2.2.5 Note.

The importance of Dioph-regularity is obvious. If a ring $R$ is Dioph-regular, then any set which can be Dioph-generated over its quotient field, can be Dioph-generated over the ring by the transitivity of Dioph-generation.

2.3 Big Picture: Diophantine Family of a Ring.

The properties of Diophantine generation discussed in the preceding sections allow us to define an equivalence relationship based on Diophantine generation.

2.3.1 Definition.

Let $R_1, R_2$ be rings with quotient fields $F_1$ and $F_2$ respectively. Assume that $F_1F_2$ is well-defined, not algebraically closed, and $F_1F_2/F_1$ and $F_1F_2/F_2$ are finite extensions. Then call $R_1$ and $R_2$ Dioph-equivalent if $R_1 \leq_{Dioph} R_2$ and $R_2 \leq_{Dioph} R_1$. We will denote this relation by $R_2 \equiv_{Dioph} R_1$.

Clearly, $\equiv_{Dioph}$ is an equivalence relation. We will call the resulting equivalence classes the Diophantine classes. It is also clear that $\leq_{Dioph}$ is a relation on Diophantine classes. Given an integrally closed ring $R$, we will consider all
the integrally closed rings whose quotient fields are either finite extensions or finite subextensions of the quotient field of $R$. Call the set of all these rings a Diophantine family of $R$. We can now rephrase some of the main problems discussed in this book:

1. What is the structure of the Diophantine family of $\mathbb{Z}$? In other words, given an integrally closed ring $R$ contained in a number field we want to know whether $R \leq_{\text{Dioph}} \mathbb{Z}$ and whether $\mathbb{Z} \leq_{\text{Dioph}} R$.

2. Let $\mathbb{F}_p$ be a finite field and let $t$ be transcendental over $\mathbb{F}_p$. Then what is the structure of the Diophantine family of $\mathbb{F}_p[t]$? As above we can rephrase the questions as follows. Let $K$ be a finite extension of $\mathbb{F}_p[t]$ and let $R$ be an integrally closed ring whose quotient field is $K$. Then when is $R \leq_{\text{Dioph}} \mathbb{F}_p[t]$ and when is $\mathbb{F}_p[t] \leq_{\text{Dioph}} R$?

These questions are clearly comprised of many problems of varying difficulty. Our next task is to classify them and determine which problems can be dealt with quickly. We also remind the reader that any integrally closed subring of a global field is a ring of $\mathcal{W}$-integers by Proposition B.1.27. So our intention is to study the Diophantine classes of $\mathcal{W}$-integers.

### 2.3.2 Horizontal and Vertical Problems for Diophantine family of $\mathbb{Z}$.

We will start with Figure 2.1, where $\mathcal{S}$ is a finite set of rational primes, $\mathcal{V}$ is a set of rational primes whose complement is finite, and $\mathcal{W}$ is an infinite set of primes whose complement is also infinite. Further, $K$ is a number field, $\mathcal{S}_K$, $\mathcal{V}_K$, $\mathcal{W}_K$ are the sets of $K$-primes lying above $\mathcal{S}$, $\mathcal{V}$, and $\mathcal{W}$ respectively. The arrows represent the direction of Dioph-generation. More precisely if we have $R_1 \rightarrow R_2$ in Figure 2.1, then $R_2 \leq_{\text{Dioph}} R_1$. The arrows are attached to the pairs of rings where we know the answer at least in some cases. We divide the problems into the two main groups: horizontal and vertical. Horizontal problems concern two rings with the same quotient field. Vertical problems concern pairs of rings whose quotient fields are different: one is a proper subfield of another. Using results from Section 2.2 we can solve one horizontal problem and a family of vertical problems. The Dioph-regularity of $\mathbb{Z}$ tells us that $\mathbb{Q} \leq_{\text{Dioph}} \mathbb{Z}$. Further, since we know that integral closures of the rings of $\mathcal{W}$-integers in the extensions are Dioph-generated, we can solve all the upward going vertical problems.

We can also determine when $O_{\mathbb{Q},\mathcal{W}} \leq_{\text{Dioph}} \mathbb{Z}$ for any set of rational primes $\mathcal{W}$. The answer is a direct consequence of Matiyasevich’s result and will be discussed in detail in the following chapter.
Figure 2.1: Horizontal and Vertical Problems for the Diophantine Family of $\mathbb{Z}$.
We know how to solve the downward vertical problem for some subrings of totally real fields, their extensions of degree 2, fields with exactly one pair of non-real embeddings and some other number fields. These problems will be discussed in Chapter 7. In all the number fields we can solve the “short” horizontal problem in any subring (i.e. define integrality at finitely many primes). We will discuss this problem in Chapter 4. In some subrings of totally real fields and their totally complex extensions of degree 2 we solve “longer” horizontal problems, i.e. define integrality at infinitely many primes. The partial solution of this problem will be discussed in Chapter 7.

2.3.3 Horizontal and Vertical Problems for Diophantine Family of $\mathbb{F}_p[t]$.

We will now consider the problems associated with the Diophantine family of a polynomial ring over a finite field of constants. Consider Figure 2.2. Here we use notations analogous to the ones we used in Figure 2.1. We also assume that $\mathcal{S}, \mathcal{W}, \mathcal{V}$ contain the valuation which is the pole of $t$. Further, $K$ as before is a finite extension of the ground field: $\mathbb{F}_p(t)$, and $O_K, O_K, \mathcal{S}_K, O_K, \mathcal{W}_K, O_K, \mathcal{V}_K$ are again integral closures of subrings of the ground field, in this case $\mathbb{F}_p[t], O_{\mathbb{F}_p(t)}, \mathcal{S}_{\mathbb{F}_p(t)}, O_{\mathbb{F}_p(t)}, \mathcal{W}_{\mathbb{F}_p(t)}, \mathcal{V}_{\mathbb{F}_p(t)}$ respectively in $K$. For the same reason as in the case of number fields, upward vertical problem follows from the fact that integral closure is Dioph-generated for the rings under consideration. “Short” horizontal problem for function fields (i.e. definability of integrality at finitely many primes) will be discussed in Chapter 4. The downward vertical problem for function fields, which has been solved to some extent for all global function fields, will be discussed in Chapter 10. Finally, the “long” horizontal problem (i.e. definability of integrality at infinitely many primes) for function fields has also been partially solved for all function fields and is also described in Chapter 10.
Figure 2.2: Horizontal and Vertical Problems for the Diophantine Family of $\mathbb{F}_p[t]$. 

\[ K \rightarrow O_{K,\mathfrak{r}_K} \rightarrow O_{K,\mathfrak{r}_K} \rightarrow O_{K,\mathfrak{r}_K} \rightarrow O_K \]

\[ \mathbb{F}_p(t) \rightarrow O_{\mathbb{F}_p(t),\mathfrak{r}_K} \rightarrow O_{\mathbb{F}_p(t),\mathfrak{r}_K} \rightarrow O_{\mathbb{F}_p(t),\mathfrak{r}_K} \rightarrow \mathbb{F}_p[t] \]
Chapter 3

Diophantine Equivalence and Diophantine Decidability.

In this chapter we will take a closer look at what Diophantine generation and Diophantine equivalence tell us about Diophantine decidability and definability over countable rings. We have already touched on these questions in our introduction. There we talked about the relationship between Diophantine definitions and Diophantine undecidability. To make this discussion more precise over rings other than the ring of rational integers, we will need to determine what the analog of a recursive function (or more informally, an algorithm) is over these rings. To formalize the notion of an algorithm over countable structures, one uses presentations. If it exists, a presentation of a given field $F$ is a homomorphism from $F$ into a field whose elements are natural numbers. Under this homomorphism all the field operations of $F$ are interpreted by restrictions of recursive functions and the image of $F$ is a recursive set. (Here we remind the reader that Appendix A contains definitions of recursive functions, recursive sets, as well as a list of references.) Not all fields and rings have such presentations. A field or ring which has such a presentation is called recursive. However, as we will see below, this notion of a presentation, is too “strong” for our purposes. The presentations which are more suitable for a discussion of Diophantine questions are called “weak presentations”. We describe these presentations in the following section. Finally, we note that most of this chapter is based on [99].

3.1 Weak Presentations.

We start with a couple of definitions.
3.1.1 Definition.

Let $R$ be a countable ring such that there exists an injective map $j : R \rightarrow \mathbb{N}$ with the following properties. There exist recursive functions $P_+, P_-, P_x : \mathbb{N}^2 \rightarrow \mathbb{N}$ such that for all $x, y \in F$, we have that

$$P_+(j(x), j(y)) = j(x + y),$$
$$P_-(j(x), j(y)) = j(x - y),$$
$$P_x(j(x), j(y)) = j(xy).$$

Then $j$ is called a weak presentation of $R$ as a ring.

Next let $F$ be a countable field. Let $j : F \rightarrow \mathbb{N}$ be a weak presentation of $F$ as a ring and assume additionally that there exists a recursive function $P_f : \mathbb{N}^2 \rightarrow \mathbb{N}$ such that for all non-zero $y \in F$ we have that

$$P_f(j(x), j(y)) = j(x/y).$$

Then $j$ is called a weak presentation of $F$ as a field.

3.1.2 Definition.

Let $R \subseteq R'$ be countable rings, let $j : R \rightarrow \mathbb{N}, j' : R' \rightarrow \mathbb{N}$ be weak presentations of $R$ and $R'$ as rings respectively. Then we say that $j'$ is an extension of $j$ if $j'|_R = \psi \circ j$, where $\psi$ is a recursive injective function with a recursive range or in other words the inverse of $\psi$ is also recursive.

Note that not every weak presentation of a ring $R$ is extendible to a weak presentation of its quotient field $F$ as a field. (For example one can construct weak presentations of $\mathbb{Q}$ as a ring which are not weak presentations of $\mathbb{Q}$ as a field. In other words division is not translated by a restriction of a computable function. For more details about such constructions see [101].)

While not all countable fields or integral domains are recursive, they all have weak presentations.

3.1.3 Proposition.

Let $R$ be a countable integral domain. Then $R$ has a weak presentation as a ring and its quotient field has a weak presentation as a field.
Proof.

By Proposition A.7.13 we have that $R \subseteq F \subseteq K$, where $K$ is a computable field. Let $j : K \to \mathbb{N}$ be a computable presentation of $K$. Then $j$ restricted to $R$ and $F$ is a weak presentation of $R$ and $F$ respectively.

### 3.2 Some Properties of Weak Presentations.

To connect the weak presentations to the subject of Diophantine definability and decidability we need to discuss some of the properties of the weak presentations. First we need to introduce additional notation.

#### 3.2.1 Notation.

Let $K$ be a countable field and $j : K \to \mathbb{N}$ be a weak presentation of $K$. Let $f : K^n \to K$ be a function defined on $D \subseteq K^n$. Then $j(f)$ will denote a function from $j(D)$ to $j(K)$ defined by the following. For all $(a_1, \ldots, a_n) \in D$ we have that $j(f)(j(a_1), \ldots, j(a_n)) = j(f(a_1, \ldots, a_n))$.

Next we note an obvious but important corollary of the definition of weak presentations.

#### 3.2.2 Lemma.

Let $R$ be a countable ring and let $j : R \to \mathbb{N}$ be a weak presentation of $R$. Let $P(X_1, \ldots, X_n)$ be a polynomial over $R$. Then $j(P) : j(R) \to j(R)$ is a restriction of a recursive function.

Proof.

A polynomial function is a composition of finitely many binary additions, subtractions and multiplications. Therefore one can proceed by induction on the number $n$ of times addition, subtraction or multiplication is used in the construction of $P$. The argument will require the use of Definition A.1.2 of recursive functions and Lemma A.1.12. The details are left to the reader.

If we are considering a weak presentation of a field, then it is just as easy to see that rational functions are also translated by restrictions of recursive functions.
3.2.3 Corollary.

Let $K$ be a countable field. Let $j : K \to \mathbb{N}$ be a weak presentation of $K$ as a field. Let $W \in K(X_1, \ldots, X_m)$ be a rational function over $K$. Then $j(W)$ is a restriction of recursive function.

**Proof.**

Let $W(X_1, \ldots, X_m) = Q_1(X_1, \ldots, X_m)/Q_2(X_1, \ldots, X_m)$ where $Q_1, Q_2$ are polynomial functions over $K$ without common factors in $K[X_1, \ldots, X_m]$. Clearly for all $X_1, \ldots, X_m \in K$ with $Q(X_1, \ldots, X_m) \neq 0$,

$$j(W)(j(X_1), \ldots, j(X_m)) = P(j(Q_1)(j(X_1), \ldots, j(X_m))), j(Q_2)(j(X_1), \ldots, j(X_m)).$$

Since $j(Q_1), j(Q_2), P_i$ are all restrictions of recursive functions, by definition of recursive functions, so is $j(W)$.

Our next task is to show that weak presentations are extendible under finite algebraic extensions.

3.2.4 Proposition.

Let $F$ be a countable field, let $j : F \to \mathbb{N}$ be a weak presentation of $F$. Let $K$ be a finite extension of $F$ of degree $n$. Let $\Omega = \{\omega_1, \ldots, \omega_n\}$ be a basis of $K$ over $F$. Then there exists a weak presentation $J : K \to \mathbb{N}$ such that $J$ restricted to $F$ is equal to $\psi \circ j$, where $\psi : \mathbb{N} \to \mathbb{N}$ is recursive with recursive inverse, and there exist recursive coordinate functions $C_1, \ldots, C_n : \mathbb{N} \to \mathbb{N}$ such that for any element $x \in K$ we have that

$$x = \sum_{i=1}^{n} J^{-1} \circ C_i \circ J(x) \omega_i, \quad (3.2.1)$$

and

$$C_i \circ J(x) \in J(F) \quad (3.2.2)$$

for all $i = 1, \ldots, n$.

**Proof.**

Let $\omega_1 = 1, \ldots, \omega_n$ be a basis of $K$ over $F$. Let $G_n : \mathbb{N}^n \to \mathbb{N}$ be a recursive function defined in Lemma A.1.14. We will construct $J : K \to \mathbb{N}$ by setting $J(\sum_{i=1}^{n} a_i \omega_i) = G_n(j(a_1), \ldots, j(a_n)) = \prod_{i=1}^{n} p_i^{j(a_i)}$. First we should observe
that for $x \in F$, we have that $J(x) = 2^{l(x)}$, and therefore by Proposition A.1.11 the first requirement of the lemma is satisfied. Secondly, for $m \in \mathbb{Z}_{>0}$ and for $i = 1, \ldots, n$, let $C_i(m) = \text{ord}_p m$, where $p_i$ is the $i$-th prime in the ascending listing of all rational primes. It is clear that $C_i$ satisfies (3.2.1) and (3.2.2), and by Lemma A.1.11, for all $i = 1, \ldots, n$, we know $C_i$ to be computable. Finally, to make $J$ into a weak presentation, we need to show that the images of field operations are extendible to total recursive functions. Let $J(\text{op})$ denote the translations of the field operations under $J$ and let $P_{\text{op}}$ denote, as before, the translation of the field operations under $j$. Then define

$$J(\pm)(m_1, m_2) = \prod_{i=1}^{n} p_i^{p_i(C_i(m_1), C_i(m_2))}.$$  

For multiplication and division the definition is a bit more complicated. For all $i, j = 1, \ldots, k$, let

$$B_{i,j,1}, \ldots, B_{i,j,k} \in F$$

be such that

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

Then for $a_1, \ldots, a_n, b_1, \ldots, b_n \in F$,

$$\sum_{i=1}^{n} a_i \omega_i \sum_{j=1}^{n} b_j \omega_j = \sum_{i,j} a_i b_j \omega_i \omega_j = \sum_{i,j,k} a_i b_j B_{i,j,k} \omega_k = \sum_{k=1}^{n} \sum_{i,j} B_{i,j,k} a_i b_j \omega_k.$$  

Let $H_k(a_1, \ldots, b_n) = \sum_{i,j} B_{i,j,k} a_i b_j$, and note that $H_k(T_1, \ldots, T_{2n})$ depends on the basis $\Omega$ only. Then

$$\sum_{i=1}^{n} a_i \omega_i \sum_{j=1}^{n} b_j \omega_j = \sum_{k=1}^{n} H_k(a_1, \ldots, a_n, b_1, \ldots, b_n) \omega_k.$$  

By Lemma 3.2.2, for all $k = 1, \ldots, n$, we know that $j(H_k)$ is extendible to a recursive function. Thus we can define

$$J(\times)(m_1, m_2) = \prod_{i=1}^{n} p_i^{p_i(H_i(C_i(m_1), \ldots, C_i(m_2), \ldots, C_i(m_2)))}.$$  

Next we move to translation of division. Since we have shown that the $J$-translation of multiplication in $K$ is a restriction of a recursive function, it is enough to show that $J$-translation of finding the multiplicative inverse is a restriction of a recursive function. By Lemma B.10.6, there exist

$$T_1, \ldots, T_n, Q \in F[x_1, \ldots, x_n]$$
depending on $F, G$ and $\Omega$ only such that $\sum_{i=1}^{n} a_i \omega_i \neq 0$ if and only if

$$Q(a_1, \ldots, a_n) \neq 0$$

and

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

Thus, we can define

$$J^{-1}(m) = \prod_{i=1}^{n} p_i^{\mu(\pi_1^i(C_1(m), \ldots C_n(m)), \mu(Q(C_1(m), \ldots C_n(m))))}.$$ 

We are now ready to start establishing connections between diophantine definability and decidability. Our first goal is to show that Diophantine definability assures relative enumerability under any weak presentation.

### 3.2.5 Proposition.

Let $R$ be a countable integral domain. Let $j : R \rightarrow \mathbb{N}$ be a weak presentation of $R$ as ring. Let $A$ be a Diophantine subset of $R^l$. Then $j(A) \leq_e j(R)$.

**Proof.**

First note that if $A$ is finite (and this includes the case of $A = \emptyset$), then $A$ is recursive by Lemma A.1.10 and computably enumerable by Lemma A.2.2. So without loss of generality we can assume that $A$ is infinite. Let

$$\psi : \mathbb{N} \rightarrow j(R)$$

be any function enumerating $j(R)$. Let $P(t_1, \ldots, t_i, x_1, \ldots, x_n)$ be a Diophantine definition of $A$ over $R$. Let

$$F(k, n+1) = (a_1, \ldots, a_{n+1}),$$

where $a_i = \text{ord}_{\rho} k$, be a function defined in Lemma A.1.14. Then by this lemma $F(k, n+1)$ is computable. Let $\pi_i : \mathbb{N}^{n+1} \rightarrow \mathbb{N}$ be projection on the $i$-th coordinate for $1 \leq i \leq n+1$. Our next function definition will use a minimization operator $\mu$ from Definition A.1.1. Now define

$$\tilde{\phi} : \mathbb{N} \rightarrow j(A) \subset j(R^l)$$

in the following fashion. First define a function $\nu : \mathbb{N} \rightarrow \mathbb{N}$ by

$$\nu(0) = (\mu t)[j(P)(\psi(\pi_1(F(t, n+1)))), \ldots, \psi(\pi_{n+1}(F(t, n+1)))) = j(0)].$$
Now define
\[
\bar{\phi}(m) = (\psi(\pi_1(F(n+1, \nu(m)))), \ldots, \psi(\pi_l(F(n+1, \nu(m))))).
\]

We now prove a more general version of Proposition 3.2.5.

3.2.6 Proposition.

Let \( R_1, R_2 \) be two integral domains such that \( R_2 \leq_{\text{Dioph}} R_1 \). Let \( F_1, F_2 \) be the fraction fields of \( R_1 \) and \( R_2 \) respectively, and let \( j : F_1 \to \mathbb{N} \) be a weak presentation of \( F_1 \). Then there exists a weak presentation \( J : F_1 F_2 \to \mathbb{N} \) such that \( J \) is an extension of \( j \) in the sense of Definition 3.1.2 and for any such extension \( J \) we have that \( J(R_2) \leq_{e} J(R_1) \).

Proof.

By Definition of Diophantine generation, there exists \( f(a_1, \ldots, a_k, b, x_1, \ldots, x_m) \) with coefficients in \( R_1 \) such that
\[
f(a_1, \ldots, a_k, b, x_1, \ldots, x_m) = 0 \Rightarrow b \neq 0, \quad (3.2.3)
\]
and
\[
R_2 = \left\{ \sum_{1}^{k} t_i w_i \mid \exists a_1, \ldots, a_k, b, x_1, \ldots, x_m \in R_1, \right. \\
\left. bt_1 = a_1, \ldots, bt_k = a_k, \\
f(a_1, \ldots, a_k, b, x_1, \ldots, x_m) = 0 \right\}.
\]
In other words,

\[ R_2 = \left\{ \sum_{i=1}^{k} \frac{a_i}{b} \omega_i \mid (a_1, \ldots, a_k, b) \in A \subset R_1 \right\}, \]

where \( A \) is a Diophantine subset of \( R_2^{k+1} \). By Proposition 3.2.4 there exists a weak presentation

\[ J : F_1F_2 \rightarrow \mathbb{N} \]

such that \( J \) is an extension of \( j \). By Proposition 3.2.5, \( J(A) \leq_e J(R_1) \). Let

\[ U(X_1, \ldots, X_k, Y) = \sum_{i=1}^{k} \frac{X_i}{Y} \omega_i \]

be a rational function over \( F_1F_2 \). Then \( J(U) \) is a restriction of a recursive function by Corollary 3.2.3. Now we can proceed in the manner analogous to Proposition 3.2.5. Let \( \bar{\phi} : \mathbb{N} \rightarrow \bar{J}(A) \) be any enumeration of \( \bar{J}(A) \). Then define

\[ \xi(m) = J(U)(\pi_1(\bar{\phi}(m)), \ldots, \pi_{k+1}(\bar{\phi}(m))). \]

Since \( \xi(m) \) is a recursive function enumerating \( R_2 \), we conclude that \( J(R_2) \leq_e \bar{J}(A) \) and therefore by transitivity of relative enumerability (see a remark following Definition A.3.2), \( J(R_2) \leq_e J(R_1) \).

### 3.2.7 Remark.

Proposition A.6.5 shows that any two recursive presentations of a finitely generated ring or field are related by a recursive function, i.e. one presentation is a composition of the other and a recursive function. This also shows that Turing degree and enumeration degree structures of the finitely generated rings and fields are invariant with respect to recursive presentations. Actually, the proof of the proposition shows a bit more. It shows that weak presentations preserve the enumeration degree structure for a finitely generated ring or field. (Weak presentations do not necessarily preserve the Turing degree structure of finitely generated objects. See for example [40].) Thus, under any weak presentation the class of r.e. sets is the same class of subsets for a finitely generated ring or field. Therefore Matiyasevich’s Theorem 1.2.2 holds independently of the weak presentation one could choose for \( \mathbb{Z} \).

Before we leave this section, we note that Proposition 3.2.6 tells us that the notion of weak presentation is the right notion to use in the study of
Diophantine/existential definability. First of all, both weak presentations and existentially definable sets exist over any ring. Secondly, Diophantine classes fit in completely inside relative enumerability classes invariant under weak presentations. We explore the last fact further by using it to show that there are infinitely many Diophantine classes.

3.3 How Many Diophantine Classes Are There?

As a consequence of the fact that over \( \mathbb{Z} \) recursive enumerability and Diophantine definability are the same we have the following result.

3.3.1 Lemma.

Let \( \mathcal{A} = \{p_n\} \) be a set of rational primes. Then \( O_{Q,\mathcal{A}} \leq \text{Dioph } \mathbb{Z} \) if and only if \( \mathcal{A} \) is recursively enumerable.

Proof.

Suppose \( \mathcal{A} \) is a recursively enumerable set of primes. Then \( U \), the set of all natural numbers that can be written as products of primes from \( \mathcal{A} \) is also recursively enumerable by Proposition A.4.2. By the Matiyasevich’s Theorem (see Theorem 1.2.2), \( U \) is Diophantine over \( \mathbb{Z} \). Let \( f_U(t, x_1, \ldots, x_m) \) be the Diophantine definition of \( U \) over \( \mathbb{Z} \). Hence we can set

\[
O_{Q,\mathcal{A}} = \left\{ \frac{x}{y} \mid x \in \mathbb{Z}, y \in \mathbb{Z}, \exists x_1, \ldots, x_m \in \mathbb{Z}, f_U(y, x_1, \ldots, x_m) = 0 \right\}
\]

and thus \( O_{Q,\mathcal{A}} \leq \text{Dioph } \mathbb{Z} \).

Suppose now \( O_{Q,\mathcal{A}} \leq \text{Dioph } \mathbb{Z} \). Then

\[
O_{Q,\mathcal{A}} = \left\{ \frac{x}{y} \mid x \in \mathbb{Z}, y \in \mathbb{Z}, \exists x_1, \ldots, x_n \in \mathbb{Z}, g(x, y, x_1, \ldots, x_m) = 0 \right\}
\]

for some polynomial \( g(x, y, x_1, \ldots, x_m) \in \mathbb{Z}[x, y, x_1, \ldots, x_m] \). Let

\[
U_Z = \{ y \in \mathbb{Z} \mid \exists x_1, \ldots, x_n \in \mathbb{Z}, g(1, y, x_1, \ldots, x_m) = 0 \}.
\]

Then \( U_Z \) is a Diophantine over \( \mathbb{Z} \) set, and by Proposition 3.2.5 and Remark 3.2.7, for any weak presentation \( j \) we have that \( j(U_Z) \leq_e j(\mathbb{Z}) \), where \( j(\mathbb{Z}) \) is r.e. Consequently, \( j(U_Z) \) is also an r.e. set. Let

\[
U = U_Z \cap \mathbb{N} = \{ m \mid m \in U_Z \}.
\]
By Proposition A.6.1 and Remark 3.2.7 again, for any weak presentation $j$ of $\mathbb{Z}$ we now have that $U \equiv_e j(U) \equiv_e j(U_\mathbb{Z})$, and therefore $U$ is recursively enumerable. Finally, by Proposition A.4.2, $U \equiv_e \mathcal{A}$. Hence $\mathcal{A}$ is recursively enumerable.

Unfortunately, all the aspects of the relationship between Diophantine definability and enumerability for rings other than $\mathbb{Z}$ are far from clear. However from Proposition 3.2.5 we do get the following fact.

3.3.2 Proposition.

There are infinitely many Diophantine classes.

Proof.

We will show that subrings of $\mathbb{Q}$ are partitioned into infinitely many Diophantine classes. From Proposition A.6.4 and Remark 3.2.7, given a set of rational primes

$$\mathcal{A} = \{p_i, i \in I\},$$

where $p_1 \leq p_2 \ldots$ is a listing of all primes in ascending order and $I$ is any subset of natural numbers, we have $J(O_{\mathbb{Q}, \mathcal{A}}) \equiv_e J(I) \equiv_e I$ under any weak presentation $J$ of $\mathbb{Q}$ as a field. On the other hand, given two sets of rational primes $\mathcal{A}_1, \mathcal{A}_2$, by Proposition 3.2.5

$$O_{\mathbb{Q}, \mathcal{A}_1} \equiv_{\text{Dioph}} O_{\mathbb{Q}, \mathcal{A}_2} \Rightarrow J(O_{\mathbb{Q}, \mathcal{A}_1}) \equiv_e J(O_{\mathbb{Q}, \mathcal{A}_2})$$

under any weak presentation of $\mathbb{Q}$ (as a field or ring). Since there are infinitely many enumeration classes (see Proposition A.3.3), we must conclude that there are infinitely many Diophantine classes.

3.4 Diophantine Generation and Hilbert’s Tenth Problem

In this section we want to investigate the very close connection between Diophantine Generation and Diophantine Undecidability. First we need to formalize exactly what we mean by unsolvability (or solvability) of HTP for an arbitrary countable ring.
3.4.1 Definition.

Let $R$ be a countable ring. We will say that HTP is decidable (undecidable) over $R$ if there exists (does not exist) a presentation $J : R \rightarrow \mathbb{N}$ and a total recursive function $f$ from the space of finite sequences of natural numbers into the set $\{0, 1\}$ such that

$$f(d, m, k, A_{i_1, \ldots, i_m, j_1, \ldots, j_k}, 0 \leq i_k, j_i \leq d)(n_1, \ldots, n_m) = 1$$

if and only if $(n_1, \ldots, n_m) = (J(x_1), \ldots, J(x_m))$, where $x_1, \ldots, x_m$ are elements of the Diophantine set whose definition over $R$ is the polynomial

$$H(x_1, \ldots, x_m, y_1, \ldots, y_k) = \sum_{0 \leq i_k, j_i \leq d} a_{i_1, \ldots, i_m, j_1, \ldots, j_k} x_1^{i_1} \cdots x_m^{i_m} y_1^{j_1} \cdots y_k^{j_k},$$

and

$$J(a_{i_1, \ldots, i_m, j_1, \ldots, j_k}) = A_{i_1, \ldots, i_m, j_1, \ldots, j_k}.$$

Note that an immediate corollary of this definition is the fact that solvability of HTP under $J$ requires that every Diophantine set is recursive under $J$.

3.4.2 Remark.

Looking at the formalization above one can conclude immediately that, despite the fact that we did not put any assumptions on $J$, without loss of generality, we can assume that $J$ is a strongly recursive presentation of $R$. Indeed, first suppose that $J$ is not recursive. Then either $J(R)$ is not recursive or the graphs of addition, subtraction or multiplication are not recursive. Since $R$ is Diophantine over $R$ and the graphs of the ring operations are also Diophantine over $R$, we conclude that under $J$ there are non-computable Diophantine sets and in this case HTP is not solvable under $J$. Finally assume that $J$ is a recursive but not strongly recursive presentation of $R$. (See Definition A.7.3 for the definition of a strongly recursive presentation.) Then under $J$, the image of the set $D = \{(x, y) : \exists z \in R_1, x = yz\}$ is not recursive. So in this case $R$ again has a Diophantine set which is undecidable under $J$.

We also should note that by Matiyasevich’s Theorem and Corollary A.6.6, $\mathbb{Z}$ has undecidable Diophantine subsets under any presentation, and so we can continue to say that HTP is unsolvable over $\mathbb{Z}$.

Next we introduce a new notion which will play an important role in this and later sections in this book – the notion of a Diophantine model.
3.4.3 Definition.

Let \( R_1, R_2 \) be two rings such that the following statements are true.

1. There exists a map
   \[
   \bar{\phi} = (\phi_1, \ldots, \phi_k) : R_1 \longrightarrow R_2^k
   \]
   such that for any Diophantine set \( D_1 \subseteq R_1^l \), there exists a Diophantine set \( D_2 \subseteq R_2^{lk} \) with the following properties:
   \[
   D = \{(\bar{\phi}(a_1), \ldots, \bar{\phi}(a_i)) : (a_1, \ldots, a_i) \in D_1\} \subseteq D_2,
   \]
   and for
   \[
   \bar{D} = \{(\bar{\phi}(a_1), \ldots, \bar{\phi}(a_i)) : (a_1, \ldots, a_i) \notin D_1\}
   \]
   we have that
   \[
   \bar{D} \cap D_2 = \emptyset.
   \]

2. Under some recursive presentations \( J_1, J_2 \) of \( R_1 \) and \( R_2 \) respectively, the map \( J_2 \circ \phi_i \circ J_1^{-1} \) is a restriction of a recursive function for all \( i = 1, \ldots, k \).

Then we will say that \( R_2 \) has a Diophantine model of \( R_1 \).

The raison d’être of the Diophantine models is made clear by the following proposition whose proof we leave to the reader.

3.4.4 Proposition.

Let \( R_1, R_2 \) be two rings such that \( R_2 \) has a Diophantine model of \( R_1 \) under some presentations \( J_1 \) and \( J_2 \) of \( R_1 \) and \( R_2 \) respectively. Assume that one of the following statements is true.

- HTP is undecidable over \( R_1 \) under \( J_1 \), and there exists an effective procedure such that given the \( J_1 \)-codes of the coefficients of a Diophantine definition over \( R_1 \) of any Diophantine subset \( D_1 \) of \( R_1 \) as its input, this procedure will produce the \( J_2 \)-codes of the coefficients for a Diophantine definition over \( R_2 \) of \( D_2 \), the Diophantine subset of \( R_2 \), containing the image of \( D_1 \) in the Diophantine model.

- There exists an undecidable (under \( J_1 \)) Diophantine set over \( R_1 \) (and therefore HTP is undecidable over \( R_1 \) under \( J_1 \)).

Then HTP is undecidable over \( R_2 \) under \( J_2 \).

The proposition below provides the connection between Diophantine models and Diophantine generation.
3.4.5 Proposition.

Let \( R_1 \leq_{\text{Dioph}} R_2 \) be two rings with residue fields \( F_1 \) and \( F_2 \) respectively. Let \( F \) be a field such that \( F_1 F_2 \subset F \), \( F/F_2 \) is a finite extension of degree \( n \), and \( F \) is not algebraically closed. Assume \( R_2 \) is strongly recursive. Then the following statements are true.

1. There exists a recursive presentation \( J \) of \( F \) such that the following conditions are satisfied:
   - \( R_2 \) is recursive under \( J \);
   - the coordinate functions from \( F \) to \( F_2 \) (as defined in Proposition 3.2.3) are recursive under \( J \) with respect to some basis of \( F \) over \( F_2 \);
   - there exists a recursive mapping \( \bar{\Lambda} = (\Lambda_1, \Lambda_2) : J(F_2) \to J(R_2)^2 \) defined by \( \bar{\Lambda}(J(x)) = (J(x_1), J(x_2)) \), where \( x_1, x_2 \in R_2, x_2 \neq 0 \) and \( x = x_1/x_2 \).

2. If \( J(R_1) \) is recursive then
   - \( R_2 \) has a Diophantine model of \( R_1 \),
   - for any set \( D_1 \subset R_1 \), Diophantine over \( R_1 \), a Diophantine definition of \( D_2 \) — the set containing the image of \( D_1 \) but no element of its complement, can be effectively (under \( J \)) and uniformly in \( D_1 \) constructed over \( R_2 \) from a Diophantine definition of \( D_1 \).

Proof.

The first assertion of the proposition is satisfied by Propositions A.7.4 and A.7.7. Next assume that \( J(R_2) \) is recursive and let \( \Omega = \{ \omega_1, \ldots, \omega_n \} \) be a basis of \( F \) over \( F_2 \) such that under \( J \) the coordinate functions \( (C_1, \ldots, C_n) \) with respect to \( \Omega \) are recursive. Let
\[
(c_1, \ldots, c_n) : F \to F_2
\]
be such that \( c_i = J^{-1} \circ C_i \circ J \). Also let \( \lambda_i = J^{-1} \circ \Lambda_i \circ J \).

Since \( R_1 \leq_{\text{Dioph}} R_2 \), for some
\[
f(A_1, \ldots, A_n, B, Z_1, \ldots, Z_m) \in R_2[A_1, \ldots, A_n, B, Z_1, \ldots, Z_m],
\]
\[
R_1 = \left\{ \frac{\sum_{i=1}^{n} a_i}{b} \omega_i : \exists z_1, \ldots, z_m \in R_2, f(a_1, \ldots, a_n, b, z_1, \ldots, z_m) = 0 \right\},
\]
(3.4.1)
where \( f(a_1, \ldots, a_n, b, z_1, \ldots, z_m) = 0 \Rightarrow b \neq 0 \). So given \( x \in R_1 \), define for \( i = 1, \ldots, n \),
\[
\phi_{2i-1}(x) = \lambda_1(c_i(x)), \phi_{2i}(x) = \lambda_2(c_i(x)),
\]
and for \( X \in \mathbb{N} \) let
\[
\Phi_{2i-j}(X) = \begin{cases} 
J \circ \phi_{2i-j} \circ J^{-1}(X) = \Lambda_k(C_i(X)), & \text{if } X \in J(R_1) \\
0, & \text{if } X \notin J(R_1). 
\end{cases}
\]

Here either \( j = 1 \) and \( k = 1 \) or \( j = 0 \) and \( k = 2 \). Observe that given our assumptions, \( \Phi = (\Phi_1, \ldots, \Phi_n) \) is recursive. Next let \( D_1 \) be a Diophantine subset of \( R_1^l \) with Diophantine definition \( g(X_1, \ldots, X_l, T_1, \ldots, T_r) \). Let \( D_2 \) consist of all \((y_1, \ldots, y_{2n}) \in R_2^{2n}\) such that
\[
\exists \bar{a}_1, \ldots, \bar{a}_l, \bar{u}_1, \ldots, \bar{u}_r \in R_2^n, \\
b_1, \ldots, b_l, v_1, \ldots, v_r, x_1, \ldots, x_l, t_1, \ldots, t_r \in R_2, \\
z_1, \ldots, z_l, \bar{w}_1, \ldots, \bar{w}_r \in R_2^m,
\]
satisfying the following system of equations.
\[
\begin{cases}
    y_{2i-1,j} b_j = y_{2i,j} a_{i,j}, & j = 1, \ldots, l, i = 1, \ldots, n \\
b_j x_j = \sum_{i=1}^{n} a_{i,j} \omega_j, \\
f(\bar{a}_j, b_j, \bar{z}_j) = 0, & j = 1, \ldots, l, \\
g(x_1, \ldots, x_l, t_1, \ldots, t_r) = 0, \\
v_j t_j = \sum_{i=1}^{n} u_{i,j} \omega_i, & j = 1, \ldots, r \\
f(\bar{u}_j, v_j, \bar{w}_j) = 0, & j = 1, \ldots, r
\end{cases}
\]
(3.4.2)

In other words, \((y_1, \ldots, y_{2n})\) is in the \( D_2 \) if and only if either for some \( i = 1, \ldots, n \) we have that \( y_{2i} = 0 \) or \( x = \sum_{i=1}^{n} \frac{y_{2i-1}}{y_{2i}} \omega_i \in D_1 \). Since
\[
x = \sum_{i=1}^{n} \frac{\lambda_1(c_i(x))}{\lambda_2(c_i(x))} \omega_i,
\]
and for all \( i = 1, \ldots, n \) we have that \( \lambda_2(C_i(x)) \neq 0 \), we conclude that \( \Phi(x) \in D_2 \) if and only if \( x \in D_1 \). Thus the proposition holds.

It is clear from Proposition 3.4.5 that in the case of Diophantine generation the first clause of Proposition 3.4.4 applies and we have the following corollary.

3.4.6 Corollary.

Let \( R_1 \) and \( R_2 \) be any two ring with \( R_1 \leq_{\text{Dioph}} R_2 \) and HTP unsolvable over \( R_1 \). Then HTP is unsolvable over \( R_2 \).
Proof.

By Remark 3.4.2 we can assume that $R_2$ is strongly recursive. Let $F$ be a defining field and let $\Omega$ be a Diophantine basis for $R_1$ over $R_2$. Then by Proposition 3.4.5 there exists a recursive presentation $J$ of $F$ such that

- $J(R_2)$ is strongly recursive,
- the coordinate functions with respect to basis $\Omega$ are computable,
- the function $\bar{\Lambda}$, as defined in Proposition 3.4.5, is computable.

Suppose now $J(R_1)$ is not recursive. As before $R_1 \leq_{\text{Dioph}} R_2$ implies that (3.4.1) holds for some

$$f(x_1, \ldots, x_n, y, z_1, \ldots, z_m) \in R_2[x_1, \ldots, x_n, y, z_1, \ldots, z_m].$$

Let $D_{R_1}$ consist of all the $2n$-tuples $(y_1, \ldots, y_{2n})$ such that there exist $a_1, \ldots, a_n, b \in R_2$ satisfying the following system of equations.

$$\begin{cases} y_{2i-1}b = y_{2i}a_i, & i = 1, \ldots, n, \\ f(a_1, \ldots, a_n, b, z_1, \ldots, z_m) = 0, \end{cases} \quad (3.4.3)$$

Then $(y_1, \ldots, y_{2n}) \in D_{R_1}$ if and only if for some $i = 1, \ldots, n$ we have that $y_{2i} = 0$ or $\sum_{i=1}^{n} \frac{y_{2i-1}}{y_{2i}}w_i \in R_1$. Thus, for any positive integer $l \in J(F)$ we have that $l \in J(R_1)$ if and only if

$$(\Lambda_1(C_1(l)), \Lambda_2(C_1(l)), \ldots, \Lambda_1(C_n(l)), \Lambda_2(C_n(l))) \in \bar{J}(D_{R_1}).$$

Therefore, if $\bar{J}(D_{R_1})$ is recursive, then so is $J(R_1)$. Consequently, if $J(R_1)$ is not recursive, then $R_2$ has an undecidable Diophantine set under $J$ and HTP is undecidable under this presentation.

Finally, suppose that $J(R_1)$ is recursive. Then conditions of Proposition 3.4.5 are satisfied and by the first clause of Proposition 3.4.4, HTP is not decidable over $R_2$ under $J$ in this case also. Hence HTP is not decidable under any presentation of $R_2$.

We should also like to note here that in practice one can almost always make use of the second clause of Proposition 3.4.4, because there are undecidable Diophantine sets over $\mathbb{Z}$. In particular the following proposition is true.
3.4.7 Proposition.

Let $R$ be a ring with a recursive presentation such that for some positive integer $k$ there exists a map

$$\bar{\tau} = (\tau_1, \ldots, \tau_k) : \mathbb{Z} \rightarrow R^k$$

with the images of the graphs of addition and multiplication being Diophantine over $R$. Then $R$ has a Diophantine model of $\mathbb{Z}$ and HTP is undecidable over $R$.

Proof.

First of all, using an inductive argument on the number of operations, similar to the argument used to prove Lemma 3.2.2, one can show that $\tau_l : \mathbb{Z}^l \rightarrow R^{kl}$ will map any Diophantine subset of $\mathbb{Z}^l$ into a Diophantine subset of $R^{kl}$. So it remains to be shown that under any recursive presentation of $R$, the map $\bar{\tau}$ will be recursive. Let $J : R \rightarrow \mathbb{N}$ be a recursive presentation of $R$. By assumption, the set $(\bar{\tau}(m), \bar{\tau}(n), \bar{\tau}(m+n))$ is a Diophantine subset of $R^{3k}$. Therefore, by Proposition 3.2.5, given that $J(R)$ is recursive, the set

$$S = \{ J^k(\bar{\tau}(m)), J^k(\bar{\tau}(n)), J^k(\bar{\tau}(m+n)), m \in \mathbb{N} \}$$

is computably enumerable. Let $f$ be a recursive function enumerating $S$. Define $g : \mathbb{N} \rightarrow R^k$ in the following manner. Let $g(0) = J^k(\tau(0))$, $g(3) = J^k(\tau(1))$, $g(6) = J^k(\tau(-1))$. Let $m$ be a positive integers and assume that $g(3^{m-1})$ has been computed. Then define

$$g(3^m) = (\pi_{2k+1}(f(l)), \ldots, \pi_{3k}(f(l))),$$

where $l$ is the smallest positive integer such that for some $\bar{u} \in J^k(R)$ we have that

$$f(l) = (g(3), g(3^{m-1}), \bar{u}).$$

Similarly, for any positive $m$, assuming $g(2 \cdot 3^{m-1})$ has been defined already, define

$$g(2 \cdot 3^m) = (\pi_{2k+1}(f(l)), \ldots, \pi_{3k}(f(l))),$$

where where $l$ is the smallest positive integer such that for some $\bar{u} \in J^k(R)$ we have

$$f(l) = (g(6), g(2 \cdot 3^{m-1}), \bar{u}).$$

If $t \in \mathbb{N}$ is not of the form $2 \cdot 3^m$ or $3^m$ for some positive integer $m$, then define $g(t) = (0, \ldots, 0)$ and observe that by definition of computable functions (using encoding of $k$-tuples described in Lemma A.1.14), given our adopted presentation $J_{\mathbb{Z}}$ of $\mathbb{Z}$ (see Proposition A.6.1), $g(m)$ is a computable function with $g(J_{\mathbb{Z}}(z)) = \tau(z)$ for all $z \in \mathbb{Z}$.
3.4.8 Remark.

We finish this section with a historical note. The term “Diophantine model” belongs to Gunther Cornelissen who introduced the terminology and the notion (in a slightly different form) in [5].
Chapter 4

Integrality at Finitely Many Primes and Divisibility of Order at Infinitely Many Primes.

In this chapter we will continue with the task of describing the known Diophantine classes of the rings of \( \mathcal{W} \)-integers of global fields. We will start with horizontal problems. The question which we will partially answer here is the following one. Does the Diophantine class of a ring of \( \mathcal{W} \)-integers change if we add to or remove from \( \mathcal{W} \) finitely many primes. As we will see below, we are able to show in many cases that the class does not change. We conjecture that this is true for all rings of \( \mathcal{W} \)-integers, but are unable to prove this at the moment.

The main tool used so far to prove the results of the type described in this section is the Strong Hasse Norm Principle (see [79], Theorem 32.9). The ideas behind the construction of a Diophantine definition of integrality at finitely many primes presented below go back to the work of Ershov and Penzin (see [65], [26]) and to the work of Julia Robinson on arithmetic definability of rational integers in algebraic number fields (see [81] and [82]). She used quadratic forms to carry out her construction. Later, Rumely generalized Robinson’s methods in his paper on arithmetic definability over global fields (see [85]). In his paper Rumely used norm equations and the Strong Hasse Norm Principle. Kim and Roush were the first to use this methodology for the purposes of showing the undecidability of some Diophantine problems over function fields. (See [42]..) They also were the first to use quadratic forms to show existential definability of order at a prime over \( \mathbb{Q} \) in [44]. The author has also used various versions of the norm method to resolve some issues of existential definability in [102], [97], [106]. Finally, we note that somewhat different ideas were used by Eisenträger in [25] to address integrality at a
prime over some global fields.

Before proceeding with the technical material, we note that in this chapter we will use Definition B.1.23 and Notation B.8.1 of the Number Theory Appendix. We start with an exposition of the main technical methods to be used in this chapter.

4.1 The Main Ideas.

In this section we survey the main ideas which are used in the sections below, omitting some technical details and proofs of some facts to simplify the presentation. The omitted details and proofs will, however, appear in the following sections.

4.1.1 Norm Equations Are Polynomial Equations.

Let $M/L$ be a finite extension of global fields. Then the equation $N_{M/L}z = h$ can be rewritten as a polynomial equation with variables and coefficients in $L$. It suffices to select a basis $\Omega = \{\omega_1, \ldots, \omega_n\}$ of $M$ over $L$ and write $z = \sum_{i=1}^n a_i \omega_i$. Then $N_{M/L}z$ becomes a polynomial in $a_1, \ldots, a_n$ with coefficients invariant under the action of any element of $\text{Gal}(M_G/L)$, where $M_G$ is the Galois closure of $M$ over $L$.

4.1.2 On Being a Norm and Divisibility of Order.

Assume that the extension $M/L$ is cyclic and $p$ is a prime of $L$ not splitting in the extension. Then if $h \in L$ is a norm of an element of $M$, $\text{ord}_p h \equiv 0 \mod [M : L]$. Thus, if $\text{ord}_p h \not\equiv 0 \mod [M : L]$, the equation $N_{M/L}z = h$ does not have solutions in $M$.

4.1.3 How Having a Pole Can Produce a Wrong Order at a Prime.

Let $u \in L$ be such that $\text{ord}_p u = -1$. Let $y \in L$. Let $n$ be any natural number. Then $y$ is integral at $p$ if and only if $n|\text{ord}_p(uy^n + u^n)$. From this point it is easy to see that we have the following implication. Let $n = [M : L]$, where $M/L$ is a cyclic extension. Let $p$ be a prime not splitting in this extension. Then if $y$ has a pole at $p$, the equation $N_{M/L}(z) = uy^n + u^n$ has no solution in $M$. Unfortunately, this will go only half way in producing the existential definability of order at a prime. We need to make sure that we have solutions
to the norm equation when \( y \) has no pole at \( p \). This is where the Strong Hasse Norm Principle comes in.

### 4.1.4 The Role of the Strong Hasse Norm Principle.

The Strong Hasse Norm Principle asserts that if the equation is cyclic, an element of the field below is a norm if and only if the element is a norm locally at every prime. In other words, if \( M/L \) is a cyclic extension as above, and \( h \in L \), then \( N_{M/L}z = h \) has solutions in \( M \) if and only if for any \( q \), prime of \( L \), and any \( \Omega \), prime of \( M \) above it, \( N_{M_{\Omega}/L_q}v = h \) has solution \( v = v(\Omega) \in M_{\Omega} \). Thus to insure that our norm equation has a solution when \( h \) does not have a pole at \( p \), we can work locally.

### 4.1.5 The Making of a Local Norm.

To begin with the problem will be immediately solved for all but finitely many primes. Indeed, if \( q \) is a prime of \( L \) and \( h \) is a unit at \( q \), while \( q \) is unramified in the local (and therefore global) extension, \( h \) is automatically a local norm at \( q \). Thus, we just have to worry about the primes which are ramified and the primes which occur in the divisor of \( h \).

Next we observe how to take care of the unramified primes occurring in the divisor of \( h \). If for some unramified prime \( q \) of \( L \) we have that \( \text{ord}_q h \equiv 0 \mod n = [M : L] \), then \( h = \pi_q^n \epsilon_q \), where \( \pi_q \in L \) is of order 1 at \( q \) and \( \epsilon_q \in L \) is a unit at \( q \). Since \( M/L \) is Galois, the relative degree of any prime will be a divisor of \( n \). (Relative degree of a prime and the divisibility requirement are explained in Lemma B.4.1.) Thus we can write \( n = f(\Omega/q)n_1 = [M_{\Omega} : L_q]n_1 \), where \( \Omega \) lies above \( q \) in \( M \) and observe that \( N_{M_{\Omega}/L_q} \pi_q^{n_1} = \pi_q^n \). Therefore \( h \) is a norm at \( q \) if an only if \( \epsilon_q \) is a norm. But the last assertion is true if \( q \) is not ramified by the argument above.

So how can we arrange for the order of \( h \) at all the “non-involved” primes occurring in its divisor to be divisible by \( n \)? By introducing another extension \( G \) of \( L \) which will depend on \( h \), and will be such that in the extension \( GL/L \) all the primes occurring in the divisor of \( h \), with orders not divisible by \( n \), ramify with ramification degree \( n \). (Roughly speaking, we will be taking the \( n \)-th root of \( h \). However we will have to be careful not to change the divisibility of order at \( p \) and so some details will have to be adjusted.) Thus in the end we will be looking to solve norm equation \( N_{MG/LG}z = h \).

Finally we will have to deal with the ramified primes, but only in the number field case. In the function field case, we can always use a constant field extension to avoid this issue. In the number field case we arrange for \( h \) to be an \( n \)-th power in \( L_q \) for every ramified prime \( q \). To insure this it is enough, by
Hensel’s Lemma, to show that $h^{\ord_q h}$, where $\ord_q \pi_q = 1$, is an $n$-th power modulo a sufficiently high power of $q$.

### 4.2 Integrality at Finitely Many Primes in Number Fields.

In this section we will show that integrality at finitely many primes is existentially definable over a number field. We will start with describing notation to be used in this section.

#### 4.2.1 Notation.

- $K$ will denote a number field.
- $q > 2$ will be a rational prime such that $K$ contains all the $q$-th roots of unity.
- $\mathfrak{p}_1, \ldots, \mathfrak{p}_l$ will be primes of $K$ not lying above $q$.
- $a \in O_K$ will be such that $a$ is not a $q$-th power modulo $\mathfrak{p}_i$ for any $i = 1, \ldots, l$. (In particular, $\ord_{\mathfrak{p}_i} a = 0$ for all $i = 1, \ldots, l$.) Let $\prod_{i=1}^{l} a_i^{r_i}$ be the divisor of $a$. (Note that such an $a$ always exists by the Strong Approximation Theorem: Theorem B.2.1.)
- For each $i = 1, \ldots, l$, let $A_i$ be the rational prime below $a_i$.
- Let $c$ be a prime of $K$ distinct from $\mathfrak{p}_i$'s, and relatively prime to $aq$.
- Let $D = \prod_j d_j^{d_j}$, an integral and possibly trivial divisor of $K$, be a product of $K$-primes $d_j$, distinct from all $\mathfrak{p}_i$, $c$ and prime factors of $q$ and $a$.
- Let $g \in K$ satisfy the following conditions.
  - $g \equiv 1 \mod aq^3$.
  - The divisor of $g$ is of the form $\frac{\prod_{\mathfrak{p} \neq c} \mathfrak{p}^{s_i}}{c^3}$, where $s_i \in \mathbb{N} \setminus \{0\}, \forall i \neq 0 \mod q$. (Such a $g \in K$ exists for some $D$ as above by Proposition B.2.2.)
- Let $r = q^{(3q[K:Q])}(q^{(q[K:Q])!} - 1)\left(\prod(A_i^{(q[K:Q])!} - 1)\right)$
- Let $s = \max\{s, d_j, 3qr_i[K:Q]\}$. 

51
Let \( v \in O_K \) and be such that \( v \equiv 1 \mod (q^3a)^r \), \( \text{ord}_\mathfrak{p} v = d_i \), and \( \text{ord}_\mathfrak{e} v = 1 \). (Existence of \( v \) follows from the Strong Approximation Theorem when it is applied the same way as in the proof of Proposition B.2.2.)

We start with a proposition containing the technical core of the section.

### 4.2.2 Proposition.

Let \( x \in K \) and let

\[
h = (q^3a)^r(g^{-1}x^{r(s+1)} + g^{-q}) + v^2.
\]

Let \( b \in O_K, b \not\equiv 0 \mod \mathfrak{p}_i \) for any \( i = 1, \ldots, l \). Let \( c \in K, c \equiv gb^q \mod \prod \mathfrak{p}_i \), \( \text{ord}_\mathfrak{e} c = -q - 1 \), \( \text{ord}_\mathfrak{p} c = -qd_j - 1 \) and \( c \) is integral at all the other primes. (Such a \( c \) exists yet again by the Strong Approximation Theorem.) Let \( \beta_x \) be a root of

\[
T^q - (h^{-1} + c).
\]

Let \( \alpha \in \bar{\mathbb{Q}} \) (the algebraic closure of \( \mathbb{Q} \)) be a root of the polynomial \( X^q - a \). Then

1. \([K(\beta_x) : K] = q\);
2. the equation

\[
\prod_{j=0}^{q-1}(a_0 + a_j \xi_q^j \alpha + \ldots + a_{q-1} \xi_q^{j(q-1)} \alpha^{q-1}) = h \quad (4.2.1)
\]

has solutions \( a_0, \ldots, a_{q-1} \in K(\beta_x) \) if and only if \( x \) is integral at \( \mathfrak{p}_i, i = 1, \ldots, l \).

**Proof.**

First of all we observe the following. If \( \text{ord}_\mathfrak{e} x > 0 \), then

\[
\text{ord}_\mathfrak{e} h = \text{ord}_\mathfrak{e}((q^3a)^r(g^{-1}x^{r(s+1)} + g^{-q}) + v^2) = \min(\text{ord}_\mathfrak{e}((g^{-1}x^{r(s+1)} + g^{-q}), \text{ord}_\mathfrak{e} v^2)) = \min(q, 2) = 2.
\]

If \( \text{ord}_\mathfrak{e} x = 0 \), then

\[
\text{ord}_\mathfrak{e} h = \text{ord}_\mathfrak{e}((q^3a)^r(g^{-1}x^{r(s+1)} + g^{-q}) + v^2) = \min(\text{ord}_\mathfrak{e}((g^{-1}x^{r(s+1)} + g^{-q}), \text{ord}_\mathfrak{e} v^2)) = \min(1, 2) = 1.
\]
If \( \text{ord}_\mathfrak{c} x < 0 \), then
\[
\text{ord}_\mathfrak{c} h = \text{ord}_\mathfrak{c} ((q^3 a)^r (g^{-1} x^{r(s+1)} + g^{-q}) + v^2)
\]
\[
= \min(\text{ord}_\mathfrak{c} ((g^{-1} x^{r(s+1)} + g^{-q}), \text{ord}_\mathfrak{c} v^2) = \min(1 + r(s + 1) \text{ord}_\mathfrak{c} x, q) < -2.
\]
Thus, at \( \mathfrak{c} \), either \( h \) has a pole of order greater than 2 or a zero of order 1 or 2. Therefore, at \( \mathfrak{c} \), it is the case that \( h^{-1} + c \) has a pole of order \( q + 1 \). Hence, \( h^{-1} + c \) is not a \( q \)-th power in \( K \), and thus by Lemma B.4.11 we have that \( [K(\beta_x) : K] = q \).

Before we proceed to the second assertion of the lemma we would like to note the following. By Lemma B.4.11, for any \( x \in K \), it is the case that \( \mathfrak{c} \) is completely ramified in the extension \( K(\beta_x)/K \). Further consider what happens to prime factors of \( \mathfrak{p} \) under this extension: these primes behave like \( \mathfrak{c} \). Indeed, if \( \text{ord}_{\mathfrak{p}} x > 0 \), then
\[
\text{ord}_{\mathfrak{p}} h = \text{ord}_{\mathfrak{p}} ((q^3 a)^r (g^{-1} x^{r(s+1)} + g^{-q}) + v^2)
\]
\[
= \min(\text{ord}_{\mathfrak{p}} ((g^{-1} x^{r(s+1)} + g^{-q}), \text{ord}_{\mathfrak{p}} v^2) = \min(qd_j, 2d_j) = 2d_j.
\]
If \( \text{ord}_{\mathfrak{p}} x = 0 \), then
\[
\text{ord}_{\mathfrak{p}} h = \text{ord}_{\mathfrak{p}} ((q^3 a)^r (g^{-1} x^{r(s+1)} + g^{-q}) + v^2)
\]
\[
= \min(\text{ord}_{\mathfrak{p}} ((g^{-1} x^{r(s+1)} + g^{-q}), \text{ord}_{\mathfrak{p}} v^2) = \min(d_j, 2d_j) = d_j.
\]
If \( \text{ord}_{\mathfrak{p}} x < 0 \), then
\[
\text{ord}_{\mathfrak{p}} h = \text{ord}_{\mathfrak{p}} ((q^3 a)^r (g^{-1} x^{r(s+1)} + g^{-q}) + v^2)
\]
\[
= \min(\text{ord}_{\mathfrak{p}} ((g^{-1} x^{r(s+1)} + g^{-q}), \text{ord}_{\mathfrak{p}} v^2) = \min(d_j + r(s + 1) \text{ord}_{\mathfrak{p}} x, qd_j) < -2d_j.
\]
Thus, at \( \mathfrak{p}_j \), either \( h \) has a pole of order greater than \( 2d_j \) or a zero of order \( d_j \) or \( 2d_j \). Therefore, at \( \mathfrak{p}_j \), we have that \( h^{-1} + c \) has a pole of order \( qd_j + 1 \). Thus, just like in the case of \( \mathfrak{c} \), by Lemma B.4.11, for all \( j \), for any \( x \in K \), we have that \( \mathfrak{p}_j \) is completely ramified in the extension \( K(\beta_x)/K \).

We now turn to the second assertion of the lemma. Note that if for some \( i \) we have that \( \text{ord}_{\mathfrak{p}_i} x < 0 \), then
\[
\text{ord}_{\mathfrak{p}_i} (g^{-1} x^{r(s+1)} + g^{-q}) < 0
\]
and
\[
\text{ord}_{\mathfrak{p}_i} (g^{-1} x^{r(s+1)} + g^{-q}) = \text{ord}_{\mathfrak{p}_i} g^{-1} x^{r(s+1)} = r(s+1) \text{ord}_{\mathfrak{p}_i} x - s_i \equiv -s_i \mod q.
\]

53
Thus,
\[
\text{ord}_{Q_i} h = \text{ord}_{Q_i}((q^3a)^r(g^{-1}x^{r(s+1)} + g^{-q}) + v^2) \not\equiv 0 \mod q.
\]
On the other hand, if \(\text{ord}_{Q_i} x \geq 0\) then
\[
\text{ord}_{Q_i} h = \text{ord}_{Q_i}((q^3a)^r(g^{-1}x^{r(s+1)} + g^{-q}) + v^2) = \text{ord}_{Q_i}g^{-q} \equiv 0 \mod q
\]
and
\[
\text{ord}_{Q_i} h = \text{ord}_{Q_i}((q^3a)^r(g^{-1}x^{r(s+1)} + g^{-q}) + v^2) < 0.
\]
Consequently, in this case \(\text{ord}_{Q_i} h \equiv 0 \mod q\). (Compare to Subsection 4.1.3.) Observe that in either case \(h^{-1} \equiv 0 \mod q_i\).

Next note that \(h^{-1} + c \equiv b^q \not\equiv 0 \mod q_i\). Thus, by Lemma B.4.11, in the extension \(K(\beta_x)/K\), each \(q_i\) is not ramified and splits completely. Therefore the residue fields of all the factors of \(q_i\) in \(K(\beta_x)\) are the same as the residue field of \(q_i\) in \(K\). Consequently, \(a\) is not a \(q\)-th power modulo any factor of \(q_i\) in \(K(\beta_x)\) and each of these factors remains prime in the extension \(K(\alpha,\beta_x)/K(\beta_x)\), again by Lemma B.4.11. This also means that \([K(\alpha,\beta_x) : K(\beta_x)]=q\) by Lemma B.4.11 yet again. Observe further that the equation in (4.2.1) has solutions \(a_0,\ldots,a_{q-1} \in K(\beta_x)\) if and only if
\[
N_{K(\alpha,\beta_x)/K(\beta_x)}(z) = h
\]
has a solution \(z \in K(\alpha,\beta_x)\).

Further, by Lemma B.4.11, \(\text{ord}_{Q_i} h \not\equiv 0 \mod q\) for some \(i\), implies (4.2.1) does not have solutions in \(K(\beta_x,\alpha\)). (Compare to Subsection 4.1.2.)

Next we show that if \(\text{ord}_{Q_i} h \equiv 0 \mod q\) for all \(i=1,\ldots,l\), then (4.2.1) will have solutions in \(K(\beta_x)\). By the Strong Hasse Norm principal, an element of \(K(\beta_x)\) is an \(K(\beta_x,\alpha)\)-norm if and only if it is a norm locally at all the valuations. To determine what is a norm locally, as we have discussed in Subsection 4.1.5, we use two main devices. First we note that locally, every unit is a norm in a non-ramified extension (see Lemma B.8.5). Secondly, using Lemmas B.8.3 and B.8.4, one can derive the following. Assume \(\gamma,\kappa\) are units of a local field \(K_q\) with \(\text{ord}_q(\kappa - \gamma^q) > 2\text{ord}_q + 1\). Then \(\kappa\) is a local \(q\)-th power. Note further that in an extension of degree \(q\) every \(q\)-th power of the field below is a norm of an element from the field above.

Suppose now that \(h\) has an order divisible by \(q\) at all \(q_i\). Let \(\tilde{\psi}_i\) be a factor of \(q_i\) in \(K(\beta_x)\). Then \(\text{ord}_{\tilde{\psi}_i} h = 0 \mod q\). Let \(\pi_{\tilde{\psi}_i}\) be a local uniformizing parameter with respect to \(\tilde{\psi}_i\) (in other words, \(\text{ord}_{\tilde{\psi}_i} \pi_{\tilde{\psi}_i} = 1\)). Then \(h\) is a norm locally at \(\tilde{\psi}_i\) in the extension \(K(\beta_x,\alpha)/K(\beta_x)\) if and only if \(u = h\pi_{\tilde{\psi}_i} \text{ord}_{\tilde{\psi}_i} h\) is a local norm at \(\tilde{\psi}_i\). But \(u\) is unit at \(\tilde{\psi}_i\) and \(\tilde{\psi}_i\) is not ramified in the extension.
Therefore, by the observation above, \( u \) is a norm locally with respect to \( \hat{\varphi}_j \).

Next we note the following. If \( \mathfrak{p} \) is a prime of \( K \) such that \( \text{ord}_\mathfrak{p} h > 0 \), then either \( \text{ord}_\mathfrak{p} h \equiv 0 \mod q \) or \( \mathfrak{p} \) is ramified completely in the extension \( K(\beta_x)/K \).

Indeed, all the poles of \( c \) are poles of \( g \), i.e. \( c \) has a pole at \( c \) and all \( \alpha_j \)'s, and we have already established that these primes are completely ramified in the extension in question. Thus, any zero of \( h \) which is not \( c \) or a \( \alpha_j \) is also a pole of \( h^{-1} + c \) and the assertion is true. On the other hand, by construction of \( h \), if \( \mathfrak{p} \neq \mathfrak{p}_i, \mathfrak{p} \neq c, \mathfrak{p} \neq \alpha_j \) is a prime of \( K \) such that \( \text{ord}_\mathfrak{p} h < 0 \), then \( \text{ord}_\mathfrak{p} h \equiv 0 \mod q \). Thus, if \( \mathfrak{p} \) is any prime of \( K(\beta_x) \) which is not a factor of any \( \mathfrak{p}_i \) and such that \( \mathfrak{p} \) occurs in the divisor of \( h \), then \( \text{ord}_\mathfrak{p} h \equiv 0 \mod q \).

Hence, if \( \mathfrak{p} \) is not a factor of any \( \mathfrak{p}_i \) or \( q \) and does not occur in the divisor \( a \), then \( \mathfrak{p} \) is unramified in the extension \( K(\beta_x, \alpha)/K(\beta_x) \) and \( h \) is a norm locally at \( \mathfrak{p} \).

Finally, we consider the primes \( \mathfrak{p} \) which are factors of \( q \) or occur in the divisor of \( a \) and thus may ramify in the extension \( K(\beta_x, \alpha)/K \). First assume that \( x \) is integral at \( \mathfrak{p} \). Then

\[
\text{ord}_\mathfrak{p}(h - 1) = r\text{ord}_\mathfrak{p} a, \tag{4.2.2}
\]

if \( \mathfrak{p} \) occurs in the divisor of \( a \) and

\[
\text{ord}_\mathfrak{p}(h - 1) = 3r\text{ord}_\mathfrak{p} q, \tag{4.2.3}
\]

if \( \mathfrak{p} \) is a divisor of \( q \).

If, on the other hand, \( x \) has a pole at \( \mathfrak{p} \), then by definition of \( s \), we have that \( (q^3 a)^x r^{(s+1)} \) has a pole at \( \mathfrak{p} \). Indeed, assume first that \( \mathfrak{p} \) is a factor of \( q \). Then

\[
\text{ord}_\mathfrak{p}(q^3 a)^x r^{(s+1)} = 3r\text{ord}_\mathfrak{p} q + r(s + 1)\text{ord}_\mathfrak{p} x < 3r[K : \mathbb{Q}] - r(s + 1)
\]

\[
\leq 3r[K : \mathbb{Q}] - r(3[K : \mathbb{Q}] + 1) < 0.
\]

Similarly, if \( \mathfrak{p} \) occurs in the divisor of \( a \), then

\[
\text{ord}_\mathfrak{p}(q^3 a)^x r^{(s+1)} = r\text{ord}_\mathfrak{p} a + r(s + 1)\text{ord}_\mathfrak{p} x
\]

\[
< rr_i[K : \mathbb{Q}] - r(s + 1) \leq rr_i[K : \mathbb{Q}] - r(3r_i[K : \mathbb{Q}] + 1) < 0.
\]

Next we note that if \( \mathfrak{p} \) occurs in the divisor of \( a \) and \( z \in \mathbb{N} \) is the size of the residue field of \( \mathfrak{p} \), then \( r \equiv 0 \mod (z - 1) \). Indeed, the size of the residue field
is $A^f_i$, where $1 \leq f \leq [K : \mathbb{Q}]$. Thus, $f!(|K : \mathbb{Q}|q)!$ and $(A^f_i - 1)|((A^{|K : \mathbb{Q}|q}| - 1)$.

Finally by construction, $r \equiv 0 \mod (A^{|K : \mathbb{Q}|q}| - 1)$. Thus, any 3-unit $e$ raised to power $r$ is equivalent to 1 modulo any prime $3$ occurring in the divisor of $a$.

Suppose now that $3$ is a factor of $q$. Let $e$ be the ramification of this factor over $\mathbb{Q}$ and let $f$ be its relative degree over $\mathbb{Q}$. Consider the size of the multiplicative group of the finite ring $O_K/3^3e$. It is equal to $q^{3ef} - q^{3ef} - (q^f - 1)$. By construction,

$$r \equiv 0 \mod q^{3ef} - q^{3ef} - (q^f - 1).$$

Thus, any element of $K$ prime to a factor 3 of $q$ in $K$, raised to the power $r$ will be equivalent to 1 modulo $3^3e(3/q)$.

Next let $3$ be a factor of $q$ or occur in the divisor of $a$. Let $\Pi = \Pi_3$ be a local uniformizing parameter. Then for some non-zero $u \in \mathbb{N}$, we have that $(\Pi^u q^3a^{s+1})^r$ is a unit at 3. Further from the discussion above it follows that if $3$ occurs in the divisor of $a$, then $(\Pi^u q^3a^{s+1})^r \equiv 1 \mod 3$, and if $3$ is a factor of $q$ in $K$, then $(\Pi^u q^3a^{s+1})^r \equiv 1 \mod 3^3e$, where $e = e(3/q)$. Next consider $h(\Pi^u)^r$. Note that for any $K(\beta_x)$-factor $3_x$ of any $K$-prime 3, $h$ is a local norm at $3_x$ in the extension $K(\beta_x, \alpha)/K(\beta_x)$ if and only if $h(\Pi^u)^r$ is a local norm at $3_x$ since the local degree is either 1 or $q$ and $r \equiv 0 \mod q$.

On the other hand, depending on whether $3$ is a factor of $q$ or occurs in the divisor of $a$,

$$h(\Pi^u)^r = (\Pi^u)^r((q^3a)^r(g^{-1}x^{r(s+1)} + g^{-q}) + \nu^2) =$$

$$(\Pi^u)^r(q^3a)^r x^{r(s+1)}g^{-1} + (\Pi^u)^r(q^3a)^r g^{-q} + (\Pi^u)^r \nu^2 \equiv g^{-1} \mod 3^\nu \equiv 1 \mod 3^\nu,$$

where $\nu$ is 1 if $3$ occurs in the divisor of $a$ and $\nu = 3e(3/q)$ if $3$ is a factor of $q$. Thus, by Hensel’s Lemma, $h(\Pi^u)^r$ is a $q$-th power in $K$ completed at 3. Consequently, $h(\Pi^u)^r$ is also a $q$-th power locally at all the factors $3_x$ of 3 in $K(\beta_x)$ and therefore it is a $K(\alpha, \beta_x)$-norm in $K(\beta_x)$.

Thus, $h$ is a local norm in $K(\beta_x)$ at all the non-archimedean valuations.

Since $K$ contains $q$-th roots of unity for $q > 2$, $K$ does not have any real embeddings and therefore all the archimedean completions of $K$ are equal to $\mathbb{C}$. Hence $h$ is automatically a local norm under all the archimedean completions.

**4.2.3 Corollary.**

The set of elements of $K$ integral at $\wp_i$ for $i = 1, \ldots, l$ is Diophantine over $K$.  

56
Proof.

First consider the left side of the equation in (4.2.1) as a polynomial in variables \(a_0, \ldots, a_{q-1}\). The coefficients of this equation are in \(K(\alpha)\). Further observation indicates that these coefficients are not moved by any element of the Galois group of \(K(\alpha)\) over \(K\) and thus must be in \(K\). So let

\[
N(a_0, \ldots, a_{q-1}) = \prod_{i=0}^{q-1} (a_0 + a_1 \xi_q^i \alpha + \ldots + a_{q-1} \xi_q^{i(q-1)} \alpha^{q-1}) \in K[a_0, \ldots, a_{q-1}]
\]

The remaining task of rewriting all the equations so that all the variable range over \(K\) can be carried out using coordinate polynomials and pseudo-coordinate polynomials as in Lemma B.7.5. We leave the details to the reader.

We will now state the main result of this section.

4.2.4 Theorem.

Let \(M\) be any number field. Let \(p\) be any prime of \(M\). Then the set of elements of \(M\) integral at \(p\) is Diophantine over \(M\).

Proof.

Let \(K = M(\xi_q)\), where \(\xi_q\) is a primitive \(q\)-th root of unity. Let \(p = \prod_{i=1}^{l} \mathfrak{p}_i^{e_i}\) be the factorization of \(p\) in \(K\). Note that since \([K: M] < q\), we have that \(e_i < q\) for all \(i\). Then by Corollary 4.2.3, the set \(I_K\) of elements of \(K\) integral at \(\mathfrak{p}_1, \ldots, \mathfrak{p}_l\) is Diophantine over \(K\). Thus by “Going Up and Then Down Method” (see Subsection 2.1.17), \(I_K \cap M\) is Diophantine over \(M\). But \(I_K \cap M\) is precisely the set of elements of \(M\) integral at \(p\).

4.3 Integrality at Finitely Many Primes over Function Fields.

In this section we will show that integrality at finitely many primes is existentially definable over function fields over finite fields of constants. In addition to Definition B.1.23 and Notation B.8.1, in this section we will also use the following notation.
4.3.1 Notation and Assumptions.

- \( K \) will denote a function field of characteristic \( p > 0 \) over a finite field of constants \( C_K \).
- \( \tilde{K} \) will denote the algebraic closure of \( K \).
- \( q \) will denote a rational prime number distinct from \( p \).
- \( K \) will contain all the \( q \)-th roots of unity.
- \( K \) will contain an element \( f \) with the divisor of the form
  \[
  \frac{\prod_{i=1}^{m} b_i^{s_i}}{\prod_{j=1}^{l} a_j^{q r_j}},
  \]
  where for \( i = 1, \ldots, m \) and \( j = 1, \ldots, l \) we have that \( a_j \) and \( b_i \) are distinct prime divisors of degree 1 and \( (s_i, q) = 1 \).
  (Existence of \( f \) will be demonstrated later.)
- Let \( B = \prod_{i=1}^{m} b_i \).
- Let \( a \in C_K \) be such that the equation
  \[
  x^q - a = 0
  \]
  has no solution in \( K \).
- Let \( z_1 \in K \) be such that it has a pole of order 1 at \( a_1 \), and \( z_1 \equiv b^q \mod B \) for some \( b \in C_K \setminus \{0\} \). (The existence of such a \( z_1 \) can be deduced from the Strong Approximation Theorem (see Theorem B.2.1).)
- Let \( k > 0, k \not\equiv 0 \mod q \) be greater than the order of any pole of \( z_1 \) in \( K \). Then let \( z_2 \in K \) be such that for some \( a \in \mathbb{N} \) with \( a > \log_q kr_1 + 2 \), \( z_2 \) has a pole of order \( q^a \) at \( a_1 \), is equivalent to 1 mod \( B \) and is integral at all the other primes of \( K \). (The existence of \( z_2 \in K \) follows from Lemma B.2.3.)
- Let \( z = z_1 z_2 \) and observe that
  - \( \text{ord}_{a_1} z = -q^a - 1 < -q^2 r_1 k - 1 \),
  - \( z \equiv b^q \mod B \).
  - If \( \text{ord}_c z < 0 \), then \( \text{ord}_c z > -k \) for any \( c \neq a_1 \).

The following proposition constitutes the technical core of this section.
4.3.2 Proposition.

Let \( w \in K \). Let \( h \) be defined by the equation
\[
    h = f^{-1}w^{q(s+1)} + f^{-q},
\]
where \( s = \max\{s_1, \ldots, s_m, r_1, \ldots, r_l\} \). Let \( \beta_w \in \bar{K} \) be a root of the following equation
\[
    T^q - (h^{-k} + z) = 0.
\]

Then for all \( w \), we have that \( \beta_w \) is of degree \( q \) over \( K \), \( \alpha \) is of degree \( q \) over \( K(\beta_w) \), and the following equation has solutions \( a_0, \ldots, a_{q-1} \in K(\beta_w) \) if and only if \( \text{ord}_{a_i} w \geq 0 \) for all \( i = 1, \ldots, m \).

\[
    \prod_{i=0}^{q-1} (a_0 + a_1 \xi_q^i \alpha + \ldots + a_{q-1} \xi_q^{i(q-1)} \alpha^{q-1}) = h
\]

Proof.

First of all, we will show that for all \( w \in K \) we have that
\[
    [K(\beta_w) : K] = [K(\beta_w, \alpha) : K(\beta_w)] = 1. \tag{4.3.6}
\]

In order to show that \( (4.3.6) \) holds, we will show that in extension \( K(\beta_w)/K \), at least one prime will have ramification degree \( q \) while the degree of the extension is at most \( q \). Since the extension above is separable, the presence of a totally ramified prime will imply that adjoining \( \beta_w \) to \( K \) results in no constant field extension by Lemma B.4.17. Thus, since \( \alpha \) was of degree \( q \) over \( C_K \), it will remain of degree \( q \) over the constant field of \( K(\beta_w) \).

Observe that in \( K \) it is the case that \( f \) has a pole of order \( qr_1 \) at \( a_1 \), so that \( f^{-1} \) and \( f^{-q} \) have zeros of order \( qr_1 \) and \( q^2r_1 \) respectively at \( a_1 \). Therefore, if \( w \) has a pole at \( a_1 \),
\[
    \text{ord}_{a_1} h = \text{ord}_{a_1} f^{-1}w^{(s+1)q} + f^{-q} = q(s+1)\text{ord}_{a_1} w + qr_1 < 0.
\]

If \( w \) is a unit at \( a_1 \), then
\[
    \text{ord}_{a_1} h = \text{ord}_{a_1} f^{-1}w^{q(s+1)} + f^{-q} = -\text{ord}_{a_1} f = qr_1.
\]

If \( w \) has a zero at \( a_1 \), then
\[
    \text{ord}_{a_1} h = \text{ord}_{a_1} f^{-1}w^{q(s+1)} + f^{-q} = -q\text{ord}_{a_1} f = q^2r_1.
\]

Thus, at \( a_1 \), \( h \) either has a pole or a zero of degree at most \( q^2r_1 \). Now consider \( h^{-k} + z \). Since at \( a_1 \), we have that \( z \) has a pole of order greater than \( q^2kr_1 \),
\[
    \text{ord}_{a_1} (h^{-k} + z) = \text{ord}_{a_1} z = -(q^2 + 1).
\]
Therefore, by Lemma B.4.11, we know that $a_1$ will ramify completely in the extension $K(\beta_w)/K$. Hence, this extension is of degree $q$ as noted above. Since at least one prime is ramified completely and the extension is separable, the constant field of $K(\beta_w)$ is the same as the constant field of $K$. Thus $\alpha$ is of degree $q$ over $K(\beta_w)$, as promised.

For future use, also note that any valuation that is a zero of $h$ is also a pole of $(h^{-k} + z)$. Further, the order of $(h^{-k} + z)$ at any such valuation, except for $a_1$ is divisible by $q$ if and only if the order of $h$ at this valuation is divisible by $q$. Thus, if $h$ has a zero at some prime $t$ and $\text{ord}_t h \not\equiv 0 \mod q$ in $K$, then $t$ ramifies completely in the extensions $K(\beta_w)/K$.

We will now proceed to the proof of the second statement of the lemma. Note that as in Subsection 4.1.1 and the number field case, again, the existence of solutions $a_0, \ldots, a_{p-1} \in K(\beta_w)$ to (4.3.5) is equivalent to existence of $u \in K(\alpha, \beta_w)$ such that

$$N_{K(\alpha, \beta_w)/K}(u) = h. \tag{4.3.7}$$

Suppose that, as in Subsection 4.1.3 and the number field case, $w \in K$ has a pole at some $b_i$. Then in $K$,

$$\text{ord}_{b_i} h = \text{ord}_{b_i} (f^{-1}w q(s+1) + f^{-q}) = q(s + 1) \text{ord}_{b_i} w - s_i \not\equiv 0 \mod q.$$

Further,

$$\text{ord}_{b_i} h < 0.$$

Next observe the following. $h^{-k} + z \equiv b^q \not\equiv 0 \mod q$. Thus, $b_i$ does not divide the discriminant of the power basis of $\beta_w$ and therefore it does not ramify in the extension $K(\beta_w)/K$ by Lemma B.4.11. Further, since the polynomial $T^q - h^{-k} + z$ splits completely modulo $b_i$, by Lemma B.4.11, we conclude that $b_i$ splits completely in the extension $K(\beta_w)/K$ and the order of $h$ at any factor of $b_i$ is not divisible by $q$ in $K(\beta_w)$. Further, since there is no constant field extension, and $b_i$ is of degree 1 in $K$, each factor of $b_i$ will be of degree 1 in $K(\beta_w)$. Thus, since (4.3.2) still has no solution in $K(\beta_w)$, we conclude that (4.3.2) has no solution modulo any factor of $b_i$ in $K(\beta_w)$. Hence, again by Lemma B.4.11, every factor of $b_i$ in $K(\beta_w)$ remains prime in $K(\beta_w, \alpha)$ and (4.3.7) will have no solution in $K(\alpha, \beta_w)$. (See Subsection 4.1.2 again as in the number field case.)

Suppose now $w$ does not have a pole at any $b_i$ for any $i = 1, \ldots, m$. We will show that in this case (4.3.7) will have a solution in $K(\alpha, \beta_w)$. By the Strong Hasse Norm Principal applied to the function field case, it is enough to show that for all primes $t$ of $K$ we have that $h$ is a local norm. Note that
no prime ramifies in the extension $K(\alpha, \beta_w)/K(\beta_w)$. Thus, as discussed in Subsection 4.1.5 and in the number field case, if $h$ is a unit at some prime $t$ of $K$, it is automatically a local norm at $t$ by Lemma B.8.5. Suppose $t$ is a pole of $h$. Then either it is a factor of $\mathfrak{a}$ or it is a pole of $w$. Since $w$ has no pole at any factor of $\mathfrak{a}$, direct calculation assures us that $h$ will have a pole at every factor of $\mathfrak{a}$ of order divisible by $q$. On the other hand, if $t$ is a pole of $w$, then, again by direct calculation, one can see that $h$ will also have a pole at $t$ of order divisible by $q$.

Assume now that $t$ is a zero of $h$. Then by the argument above it is a pole of $h^{-k} + z$. Further, since $k \not\equiv 0 \pmod{q}$, for $t \neq a_1$, $\text{ord}_t h \not\equiv 0 \pmod{q}$ if and only $\text{ord}_t h^{-k} + z \not\equiv 0 \pmod{q}$. Thus, if $\text{ord}_t h \not\equiv 0 \pmod{q}$, $t$ is ramified completely in the extension $K(\beta_w)/K$. As we have discussed above, $a_1$ ramifies in the extension $K(\beta_w)/K$ under all circumstances. Hence, if $t_{K(\beta_w)}$ is a prime of $K(\beta_w)$ lying above $t$, then $\text{ord}_{t_{K(\beta_w)}} h \equiv 0 \pmod{q}$.

Summarizing the discussion above, we conclude that for every prime $t_{K(\beta_w)}$ of $K(\beta_w)$ we have that

$$h = \pi_{t_{K(\beta_w)}}^{bq} \epsilon_{t_{K(\beta_w)}},$$

where

$$\text{ord}_{t_{K(\beta_w)}} \pi_{t_{K(\beta_w)}} = 1,$$

$b$ is an integer and

$$\text{ord}_{t_{K(\beta_w)}} \epsilon_{t_{K(\beta_w)}} = 0.$$

For every prime $t_{K(\beta_w, \alpha)}$ of $K(\beta_w, \alpha)$, let $n_{t_{K(\beta_w, \alpha)}}$ be the local degree at the prime $t_{K(\beta_w)}$ below in $K(\beta_w)$, i.e.

$$n_{t_{K(\beta_w, \alpha)}} = [K(\beta_w, \alpha)_{t_{K(\beta_w, \alpha)}} : K(\beta_w)_{t_{K(\beta_w)}}].$$

Since $K$ contains $q$-th roots of unity, by Lemma B.4.11, the local degree is either 1 or $q$. If the local degree 1, then $h$ is automatically a norm. On the other hand if the local degree is $q$, then $\pi_{t_{K(\beta_w)}}^{bq}$ is a norm of $\pi_{t_{K(\beta_w)}}^{b}$ and as above, since the extension is not ramified, $\epsilon_{t_{K(\beta_w)}}$ is also a norm. Thus, $h$ is a $K(\beta_w)$-norm of an element from $K(\beta_w, \alpha)$.

We now state a corollary whose proof is completely analogous to Corollary 4.2.3.

4.3.3 Corollary.

The set of elements of $K$ integral at $\mathfrak{p}_i$ for $i = 1, \ldots, m$, is Diophantine over $K$.

The corollary above paves the way for the main result of this section.
4.3.4 Theorem.

Let \( M \) be a function field of positive characteristic \( p \) over a finite field of constants. Let \( p \) be any prime of \( M \). Then the set of elements of \( M \) integral at \( p \) is Diophantine over \( M \).

Proof.

The proof of this theorem is quite similar overall to the proof of Theorem 4.2.4, in particular in its use of “Going Up and Then Down Method”, but some details are different. Let \( q \neq p \) be another prime of \( M \). Let \( f \in K \) be an element with the divisor of the form \( \frac{p^c}{q^r} \) for some positive integers \( c, r \). (We can always take \( c = h_M \deg(q), r = h_M \deg p \).) Let \( q \) be a rational prime different from \( p \) and prime to \( rc \). Let \( M_1 = M(\xi_q) \), where \( \xi_q \) is a primitive \( q \)-th root of unity. By Lemma B.4.17, no prime of \( M \) will ramify in the extension \( M(\xi_q)/M \). Thus the divisor of \( f \) in this extension is of the form

\[
\prod_{i=1}^{n} p_i^{c_i} \prod_{j=1}^{m} q_j^{r_j},
\]

where \( p_1, \ldots, p_n \) are distinct factors of \( p \) in \( M(\xi_q) \), and \( q_1, \ldots, q_m \) are distinct factors of \( q \) in \( M(\xi_q) \). Let \( v \in M(\xi_q) \) be such that for all \( j \) we have that \( \text{ord}_{\xi_q} v \equiv 0 \mod q \), and for some \( b \neq 0 \), for all \( i \), we have that \( v \equiv b^q \mod p_i \). Such a \( v \) exists by the Strong Approximation Theorem. Let \( M_1 = M(\xi_q, \delta) \), where \( \delta \) is a root of the polynomial \( T^q - v \). By Lemma B.4.11, for all \( i \), we have that \( p_i \) splits completely into distinct factors, and for all \( j \), we have that \( q_j \) is completely ramified in the extension. Thus in \( M_1 \), the divisor of \( f \) is now of the form

\[
\prod_{i=1}^{n} \prod_{u=1}^{q} \xi_{i,u}^{r_{i,u}} \prod_{j=1}^{m} b_j^{r_j},
\]

where for all \( i \), we have that \( v_{i,1}, \ldots, v_{i,q} \) are all the distinct factors of \( p_i \), and for all \( j \), we have that \( v_j \) is the only factor of \( q_j \) in \( M_1 \). Finally, let \( C_{i,u} \) be the residue field of \( v_{i,u} \) and let \( C_j \) be the residue field of \( b_j \). Let

\[
K = MC_{1,1} \ldots C_{n,q}C_1 \ldots C_m.
\]

Then in \( K \), each prime factor of the divisor of \( f \) in \( M_1 \) will split into distinct factors of relative degree one by Lemma B.4.15 and Lemma B.4.16. Thus, in \( K \), the divisor of \( f \) will be of the form required by Notation 4.3.1, while the field \( K \) will contain the required roots of unity. By Corollary 4.3.3, the set \( I_K \) of elements of \( K \) integral at all the factors of \( p \) in \( K \) is Diophantine over \( K \). Thus, by Going Up and Then Down Method (see Subsection 2.1.17), \( I_K \cap M \) is Diophantine over \( M \). But \( I_K \cap M \) consists precisely of elements of \( M \) integral at \( p \).
4.4 **Divisibility of Order at Infinitely Many Primes Over Number Fields.**

In this section we take the first steps towards being able to say something about order at infinite sets of primes. What we mean by “divisibility of order at infinitely many primes” is a statement that for some rational prime $q$, the order of an element at primes of the field contained in an infinite set, is divisible by $q$ or is non-negative. As above, the proofs in the number field case and the function field case are very similar but not identical, primarily because in the function field case we can arrange for an extension to be unramified while it is not always possible in the number field case. As usual, we start with a notation list.

### 4.4.1 Notation.

- Let $K$ denote a number field, and let $\mathcal{P}(K)$ denote the set of non-archimedean primes of $K$.
- Let $q$ denote a prime number.
- Let $t$ denote a prime number equivalent to 1 modulo $q^2$ such that $K$ and $\mathbb{Q}(\xi_t)$, where $\xi_t$ is a primitive $t$-th root of unity, are linearly disjoint over $\mathbb{Q}$. (Such a prime exists by Theorem 5.9, Chapter IV of [37] and by Corollary B.3.11.)
- Let $T$ be the set of prime factors of the divisor of $t$ in $K$. Let $\mathfrak{T} = \prod_{t \in T} t$.
- Let $a_1, \ldots, a_k \in O_K$ be integers representing every equivalence class modulo $\mathfrak{T}q$.
- Let $\mathfrak{A}$ be the set of primes of $K$ such that $a \in \mathfrak{A}$ if and only if $a \not\in \mathfrak{T}$ and for some $i = 1, \ldots, k$, we have that $\text{ord}_a a_i \neq 0$.
- Let $\mathfrak{Q}$ be the set consisting of all the factors of the divisor of $q$ in $K$.
- Let $x \in K \setminus \{0\}$ be such that $\text{ord}_a x \geq 0$ for all $a \in \mathfrak{A}$.
- For $i = 1, \ldots, k$ and $x$ as above, let $\alpha_i(x) = \alpha_i \in \bar{\mathbb{Q}}$ be such that $\alpha_i^q = 1 + \frac{1}{a_i x}$. Further, if $1 + \frac{1}{a_i x}$ is a $q$-th power of an element in $K$, then let $\alpha_i(x) \in K$. (Here $\bar{\mathbb{Q}}$ is the algebraic closure of $\mathbb{Q}$.)
- Let $G_i = K(\alpha_i(x))$. 

63
Our first job is to establish the existence of a cyclic extension of $K$ to use with the Strong Hasse Norm principle.

### 4.4.2 Lemma.

There exists $\delta \in \tilde{\mathbb{Q}}$ such that $K(\delta)/K$ is a cyclic extension of degree $q$, $\delta$ and all of its conjugates are totally real, and the factors of the $K$-divisor of $t$ are the only primes possibly ramifying in this extension.

**Proof.**

By assumption we have that $K$ and $\mathbb{Q}(\xi_t)$ are linearly disjoint over $\mathbb{Q}$. Note further that $\mathbb{Q}(\xi_t + \xi_t^{-1})$ is a totally real cyclic extension of $\mathbb{Q}$ of degree $(t - 1)/2 \equiv 0 \mod q$. Next, if $\sigma$ is a generator of $\text{Gal}(\mathbb{Q}(\xi_t + \xi_t^{-1})/\mathbb{Q})$, then let $L$ be the fixed field of $\sigma^q$. In this case $L/\mathbb{Q}$ is a cyclic extension of $\mathbb{Q}$ of degree $q$. Let $\delta \in O_L$ be such that $L = \mathbb{Q}(\delta)$. Then $K(\delta)/K$ is a cyclic extension of degree $q$ by Lemma B.3.5, and $\delta$ and all of its conjugates are real. Since elements of $\mathcal{T}$ are the only primes dividing the discriminant of the power basis of $\xi_t$, these are the only primes possibly ramifying in the extension $K(\xi_t)/K$, by Proposition 8, Chapter III, Section 2 of [46], and therefore the only primes possibly ramifying in the extension $K(\delta)/K$, by Proposition B.1.12.

### 4.4.3 Notation.

From now on, let $\delta$ be a generator of a cyclic extension of degree $q$ over $K$ and let $\mathcal{V}$ be the set of all primes of $K$ not splitting in the extension $K(\delta)/K$ and not in $\mathcal{A} \cup \mathcal{Q}$.

Our next task is to consider the behavior of various primes in the extensions $G_i/K$, as well as the degrees of these extensions.

### 4.4.4 Lemma.

The following statements are true.

1. Either $[G_i : K] = q$ or $G_i = K$.

2. Suppose there exists $p \in \mathcal{V}$ such that $\text{ord}_p x < 0$. Then
   
   (a) $p$ will have a factor $\mathfrak{q}_i$ of relative degree 1 in the extension $G_i/K$ for all $i = 1, \ldots, k$. 

64
(b) \( \wp \) will not split in the extension \( G_i(\delta)/G_i \).

(c) \( [G_i(\delta) : G_i] = q \)

3. Let \( p \) be a prime of \( K \) such that \( \text{ord}_p a_i x > 0 \). Then either \( \text{ord}_p a_i x \equiv 0 \mod q \), or \( [G_i : K] = q \) and \( p \) is ramified completely in the extension. (Thus, in any case, if \( \wp \) is a prime above \( p \) in \( G_i \), then \( \text{ord}_\wp a_i x \equiv 0 \mod q \).)

4. For all \( x \in K \) and all \( i = 1, \ldots, k \), if \( [G_i(\delta) : G_i] \neq q \) then \( K(\delta) = G_i(\delta) = G_i \). If \( [G_i(\delta) : G_i] = q \) and \( K \neq G_i \) then the fields \( K(\delta) \) and \( G_i \) are linearly disjoint over \( K \).

5. Let \( q \) be a prime of \( K \) such that \( q \not\in V \cup A \cup T \). Let \( \Omega \) be a prime of \( G_i \) above \( q \). Then \( \Omega \) splits completely in the extension \( G_i(\delta)/G_i \).

6. If \( \Omega \) is a prime of \( G_i(\delta) \) ramified over \( G_i \), then it lies above a prime of \( T \).

**Proof.**

Consider the extension \( G_i/K \). Note that \( \alpha_i(x) \) is a root of the polynomial

\[
T^q - \left(1 + \frac{1}{a_i x}\right). \tag{4.4.1}
\]

and unless \( 1 + \frac{1}{a_i x} \) is a \( q \)-th power in \( K \), we have that \( \alpha_i(x) \) generates an extension of degree \( q \) over \( K \), by Lemma B.4.11. Thus given our assumptions, either \( G_i = K \) or \( [G_i : K] = q \).

Now let \( p \in V \) be a prime such that \( \text{ord}_p x < 0 \). If \( G_i = K \), then assertions (2a)–(2c) are trivially satisfied. Suppose now that \( [G_i : K] = q \) and observe that \( 1 + \frac{1}{a_i x} \equiv 1 \mod p \). Thus \( p \) does not ramify in the extension \( G_i/K \) by Lemma B.4.11, and by Lemma B.4.12, the power basis of \( \alpha_i(x) \) is an integral basis with respect to \( p \). Further we note that the equation in (4.4.1) has a root modulo \( p \). Therefore by Lemma B.4.13, \( p \) has factor \( \wp \) of relative degree 1 in \( G_i \). Also, by Lemma B.4.35, there exists \( \delta_p \in K(\delta) \) such that \( K(\delta) = K(\delta_p) \), the power basis of \( \delta_p \) is an integral basis of \( K(\delta_p) \) over \( K \) with respect to \( p \), and the monic irreducible polynomial of \( \delta_p \) over \( K \) remains irreducible over the residue field of \( p \). Thus, the monic irreducible polynomial of \( \delta_p \) over \( K \) remains irreducible over the residue field of \( \wp \) (and consequently over \( G_i \)). Hence, for any \( i \), by Lemma B.4.12, \( \wp \) does not split in the extension \( G_i(\delta_p)/G_i \) and \( [G_i(\delta) : G_i] = q \).
Next let \( q \) be a prime of \( K \) such that \( \text{ord}_q a_i x > 0 \). Then we have two possibilities: either
\[
\text{ord}_p a_i x \equiv 0 \mod q
\]
or \( 1 + \frac{1}{a_i x} \) is not a \( p \)-th power in \( K \) and \( p \) is ramified completely in the non-trivial extension \( G_i/K \). In any case, if \( \mathfrak{p} \) is a factor of \( p \) in \( G_i \), then \( \text{ord}_p a_i x \equiv 0 \mod q \).

Next note that if \( [G_i(\delta) : G_i] \neq q \), then \( K(\delta) \) and \( G_i \) are not linearly disjoint over \( K \) by Lemma B.3.1. Since \( K(\delta)/K \) is a Galois extension, by Lemma B.3.3, the lack of linear disjointness implies that \( K(\delta) \cap G_i \) is strictly bigger than \( K \). As we are dealing with extensions of prime degree, we must conclude that in this case \( G_i = K(\delta) = G_i(\delta) \). On the other hand, if \( [G_i(\delta) : G_i] = q \), then by Lemma B.3.1 we conclude that \( G_i \) and \( K(\delta) \) are linearly disjoint over \( K \).

Now, let \( q \notin \mathcal{V} \cup \mathcal{A} \cup \mathcal{T} \) and assume \( K \neq G_i \). Let \( \mathfrak{q} \) be a prime of \( G_i \) above \( q \) and let \( \mathfrak{q} \) be the \( G_i(\delta) \)-prime above \( \mathfrak{q} \). By Lemma B.4.1, it is enough to show that the decomposition group of \( \mathfrak{q} \) over \( G_i \) is trivial. Let \( \sigma \in \text{Gal}(G_i(\delta)/G_i) \setminus \{\text{id}\} \). Without loss of generality, we can assume \( G_i(\delta) \neq G_i \), and, therefore, \( G_i \) and \( K(\delta) \) are linearly disjoint over \( K \). Then by Lemma B.3.5, \( \sigma \) restricted to \( K(\delta) \) is not the identity element of \( \text{Gal}(K(\delta)/K) \). Note that \( \mathfrak{q} \cap K(\delta) \) lies above \( q \). Since \( q \) splits completely in \( K(\delta) \), the decomposition group of \( \mathfrak{q} \cap K(\delta) \) is trivial and therefore \( \sigma|_{K(\delta)}(\mathfrak{q} \cap K(\delta)) \neq \mathfrak{q} \cap K(\delta) \). Hence \( \sigma(\mathfrak{q}) \neq \mathfrak{q} \) and the decomposition group of \( \mathfrak{q} \) is trivial.

Next suppose \( \mathfrak{q} \) is a prime of \( G_i(\delta) \) ramified in the extension \( G_i(\delta)/G_i \). Assuming the extension is not trivial, we must conclude that \( \mathfrak{q} \) is completely ramified and the inertia group of \( \mathfrak{q} \) over \( G_i \) is of size \( q \), equal to \( \text{Gal}(G_i(\delta)/G_i) \). In this case, however, the inertia group of \( \mathfrak{q} \cap K(\delta) \) is equal to \( \text{Gal}(K(\delta)/K) \) and therefore, \( \mathfrak{q} \cap K(\delta) \) is completely ramified in the extension \( K(\delta)/K \).

Next we prove the main technical result of this section.

**4.4.5 Proposition.**

The equation
\[
N_{G_i(\delta)/G_i}(z) = a_i x
\]
has a solution \( z \in G_i(\delta) \) for some \( i \) if and only if the order of every pole of \( x \) at primes of \( \mathcal{V} \) is divisible by \( q \).
Proof.

Suppose that for some \( p \in \mathcal{V} \) we have that \( \text{ord}_p x < 0 \). Then, given our assumptions on \( x \), we know that \( p \not\in \mathcal{A} \). Further, by Lemma B.4.3 and Lemma 4.4.4, for any \( i = 1, \ldots, k \), we know that \( a_i x \) cannot be a norm in the extension \( G_i(\delta)/G_i \) unless \( \text{ord}_\mathfrak{p} x \equiv 0 \mod q \), where \( \mathfrak{p} \) is a factor of \( p \) in \( G_i \) of relative degree 1 over \( p \), and \( \mathfrak{p} \) does not split in the extension \( G_i(\delta)/G_i \). But since \( \mathfrak{p} \) is not ramified over \( p \), we have that

\[
\text{ord}_\mathfrak{p} x \equiv 0 \mod q \Leftrightarrow \text{ord}_p x \equiv 0 \mod q.
\]

Suppose now that for all \( p \in \mathcal{V} \) we have that \( \text{ord}_p x < 0 \Rightarrow \text{ord}_p x \equiv 0 \mod q \).

Let \( q \) be a prime of \( G_i \). Let \( \mathfrak{Q} \) be a prime above it \( G_i(\delta) \). We would like to determine the possible values of local degree \( [(G_i(\delta))_{\mathfrak{Q}} : (G_i)_q] \), where \( (G_i(\delta))_{\mathfrak{Q}}, (G_i)_q \) are completions of \( G_i(\delta) \) and \( G_i \) under \( \mathfrak{Q} \) and \( q \) respectively. First of all, if the global degree is equal to 1, then the local degree is 1. Secondly, if the global degree is not 1, by Lemma 4.4.4, the global degree is \( q \) and the global extension is cyclic. Thus, by Lemma B.4.1, for any prime \( q \) of \( G_i \), either the relative degree and the ramification degree are 1, or the relative degree is \( q \) and the ramification degree is 1, or the ramification degree is \( q \) and the relative degree is 1. In the cases where the local degree is 1, we know that \( a_i x \) is automatically a local norm. In the cases where the prime is unramified and the relative degree is \( q \), it is enough to arrange, as in the preceding sections, that the order of \( a_i x \) at the prime is divisible by \( q \). Finally, in the case of ramified primes, it is enough to demonstrate that \( a_i x \) is a \( q \)-th power locally. Keeping this plan in mind, let’s examine \( a_i x \). We will divide all the primes of \( G_i \) into five categories.

1. Primes of \( G_i \) lying above the primes in \( \mathcal{P}(K) \setminus \mathcal{T} \) and such that they do not occur in the divisor of \( a_i x \).

2. Primes of \( G_i \) lying above the primes of \( \mathcal{P}(K) \setminus \mathcal{T} \) and such that they are zeros of \( a_i x \).

3. Primes of \( G_i \) lying above the primes in \( \mathcal{V} \) and such that they are poles of \( a_i x \).

4. Primes of \( G_i \) lying above the primes in \( \mathcal{P}(K) \setminus (\mathcal{V} \cup \mathcal{A} \cup \mathcal{T}) \) and such that they are poles of \( a_i x \).

5. Primes of \( G_i \) lying above the primes of \( \mathcal{T} \).
First of all, by Lemma 4.4.4, any prime of $G_i$ ramifying in the extension $G_i(\delta)/G_i$ lies above a $\mathcal{T}$-prime of $K$. Also from Lemma 4.4.4 we know that for any $G_i$-prime $\mathfrak{p}$ from Categories 1 – 3, for all $i = 1, \ldots, k$, we have that $\text{ord}_{\mathfrak{p}} a_i x \equiv 0 \mod q$, and thus $a_i x$ is a local norm at such a prime. If $\mathfrak{p}$ is a prime of Category 4, then by Lemma 4.4.4, $\mathfrak{p}$ splits completely in the extension $G_i(\delta)/G_i$ and therefore $a_i x$ is a local norm at any such prime for any $i$ as above.

Finally, for some $i = 1, \ldots, k$, we have that $a_i x$ is a $q$-th power in $K_t$ for all $t \in \mathcal{T}$. Indeed, for every $t \in \mathcal{T}$ we can write $x = \varepsilon(t) \pi_t^{q r}$, where $\varepsilon(t)$ is a unit at $t$, $\text{ord}_t \pi_t = 1$, $l \in \mathbb{Z}$, and $0 \leq r < q$. So we can pick $a_i$ such that for all $t \in \mathcal{T}$, we have that $a_i \equiv \pi_t^{q r} \mu_t \mod t^q$ and $\mu_t \equiv \varepsilon^{-1}_t \mod t$. Then $a_i x \pi_t^{-(l+1)q} \equiv 1 \mod t$ and by a version of Hensel’s Lemma (see Lemma B.8.3), $a_i x$ is a $q$-th power in $K_t$ for all $t \in \mathcal{T}$. Therefore, by choosing a correct $a_i$, we can make sure that $a_i x$ is a norm locally at any prime potentially ramified in the extension $G_i(\delta)/G_i$.

Finally, we need to account for infinite primes. If a completion of $G_i$ is $\mathbb{C}$, then of course every element of the completion is a norm (since the local degree is 1). If a completion of $G_i$ is $\mathbb{R}$, then the completion of $G_i(\delta)$ is also $\mathbb{R}$, since all the conjugates of $\delta$ are real. Thus the local degree is 1 again and every element is a norm.

We are now ready to state the main theorem of this section.

**4.4.6 Theorem.**

Let $\mathcal{W} = P(K) \setminus \mathcal{A}$. Then the set

$$A_\mathcal{V} = \{ h \in O_{K,\mathcal{W}} | \forall p \in \mathcal{V}, \text{ord}_p h \geq 0 \lor \text{ord}_p h \equiv 0 \mod q \}$$

is Diophantine over $K$.

**Proof.**

The proof of this proposition is similar to the proof of Corollary 4.2.3 but we have a complication: $[G_i(\beta) : G_i]$ and $[G_i : K]$ can be either 1 or $q$. We will start before with the norm polynomial.

$$N(X_0, \ldots, X_{q-1}) = \prod_{j=1}^{q} \sum_{i=0}^{q-1} X_i \sigma_j(\delta)^i,$$
where $\sigma_1 = \text{id}, \ldots, \sigma_{q-1}$ are all the automorphisms of $\mathbb{Q}(\delta)$. Note that all the coefficients of $N(X_0, \ldots, X_{q-1})$ are in $K(\delta)$ but are invariant under the action of $\text{Gal}(K(\delta)/K)$ and therefore are actually in $K$. We are interested in solving

$$N(X_0, \ldots, X_{q-1}) = a_i x,$$  \hspace{1cm} (4.4.5)$$

with $X_0, \ldots, X_{q-1} \in G_i$. It is clear that we need to consider two cases: $G_i(\delta) \neq G_i$ and $G_i(\delta) = G_i$. In the first case the equation in (4.4.5) has solutions $X_0, \ldots, X_{q-1} \in G_i$ if and only if the equation in (4.4.2) has solution $z \in G_i(\delta)$. Suppose now, that $G_i = G_i(\delta)$. Then $G_i = K(\delta)$ and $G_i$ contains all the conjugates of $\delta$ over $K$. Keeping this in mind consider the following linear system:

$$
\begin{pmatrix}
1, \sigma_1(\delta), \ldots, \sigma_1(\delta)^{q-1} \\
1, \sigma_2(\delta), \ldots, \sigma_2(\delta)^{q-1} \\
\vdots, \ldots, \ldots, \\
1, \sigma_q(\delta), \ldots, \sigma_q(\delta)^{q-1}
\end{pmatrix}
\begin{pmatrix}
X_0 \\
X_1 \\
\vdots \\
X_{q-1}
\end{pmatrix}
= 
\begin{pmatrix}
a_i x \\
1 \\
\ldots \\
1
\end{pmatrix}
$$  \hspace{1cm} (4.4.6)$$

Note that the determinant of the system is non-zero, because its square is the discriminant of the the power basis of $\delta$ over $K$. Therefore this system can be solved in $G_i$ and the solution will satisfy the equation in (4.4.5).

Summarizing the discussion, we can now assert that the equation in (4.4.5) has solutions $X_0, \ldots, X_{q-1}$ in $G_i$ if and only if the equation in (4.4.2) has a solution $z \in G_i(\delta)$, which happens if and only if $x \in A_i$. Now the assertion of the Theorem follows from Lemma B.7.5.

We will now address the issue of making the set $\mathcal{V}$ bigger.

4.4.7 Theorem.

Let $K$ be a number field. Let $q$ be a prime. Then for any $\epsilon > 0$, there exists a set $\mathcal{V}$ of $K$-primes of Dirichlet density greater than $1 - \epsilon$ and a finite set $\mathcal{A}$ such that the set

$$A_{q,\mathcal{V}} = \{ h \in O_K, \forall p \in \mathcal{V}, \text{ord}_p h \geq 0 \lor \text{ord}_p h \equiv 0 \text{ mod } q \},$$  \hspace{1cm} (4.4.7)$$

where $\mathcal{V} = \mathcal{P}(K) \setminus \mathcal{A}$, is Diophantine over $K$. (For definition of Dirichlet density the reader is referred to Section B.5 of the Number Theory Appendix.)

Proof.

Let $t_1, \ldots, t_n$ be prime numbers such that $t = t_i$ satisfies the conditions of Notation 4.4.1. For each $i = 1, \ldots, n$, define $A_i$ and $\mathcal{V}_i$ as $\mathcal{A}$ and $\mathcal{V}$ in
Notation 4.4.1 and 4.4.3 respectively. Let $\mathcal{V} = \bigcup_{i=1}^{n} \mathcal{V}_i$, let $\mathcal{A} = \bigcup_{i=1}^{n} \mathcal{A}_i$, and let $\mathcal{W} = \mathcal{P}(K) \setminus \mathcal{A}$. Then by Theorem 4.4.6 and from the fact that an intersection of Diophantine sets is Diophantine, the set

$$A_q = \{ x \in O_K \mid \forall p \in \mathcal{V}, \operatorname{ord}_p x \geq 0 \lor \operatorname{ord}_p x \equiv 0 \mod q \}$$

is Diophantine over $K$. To finish the proof of the theorem, it is enough to show that the natural density of $\mathcal{V}$ is greater than $1 - \varepsilon$ for sufficiently large $n$, since $K(\xi_i)$ and $K(\xi_j, j = 1, \ldots, n, j \neq i)$ are linearly disjoint over $K$. (Linear disjointness is a consequence of an argument similar to the one used to prove Lemma B.3.10.) This is done in Lemma B.5.7.

We next consider the function field version of the results above.

### 4.5 Divisibility of Order at Infinitely Many Primes Over Function Fields.

**4.5.1 Proposition.**

Let $q$ be a rational prime and let $K$ be a function field over a finite field of constants of characteristic $p > 0$, $p \neq q$. Let $h \in K$, let $\alpha$ in the algebraic closure of $K$ be the root of the equation $T^q - (1 + h^{-1})$, let $\beta$ be an element of the algebraic closure of $C_K$, the constant field of $K$, of degree $q$ over $C_K$, let $G = K(\alpha)$, let $\mathcal{W}$ be the set of all $K$-primes not splitting in the extension $K(\beta)/K$, and consider the following norm equation.

$$\mathcal{N}_{G(\beta)/G} z = h \quad (4.5.1)$$

Then this equation has a solution $z \in G(\beta)$ if and only if for all primes $p \in \mathcal{W}$, either $h$ is integral at $p$ or $\operatorname{ord}_p h \equiv 0 \mod q$.

**Proof.**

The proof of this proposition is very similar to the proof of Proposition 4.4.5, but the situation is actually simpler because, by Lemma B.4.17, there are no ramified primes in the extension $G(\beta)/G$. We leave the details to the reader.

We now state the function field analog of Theorem 4.4.6.
4.5.2 Theorem.

Let \( q \) be a rational prime and let \( K \) be a function field over a finite field of constants of characteristic \( p > 0, p \neq q \). Let \( \beta \) be an element of the algebraic closure of \( C_K \), the constant field of \( K \), of degree \( q \) over \( C_K \). Let \( \mathcal{W} \) be the set of all primes of \( K \) not splitting in the extension \( K(\beta)/K \). Then the set
\[
A_{\mathcal{W}} = \{ h \in K | \forall \mathfrak{p} \in \mathcal{W}, \text{ord}_\mathfrak{p} h \geq 0 \lor \text{ord}_\mathfrak{p} h \equiv 0 \mod q \} \tag{4.5.2}
\]
is Diophantine over \( K \).

(The proof of this theorem is almost identical to the proof of Theorem 4.4.6.)

Finally, we show that the Dirichlet density of the set of “covered” primes is arbitrarily close to 1. (For a definition of Dirichlet density over function fields the reader is again referred to Section B.5 of the Number Theory Appendix.)

4.5.3 Theorem.

Let \( q \) be a rational prime and let \( K \) be a function field over a finite field of constants of characteristic \( p > 0, p \neq q \). Then for any \( \varepsilon > 0 \), there exists a set \( V \) of \( K \)-primes of density greater than \( 1 - \varepsilon \) such that the set
\[
A_{q,V} = \{ h \in K | \forall \mathfrak{p} \in V, \text{ord}_\mathfrak{p} h \geq 0 \lor \text{ord}_\mathfrak{p} h \equiv 0 \mod q \} \tag{4.5.3}
\]
is Diophantine over \( K \).

Proof.

Let \( n \) be any positive integer. The field of constants of \( K \), as any finite field, has an extension of degree \( q^n \), and this extension is cyclic. (See Section 5, Chapter VII of [47].) Let \( K_0 = K \subset K_1 \subset \ldots \subset K_n \) be the corresponding tower of cyclic extensions with \( [K_{i+1}:K_i] = q \). Let \( \mathcal{W}_i \) be a set of primes of \( K_i \) not splitting in the extension \( K_{i+1}/K_i \). Then the set
\[
A_{\mathcal{W}_i,K_i} = \{ h \in K_i | \forall \mathfrak{p} \in \mathcal{W}_i,K_i, \text{ord}_\mathfrak{p} h \geq 0 \lor \text{ord}_\mathfrak{p} h \equiv 0 \mod q \} \tag{4.5.4}
\]
is Diophantine over \( K_i \). Let \( \mathcal{W}_{i,K} \) be the set of \( K \)-primes lying below the primes in the set \( \mathcal{W}_i,K_i \). Let
\[
A_{\mathcal{W}_i,K} = \{ h \in K | \forall \mathfrak{p} \in \mathcal{W}_i,K, \text{ord}_\mathfrak{p} h \geq 0 \lor \text{ord}_\mathfrak{p} h \equiv 0 \mod q \}
\]
Then \( A_{\mathcal{W}_i,K} = A_{\mathcal{W}_i,K_i} \cap K \) and by “Going Up and Then Down” method, \( A_{\mathcal{W}_i,K} \) is Diophantine over \( K \). Let \( \mathcal{W}_K = \bigcup_{i=1}^{n} \mathcal{W}_i,K \). Then from properties of Diophantine definitions we can conclude that
\[
A = \bigcap_{i=1}^{n} A_{\mathcal{W}_i,K} = \{ h \in K | \forall \mathfrak{p} \in \mathcal{W}_K, \text{ord}_\mathfrak{p} h \geq 0 \lor \text{ord}_\mathfrak{p} h \equiv 0 \mod q \}
\]
is also Diophantine over $K$. Further, by Lemma B.5.8, for $n$ sufficiently large, $\mathcal{W}_K$ has the desired Dirichlet density.
Chapter 5

Bound Equations for Number Fields and Their Consequences.

This chapter is devoted to existential definability of bounds on the height of a number field element. We will consider two ways of bounding the height. The first method (due to Denef in [18]) relies on quadratic forms and is most effective over totally real fields. The second method relies on divisibility and thus depends on the choice of the ring. The influence of divisibility depends on whether any primes are allowed to occur in the denominator of the divisors of elements of the ring. We will discuss this aspect of the matter in great detail below. Denef was also the first to use the divisibility method for bounding height over the rings of integers in the context of existential definability (see [18] again). The author extended Denef’s divisibility method for use with bounds in rings of algebraic numbers. These kinds of bounds were used in [103], [105], [110] and in a slightly modified way in [73].

5.1 Real Embeddings.

In this section we show how to use quadratic forms to impose bounds on archimedean valuations when the corresponding completion of the number field is \( \mathbb{R} \). The following lemma and its corollary constitute the technical foundation of the method. They are taken from [18].

5.1.1 Lemma.

Let \( K \) be a number field. Let \( x \in K \). Let \( x = x_1, \ldots, x_n \) be all the conjugates of \( x \) over \( \mathbb{Q} \). Let \( c \in K \), and let \( c_1 = c, \ldots, c_n \) be all the conjugates of \( c \) over \( \mathbb{Q} \). Suppose \( c_i < 0 \) whenever \( x_i < 0 \). Then there exist \( y_1, \ldots, y_4 \in K \) such that \( x = y_1^2 + y_2^2 + cy_3^2 + y_4^2 \).
Proof.

By the Hasse-Minkowskii Theorem, a quadratic form represents an algebraic number over a number field if and only if it represents the number locally. (See [64] for more details on Hasse-Minkowskii Theorem.) Any quadratic form in four variables over a local field is universal, that is, it represents any element of the field (see [64]). So the real embeddings are the only ones we have to check. However, if for some \( i \) we have that \( x_i \geq 0 \), then \( x_i = (\sqrt{x_i})^2 + 0^2 + c_i 0^2 + 0^2 \). On the other hand if \( x_i < 0 \), then \( c_i < 0 \). Thus, \( x_i/c_i \) is a square in the completion of the corresponding embedding of \( K \).

5.1.2 Corollary.

Let \( K \) be a number field, let \( \mathcal{V} \) be any subset of its non-archimedean primes. Let \( \sigma: K \to \mathbb{C} \) be any real embedding of \( K \) into \( \mathbb{C} \). Then the set

\[
\{(x, y) \in K^2 | \sigma(x) \geq \sigma(y)\}
\]

has a Diophantine definition over \( O_{K, \mathcal{V}} \).

Proof.

It is enough to consider the case of \( y = 0 \). Let \( c \in K \) be such that \( \sigma(c) > 0 \) and \( \tau(c) < 0 \) for any real embedding \( \tau \) of \( K \) not equal to \( \sigma \). (Such a \( c \) exists by the Strong Approximation Theorem.) Then \( \sigma(x) \geq 0 \) if and only if \( x = y_1^2 + y_2^2 + c y_3^2 + y_4^2 \) by Lemma 5.1.1. Thus the corollary follows from Note 2.2.5.

5.2 Using Divisibility in the Rings of Algebraic Integers.

In this section we start the discussion of divisibility as a method for bounding heights over number fields. As will become clear below, divisibility produces the best results when used over the rings of integers. Thus, it is over the rings of integers that we consider this method first. (We remind the reader that a discussion of rings of integers and \( S \)-integers of number fields can be found in the Number Theory appendix (Appendix B).)

It turns out that the foundation of the divisibility method can be found in solving some linear systems as we do in the following lemma.
5.2.1 Lemma.

Let $K$ be a number field of degree $n$ over $\mathbb{Q}$. Let $x, y \in O_K \setminus \{0\}$ and assume that for $i = 0, \ldots, n$, we have that $(l_i - x)\big| y$ in the ring of integers of $K$, where $l_0 = 0, l_1, \ldots, l_n$ are distinct natural numbers. Then there exists a constant $C$, depending on $n, l_1, \ldots, l_n$ only, such that all the coefficients of the characteristic polynomial of $x$ over $\mathbb{Q}$ are less than $C|N_{K/\mathbb{Q}}(y)|$.

Proof.

If $(l_i - x)\big| y$ then $N_{K/\mathbb{Q}}(l_i - x) = c_i N_{K/\mathbb{Q}}(y)$, where $c_i \in \mathbb{Q}$ and $|c_i| < 1$. On the other hand,

$$N_{K/\mathbb{Q}}(l_i - x) = \prod_{j=1}^{n}(l_i - \sigma_j(x)) = a_0 + a_1 l_i + \ldots + l_i^n,$$

where $\sigma_1 = \text{id}, \ldots, \sigma_n$ are all the embeddings of $K$ into $\mathbb{C}$ and $F(T) = a_0 + a_1 T + \ldots + a_{n-1} T^{n-1} + T^n$ is the characteristic polynomial of $x$ over $\mathbb{Q}$. Thus, considered together, $n + 1$ equations $F(l_i) = c_i N_{K/\mathbb{Q}}(y)$ can be viewed as a system of $n + 1$ linear equations in variables $a_0, \ldots, a_{n-1}, a_n = 1$. In matrix form this system looks as follows:

$$
\begin{pmatrix}
1 & \ldots & 0 & 0 \\
1 & \ldots & l_1^{n-1} & l_1^n \\
\vdots & \ldots & \ldots & \ldots \\
1 & \ldots & l_{n-1}^{n-1} & l_{n-1}^n \\
1 & \ldots & l_n^{n-1} & l_n^n
\end{pmatrix}
\begin{pmatrix}
a_0 \\
a_1 \\
\vdots \\
a_{n-1} \\
1
\end{pmatrix}
= \begin{pmatrix}
c_0 N_{K/\mathbb{Q}}(y) \\
c_1 N_{K/\mathbb{Q}}(y) \\
\vdots \\
c_{n-1} N_{K/\mathbb{Q}}(y) \\
c_n N_{K/\mathbb{Q}}(y)
\end{pmatrix}.
$$

(5.2.1)

Observe that the determinant of this system is a non-zero Vandermonde determinant whose value depends on the choice of constants $l_1, \ldots, l_n$ only. If we solve this system using Cramer’s rule we will obtain the following expression for each $a_i$:

$$a_i = \frac{1}{\det} \begin{vmatrix}
1 & \ldots & c_0 N_{K/\mathbb{Q}}(y) & \ldots & 0 \\
1 & \ldots & c_1 N_{K/\mathbb{Q}}(y) & \ldots & l_1^n \\
\vdots & \ldots & \ldots & \ldots & \ldots \\
1 & \ldots & c_{n-1} N_{K/\mathbb{Q}}(y) & \ldots & l_{n-1}^n \\
1 & \ldots & c_n N_{K/\mathbb{Q}}(y) & \ldots & l_n^n
\end{vmatrix},
$$

(5.2.2)
where the column \((c_j N_{K/Q}(y)), j = 0, \ldots, n\) replaced the \(i\)-th column of the original matrix, and therefore we have that

\[
a_i = N_{K/Q}(y) - \begin{vmatrix}
1 & \ldots & c_0 & \ldots & 0 \\
1 & \ldots & c_1 & \ldots & l_1^n \\
\vdots & \ddots & \vdots & \ddots & \vdots \\
1 & \ldots & c_{n-1} & \ldots & l_{n-1}^n \\
1 & \ldots & c_n & \ldots & l_n^n \\
\end{vmatrix}
\]  

(5.2.3)

Since \(|c_i| < 1\), we can conclude that our lemma holds.

A quick corollary of this lemma is the following fact.

### 5.2.2 Corollary.

Let \(K/E\) be an extension of number fields, let

\[
\Omega = \{\omega_1, \ldots, \omega_m\} \subset O_K
\]

be a basis of \(K\) over \(E\). Let \(x, y \in O_K \setminus \{0\}\) and assume that for \(i = 0, \ldots, n\), where \(n = [K : \mathbb{Q}]\), we have that \((l_i - x)\big|_y\) for distinct natural numbers \(l_0 = 0, l_1, \ldots, l_n\). Then there exists a constant \(\bar{C} \in \mathbb{Q}\), depending on \(n, l_1, \ldots, l_n\) and \(\Omega\) only, such that the following statements are true.

1. If \(\sigma : K \rightarrow \mathbb{C}\) is an embedding, then \(|\sigma(x)| \leq \bar{C}|N_{K/Q}(y)|\).

2. We can write \(x = \sum_{i=1}^m b_i \omega_i\), with \(b_i \in E\), \(|\sigma(b_i)| \leq \bar{C}|N_{K/Q}(y)|\) for any \(\sigma\) - embedding of \(K\) into \(\mathbb{C}\).

**Proof.**

From the preceding lemma we can conclude that all the coefficients of the characteristic polynomial of \(x\) over \(\mathbb{Q}\) are bounded by \(C|N_{K/Q}(y)|\), where \(C\) is a positive constant depending on \(n, l_1, \ldots, l_n\) only. Let

\[
F(T) = a_0 + a_1 T + \ldots + a_{n-1} T^{n-1} + T^n
\]
be this polynomial. Then for all embeddings \( \sigma \) of \( K \) into \( \mathbb{C} \), we have that
\[
\sigma(x)^n = -a_0 - a_1 \sigma(x) - \ldots - a_{n-1} \sigma(x)^{n-1}.
\]
If \( |\sigma(x)| > 1 \), then
\[
|\sigma(x)| \leq |a_0| + |a_1| + \ldots + |a_{n-1}| \leq nC|N_{K/Q}(y)|.
\]
Thus, letting \( \tilde{C} = \max(1, nC) \), we can conclude that \( |\sigma(x)| \leq \tilde{C}|N_{K/Q}(y)| \).

Next let \( x_1 = x, \ldots, x_n \) be all the conjugates of \( x \) over \( \mathbb{Q} \). Without loss of generality assume that \( x_1, \ldots, x_m \) are all the conjugates of \( x \) over \( E \) and let \( \omega_{1,1} = \omega_1, \ldots, \omega_{1,m} \) be all the conjugates of \( \omega_1 \) over \( E \). Then consider the following linear system of equations in variables \( b_1, \ldots, b_m \).
\[
x_j = \sum_{i=1}^{m} b_i \omega_{i,j}, j = 1, \ldots, m, b_i \in E.
\]
If we solve this system using Cramer’s rule as in Lemma 5.2.1 and keep in mind the bounds for \( x_1, \ldots, x_m \), we will conclude that \( |b_i| \leq \tilde{C}|N_{K/Q}(y)| \) for some positive constant \( \tilde{C} \) depending on \( \tilde{C} \) and \( \Omega \) only, again exactly in the same fashion as in Lemma 5.2.1.

Next let \( \sigma \) be an embedding of \( K \) into \( \mathbb{C} \). Applying \( \sigma \) to the system above, we get
\[
\sigma(x_j) = \sum_{i=1}^{m} \sigma(b_i) \sigma(\omega_{i,j}), j = 1, \ldots, m, b_i \in E.
\]
Thus, we can obtain a bound as above for \( \sigma(b_i) \) for any \( \sigma \) – embedding of \( K \) into \( \mathbb{C} \) and all \( i = 1, \ldots, m \).

**Note.**

Before we finish this discussion of bounds, we should note that assuming \( y \) is not a unit, we can replace the bound \( \tilde{C}|N_{K/Q}(y)| \) in Lemma 5.2.1 and Corollary 5.2.2 by \( |N_{K/Q}(y)|^c \), for sufficiently large positive \( c \in \mathbb{N} \). It is often useful to have a bound not just for \( |\sigma(b_i)| \) but for \( |N_{K/Q}(Db_i)| \), where \( D \) is a constant depending on the basis. It is clear that we can increase \( c \) to obtain the inequality \( |N_{K/Q}(Db_i)| < |N_{K/Q}(y)|^c \).

**5.3 Using Divisibility in Bigger Rings.**

In this section we show how we can modify the divisibility method to make it work over some rings \( \mathcal{O}_{K, \mathcal{W}} \), where \( \mathcal{W} \) is not empty.
5.3.1 When is division really division?

Let $x, y \in O_K \setminus \{0\}$ and suppose

$$x \mid y \text{ in } O_{K,W}. \quad (5.3.1)$$

In general we cannot conclude that (5.3.1) implies that $x \mid y \text{ in } O_K$. However if we assume that the divisor of $x$ has no primes from $W$, then the implication is valid.

From the observation above, it follows that we need a mechanism for producing elements of $O_{K,W}$ without primes of $W$ in the numerators of their divisors. Here is one way to accomplish this.

5.3.2 Avoiding Primes Allowed in the Denominator of the Divisors.

Let $M/K$ be a finite extension of number fields. Let $\alpha \in O_K$ be a generator of this extension. Let $F(T)$ be the monic irreducible polynomial of $\alpha$ over $K$. Let $W$ consist of all the primes which do not divide the discriminant of $\alpha$, and do not have relative degree 1 factors in $M$. Then for all $p \in W$, for all $x \in K$ we have that $\text{ord}_p F(x) \leq 0$. (This follows from Lemma B.4.18.)

We are now ready to adjust our divisibility method for use in bigger rings.

5.3.3 Lemma.

Let $K/E$ be a number field extension of degree $s$, let $[K : \mathbb{Q}] = n$. Let $\gamma \in O_K$ generate $K$ over $E$. Let $G_u(T) \in O_K[T], u = 1, \ldots, n + 1$ be distinct monic irreducible over $K$ polynomials. Let $\frac{\alpha}{\beta} \in K$ with $\alpha, \beta \in O_K$ and relatively prime to each other. Let $y \in O_K \setminus \{0\}$ be such that $y$ is not an integral unit, and

$$\frac{y}{G_u(\alpha/\beta - l_i)} \in O_K, i = 0, \ldots, n \text{ deg}(G_u) : \mathbb{Q}, u = 1, \ldots, n + 1, \quad (5.3.2)$$

where $l_0 = 0, \ldots, l_z, z = \max_u([n \text{ deg}(G_u) : \mathbb{Q}])$ are distinct natural numbers. Let

$$N_{K/\mathbb{Q}}(\beta)\alpha = e_0 + e_1\gamma + \ldots + e_{s-1}\gamma^{s-1} \quad (5.3.3)$$

Then there exists a constant $c > 0$ depending on $l_0, \ldots, l_z, K, G_u(T)$ only such that

$$|N_{K/\mathbb{Q}}(D_e_i)| < |N_{K/\mathbb{Q}}(y)|^c, i = 0, \ldots, s - 1, \quad (5.3.4)$$
where $D$ is the discriminant of the power basis of $\gamma$.

**Proof.**

Let $C$, be defined as in Lemma B.10.8 with $\bar{\tau}$ being the set of roots of $G_u$. Since $G_1, \ldots, G_{n+1}$ are irreducible and distinct, the sets of roots of polynomials $G_1, \ldots, G_{n+1}$ are pairwise disjoint. Then $C > 0$ and by Lemma B.10.8 applied to conjugates of $\alpha/\beta$ over $\mathbb{Q}$ in place of $z_1, \ldots, z_n$, for some $u = 1, \ldots, n+1$, for any $\tau$, a root of $G_u(T)$, and any $\sigma$, embeddings of $K$ into $\mathbb{C}$, we have that $|\sigma(\alpha/\beta) - \tau| > C/2$. For this $u$, denote the field generated by a root $\tau$ of $G_u(T)$, and any $\sigma$, embeddings of $K$ into $\mathbb{C}$, we have that $|\sigma(\alpha/\beta)| \leq \frac{C}{2}$. For this $u$, denote the field generated by a root $\tau$ of $G_u(T)$ by $M$, denote $G_u$ by $H$, and let $q = \deg(G_u)$. Then in $M$ we have that

$$\frac{y}{\prod_{\tau}(\alpha/\beta - l_i - \tau)} = \frac{y\beta^q}{\prod_{\tau}(\alpha - l_i\beta - \tau)} \in O_M. \quad (5.3.5)$$

Since $(\alpha, \beta) = 1$ in $O_K$, it follows that $(\beta, \alpha - l_i \beta - \tau \beta) = 1$ in $O_M$. Thus, for each $i$ we have that

$$\frac{y}{\alpha - l_i \beta - \tau \beta} \in O_M.$$

Therefore,

$$|N_{M/Q}(\alpha - l_i \beta - \tau \beta)| \leq |N_{K/Q}(y)|^q,$$

$$|N_{M/Q}(\beta)| |N_{M/Q}(\alpha/\beta - l_i - \tau)| \leq |N_{K/Q}(y)|^q.$$

Using the fact that $|N_{M/Q}(\beta)| \geq 1$, we can conclude that

$$|N_{M/Q}(\alpha/\beta - l_i - \tau)| \leq |N_{K/Q}(y)|^q. \quad (5.3.6)$$

On the other hand, using $i = 0$ and the inequality $|\sigma(\alpha/\beta) - \sigma(\tau)| > C/2$, applied to all embeddings $\sigma$ of $M$ into $\mathbb{C}$, we can conclude that

$$|N_{K/Q}(\beta)| = |N_{M/Q}(\beta)|^{1/q} \leq (C/2)^{-[K:Q]|N_{K/Q}(y)|}.$$

From (5.3.6), by an argument similar to the one used to prove Lemma 5.2.1 and Corollary 5.2.2, we can conclude that there exists a positive constant $\tilde{C}$, depending on $l_0, \ldots, l_z, K$, and $G_1(T), \ldots, G_{n+1}(T)$ only, such that

$$|\sigma(\alpha/\beta)| \leq \tilde{C}|N_{K/Q}(y)|^q \quad (5.3.7)$$

for all $\sigma$, embeddings of $M$ into $\mathbb{C}$, and

$$N_{K/Q}(\beta)\alpha/\beta = e_0 + e_1 \gamma + \ldots + e_{s-1} \gamma^{s-1}, \quad (5.3.8)$$

where $e_0, e_1, \ldots, e_{s-1} \in E$, while for all embeddings $\sigma$ of $K$ into $\mathbb{C}$ we have that

$$|\sigma(e_j)| \leq \hat{C}|N_{K/Q}(y)|^{q+1} \quad (5.3.9)$$
where \( \hat{C} \) is a positive constant depending on \( \gamma, l_0, \ldots, l_z, K, \) and \( G_1(T), \ldots, G_{n+1}(T) \) only. Since \( y \) is not an integral unit and \( |N_{K/Q}(y)| \geq 2 \), for some positive constant \( c \) depending on \( \gamma, l_0, \ldots, l_z, K, \) and \( G_1(T), \ldots, G_{n+1}(T) \) only, we have that

\[
|N_{K/Q}(D_e)| < |N_{K/Q}(y)|^c,
\]  

(5.3.10)

where \( D \), as above, is the discriminant of the power basis of \( \gamma \) over \( E \).

5.3.4 Corollary.

Let \( K, E, s, n, \gamma, G_1(T), \ldots, G_{n+1}(T), z, \alpha, \beta, l_0, \ldots, l_z, e_0, \ldots, e_{s-1} \) be again as above. Assume also that \( K/E \) is Galois and \( G_1(T), \ldots, G_{n+1}(T) \in O_E[T] \). Let

\[
\mathcal{W} \text{ be a set of non-archimedean primes of } K \text{ such that for all } u = 1, \ldots, n+1, \text{ all } x \in K, \text{ all } p \in \mathcal{W}, \text{ we have that } \operatorname{ord}_p G_u(x) \leq 0. \]

Let \( v \in O_K, \mathcal{W} \{0\} \) be such that \( v \) is not a unit of \( O_K, \mathcal{W} \) and is such that

\[
\frac{v^{h_K}}{G_u(\alpha/\beta - l_i)} \in O_K, \mathcal{W}, i = 0, \ldots, n \deg(G_u), u = 1, \ldots, n + 1,
\]  

(5.3.11)

where \( h_K \) is the class number of \( K \).

Then there exists a constant \( c > 0 \) depending on \( l_0, \ldots, l_z, K, \) and \( G_1(T), \ldots, G_{n+1}(T) \) only such that \( v^{h_K} = yw, y \in O_K, \) the divisor of \( y \) has no primes from \( \mathcal{W} \), the divisor of \( w \) consists of primes in \( \mathcal{W} \) only, and

\[
|N_{K/Q}(D_e)| < |N_{K/Q}(y)|^c, i = 0, \ldots, s - 1,
\]  

(5.3.12)

where \( D \) is the discriminant of the power basis of \( \gamma \) over \( E \).

Proof.

Given our assumptions on \( \mathcal{W} \) and \( G_1, \ldots, G_{n+1}, \) for any prime \( p \in \mathcal{W} \) we have that \( \operatorname{ord}_p G_u(\alpha/\beta - l_i) \leq 0. \) Thus, for all \( u, \) all the primes in the numerator of the divisor of \( G_u(\alpha/\beta - l_i) \) must be canceled by the numerator of the divisor of \( v^{h_K}. \) Note that \( v^{h_K} = yw, \) where the divisor of \( y \) is integral and is a product of powers of all the primes outside \( \mathcal{W} \) occurring in the divisor of \( v^{h_K}, \) while \( w \) has a divisor composed of primes from \( \mathcal{W} \) only. Then, for all \( u \) we have that \( \frac{y}{G_u(\alpha/\beta - l_i)} \in O_K. \) Now the corollary follows from Lemma 5.3.3.

We finish this section with a special case of the corollary above.

5.3.5 Corollary.

Let \( K, E, s, n, \gamma, G_1(T), \ldots, G_{n+1}(T), z, \alpha, \beta, l_0, \ldots, l_z, e_0, \ldots, e_{s-1} \) be again as above. Assume also that \( K/E \) is Galois and \( G_1(T), \ldots, G_{n+1} \in O_E[T]. \) Let
$v \in E \cap O_{K,W} \setminus \{0\}$ be such that $v$ is not a unit of $W$ and is such that
\[
\frac{v^{h_E}}{G_u(\alpha/\beta - l_i)} \in O_{K,W}, \ i = 0, \ldots, n \deg(G_u), u = 1, \ldots, n + 1,
\]
where $h_E$ is the class number of $E$.

Then there exists a constant $c > 0$ depending on $\gamma, l_0, \ldots, l_z, K,$ and $G_1(T), \ldots, G_{n+1}$ only, such that $v^{h_E} = yw, y \in O_E$, the divisor of $y$ has no primes from $W$, the divisor of $w$ consists of primes in $W$ only, and
\[
|N_{K/Q}(D_{e_i})| < |N_{K/Q}(y)|^c, \ i = 0, \ldots, s - 1,
\]
(5.3.14)

**Proof.**

Let $\bar{W}$ be the closure of $W$ over $E$. Given our assumptions on the extension $K/E, W$ and $G_1, \ldots, G_{n+1}$, for any prime $p \in \bar{W}$, we have that $\text{ord}_p G_u(\alpha/\beta - l_i) \leq 0$. Thus, as above, for all $u$, all the primes in the numerator of the divisor of $G_u(\alpha/\beta - l_i)$ must be canceled by the numerator of the divisor of $v^{h_E}$. However, since $v \in E$, we can write $v^{h_E} = yw$, with $y, w \in E$, the divisor of $y$ integral and a product of powers of all the primes outside $\bar{W}$ occurring in the divisor of $v^{h_E}$, while $w$ has a divisor composed of primes from $\bar{W}$ only. Then, as before, for all $u$ we have that $\frac{y}{G_u(\alpha/\beta - l_i)} \in O_K$ and this corollary also follows from Lemma 5.3.3.
Chapter 6

Units of Rings of \( \mathcal{W} \)-integers of Norm 1.

\( \mathcal{W} \)-units play an important role in construction of Diophantine definitions over number fields. In this chapter we discuss some properties of these units.

6.1 What Are the Units of the Rings of \( \mathcal{W} \)-integers?

6.1.1 Definition.

Let \( K \) be a number field. Let \( \mathcal{W} \) be a collection of its non-archimedean primes. Let \( x \in K \) be such that its divisor is a product of powers of elements of \( \mathcal{W} \). Then \( x \) is called a \( \mathcal{W} \)-unit. If \( \mathcal{W} \) is empty, then a \( \mathcal{W} \)-unit is just an integral unit of \( K \), i. e. an algebraic integer whose multiplicative inverse is also an algebraic integer.

Next we list some useful properties of these units. The first one is a generalization of a well-known Dirichlet Unit Theorem.

6.1.2 Proposition.

Let \( K \) and \( \mathcal{W} \) be as above. Then \( \mathcal{W} \)-units form a multiplicative group. If the number of primes in \( \mathcal{W} \) is finite, then the rank of this group is equal to the rank of the integral unit group plus the number of elements in \( \mathcal{W} \). (See the generalized version of the Dirichlet Unit Theorem in \([64]\).)

The next lemma is a direct consequence of the definition of the rings of \( \mathcal{W} \)-integers. (See Definition \( \text{B.1.20} \).)
6.1.3 Lemma.
Let $K$ and $\mathcal{W}$ be again as above. Then the only invertible elements of $O_{K,\mathcal{W}}$ (or the only units of $O_{K,\mathcal{W}}$) are the $\mathcal{W}$-units.

The next lemma is important in making sure that the divisibility conditions discussed in the chapter on the bound equations over number fields can be satisfied.

6.1.4 Lemma.
Let $A$ be any integral divisor of a number field $K$ relatively prime to any prime in a set of non-archimedean $K$-primes $\mathcal{W}$. Then there exists a positive $k(A) = k \in \mathbb{N}$ such that for any natural number $l \equiv 0 \mod k$, for any $\mathcal{W}$-unit $\varepsilon$, it follows that $\varepsilon^l - 1 \equiv 0 \mod A$.

Proof.
The lemma follows from the fact that $O_{K,\mathcal{W}}$ modulo $\mathfrak{a}$ is a finite ring (by Proposition B.1.28) with a finite multiplicative group. We can set $k$ equal to the order of this group.

Using the proposition above we derive a corollary which will have a role in the “Weak Vertical Method” described in Chapter 7.

6.1.5 Corollary.
Let $E$ be a subfield of $K$. Let
$$\Omega = \{1, \omega_2, \ldots, \omega_n\} \subset O_K$$
be a basis of $K$ over $E$. Let $\mathcal{S}$ be set of $K$-primes closed under conjugation over $E$. (By “closed under conjugation” we mean that given a set of all $K$-factors of an $E$-prime, either the whole set is in $\mathcal{S}$ or no element of the set is in $\mathcal{S}$. This way the expression “closed under conjugation” makes sense even if $K/E$ is not Galois.) Let $\mathfrak{B}$ be any integral divisor of $E$ relatively prime to any prime of $\mathcal{S}$. Then there exists a positive $l = l(\mathfrak{B}) \in \mathbb{N}$, such that for any positive $m \equiv 0 \mod l$, for any $\mathcal{S}$-unit $\varepsilon$ we have that
$$\varepsilon^m = c_1 + c_2 \omega_2 + \ldots + c_n \omega_n,$$
where for all $i = 1, \ldots, n$ it is the case that $c_i \in O_{K,\mathcal{S}} \cap E$ with $c_1 \equiv 1 \mod \mathfrak{B}$, and $c_i \equiv 0 \mod \mathfrak{B}$ for $i = 2, \ldots, n$. 
Proof.

Indeed, let \( \mathcal{D} = \mathcal{D}_1 \mathcal{D}_2 \) be the \( E \)-divisor of the discriminant of \( \Omega \), where \( \mathcal{D}_1 \) is an integral divisor, prime to all the primes in \( \mathcal{T} \), while all the primes comprising \( \mathcal{D}_2 \) are in \( \mathcal{T} \). (Such a factorization of \( \mathcal{D} \) exists given our assumptions on \( \mathcal{T} \).) Let

\[
I = k(\mathcal{D}_1^{h_E} \mathfrak{B}^{h_E})
\]

where \( h_E \) is the class number of \( E \). Then by definition of \( k(\mathcal{D}_1^{h_E} \mathfrak{B}^{h_E}) \), we have that for any \( m \equiv 0 \mod l \), it follows that

\[
\varepsilon^m - 1 \equiv 0 \mod \mathcal{D}_1^{h_E} \mathfrak{B}^{h_E}.
\]

Let \( B \in E \) be an element whose divisor is \( \mathfrak{B}^{h_E} \). Consider

\[
(\varepsilon^m - 1)B^{-1} \equiv 0 \mod \mathcal{D}_1^{h_E}
\]

in \( \mathcal{O}_{K, \mathcal{T}} \). By Lemma B.4.12 of the appendix,

\[
(\varepsilon^m - 1)B^{-1} = a_1 + a_2 \omega_2 + \ldots + a_n \omega_n,
\]

where for any \( q \notin \mathcal{T} \) we have that \( \text{ord}_q a_i \geq 0 \) for \( i = 1, \ldots, n \). Further,

\[
\varepsilon^m - 1 = Ba_1 + Ba_2 \omega_2 + \ldots + Ba_n \omega_n,
\]

and thus,

\[
\varepsilon = c_1 + c_2 \omega_2 + \ldots + c_n \omega_n,
\]

where \( c_i \in E \), and for any \( K \)-prime \( p \notin \mathcal{T} \), we have that

\[
\text{ord}_p (c_1 - 1) \geq \text{ord}_p B \geq \text{ord}_p \mathfrak{B},
\]

while for \( i = 2, \ldots, n \) we know that

\[
\text{ord}_p c_i \geq \text{ord}_p B \geq \text{ord}_p \mathfrak{B}.
\]

The next lemma discusses a property of integral units of some fields.

\subsection{6.1.6 Lemma.}

Let \( M/K \) be a number field extension of degree 2 where \( K \) is totally real and \( M \) is totally complex. Then there exists \( m \in \mathbb{N} \) such that for every integral unit \( \varepsilon \) in \( M \) and every \( k \equiv 0 \mod m \) we have that \( \varepsilon^k \in \mathcal{O}_K \).
Proof.

Dirichlet Unit Theorem implies that the integral unit group of $K$ is of the same rank as the integral unit group of $M$. Since the integral unit groups are finitely generated, this means that there exists $m \in \mathbb{N}$ such that for every integral unit $\varepsilon$ in $M$ and every $k \equiv 0 \mod m$, we have that $\varepsilon^k \in O_K$. (See [37] for a discussion of Dirichlet Unit Theorem.)

6.2 Norm Equations of Units.

In this section we again encounter norm equations, though we will put them to a different use. (Compare this section to Chapter 4.)

6.2.1 Proposition.

Let $M/K$ be a number field extension. Let $\mathcal{W}_K$ be a subset of non-archimedean primes of $K$. Let $\mathcal{W}_M$ be the set of all the primes of $M$ lying above the primes of $\mathcal{W}_K$. Consider the following equation

$$N_{M/K}(x) = 1, \quad (6.2.1)$$

where $x \in M$. Then the following statements are true.

1. The set

$$\{x \in O_{M,\mathcal{W}_M} : N_{M/K}(x) = 1\} \quad (6.2.2)$$

is a multiplicative group. In particular, if $\varepsilon \in O_{M,\mathcal{W}_M}$ is a solution to the equation (6.2.1), then $\varepsilon^n$ is also a solution. Further

$$\frac{\varepsilon^n - 1}{\varepsilon - 1} \equiv n \mod (\varepsilon - 1) \text{in } \mathbb{Z}[\varepsilon]. \quad (6.2.3)$$

2. If $\mathcal{W}_K$ is a finite set, then the rank of the group defined in (6.2.2) is equal to the difference of the ranks of the $\mathcal{W}_M$-unit group in $M$ and the $\mathcal{W}_K$-unit group in $K$.

3. If a $K$-prime $q$ does not split in the extension $M/K$ and $x$ is any solution of (6.2.1), then $\text{ord}_Q x = 0$ for the sole factor $Q$ of $q$ in $M$.

4. If $t$ is a prime of $K$ and $\mathcal{I}_1, \mathcal{I}_2$ are two factors of $t$ in $M$. Then (6.2.1) has a solution $x$ with the divisor of the form $\frac{\mathcal{I}_1^{r_1}}{\mathcal{I}_2^{r_2}}$. 

85
5. Let \( \mathcal{V}_M \) be the set of all the primes of \( \mathcal{U}_M \) lying above primes of \( \mathcal{U}_K \) splitting in the extension \( M/K \). Then the only solutions to (6.2.1) in \( O_M, \mathcal{U}_M \) are the \( \mathcal{V}_M \)-units. (In particular, if \( \mathcal{V}_M \) is empty, then all the solutions are integral.)

**Proof.**

1. The first assertion of the lemma is true because non-zero \( \mathcal{U}_M \)-integers and solutions to the norm equation (6.2.1) form multiplicative groups.

2. The second assertion of the lemma is true because the norm map is a homomorphism from the group of \( \mathcal{U}_M \)-units to the group of \( \mathcal{U}_K \)-units. The image of the homomorphism is of the same rank as the group of \( \mathcal{U}_K \)-units. Indeed, if \( \delta \) is a \( \mathcal{U}_K \)-unit, then \( \delta^{[M:K]} \) is in the image of the group of \( \mathcal{U}_M \)-units under the norm map. Thus the image of the norm map is of finite index in the group of \( \mathcal{U}_K \)-units.

3. The third assertion of the lemma can be derived from the following considerations. Let \( \prod \mathfrak{p}_i^{a_i}, a_i \in \mathbb{Z} \) be the divisor of a solution in \( M \) to (6.2.1). Let \( p_i \) be the prime below \( \mathfrak{p}_i \) in \( K \). Then \( \prod p_i^{f_i a_i} \), where \( f_i \) is the relative degree of \( \mathfrak{p}_i \) over \( p_i \), is the trivial divisor. (See Chapter I, Section 8 of [37].) Thus, for each \( i \), there exists \( j \), such that \( p_i = p_j \). In other words, the prime \( p_i = p_j \) splits in the extension \( M/K \).

4. To see that the fourth statement of the lemma is true, note the following. If \( h_M \) is the class number of \( M \), then \( M \) has an element with the divisor of the form \( \prod \mathfrak{f}_1^{f_1 a_1}, \mathfrak{f}_2^{f_2 a_2} \), where \( f_1, f_2 \) are relative degrees of \( \mathfrak{f}_1 \) and \( \mathfrak{f}_2 \) over \( K \) respectively. The norm of this divisor is trivial. So if \( x \in M \) has the divisor of this form, the \( K \)-norm of \( x \) is an integral unit \( \delta \). Let \( y = \delta^{-1} x^{[M:K]} \). Then \( N_{M/K}(y) = 1 \).

5. The final statement of the lemma can be derived from Part 3 and the following fact. Any solution in \( O_M, \mathcal{U}_M \) to (6.2.1) is a unit of the ring \( O_M, \mathcal{U}_M \) and thus must be a \( \mathcal{U}_M \)-unit.

Next we consider the norm equations of units in more specific situations.

**6.2.2 Lemma.**

Let \( K \) be a totally real field of degree \( n \) over \( \mathbb{Q} \) and let \( M/K \) be a degree 2 extension. Let \( \overline{\mathbb{Q}} \) denote a fixed algebraic closure of \( \mathbb{Q} \). Then there exists \( d \in O_K \) satisfy the following conditions:
• \( d \) is not a square of \( K \).

• For all embeddings \( \sigma : M \rightarrow \bar{Q} \) such that \( \sigma(M) \not\subset \mathbb{R} \) we have that \( \sigma(d) > 0 \).

• For all embeddings \( \sigma : M \rightarrow \bar{Q} \) such that \( \sigma(M) \subset \mathbb{R} \) we have that \( \sigma(d) < 0 \).

Further the rank of the multiplicative group
\[
\Xi_M = \{ \varepsilon \in O_{M(\sqrt{d})} : N_{M(\sqrt{d})/M}(\varepsilon) = 1 \}
\]
is equal to the rank of the multiplicative group
\[
\Xi_K = \{ \varepsilon \in O_{K(\sqrt{d})} : N_{K(\sqrt{d})/K}(\varepsilon) = 1 \},
\]
and for some non-zero \( k \in \mathbb{N} \), depending on \( M, K \) and \( d \) only, for any \( \varepsilon \in \Xi_M \) we have that \( \varepsilon^k \in \Xi_K \).

**Proof.**

First of all we observe the following. Since \( M/K \) is an extension of degree 2, for some \( a \in K \) we have that \( M = K(\sqrt{a}) \). Therefore for any \( \sigma \) as above, \( \sigma(M) \) is real if and only if \( \sigma(a) > 0 \). Hence, the last two conditions on \( d \) can be restated in the following form: for any embedding \( \tau : K \rightarrow \bar{Q} \) we have that \( \tau(a) \) and \( \tau(d) \) have different signs. Now existence of \( d \) follows by the Strong Approximation Theorem (Theorem B.2.1.)

Next note that by construction of \( d \), any embedding of \( M(\sqrt{d}) \) into \( \bar{Q} \) will be non-real. Since \([M(\sqrt{d}) : \mathbb{Q}] = 4n\), by Dirichlet Unit Theorem, the rank of the integral unit group of \( M(\sqrt{d}) \) is \( 2n - 1 \). Proceeding further, let \( r \) be the number of embeddings \( \tau \) of \( K \) into \( \bar{Q} \) such that \( \tau(a) > 0 \), and let \( s \) be the number of embeddings \( \tau \) such that \( \tau(a) < 0 \). Obviously \( r + s = n \). Further, \( M \) will have \( 2r \) real and \( 2s \) non-real embeddings. Thus the rank of the integral unit group of \( M \) is \( 2r + s - 1 \) and the rank of \( \Xi_M \) is \( 2n - 1 - 2r - s + 1 = s \).

On the other hand, \( K(\sqrt{d}) \) will have \( 2s \) real and \( 2r \) non-real embeddings into \( \bar{Q} \). So that the rank of the integral unit group of \( K(\sqrt{d}) \) is \( 2s + r - 1 \). Thus the rank of \( \Xi_K \) is \( 2s + r - 1 - r - s + 1 = s \) also, and the second assertion of the lemma holds.

To prove the last assertion, by Lemma B.3.1, it is enough to show that the fields \( M \) and \( K(\sqrt{d}) \) are linearly disjoint over \( K \). Indeed, linear disjointness of \( M \) and \( K(\sqrt{d}) \) over \( K \) would imply that any element \( x \in K(\sqrt{d}) \) satisfies the same irreducible polynomial over \( K \) as over \( M \), and therefore has the same conjugates over \( M \) as over \( K \). The last statement implies that
\[
N_{M(\sqrt{d})/M}(x) = N_{K(\sqrt{d})/K}(x).
\]
and therefore, $\Xi_K \subseteq \Xi_M$. Further, since extensions $M/K$ and $K(\sqrt{d})$ are both Galois, by Lemma B.3.3, to show that $K(\sqrt{d})$ and $M$ are linearly disjoint over $K$, it is enough to show that $M \cap K(\sqrt{d}) = K$ or, in other words, it is enough to show that $K(\sqrt{d}) \neq M$. But by construction of $d$ one of these fields is real while the other is not. Therefore, they cannot coincide.

### 6.3 Pell Equation.

Under certain circumstances we can say more about the integral solutions to unit norm equations. In this section we look at a very particular norm equation for an extension of degree 2: Pell equation. More specifically, we are interested in equations of the following form:

$$X^2 - (a^2 - 1)Y^2 = 1. \quad (6.3.1)$$

If $K$ is a number field and $X, Y, a \in K$ with $a^2 - 1$ not a square of $K$, then (6.3.1) asserts that an element $X + \sqrt{a^2 - 1}Y$ of $K(\sqrt{a^2 - 1})$ has $K$-norm equal to 1. Solutions to this equation have very nice properties described below, and these properties serve as the foundation for the construction of a Diophantine definition of $\mathbb{Z}$ over the rings of integers of totally real number fields and fields with exactly one pair of non-real embeddings. Pell equation also played a prominent role in a solution of the original Hilbert’s Tenth Problem. For more detail on the role of this remarkable equation see a very nice article of Martin Davis ([12]). Finally we note that the material presented in this section originally appeared in [15], [68], and [95].

Some properties of Pell equation manifest themselves over any number field, while others depend on the field. We start with the first kind after introducing the initial notation set.

### 6.3.1 Notation.

- Let $K$ denote a number field of degree $n$ over $\mathbb{Q}$.
- Let $a \in O_K$ denote a $K$-integer such that $d = a^2 - 1$ is not a square in $K$.
- Let $a_1 = a, \ldots, a_n$ be all the conjugates of $a$ over $\mathbb{Q}$.
- If $d = a^2 - 1$ is a positive real number, then let $\sqrt{a^2 - 1}$ have the usual meaning, i.e. the positive real number whose square is $a^2 - 1$. Otherwise, let $\sqrt{a^2 - 1}$ be one of the two complex numbers whose square is $(a^2 - 1)$. 88
• Let $\delta = \delta(a) = \sqrt{a^2 - 1}$.
• Let $\epsilon = \epsilon(a) = a + \delta(a)$.
• Let $x_m = x_m(a), y_m = y_m(a) \in O_K, m \in \mathbb{Z}$ be such that
  \[ x_m + \delta y_m = \epsilon^m. \]

Now we list the more general properties of Pell equation.

6.3.2 Lemma.

The following statements are true.

1. $h \mid m \Rightarrow y_h \mid y_m$ for all $h, m \in \mathbb{Z} \setminus \{0\}$.
2. $x_{2km} \equiv \pm 1 \mod x_m$ for all $k, m \in \mathbb{Z}$.
3. $x_m \mid y_{2km}$ for all $k, m \in \mathbb{Z}$.
4. $y_m(a) \equiv m \mod (a - 1)$ for all $m \in \mathbb{Z}$.
5. For $k, l \in \mathbb{N}$ we have that $x_{k \pm l} = x_k x_l \pm (a^2 - 1)y_k y_l$.
6. For $k, l \in \mathbb{N}$ we have that $y_{k+l} = x_k y_l \pm x_l y_k$.
7. $x_{2m \pm j} \equiv \pm x_j \mod x_m$ for all $j, m \in \mathbb{Z}$.
8. If $b, c \in O_K, \delta(b) \notin K$, and $a \equiv b \mod c$, then for all $m \in \mathbb{Z}$ we have
   \[ x_m(a) \equiv x_m(b) \mod c \]
   and
   \[ y_m(a) \equiv y_m(b) \mod c. \]

Proof.

First of all, observe that for any $m \in \mathbb{Z}$ we have that $x_{-m} = x_m$ and $y_{-m} = -y_m$. So without loss of generality we can assume that all the indices are non-negative. Next we note that the properties listed above will follow from the formulas for $y_m(a)$ and $x_m(a)$ in terms of $m$ and $a$ or in terms of $x_h(a)$ and
\( y_h(a) \) when \( h \mid m \), which we obtain simply by using Binomial Theorem. Indeed let \( h \mid m \), let \( l = \frac{m}{h} \) and observe the following.

\[
(a + \delta)^m = (x_h + \delta y_h)^l = \sum_{i=0}^{l} \binom{l}{i} x_h^{l-i} y_h^i \delta^i.
\]

Thus, if \( l \) is even, we have

\[
(a + \delta)^m = \sum_{j=0}^{l/2} \binom{l}{2j} x_h^{l-2j} y_h^{2j} d^j + \frac{(l-2)/2}{l} \sum_{j=0}^{l/2} \binom{l}{2j+1} x_h^{l-2j-1} y_h^{2j+1} d^j.
\]

If \( l \) is odd, then

\[
(a + \delta)^m = \sum_{j=0}^{(l-1)/2} \binom{l}{2j} x_h^{l-2j} y_h^{2j} d^j + \frac{(l-1)/2}{l} \sum_{j=0}^{(l-1)/2} \binom{l}{2j+1} x_h^{l-2j-1} y_h^{2j+1} d^j.
\]

Hence, we have the formulas

\[
x_m = \sum_{0 \leq j \leq l/2} \binom{l}{2j} x_h^{m-2j} y_h^{2j} d^j, \tag{6.3.2}
\]

and

\[
y_m = \sum_{0 \leq j \leq (l-1)/2} \binom{l}{2j+1} x_h^{m-2j-1} y_h^{2j+1} d^j. \tag{6.3.3}
\]

Thus Part 1 follows directly from (6.3.3).

To see that Part 2 holds, observe that

\[
x_{2mk} = x_m^{2k} + \binom{m}{2k-2} x_m^{2k-2} d y_m^2 + \ldots + (dy_m^2)^k \equiv (-1)^k \text{ mod } x_m.
\]

Similarly, we observe that

\[
y_{2mk} = 2k x_m^{2k-1} y_m + \ldots + 2k x_m y_m^{2k-1} d^{k-1} \equiv 0 \text{ mod } x_m,
\]

and Part 3 holds.

Next set \( h = 1 \), \( x_h = a \), \( y_h = 1 \), and observe that

\[
y_m = \sum_{0 \leq j \leq (m-1)/2} \binom{m}{2j+1} a^{m-2j-1} d^j. \tag{6.3.4}
\]

Thus, modulo \( a - 1 \) we have that \( y_m \equiv \binom{m}{1} = m \) and Part 4 is proved.
Now we note that Part 5 and Part 6 follow from the fact that for natural numbers \( l \) and \( k \) we have that \( \varepsilon_{l\pm k} = \varepsilon_l \varepsilon_{\pm k} \). Thus,

\[
x_{2m \pm j} = x_m x_j \pm (a^2 - 1)y_m y_j = (x_m^2 + (a^2 - 1)y_m^2)x_j \pm (a^2 - 1)(2x_m y_m)y_j \\
= (2x_m^2 - 1)x_j \pm (a^2 - 1)(2x_m y_m)y_j \equiv -x_j \mod x_m
\]

Part 8 follows by induction using addition formulas.

Our next step is to specialize our discussion to a class of number fields. We will now need a second notation set.

### 6.3.3 Notation.

- From now on till the end of this section \( K \) will denote a totally real number field (abbreviated as "tr" in the future) or a number field with exactly one pair of non-real embeddings (abbreviated as "opnr" in the future).
- Let \( \sigma_1 = \text{id}, \ldots, \sigma_n : K \rightarrow \mathbb{C} \) be all the embeddings of \( K \) into \( \mathbb{C} \).
- If \( K \) has exactly one pair of non-real embeddings, then assume that \( K, \sigma_2(K) \not\subseteq \mathbb{R} \), and for any \( x \in K \) we have \( \sigma_2(x) \) equal to \( \bar{x} \), the complex conjugate of \( x \).
- Let \( I_0(K) = \{1\} \), if \( K \) is tr, and let \( I_0(K) = \{1, 2\} \) if \( K \) is opnr.
- Let \( a \) be a \( K \)-element which satisfies the following inequalities:
  
  - \(|a_i| > 2^{n+2} \) for \( i \in I_0 \),
  - \( 0 < a_i < \frac{1}{2} \), \( i \not\in I_0 \),

  where \( \sigma_i(a) = a_i \).
- Let \( M = K(\delta) \). (Given our assumptions on \( a \), it follows immediately that if \( K \) is tr, then \( M \) has exactly two real embeddings, and if \( K \) is opnr, then \( M \) is totally complex.)
- For \( i = 1, \ldots, n \) and \( j = 1, 2 \), let \( \sigma_{i,j} \) be one of the two extensions of \( \sigma_i \) to \( M \). Also let \( \sigma_{1,1} = \text{id} \).
- For \( i = 1, \ldots, n \), let \( \varepsilon_i = \sigma_{i,1}(\varepsilon) \) if \( |\sigma_{i,1}(\varepsilon)| \geq 1 \), and let \( \varepsilon_i = \sigma_{i,2}(\varepsilon) \) if \( |\sigma_{i,1}(\varepsilon)| < 1 \).
- For \( i = 1, \ldots, n \), let \( \delta_i = \sigma_{i,1}(\delta) \). Then \( \sigma_{i,2}(\delta) = -\delta_i \).
• Let \( C \) be a real constant defined in Lemma 6.3.6. Let \( e \in \mathbb{N} \) be such that
\[
|\epsilon_1^e| > \frac{4|\delta_1|m_0}{Cn-m_0},
\]
where \( m_0 = |I_0| \).

• Let \( G = \left\{ u - \delta v : u, v \in O_K, u^2 - (a^2 - 1)v^2 = 1 \right\} \).

• Let \( H = \{ \mu \in O_M : N_{M/K}(\mu) = 1 \} \).

• Let \( U_M, U_K \) be the groups of integral units of \( M \) and \( K \) respectively.

First we need to establish some facts concerning the size of the absolute value of all the conjugates of \( \delta(a) \) and \( \epsilon(a) \) in \( H \).

### 6.3.4 Lemma.

The following inequalities hold:

1. \(|a_i|/2 < |\sigma_{i,j}(\delta)| < |a_i| + 1\), where \( i \in I_0(K), j = 1, 2; \)

2. \(\frac{1}{2} < |\sigma_{i,j}(\delta)| < 1\), for \( i \notin I_0(K), j = 1, 2. \)

3. Let \( \mu \in H \). Then for \( i \notin I_0 \) we have that \(|\sigma_{i,j}(\mu)| = 1\). Further, if \( \mu \) is not a root of unity, then either \(|\mu| > 1\) or \(|\mu^{-1}| > 1\).

4. \(|a| - \sqrt{|a^2 - 1|} < 1\)

5. Assuming \(|\epsilon| > 1\), we have that \(|a| < |\epsilon| < 2|a|\).

6. \( \epsilon(a) \) is not a root of unity.

**Proof.**

The proof follows directly from our assumptions. Indeed, note that since \(|a_i| > 2^{2n+2}\) for \( i \in I_0(K) \) with \( n \geq 2 \), we have that \( \frac{3}{4}|a_i|^2 > 1 \) for such an \( i \).

Thus, we conclude that
\[
|a_i|^2/4 < |a_i|^2 - 1 \leq |\sigma_{i,j}(\delta)|^2 = |a_i^2 - 1| \leq |a_i|^2 + 1 < (|a_i| + 1)^2,
\]
and the first assertion of the lemma holds.

Next, let \( i \notin I_0(K) \). Then
\[
\frac{3}{4} < 1 - a_i^2 < 1,
\]
and the second assertion of the lemma holds.
and for \( j = 1, 2 \) we have \( \frac{1}{2} < |\sigma_{ij}(\delta)| < 1 \).

Finally, let \( \mu \in H \). Then \( \mu = x - y\delta \), with \( x, y \in K \). If \( i \not\in I_0 \), then \( \sigma_{ij}(\delta) = \pm \sqrt{\sigma_i(a)^2 - 1} \), where \( \sigma_i(a) \in \mathbb{R} \) and \( 0 < \sigma_i(a) < \frac{1}{2} \). Thus, for \( i \not\in I_0 \), we have that \( \sigma_i(a)^2 - 1 < 0 \) and \( \pm \delta \in i\mathbb{R} \). Since, \( \sigma_i(K) \subset \mathbb{R} \), we conclude that

\[
\sigma_{i,1}(\mu) = \sigma_i(x) - \sigma_{i,1}(\delta)\sigma_i(y)
\]

and

\[
\sigma_{i,2}(\mu) = \sigma_i(x) - \sigma_{i,2}(\delta)\sigma_i(y) = \sigma_i(x) + \sigma_{i,1}(\delta)\sigma_i(y)
\]

are complex conjugates whose product is 1. Therefore, \( |\sigma_{i,1}(\mu)| = |\sigma_{i,2}(\mu)| = 1 \).

Suppose now that \( \mu \in H \) and \( |\mu| = 1 \). Then given our assumptions on \( \sigma_1 \) and \( \sigma_2 \) for the case of \( K \) being \textit{opnr}, for both kinds of fields, we have \( |\sigma_{i,j}(\mu)| = 1 \) for all values of \( i \) and \( j \). This would make \( \mu \) a root of unity. Thus the third assertion of the lemma follows.

The next inequality

\[
|a| - \sqrt{|a^2 - 1|} < 1
\]  

(6.3.5)

is equivalent to \( |a|^2 - 2|a| + 1 < |a^2 - 1| \). But

\[
|a|^2 + 1 < |a|^2 + 2|a| - 1 \leq |a^2 - 1| + 2|a|
\]

and therefore (6.3.5) holds. To see that if \( |\varepsilon| > 1 \) then \( |\varepsilon| > |a| \), consider the following inequalities.

\[
|a| - \sqrt{|a^2 - 1|} \leq 2|a|^2 + 2a\sqrt{|a^2 - 1|} - 1 = 2|\varepsilon||a| - 1
\]

or in other words,

\[
|\varepsilon|^2 - 2|a| |\varepsilon| + 1 = (|\varepsilon| - |a| - \sqrt{|a^2 - 1|})(|\varepsilon| - |a| + \sqrt{|a^2 - 1|}) \geq 0.
\]

Thus, either,

\[
0 < |\varepsilon| \leq |a| - \sqrt{|a^2 - 1|} < 1,
\]  

(6.3.6)

by the argument above, or

\[
|\varepsilon| \geq |a| + \sqrt{|a^2 - 1|} > |a|.
\]  

(6.3.7)

Now to show that \( |\varepsilon| = |a + \sqrt{a^2 - 1}| < 2|a| \), it is enough to observe that \( |\sqrt{a^2 - 1}| < |a| \).

Finally, from Inequalities (6.3.6) and (6.3.7) it follows that \( |\varepsilon| \neq 1 \) and therefore it is not a root of unity.

Our next job is to show that \( \varepsilon(a) \) essentially generates the group \( G \).
6.3.5 Lemma.

Let $\mu \in G$. Then for some $k \in \mathbb{Z}$ we have $\mu = \xi \varepsilon(a)^k$, where $\xi$ is a root of unity.

Proof.

Consider $N_{M/K} : U_M \to U_K$. Then $H$ is the kernel of this map. Further, the image of the map is of finite index in $U_K$, since every square of an integral unit of $K$ is in the image. Thus rank of $H$ is equal to $\text{rank}(U_M) - \text{rank}(U_K)$. Direct calculation using Dirichlet Unit Theorem and our assumptions on $a$, imply that for both types of $K$ ($tr$ and $opnr$) this difference is $1$. Since $G \subseteq H$, the rank of $G$ is at most $1$, but since $a - \delta \in G$, we know that it is exactly one. Further, the torsion free part of $G$ is isomorphic to a $\mathbb{Z}$-module, and thus to a free module, and therefore we conclude that modulo roots of unity, every element of $G$ is an integer power of some $M$-unit $\nu$ with a $K$-norm equal to $1$.

Without loss of generality, we can assume that $|\nu| > 1$ and $\varepsilon(a) = \xi \nu^l$, where $l \neq 0$ and $\xi$ is a root of unity. We want to show that $|l| = 1$. To that effect let $\nu = x + \delta y$, with $x, y \in O_K$, and observe that $2\delta |(\nu - \nu^{-1})$. Consequently, $|N_{M/Q}(2\delta)| \leq |N_{M/Q}(\nu - \nu^{-1})|$. On the other hand, we have that

$$|N_{M/Q}(\nu - \nu^{-1})| = 2^{2n} \prod_{i \in I_0, j=1,2} |\sigma_{i,j}(\delta)| \prod_{i \notin I_0, j=1,2} |\sigma_{i,j}(\delta)| > (4|\delta|^{2m_0} > (a^2)^{m_0},$$

by Lemma 6.3.4. At the same time, we have

$$|N_{M/Q}(\nu - \nu^{-1})| = \prod_{i \in I_0, j=1,2} |\sigma_{i,j}(\nu) - \sigma_{i,j}(\nu^{-1})| \prod_{i \notin I_0, j=1,2} |\sigma_{i,j}(\nu) - \sigma_{i,j}(\nu^{-1})|$$

$$< 2^{2n-2m_0}|\nu - \nu^{-1}|^{2m_0} \leq 2^{2n-2m_0}(|\nu| + 1)^{2m_0} < 2^{2n}|\nu|^{2m_0}.$$ 

Thus we obtain the inequality $|a|^{2m_0} < 2^{2n}|\nu|^{2m_0}$. Suppose now that $\varepsilon_1 = \xi \nu^l$, where $l \geq 2$ and $\xi$ is a root of unity. Then $|a|^2 < 2^{2n}|\varepsilon_1 | < 2^{2n}|a|$ and we have a contradiction of one of our assumptions on $a$.

Having established the nature of elements of $G$, we continue to explore the properties of powers of $\varepsilon = \varepsilon(a)$.

6.3.6 Lemma.

The following statements are true.

1. $k < |\sigma_i(x_k(a))|$ for $i \in I_0$ and any $k \in \mathbb{N}$. 

94
2. There exists a constant $C$, depending on $a$ and $K$ only, such that for any $k \in \mathbb{N} \setminus \{0\}$, there exists $m, h \in k\mathbb{N}$ with the property
\[|\sigma_i(x_m)| > \frac{1}{2}, i \not\in I_0,\] (6.3.8)
and
\[|\sigma_i(y_h)| > C, i \not\in I_0.\] (6.3.9)

3. If $\sigma_i(y_{eh})$ satisfies (6.3.9) for $i \not\in I_0$, then
   (a) $y_{eh}|y_{em} \Rightarrow h|m$,
   (b) $y_{eh}^2|y_{em} \Rightarrow hy_{eh}|m$,
where the integer constant $e$ was defined in Notation 6.3.3.

4. If $\sigma_i(x_m)$ satisfies (6.3.8) for $i \not\in I_0$, then
   \[x_k \equiv \pm x_j \mod x_m \Rightarrow k \equiv \pm j \mod m.\]

5. For any non-zero $m \in \mathbb{Z}$, $C_1, C_2 \in \mathbb{R}^+$, there exists a positive $s \in \mathbb{N}$ such that
   \[b = (x_m^2 + y_m^2(a^2 - 1))^{2s}(x_m^4 + a(1 - x_m^2)^2).\]
   has the following properties:
   (a) $b \equiv 1 \mod y_m(a)$;
   (b) $b \equiv a \mod x_m(a)$;
   (c) $\sigma_i(b) > C_1$ for $i \in I_0$ and $0 < \sigma_i(b) < C_2$ for $i \not\in I_0$. In particular, it can be arranged that $b$ satisfies requirements listed for $a$ in Notation 6.3.1 and 6.3.3.

**Proof.**

1. Since $\varepsilon$ is not a root of unity, by Lemma 6.3.4, either $|\varepsilon| > 1$ or $|\varepsilon|^{-1} > 1$. Thus, by the same lemma, either $\varepsilon$ or $\varepsilon^{-1}$ is of bigger absolute value than $a$. On the other hand,
   \[|x_m| = \frac{\varepsilon^m + \varepsilon^{-m}}{2} \geq \frac{|a|^m - 1}{2} > \frac{2^{2nm} - 1}{2} > m\]
since $n \geq 2$. 

95
2. Let \( k \in \mathbb{N} \) be given. Consider the set \( \{ \varepsilon_j, j \not\in I_0 \} \). By Lemma 6.3.4, \(|\varepsilon_j| = 1\). Thus, for each \( j \not\in I_0 \) we have that \( \varepsilon_j = e^{i\theta_j} \), where \( \frac{\theta_j}{\pi} \not\in \mathbb{Q} \).

(Otherwise, \( \varepsilon_j \) is a root of unity.) Let \( \alpha_j = \frac{\theta_j}{\pi} \) and let \( A = \{ \alpha_j, \ldots, \alpha_{j_0} \} \) be a maximal subset of \( \{ \alpha_j, j \in I_0 \} \) with respect to the linear independence of the set \( \{1, \alpha_j, \ldots, \alpha_{j_0} \} \) over \( \mathbb{Q} \). Since, by a preceding observation, for all \( j \in I_0 \) we have \( \alpha_j \not\in \mathbb{Q} \), we know that \( A \) is not empty. Let \( J_0 = \{ j_1, \ldots, j_{j_0} \} \). Then for any \( r \not\in I_0 \), for some \( b, b_{r,j} \in \mathbb{Z} \), we have that \( \varepsilon_r^{b_{r,j}} = \prod_{j \in I_0} \varepsilon_j^{b_{r,j}} \). Thus, if we let \( b = \prod_{r \not\in I_0} b_r \), then for all \( r \not\in I_0 \), for some \( a_{r,j} \in \mathbb{Z} \), we have that \( \varepsilon_r^{b_{r,j}} = \prod_{j \in I_0} \varepsilon_j^{a_{r,j}} \). Consequently, we conclude that for all \( r \not\in I_0 \), for any \( l \in k\mathbb{Z} \), we also have that

\[
\varepsilon_r^{\lambda} = \prod_{j \in I_0} \varepsilon_j^{\lambda_{r,j}} = \prod_{j \in I_0} e^{i\pi \lambda_{r,j}\alpha_j} = e^{i\pi \sum_{j \in I_0} \lambda_{r,j}\alpha_j} = \cos(\pi \sum_{j \in I_0} \lambda_{r,j}\alpha_j) + i \sin(\pi \sum_{j \in I_0} \lambda_{r,j}\alpha_j) = \sigma_r(x_{ib}) \pm \sigma_r(y_{ib}).
\]

Let \( m = \max_{r,j} \{|a_{r,j}|\} \). Since \(|\cos(\pi \theta)|\) is a continuous function, for any \( \lambda_1 > 0 \) there exists \( \lambda_2 > 0 \) such that \(|\theta| < \lambda_2 \Rightarrow 1 - |\cos(\pi \theta)| < \lambda_1 \). By Kronecker’s Theorem (see Theorem 442, Chapter XXIII of [36]), there exists \( l \in k\mathbb{N} \) such that for all \( j \in J_0 \) there exists \( l_j \in \mathbb{Z} \) with the property that \(|l\alpha_j - l_j| < \frac{\lambda_2}{mn}\). Then

\[
\left| \sum_{j \in J_0} l_{r,j}\alpha_j - \sum_{j \in J_0} a_{r,j}l_j \right| < \lambda_2,
\]

and therefore

\[
1 - |\sigma_r(x_{ib})| = 1 - \left| \pm \cos(\pi \sum_{j \in J_0} l_{r,j}\alpha_j - \pi \sum_{j \in J_0} a_{r,j}l_j) \right| < \lambda_1.
\]

If we select \( \lambda_1 < \frac{1}{2} \), then for all \( r \not\in I_0 \) we have that \(|\sigma_r(x_{ib})| > \frac{1}{2} \).

Next for \( r \not\in I_0 \), let \( A_r = \sum_{j \in J_0} a_{r,j} \). Let \( A \in \mathbb{N} \) be such that \( A > \max_{r \not\in I_0} \{|A_r|\} \) and \( \text{ord}_2 \frac{A}{A} \leq 0 \) for all \( r \not\in I_0 \). Since \(|\sin \pi \theta|\) is a continuous function, it is equicontinuous on any closed and bounded interval. Thus, for any \( \lambda_1 > 0 \) there exists \( 0 < \lambda_2 < \frac{1}{4} \) such that for any \( \theta_1, \theta_2 \in [-1, 1] \) with \(|\theta_1 - \theta_2| < \lambda_2 \), we have that \(|\sin(\pi \theta_1) - \sin(\pi \theta_2)| < \lambda_1 \). Next choose \( l \in k\mathbb{Z} \) so that for all \( j \in J_0 \), for some \( l_j \in \mathbb{Z} \), we have \(|l\alpha_j - l_j - \frac{1}{2A}| < \frac{\lambda_2}{2A} \). Then for all \( r \not\in I_0 \) we have that

\[
\left| \sum_{j \in J_0} (l_{r,j}\alpha_j - l_ja_{r,j} - \frac{a_{r,j}}{2A}) \right| < \lambda_2.
\]
Thus,
\[ \left| \sum_{j \in J_0} (l_{ar,j} \alpha_j - l_{ar,j}) - \frac{A_r}{2A} \right| < \lambda_2. \]
and, therefore for \( \lambda_1 < \frac{1}{2} \sin(\frac{\pi A_r}{2A}) \) we can conclude that
\[ |\sigma_{r,1}(\delta)\sigma_r(y_{ib})| = |\sin(\pi \sum_{j \in J_0} l_{ar,j} \alpha_j)| = |\sin(\pi \sum_{j \in J_0} l_{ar,j} \alpha_j - l_{ar,j})| > \frac{1}{2} |\sin(\frac{\pi A_r}{2A})|, \]
where \( \sin(\frac{\pi A_r}{2A}) \neq 0 \), since \( A_r / 2A \not\in \mathbb{Z} \) by construction of \( A \). Thus, we can set
\[ C = \min_r \frac{|\sin(\frac{\pi A_r}{2A})|}{|\sigma_{r,1}(\delta)|} > 0. \]

3. Let \( r, q \in \mathbb{N} \) and \( 0 < r < q \). Assume also that \( |\sigma_i(y_{eq})| > C \) for all \( i \not\in I_0 \). Then
\[
|N_{M/Q}(y_{er})| = \prod_{i=1}^n \prod_{j=1}^2 |\sigma_{i,j}\left(\frac{\varepsilon_{er} - \varepsilon_{-er}}{2\delta}\right)| \\
\leq \prod_{i \in I_0} \frac{|(\varepsilon_{i}^{er} - \varepsilon_{-i}^{er})(\varepsilon_{i}^{er} - \varepsilon_{i}^{er})|}{4|\delta_i|^2} \prod_{i \not\in I_0} \frac{1}{|\delta_i|^2} \\
\leq \frac{4|\varepsilon_1|^{2em_0r}}{4^{m_0}|N_{K/Q}(a^2 - 1)|} < \frac{|\varepsilon_1|^{2em_0r}}{4^{m_0-1}}.
\]
So finally,
\[ |N_{K/Q}(y_{eq})| \leq \frac{|\varepsilon_1|^{em_0r}}{2^{m_0-1}}. \]
On the other hand,
\[
|N_{K/Q}(y_{eq})| = \prod_{i=1}^n |\sigma_i(y_{eq})| \geq C^{n-m_0} \prod_{i \in I_0} |\sigma_i(y_{eq})| \\
\geq C^{n-m_0} \prod_{i \in I_0} \frac{|\varepsilon_i^{eq} - \varepsilon_i^{-eq}|}{2|\delta_i|} \geq C^{n-m_0} \frac{|\varepsilon_1|^{eq} - 1)^{m_0}|2^{m_0}|\delta_1|^{m_0}} \geq C^{n-m_0} \frac{|\varepsilon_1|^{m_0eq}}{2^{m_0+1}|\delta_1|^{m_0}}.
\]
Thus, since, by assumption on \( \varepsilon \), we have that
\[ |\varepsilon_1|^{eq} > \frac{4|\delta_1|^{m_0}}{C^{n-m_0}}, \]
we can conclude that \( |N_{K/Q}(y_{eq})| > |N_{K/Q}(y_{er})| \).

Suppose now that \( y_{eq} \mid y_{el} \). Write \( l = sq + r \), where \( 0 \leq r < q \). Assume \( r > 0 \). Then \( y_{el} = y_{seq+er} = y_{seq}x_{er} + x_{seq}y_{er} \). By Lemma 6.3.2, we know
that $y_{eq}|y_{seq}$ and thus, $y_{eq}|y_{seq}x_{er}$. But since $(y_{seq}, x_{seq}) = 1$ we conclude that $(y_{eq}, x_{seq}) = 1$. So $y_{eq}|y_{er}$, but this is impossible by the argument above, and consequently $r = 0$.

Let’s examine now the second divisibility condition: $y_{eq}^2|y_{el}$. Now we know that $q|l$ and thus $l = qs$. Therefore, using Binomial Theorem we establish that

$$y_{eq} = \sum_{0 \leq j \leq (l-1)/2} \binom{s}{2j+1} x_{eq}^{s-2j-1} y_{eq}^{2j+1} d^j.$$  

Thus,

$$\frac{y_{eq}}{y_{eq}} = s x_{eq}^{s-1} + y_{eq}(\ldots),$$

and, since $(y_{eq}, x_{eq}) = 1$, we conclude that $y_{eq}|s$.

4. As above we have to start with some inequalities concerning norms. Let $m$ be a positive integer and assume that $x_m$ satisfies Inequality (6.3.8). Let $r_1, r_2$ be positive integers such that $r_1 < m$, and $r_2 < m$. We claim that under these assumptions

$$N_{K/Q}(x_{r_1} \pm x_{r_2}) < N_{K/Q}(x_m),$$  

and

$$N_{K/Q}(x_{r_1}) < N_{K/Q}(x_m).$$  

In estimating the norms we will proceed pretty much in the same manner as above, by expressing $x_m, x_{r_1}$, and $x_{r_2}$ as differences of powers of $\varepsilon$. Thus,

$$|N_{K/Q}(x_m)| = \prod_{i \in I_0} |\sigma_i(x_m)| \prod_{i \notin I_0} |\sigma_i(x_m)| \geq \frac{1}{2^{n-m_0}} \prod_{i \in I_0} \left| \varepsilon_i^m + \varepsilon_i^{-m} \right| \geq \left( |\varepsilon_1|^{m-1} \right)^{m_0}.$$  

Without loss of generality we can assume that we have $r_1 \leq r_2 < m$ and the following upper bound for the norm of $x_{r_1} \pm x_{r_2}$:

$$|N_{K/Q}(x_{r_1} \pm x_{r_2})| = \prod_{i \in I_0} |\sigma_i(x_{r_1} \pm x_{r_2})| \prod_{i \notin I_0} |\sigma_i(x_{r_1} \pm x_{r_2})|.$$

$$\leq 2^{n-m_0} \prod_{i \in I_0} \left| \varepsilon_i |^{r_1} + |\varepsilon_i|^{r_2} + |\varepsilon_i|^{-r_1} + |\varepsilon_i|^{-r_2} \right| \leq 2^{n-m_0} (|\varepsilon_1|^{r_2} + 1)^{m_0}.$$  

Thus, in this case it is enough to show that

$$2^{n-m_0} (|\varepsilon_1|^{r_2} + 1)^{m_0} < \left( \frac{|\varepsilon_1|^{m-1} m_0}{2^n} \right).$$  

98
Next we note that $|\varepsilon_1|^2 + 1 < 2|\varepsilon_1|^2$ and $|\varepsilon_1|^m - 1 > \frac{1}{2} |\varepsilon_1|^m$, while $m_0 \geq 1$. Therefore to show that (6.3.12) holds, it is enough to show that

$$2^{2n+1}|\varepsilon_1|^s < |\varepsilon_1|^m \Leftrightarrow 2^{2n+1} < |\varepsilon_1|^{m-s}.$$  \hfill (6.3.13)

But by Lemma 6.3.4 and assumptions on $a$, we have the following inequalities

$$2^{2n+1} < 2^{2n+2} < |a| < |\varepsilon_1| \leq |\varepsilon_1|^{m-s}.$$  

Thus, (6.3.10) holds.

Suppose now that $x_j \equiv \pm x_i \mod x_m$. We can write $j = 2mj_l \pm r_1$, $l = 2ml_i \pm r_2$, where $|r_1| \leq m, |r_2| \leq m$. Then $x_j = x_n x_{2m_j_l} \pm dy_n y_{2m_j_l} \equiv \pm x_n$ by Lemma 6.3.2. Similarly, $x_i \equiv \pm x_n \mod x_m$. Consequently, we have $x_r \equiv \pm x_n \mod x_m$. Thus, if $r_1 \neq r_2$, we have a contradiction with Inequality (6.3.10) or Inequality (6.3.11).

5. First of all we observe that for all $m \in \mathbb{Z}$, we have that $|\sigma_i(x_m)| < 1$ for $i \notin I_0$ and $|\sigma(x_m)| > 1$ for $i \in I_0$. Indeed,

$$|\sigma_i(x_m)| = \left| \frac{\sigma_{i,1}(\varepsilon^m + \varepsilon^{-m})}{2} \right|,$$

where for $i \notin I_0$, we know that

$$|\sigma_{i,1}(\varepsilon^m)| = |\sigma_{i,1}(\varepsilon^{-m})| = 1.$$

The only way the absolute value of the sum of two complex numbers can be equal to the sum of their absolute values, is for both numbers to have the same argument. In our case this would require $\varepsilon^m = \pm 1$, contradicting our assumptions on $a$ and $m$. Thus, $|\sigma_i(x_m)| < 1$ for $i \notin I_0$ and all $m \neq 0$. Similarly, for $i \in I_0$ we have by Lemma 6.3.4 that

$$|\sigma_i(x_m)| = \left| \frac{\sigma_{i,1}(\varepsilon^m + \varepsilon^{-m})}{2} \right| > \frac{1}{2} |\varepsilon^m| - 1 > \frac{1}{2} |a_i| - 1 > 2^{2n+1} - 1 > 1.$$

Next we have that

$$\sigma_i(b) = (\sigma_i(x_m)^2 + \sigma_i(y_m)^2(a_i^2 - 1))2^s(\sigma_i(x_m)^4 + a_i(1 - \sigma_i(x_m^2)^2))$$

$$= (\sigma_i(x_m)^2 - \sigma_i(y_m)^2(1 - a_i^2))2^s(\sigma_i(x_m)^4 + a_i(1 - \sigma_i(x_m^2)^2)),$$

where for $i \in I_0$ we have that $a_i > 1$, while for $i \notin I_0$ we have that $0 < a_i < 1$. Consequently, for $i \in I_0$ we have that

$$\sigma_i(x_m)^2 + \sigma_i(y_m)^2(a_i^2 - 1) > \sigma(x_m)^2 > 1,$$
and for \( i \not\in I_0 \) we have that
\[
\sigma_i(x_m)^2 - \sigma_i(y_m)^2(1 - a_i^2) < \sigma_i(x_m)^2 < 1,
\]
while at the same time
\[
\sigma_i(x_m)^2 - \sigma_i(y_m)^2(1 - a_i^2) = 2\sigma(x_m)^2 - 1 > -1.
\]
Hence for \( i \not\in I_0 \) it is the case that
\[
|\sigma_i(x_m)^2 - \sigma_i(y_m)^2(1 - a_i^2)| < 1.
\]
Thus, since \( m \) is fixed, we can choose \( s \) to make \( |\sigma_i(b)| \) arbitrarily large for \( i \in I_0 \) and arbitrarily small for \( i \not\in I_0 \). In particular we can arrange that \( |\sigma_i(b)| > 2^{2n+2} \) for \( i \in I_0 \) and \( |\sigma_i(b)| < \frac{1}{2} \) for \( i \not\in I_0 \).

Note also that for all \( i \) we have that \( \sigma_i(b) > 0 \). Indeed, the first term in the product is a square and the second term is a sum of a square and a positive number times a square.

Further, for \( i \not\in I_0 \) we have that \( \sigma_i(b^2 - 1) < 0 \) cannot be a square in \( \sigma_i(K) \) and therefore \( b^2 - 1 \) is not a square in \( K \). Finally, the equivalencies in the statement of the lemma will hold simply because
\[
x_m^2 \equiv 1 \mod y_m,
\]
\[
(a^2 - 1)y_m^2 \equiv -1 \mod x_m,
\]
and
\[
1 - x_m^2 \equiv 1 \mod x_m^2.
\]

### 6.4 Non-integral Solutions of Some Unit Norm Equations.

In this section we will consider solutions to norm equations which are not integral. We will continue to call these solutions units because they will be units of some rings of \( \mathcal{W} \)-integers. (We remind the reader that we use the term “\( \mathcal{W} \)-integers” for the cases where \( \mathcal{W} \) is infinite, as well as for the cases where \( \mathcal{W} \) is finite.) If we select the set \( \mathcal{W} \) properly with respect to the extensions under consideration, the set of solutions to our norm equations will once again serve as a basis for Diophantine definitions we seek.
6.4.1 Proposition.

Let $K$ be totally real number field. Let $F$ be a subextension of $K$ such that extension $K/F$ is cyclic. Let $L$ be a totally complex extension of degree 2 of $\mathbb{Q}$ and let $E$ be a totally real cyclic extension of $\mathbb{Q}$ of prime degree $p > 2$. Assume that $p$ is relatively prime to $[K : \mathbb{Q}]$. These extensions are described in the following picture.

Next consider the system of norm equations

$$\begin{align*}
N_{E/K}(x) &= 1, \\
N_{E/L}(x) &= 1.
\end{align*}$$

(6.4.1)

Let $\mathfrak{p}_K$ consist of primes of $K$ not splitting in the extension $KE/K$. Let $\mathfrak{p}$ be a prime of $K$ satisfying the following conditions.

1. $\mathfrak{p}$ must lie above an $F$-prime $\mathfrak{p}_F$ not splitting in the extension $K/F$. (This is where we need $K/F$ to be cyclic. Otherwise we might have no primes which do not split.)

2. $\mathfrak{p}_F$ should split completely in the extension $FL/F$.

3. $\mathfrak{p}$ should split completely in the extension $EKL/K$. 

101
Let $\mathcal{W}_K = \mathcal{W}_K \cup \{\wp\}$. Let $\mathcal{W}_{KLE}$ be the set of primes of $KLE$ lying above the primes of $\mathcal{W}_K$. Let $r \in \mathbb{N}$ satisfy the following requirements.

1. Let $m \in \mathbb{N}$ be such that for any root of unity $\xi \in LKE$, we have $\xi^m = 1$. Then $r \equiv 0 \mod 2m$.

2. Also $\frac{r}{m} \equiv 0 \mod h_{LEF} – the class number of $FEL$.

Let $x \in O_{KLE,W_{KLE}}$ be a solution to System (6.4.1). Then $x^r \in LEF$. Further, the set of non-root of unity solutions to the system in $O_{KLE,W_{KLE}}$ is not empty.

**Proof.**

First of all, by Lemma B.3.3, we have that $[LKE : EK] = 2, [LEK : LK] = p, [LEF : EF] = 2, [LEF : LF] = p$. Further, the fields $KE, FE$ are totally real and the fields $LK, LKE, FL, FLE$ are totally complex. From Proposition 6.2.1 we can conclude that if $x \in LKE$ is a solution to this system then the divisor of $x$ must be composed of the primes lying above primes of $EK$ and $LK$ splitting in the extensions $LEK/EK$ and $LEK/LK$ respectively. Given the fact that both extensions are cyclic of distinct prime degrees, we can conclude that $LEK$-primes occurring in the divisor of $x$ lie above $K$-primes splitting completely in the extension $LEK/K$. Further, since $LEK/EK$ is a totally complex extension of degree 2 of a totally real field, all the integral solutions to this system of norm equations have to be roots of unity. Absence of non-root of unity integral solutions leads to the following consequence. Let $x_1, x_2$ be two solutions to the first equation of the norm system above such that $x_1$ and $x_2$ have the same divisor. Then $x'_1 = x'_2$.

Given our assumptions on $\wp_F$ and $\wp$ and the degrees of the extensions, by Lemma B.4.8, no factor of $\wp_F$ in $FEL$ will split in the extension $KEL/FEL$. By our choice for the membership in $\mathcal{W}_K$, we have that $x$ is a solution to our system while being an element of the integral closure of $O_{K,\mathcal{W}}$ in $LEK$ only if the divisor of $x$ consists of the factors of $\wp$ in $LKE$.

Let $p$ be a factor of $\wp$ in $LEK$. Then, by Lemma B.3.5 and by Lemma B.3.6, we have that

$$\text{Gal}(LEK/LK) \cong \text{Gal}(EK/K) \cong \text{Gal}(E/Q),$$

$$\text{Gal}(LEK/EK) \cong \text{Gal}(LK/K) \cong \text{Gal}(L/Q),$$

$$\text{Gal}(LEK/K) \cong \text{Gal}(LEK/EK) \times \text{Gal}(LEK/LK).$$

Let $\sigma_L$ be a generator of $G(LEK/EK)$, and let $\sigma_E$ be a generator of $G(LEK/LK)$. Then $\sigma_L \sigma_E = \sigma_E \sigma_L$ will generate $G(LEK/K)$. Since $\wp$ splits completely in the extension $LEK/K$, if $\tau_1, \tau_2 \in G(LEK/K)$ are such that $\tau_1(p) = \tau_2(p)$
for some \( KLE \)-factor \( p \) of \( \Psi \), then \( \tau_1 = \tau_2 \). Denote \( \sigma_i^j(p) \) by \( p_{ij} \), where \( i = 1, 2 \) and \( j = 1, \ldots, p \). Suppose now that \( z \in O_{KLE,w_{KLE}} \) is a solution to the norm system. Then the divisor of \( z \) is of the form \( 3 = \prod p_{ij}^{a_{ij}} \) with
\[
\sum_{ij} a_{ij} = 0. \tag{6.4.2}
\]

Since each \( p_{ij} \) is the only unramified factor of the prime below it in \( FLE \), we can consider \( Z \) as a divisor of \( FLE \). Let \( w \) be an element of \( FLE \) whose divisor is \( Z \) over \( FE \). Then, as in the argument used in Proposition 6.2.1, we have that (6.4.2) implies that \( N_{FLE/FE}(\nu - w^2) = 1 \), where \( \nu \in FE \) is an integral unit.

Next we observe that \( FLE \cap KE = FE \) since \( FE \) is the largest totally real subfield contained in \( FLE \). Thus \( FLE \) and \( KE \) are linearly disjoint over \( FE \) by Lemma B.3.3. Therefore, \( N_{KLE/KE}(\nu - w^2) = N_{FLE/FE}(\nu - w^2) = 1 \).

Are we guaranteed to have such solutions? Indeed, we are. Let \( y \in LEK \) be such that its divisor is \( p^a \), where \( a \in \mathbb{N} \). (Such a \( y \) certainly exists if \( a \equiv 0 \mod h_{LEK} \), the class number of \( LEK \).) Next consider
\[
x = \frac{y \sigma_E \sigma_L (y)}{\sigma_L (y) \sigma_E (y)} = \frac{y / \sigma_L (y)}{\sigma_E (y) / \sigma_E \sigma_L (y)} = \frac{y / \sigma_E (y)}{\sigma_L (y) / \sigma_L \sigma_E (y)}.
\]

We claim that \( x \) is not a root of unity and satisfies the norm system above. First of all note that since \( y = u / \sigma_L (u) = v / \sigma_E (v) \), \( EK \)-norm and \( LK \)-norm of \( y \) are equal to 1. Secondly, note that the divisor of \( x \) is of the form
\[
\left( \frac{p \sigma_E \sigma_L (p)}{\sigma_L (p) \sigma_E (p)} \right)^a.
\]

But by the argument above, the primes \( p, \sigma_L (p), \sigma_E (p), \sigma_E \sigma_L (p) \) are all distinct. Thus the divisor of \( x \) is not trivial and \( x \) is not a root of unity.

The next proposition addresses the issue of existence of a prime \( \Psi \) satisfying all the requirements listed above.

### 6.4.2 Proposition.

Let \( K, F, L, E, p \) be as above. Then there are infinitely many primes \( \Psi_F \) satisfying the following conditions.

1. \( \Psi \) lies above an \( F \)-prime \( \Psi_F \) not splitting in the extension \( K/F \).
2. \( \Psi_F \) splits completely in the extension \( FEL/F \).
3. \( \Psi \) splits completely in the extension \( EKL/K \).
Proof.

Consider the extension $KEL/F$. By Lemma B.3.3, the fields $K, FE, LF$ are pairwise linearly disjoint over $F$ Galois extensions of $F$, and therefore by Lemma B.3.6 we have that

$$\text{Gal}(KLE/F) \cong \text{Gal}(K/F) \times \text{Gal}(LF/F) \times \text{Gal}(EF/F).$$

Let $\sigma_K$ be the generator of $\text{Gal}(KLE/FE) \cong \text{Gal}(K/F)$, where the congruence holds by Lemma B.3.5. Further, by the same lemma, the restriction of $\sigma_K$ to $K$ generates $\text{Gal}(K/F)$. Now let $p_{KLE}$ be a prime whose Frobenius automorphism is $\sigma_K$. Then $p_K = p_{KLE} \cap K$ is not moved by the restriction to $\sigma_K$ to $K$. Hence $p_K$ is the only factor above $p_F = p_K \cap F$. On the other hand, the decomposition group of $p_{KLE}$ over $K$ is equal to $\text{Gal}(KLE/K) \cap G(p_{KLE})$, where $G(p_{KLE})$ is the decomposition group of $p_{KLE}$ over $F$. But this intersection contains identity only. Therefore, $p_K$ splits completely in the extension $KLE/K$. Let $p_{FLE} = p_{KLE} \cap FLE$. Then

$$G_{\text{over } F}(p_{FLE}) \cong G_{\text{over } F}(p_{KLE}) / G_{\text{over } FLE}(p_{KLE}) = \{\text{id}\},$$

where $G_{\text{over } F}(p_{FLE})$ is the decomposition group of $p_{FLE}$ over $F$, $G_{\text{over } F}(p_{KLE})$ is the decomposition group of $p_{KLE}$ over $F$, and $G_{\text{over } FLE}(p_{KLE})$ is the decomposition group of $p_{KLE}$ over $FLE$. Thus, $p_F$ splits completely in the extension $FLE/F$. Now our assertion follows by Chebotarev Density Theorem.

The next proposition is a generalization of Lemma 6.1.6 for the case of $\mathcal{W}$-units.

6.4.3 Proposition.

Let $L$ be a totally real field. Let $d \in L$ be such that $L(\sqrt{d})$ is a totally complex extension of $\mathbb{Q}$. Let $K$ be a totally real cyclic extension of $L$ of odd prime degree $p$. Let $\mathcal{W}_{L(\sqrt{d})}$ be a set of primes of $L(\sqrt{d})$ not splitting in the extension $K(\sqrt{d})/L(\sqrt{d})$. Let $\epsilon$ be an element of the integral closure of $O_{L(\sqrt{d}), \mathcal{W}_{L(\sqrt{d})}}$ in $K(\sqrt{d})$. Then the following statements are true.

- If $\epsilon$ satisfies
  $$N_{K(\sqrt{d})/L(\sqrt{d})}(\epsilon) = 1 \quad (6.4.3)$$
  Then $\epsilon \in O_{K(\sqrt{d})}$.
- There exists a natural number $m$ depending on $K, L, d$ only, such that $\epsilon^m \in K$. 

104
Proof.

Since \( \varepsilon \) is an element of the integral closure of \( O_{L(\sqrt{d}), W_{L(\sqrt{d})}} \) in \( K(\sqrt{d}) \), by Proposition 6.2.1, the only primes which can appear in the denominator of its divisor are the factors of the primes in \( \mathfrak{p}_{L(\sqrt{d})} \). On the other hand, since \( N_{K(\sqrt{d})/L(\sqrt{d})}(\varepsilon) = 1 \), we must conclude that every prime appearing in the divisor of \( \varepsilon \) must have a distinct conjugate over \( L(\sqrt{d}) \). This is not true of primes in \( \mathfrak{p}_{L(\sqrt{d})} \), by construction. Therefore, the only elements of the integral closure of \( O_{L(\sqrt{d}), W_{L(\sqrt{d})}} \) in \( K(\sqrt{d}) \) satisfying (6.4.3) are integral units. On the other hand, since the integral unit group of \( K(\sqrt{d}) \) has the same rank as the integral unit group of \( K \), there exists a natural number \( m > 0 \) such that the \( m \)-th powers of any integral unit in \( K(\sqrt{d}) \) is in \( K \). Hence, the lemma is true.
Chapter 7

Diophantine Classes over Number Fields.

In this chapter we prove the main known results concerning Diophantine classes of the rings of integers and \( \mathcal{W} \)-integers of number fields. We start with constructing Diophantine definitions of \( \mathbb{Z} \) over some of these rings. Next we use these definitions to put together parts of the big picture of the Diophantine classes of the rings of \( \mathcal{W} \)-integers of number fields discussed in Chapter 1. Most of the chapter is taken by proving vertical results, i.e. resolving problems of the following nature. Let \( R_1 \subset R_2 \) be integral domains with quotient fields \( F_1, F_2 \) respectively, such that \( R_1 \) is integrally closed in \( R_2 \) and \( F_2/F_1 \) is a non-trivial finite field extension. Then give a Diophantine definition of \( R_1 \) over \( R_2 \) or alternatively show that \( R_1 \leq_{\text{Dioph}} R_2 \).

The proofs of all the vertical results presented in this book can be classified as being done by one of two vertical methods which we named “weak” and “strong”. These methods were developed by Denef and Lipshitz in [15], [19] and [18] and subsequently used by Pheidas in [68] and the author in [95], [103], [105], [110], [97], and [107].

Before presenting the details of constructions for particular rings, we describe the main features of the weak and strong vertical methods.

7.1 Vertical Methods of Denef and Lipshitz.

7.1.1 The Weak and the Strong.

As we have noted above, the method used to solve vertical problems over number fields has two versions: a “weak” version and a “strong” version. In the weak version, the norm equations in combination with some bound
equations assert that if solutions can be found in the ring above, for a given value of a parameter, then this value is in the ring below. And conversely, if the parameter is equal to a rational integer, then the solutions will be found in the ring above. In the strong version, the norm equations in combination with the bound equations will assert that the solutions can be found in the ring above if and only if the parameter is equal to a specific element below, for example, a rational integer.

What method is used depends on the kind of control we exercise over the solutions of the norm equations as will be demonstrated by the examples below. We will start with a formal description of the weak version of the vertical method.

7.1.2 The Weak Version of the Vertical Method.

Let $K/F$ be a number field extension with a basis $\Lambda = \{1, \alpha, \ldots, \alpha^{m-1}\} \subset O_K$. Let $x \in O_K$, $w, y \in O_F$. Assume that $y$ is not zero and is not an integral unit. Let $c \in \mathbb{N}$ be fixed, let $n = [K : \mathbb{Q}]$. Suppose that the following equalities and inequalities hold.

\[ x = \sum_{i=0}^{m-1} a_i \alpha^i, a_i \in F, \quad (7.1.1) \]
\[ |N_{K/\mathbb{Q}}(D a_i)| \leq |N_{K/\mathbb{Q}}(y)^c|, \quad (7.1.2) \]

where $D$ is the discriminant of $\Lambda$, and

\[ x \equiv w \mod y^{2c}. \quad (7.1.3) \]

Then $x \in O_F$.

**Proof.**

From (7.1.1) and (7.1.3), we conclude that

\[ x - w = (a_0 - w) + a_1 \alpha + \ldots + a_{n-1} \alpha^{m-1} \equiv 0 \mod y^{2c}. \]

Thus,

\[ \frac{x - w}{y^{2c}} = \frac{a_0 - w}{y^{2c}} + \frac{a_1}{y^{2c}} \alpha + \ldots + \frac{a_{m-1}}{y^{2c}} \alpha^{m-1} \in O_K. \]

By Lemma B.4.12 of the Number Theory Appendix, for $i = 1, \ldots, m-1$ we have that $\frac{D a_i}{y^{2c}} \in O_F$, and therefore $|N_{K/\mathbb{Q}}(D a_i)| \geq N_{K/\mathbb{Q}}(y^{2c})$ or $|N_{K/\mathbb{Q}}(a_i)| = 0$. On the other hand, from (7.1.2) we conclude that

\[ |N_{K/\mathbb{Q}}(D a_i)| \leq |N_{K/\mathbb{Q}}(y)^c| < N_{K/\mathbb{Q}}(y)^{2c}, \]

107
since \( y \) is not an integral unit. Hence, for \( i = 1, \ldots, m \), we have that \( |N_{K/Q}(a_i)| = 0 \), and therefore \( a_i = 0 \), for \( i = 1, \ldots, m - 1 \). Consequently, \( x \in O_F \).

### 7.1.3 The Strong Version of the Vertical Method.

Let \( K/F \) be a number field extension. Let \( x, y \in O_K, w \in O_F \). Assume that \( y \) is not zero and is not an integral unit. Let \( c \in \mathbb{N} \) be fixed. Assume that the following equations and inequalities are satisfied. For all embeddings \( \sigma \) of \( K \) into \( \mathbb{C} \),

\[
|\sigma(x)| \leq |N_{K/Q}(y^c)|, \quad (7.1.4)
\]

\[
|\sigma(w)| \leq |N_{K/Q}(y^c)|, \quad (7.1.5)
\]

\[
x \equiv w \mod 2y^{2cn} \text{ in } O_K, \quad (7.1.6)
\]

where \( n = [K : Q] \). Then \( x = w \in O_F \).

**Proof.**

From (7.1.6) we can conclude that either \( x = w \) or \( |N_{K/Q}(x-w)| \geq 2^nN_{K/Q}(y^{2cn}) \).

On the other hand, from inequalities (7.1.4) and (7.1.5) we conclude that

\[
|N_{K/Q}(x-w)| \leq 2^nN_{K/Q}(y^{nc}).
\]

Since \( y \) is not an integral unit, \( |N_{K/Q}(y^{nc})| < N_{K/Q}(y^{2cn}) \). Thus, we must conclude that \( x = w \).

### 7.1.4 Remark.

The difference between the weak and the strong vertical methods ultimately boils down to the fact that in using the weak method, one does not have to have a bound on the element of the smaller field in the congruence, while such a bound is necessary for the stronger method.

### 7.2 Integers of Totally Real Number Fields and Fields with Exactly One Pair of Non-real Embeddings.

In this section we discuss a construction of a Diophantine definition of \( \mathbb{Z} \) over the rings of algebraic integers of the totally real number fields and the fields
with exactly one pair of non-real embeddings. The result concerning totally real number fields was originally proved by Denef in [18]. The construction for the fields with exactly one pair of non-real embeddings was first carried out independently by Pheidas in [68] and the author in [95]. We will closely follow these constructions which are examples of the strong vertical method.

In what follows $K, a, e, n, C, \sigma_i, \sigma_{i,j}, d, \delta, \varepsilon_i, l_0, m_0$ will be defined as in Notation lists 6.3.1 and 6.3.3. Further let $c$ be the constant from the note following Corollary 5.2.2. Now consider the following equations with all the variables ranging over $O_K$:

\[
x^2 - (a^2 - 1)y^2 = 1, \quad (7.2.1)
\]

\[
\bar{w}^2 - (a^2 - 1)\bar{z}^2 = 1, \quad (7.2.2)
\]

\[
w - \delta z = (\bar{w} - \delta \bar{z})^e, \quad (7.2.3)
\]

\[
u^2 - (a^2 - 1)v^2 = 1, \quad (7.2.4)
\]

\[
s^2 - (b^2 - 1)v^2 = 1, \quad (7.2.5)
\]

\[
0 < \sigma_i(b) \leq 2^{-16}, |\sigma_i(z)| \geq C, |\sigma_i(u)| \geq \frac{1}{2}, i \not\in I_0, \quad (7.2.6)
\]

\[
v \neq 0, \quad (7.2.7)
\]

\[
z^2 \mid v, \quad (7.2.8)
\]

\[
b \equiv 1 \text{ mod } z, b \equiv a \text{ mod } u, \quad (7.2.9)
\]

\[
s \equiv x \text{ mod } u, \quad (7.2.10)
\]

\[
t \equiv \xi \text{ mod } z, \quad (7.2.11)
\]

\[
\prod_{i=0}^{n-1} (i - \xi)(i - x) \mid f, \text{ where } f \neq 0 \text{ and } (2^nf^{cn}) \mid z, \quad (7.2.12)
\]

Before we explore the meaning of these equations for the variables involved, we should note that (7.2.6) can be rewritten in a Diophantine form by Corollary 5.1.2. Further, Condition (7.2.7) is Diophantine by Proposition 2.2.4.

Now assume that the equations in (7.2.1) - (7.2.12) have solutions in $O_K$. We show that this assumption implies that $\xi \in \mathbb{Z}$. Indeed, using Lemma 6.3.5, our assumptions on $a$ and the part of (7.2.6) which has to do with $\sigma_i(b)$, we can conclude the following from (7.2.1)-(7.2.5):

\[x = \pm x_k(a), y = \pm y_k(a),\]
\[ w = \pm x_{eh}(a), \quad z = \pm y_{eh}(a), \]
\[ u = \pm x_m(a), \quad v = \pm y_m(a), \]
\[ s = \pm x_j(b), \quad t = \pm y_j(b) \]

for some \( k, h, m, j \in \mathbb{N} \), where we again use Notation 6.3.1. (To see that \( b \) satisfies the appropriate assumptions, note the following. Since \( b \in O_K \) we have that \( \prod_{i \in I_0} |\sigma_i(b)| \prod_{i \notin I_0} |\sigma_i(b)| \geq 1 \). Thus, (7.2.6) implies that \( \prod_{i \in I_0} |\sigma_i(b)| \geq 2^{16(n-m_0)} \). If \( m_0 = 1 \) we have that \( |b| > 2^{16(n-1)} > 2^{2n+2} \) for \( n \geq 2 \). If \( m_0 = 2 \), then \( n \geq 3 \) and \( |b_1| > 2^{8(n-2)} \). In this case we have \( 2^{8(n-2)} \geq 2^{2n+2} \), and therefore the size requirement for \( b \) is satisfied also.) Thus (7.2.6)-(7.2.11) can be rewritten as the following equations.

\[ |\sigma_i(y_{eh}(a))| \geq C, \quad |\sigma_i(x_m(a))| \geq \frac{1}{2}, \quad i \notin I_0. \quad (7.2.13) \]
\[ y_m(a) \neq 0; \quad (7.2.14) \]
\[ y_{eh}^2(a) y_m(a) \quad (7.2.15) \]
\[ b \equiv 1 \text{ mod } y_{eh}(a), \quad b \equiv a \text{ mod } x_m(a), \quad (7.2.16) \]
\[ x_j(b) \equiv \pm x_k(a) \text{ mod } x_m(a), \quad (7.2.17) \]
\[ \pm y_j(b) \equiv \xi \text{ mod } y_{eh}(a). \quad (7.2.18) \]

From Lemma 6.3.6 and (7.2.13) we also have the following congruences.

\[ y_j(b) \equiv j \text{ mod } (b-1) \Rightarrow y_j(b) \equiv j \text{ mod } y_{eh}(a) \text{ by (7.2.16)}, \quad (7.2.19) \]
\[ j \equiv \pm \xi \text{ mod } y_{eh}(a) \text{ by (7.2.18)}, \quad (7.2.20) \]
\[ x_j(b) \equiv \pm x_j(a) \text{ mod } x_m(a) \text{ by (7.2.16)}, \quad (7.2.21) \]
\[ x_j(a) \equiv \pm x_k(a) \text{ mod } x_m(a) \text{ by (7.2.17)}, \quad (7.2.22) \]
\[ k \equiv \pm j \text{ mod } m, \text{ by (7.2.22)}, \quad (7.2.23) \]
\[ y_{eh}(a) \mid m \text{ by (7.2.15)}, \quad (7.2.24) \]
\[ k \equiv \pm j \text{ mod } y_{eh}(a) \text{ by (7.2.23) and (7.2.24)}, \quad (7.2.25) \]
\[ k \equiv \pm \xi \text{ mod } 2^n f c^n \text{ by (7.2.12) and (7.2.20)}. \quad (7.2.26) \]

From Lemma 6.3.6 we also have that \( k < |x_k(a)| \). Thus, by Lemma 5.2.1 and (7.2.12) we conclude that \( k < |x_k(a)| \leq |N_{K/Q}(f)|^c \). Similarly, for \( i = 1, \ldots, n \), we have that \( |\xi_i| \leq |N_{K/Q}(f)|^c \). Therefore, by the strong version of the vertical method, \( \xi = \pm k \in \mathbb{Z} \).
Next we show that if \( \xi \in \mathbb{N}, \xi > n \) (so that \( \prod_{i=0}^{n-1}(i - \xi) \neq 0 \)), \( 7.2.1 \)-\( 7.2.12 \) can be satisfied in all other variables in \( O_K \). Set \( k = \xi, x = x_k(a), y = y_k(a) \). Then \( 7.2.1 \) is satisfied. By the properties of \( \mathcal{W} \)-units (see Section 6.1.1) and by properties of solutions to Pell equations (see Section 6.3), we can find \( h \in \mathbb{N} \) such that \( 7.2.12 \) is satisfied with \( z = y_{eh}(a) \) and \( |\sigma_i(y_{eh})| \geq C \) for all \( i \not\in I_0 \). Set \( w = x_{eh}(a) \). Then \( 7.2.3 \) and the \( z \)-part of \( 7.2.6 \) are satisfied. By the properties of \( \mathcal{W} \)-units and by properties of solutions to Pell equations again, we can find \( m \in \mathbb{N} \) such that \( 7.2.8 \) are satisfied. By Lemma 6.3.2, there exists \( b \in O_K \) satisfying the \( b \)-part of \( 7.2.6 \) and \( 7.2.9 \). Set \( s = x_k(b), t = y_k(b) \). Then \( 7.2.5 \) is satisfied. Finally, set \( \bar{w} = x_p(a), \bar{z} = y_p(a) \) and the properties of solutions to Pell equations will assure that the remaining conditions are also satisfied.

We summarize the discussion in this section in the following theorem.

7.2.1 Theorem.

Let \( K \) be a number field which is totally real or has exactly two conjugate non-real embeddings. Then \( Z \equiv \text{Dioph} O_K \).

7.3 Integers of Extensions of Degree 2 of Totally Real Number Fields.

In this section we present a construction of a Diophantine definition of \( O_K \) over \( O_M \), where \( K \) is a totally real number field and \( M \) is an extension of degree 2 of \( K \). This result was originally proved by Jan Denef and Leonard Lipshitz in [19]. We will use the Weak Vertical Method to reach our goal.

Let \( a \in O_K \) be such that \( M = K(\sqrt{a}) \). Let \( d \) be defined as in Lemma 6.2.2. Let \( n = [K : \mathbb{Q}] \). Let \( c \) be a constant from Note following Corollary 5.2.2 adjusted for \( D = 4a \). Now consider the following equations with all the variables ranging over the specified domains and \( k \) defined as in Lemma 6.2.2.

\[
N_{M(\sqrt{d})/M}(\varepsilon) = 1, \varepsilon \in O_M[\sqrt{d}], \quad (7.3.1)
\]

\[
N_{M(\sqrt{d})/M}(\delta) = 1, \delta \in O_M[\sqrt{d}], \quad (7.3.2)
\]

\[
N_{M(\sqrt{d})/M}(\gamma) = 1, \gamma \in O_M[\sqrt{d}], \quad (7.3.3)
\]

\[
\varepsilon^k - 1 = w(\delta^k - 1), w \in O_M[\sqrt{d}], \delta^k - 1 \neq 0, \quad (7.3.4)
\]
\[ x - w = (\delta^k - 1)u, \ u \in \mathcal{O}_M[\sqrt{d}], \ x \in \mathcal{O}_M. \]  
(7.3.5)

\[ (\gamma^k - 1)^{2c}v = (\delta^k - 1), \ v \in \mathcal{O}_M[\sqrt{d}], \]  
(7.3.6)

\[ 2 \prod_{i=0}^{2n} (i - x)y = (\gamma^k - 1), \ y \in \mathcal{O}_M[\sqrt{d}], \ \gamma^k - 1 \neq 0. \]  
(7.3.7)

We claim the following.

1. If these equations are satisfied with variables ranging over the specified domains, then \( x \in \mathcal{O}_K \).

Proof. From (7.3.1)–(7.3.3), by Lemma 6.2.2, we conclude that \( \varepsilon^k, \delta^k, \gamma^k \in \mathcal{O}_{K(\sqrt{d})} \). Therefore equation (7.3.4) implies that \( w \in \mathcal{O}_{K(\sqrt{d})} \) also. Further from equation (7.3.7), by Lemma 5.3.3, we also have

\[ x = a_0 + a_1\sqrt{d}, \ \text{where} \ a_0, a_1 \in K(\sqrt{d}); \]  
(7.3.8)

and

\[ N_{M(\sqrt{d})/Q}(4da_1) \leq N_{M(\sqrt{d})/Q}(\gamma^k - 1)^c. \]  
(7.3.9)

(We note that we included 2 in the product dividing the \( \gamma^k - 1 \) to make it obvious that \( \gamma^k - 1 \) is not an integral unit.) Now by the Weak Vertical Method applied to (7.3.5) we conclude that \( x \in \mathcal{O}_{K(\sqrt{d})} \). Since by assumption \( x \) is also in \( M \), and \( K(\sqrt{d}) \cap M = K \) as in Lemma 6.2.2, we conclude that \( x \in \mathcal{O}_K \).

2. If not all conjugates of \( a \) over \( \mathbb{Q} \) are real, then equations (7.3.1)-(7.3.7) can be satisfied for any \( x \in \mathbb{N}, x > 2n \). (If all the conjugates of \( a \) are positive, then \( M = K(\sqrt{d}) \) is a totally real field. We took care of totally real fields in Section 7.2.)

Proof. Indeed, if not all conjugates of \( a \) over \( \mathbb{Q} \) are positive, then \( K(\sqrt{d}) \) is not a degree 2 non-real extension of \( \mathbb{Q} \), and therefore \( K(\sqrt{d}) \) has integral units which are not roots of unity. Further, \( K(\sqrt{d}) \) has real embeddings and therefore it does not have roots beyond 1 and \(-1\). (We remind the reader that by construction of \( d \), we have that for every embedding \( \sigma \) of \( M(\sqrt{d}) \) into its algebraic closure, \( \sigma(\sqrt{d}) \) is a real field if and only if \( \sigma(M) \) is not a real field.) Let \( \lambda \neq \pm 1 \) be an integral unit of \( K(\sqrt{d}) \). Let \( x \in \mathbb{N} \) be given. From the discussion in the section on \( \mathcal{W} \)-units, it is clear that for some positive \( l \in \mathbb{N} \), we have that

\[ 2 \prod_{i=0}^{2n} (i - x)(\lambda^l - 1). \]  
(The assumption that \( x > 2n \) insures that the product is not zero.) Let \( \gamma = \lambda^l \). Then (7.3.7) is satisfied. By the same argument as above, there exists a non-zero \( r \in \mathbb{N} \) such that
\[(\gamma - 1)^{2c}(\lambda' - 1)\]. Let \(\delta = \lambda'\). Finally, let \(\varepsilon = \delta^x\). Thus, all the remaining equations are satisfied. Since \(O_K\) has an integral basis over \(\mathbb{Z}\), the last observation concludes our proof.

The only remaining task is to rewrite the norm equations in polynomial form and adjust all the other equation to make sure the variables range over \(O_M\) as opposed to \(O_M[\sqrt{d}]\). The first task has been discussed already in the chapter on definability of order (see Subsection 4.1.1) and the second one can be done using coordinate polynomials (see Section B.7).

Taking into account the transitivity of Diophantine generation and Theorem 7.2.1 we see that we have proved the following theorem.

### 7.3.1 Theorem.

Let \(K\) be any extension of degree 2 of a totally real field. Then \(O_K \equiv_{\text{Dioph}} \mathbb{Z}\).

This theorem has an easy corollary which is of some interest.

### 7.3.2 Corollary.

Let \(K\) be an abelian number field. Then \(O_K \equiv_{\text{Dioph}} \mathbb{Z}\).

**Proof.**

First of all we observe that any abelian number field is either totally real or an extension of degree 2 of a totally real number field. Indeed, if a Galois extension is not totally real, it is not a subfield of \(\mathbb{R}\), and therefore complex conjugation must be an element of its Galois group over \(\mathbb{Q}\). In this case the fixed field of complex conjugation must be a real abelian extension of \(\mathbb{Q}\), and therefore totally real. This totally real subfield will of course be a subfield of degree 2. (An alternative approach to proving this fact will involve Kronecker-Weber Theorem ([37], Chapter V, Theorem 5.9) stating that all abelian extensions are subfields of cyclotomics which are extensions of degree 2 of totally real fields. To finish the job we need to apply the transitivity of Dioph-generation.)
7.4 The Main Results for the Rings of \( \mathcal{W} \)-integers and an Overview of the Proof.

Below we state the strongest results concerning definability of \( \mathbb{Z} \) over large rings of \( \mathcal{W} \)-integers. They provide a measure of how close we have come to proving Diophantine undecidability of a number field and how far we are yet to travel. Poonen’s results will bring us considerably closer.

Before we proceed we would like to remind the reader that an introductory discussion of rings of \( \mathcal{W} \)-integers can be found in Section B.1 of the Number Theory Appendix.

**Theorem 7.9.4.**

Let \( M \) be a totally real field or a totally complex extension of degree 2 of a totally real field. Then for any \( \varepsilon > 0 \) there exists a set \( \mathcal{W}_M \) of primes of \( M \) whose Dirichlet density is bigger than \( 1 - [M : \mathbb{Q}]^{-1} - \varepsilon \) and such that \( \mathbb{Z} \) has a Diophantine over \( O_{M, \mathcal{W}_M} \).

**Theorem 7.9.5.**

Let \( M \) be as above and let \( \varepsilon > 0 \) be given. Let \( \mathcal{S}_Q \) be the set of all the rational primes splitting in \( M \). (If the extension is Galois but not cyclic, \( \mathcal{S}_Q \) contains all the rational primes.) Then there exists a set of \( M \)-primes \( \mathcal{W}_M \) such that the set of rational primes \( \mathcal{W}_Q \) below \( \mathcal{W}_M \) differs from \( \mathcal{S}_Q \) by a set contained in a set of Dirichlet density less than \( \varepsilon \) and such that \( \mathbb{Z} \) is existentially definable over \( O_{M, \mathcal{W}_M} \).

In this section we give an overview of the proofs of the theorems above. We start with a picture and a series of observations.

Let \( \mathcal{W}_K \) be a set of primes of a number field \( K \). Let \( \mathfrak{p}_K \) be a prime of \( K \) such that some conjugate of \( \mathfrak{p}_K \) over \( \mathbb{Q} \) is not in \( \mathcal{W}_K \). Let \( \mathfrak{p}_Q \) be the rational prime
below \( P \). Let \( x \in \mathbb{Q} \) be such that \( \text{ord}_{\mathbb{Q}} x < 0 \). Then \( x \notin O_{K, W_K} \). Indeed, let \( \Omega_K \) be a conjugate of \( P \) over \( \mathbb{Q} \) that is not in \( W_K \). Then \( \Omega_K \) is a factor of \( P \) in \( K \) and therefore \( \text{ord}_{\mathbb{Q}} x < 0 \). Since \( x \) has a pole at a prime outside \( W_K \), \( x \) is not an element of \( O_{K, W_K} \).

Suppose now that \( W_K = W_K \cap S_K \), where \( W_K \) consists exclusively of primes \( P \) such that \( P \) has a \( \mathbb{Q} \)-conjugate not in \( W_K \), \( S_K \) consists of primes all of whose \( \mathbb{Q} \)-conjugates are in \( W_K \), and \( S_K \) is finite. Then \( O_{K, W_K} \cap \mathbb{Q} = O_{\mathbb{Q}, W_Q} \), where \( W_Q \) – the set of rational primes below the primes of \( S_K \), is a finite set. If we were able to show that \( O_{K, W_K} \cap \mathbb{Q} \leq_{\text{Dioph}} O_{K, W_K} \), (7.4.1) then using the fact that \( \mathbb{Z} \leq_{\text{Dioph}} O_{\mathbb{Q}, W_Q} \) and transitivity of Dioph generation, we could conclude that \( \mathbb{Z} \leq_{\text{Dioph}} O_{K, W_K} \). Thus the problem is reduced to a vertical question and we have to determine for which \( W_K \) we can show that (7.4.1) holds. However there is a price to pay for this reduction – the density of \( W_K \), as we will see below, cannot in general exceed \( 1 - [K : \mathbb{Q}]^{-1} \).

We start with the class of fields we know the most about – totally real number fields. First of all, we consider the following. Let \( K \) be a totally real number field and let \( M \) be its Galois closure over \( \mathbb{Q} \). Then \( M \) is also a totally real number fields. Further, let \( W_K \) be a set of primes of \( K \) and \( W_M \) the set of primes of \( M \) above the primes of \( W_K \). Then \( O_{M, W_M} \) is the integral closure of \( O_{K, W_K} \) in \( M \) and \( O_{M, W_M} \leq_{\text{Dioph}} O_{K, W_K} \) by Proposition 2.2.1. Suppose we could show that Relation (7.4.1) holds for \( M \) and \( W_M \) instead of \( K \) and \( W_K \). Then by transitivity of Dioph-generation \( O_{M, W_M} \cap \mathbb{Q} \leq_{\text{Dioph}} O_{K, W_K} \). But

\[
O_{M, W_M} \cap \mathbb{Q} = (O_{M, W_M} \cap K) \cap \mathbb{Q} = O_{K, W_K} \cap \mathbb{Q}.
\]

Thus, Relation (7.4.1) holds in this case. Consequently, without loss of generality, we can assume that \( K/\mathbb{Q} \) is a Galois extension.

Now let \( F_1, \ldots, F_r \) be all the cyclic subextensions of \( K \) over \( \mathbb{Q} \). Suppose further that for \( i = 1, \ldots, r \), we have that

\[
O_{K, W_K} \cap F_i \leq_{\text{Dioph}} O_{K, W_K}.
\]

By the Finite Intersection Property (see Section 2.1.19), we then have

\[
O_{K, W_K} \cap F_1 \cap \ldots \cap F_r \leq_{\text{Dioph}} O_{K, W_K}.
\]

But \( F_1 \cap \ldots \cap F_r = \mathbb{Q} \) because elements of the intersection are not moved by any cyclic subgroup of \( \text{Gal}(K/\mathbb{Q}) \), and, therefore, by any element of \( \text{Gal}(K/\mathbb{Q}) \).
Consequently, $O_{K,\mathcal{W}_r} \cap F_1 \cap \ldots \cap F_r = O_{K,\mathcal{W}_r} \cap \mathbb{Q}$ and we have the desired result. Thus, it is enough to solve the vertical problem for the case of cyclic extensions of totally real number fields.

To solve the problem in the cyclic case, we will apply the Weak Vertical Method which requires bounds on the elements of the ring. To impose bounds we will use technique from Chapter 5. We will require that $\mathcal{W}_K$ consist of primes not splitting in certain extensions of $K$. This requirement will impose an independent constraint on the densities of prime sets we will consider for the vertical problem – these densities will have to be strictly less than 1 though they can come arbitrarily close to 1. If we combine the constraint on density coming from the bound equations together with the constraint on the densities due to the method for reducing the problem of defining $\mathbb{Z}$ to a vertical problem, we conclude that we will be able to consider prime set $\mathcal{W}_K$ of density strictly less than $1 - [K : \mathbb{Q}]^{-1}$, but arbitrarily close to $1 - [K : \mathbb{Q}]^{-1}$.

7.5 The Main Vertical Definability Results for Rings of $\mathcal{W}$-integers in Totally Real Number Fields.

Most of this section is devoted to proving a vertical result (Theorem 7.5.6) described above, which will provide a route towards a Diophantine definition of $\mathbb{Z}$ over “large” rings of $\mathcal{W}$-integers. As we have observed earlier, it is sufficient to prove a special case of the problem – the case of a cyclic extension, and this case can be done by the Weak Vertical Method. We start with a notation list for this section.

7.5.1 Notation.

- Let $K$ be a totally real number field with $[K : \mathbb{Q}] = n$.
- Let $F$ be a subextension of $K$ such that the extension $K/F$ is cyclic and $[K : F] = m$.
- Let $L$ be a totally complex extension of degree 2 of $\mathbb{Q}$.
- Let $E$ be a totally real cyclic extension of $\mathbb{Q}$ of degree $p > 2$ with $(p, n) = 1$.
- Let $\delta \in O_{EL}$ be a generator of $EL$ over $\mathbb{Q}$.
- Let $G_0(T)$ be the monic irreducible polynomial of $\delta$ over $\mathbb{Q}$.
• For \( i = 1, \ldots, n \), let \( G_i(T) = G_0(T + i) \).

• Let \( \mathcal{V}_K \) be a set of primes of \( K \) satisfying the following requirements:

  1. Any prime of \( \mathcal{V}_K \) does not split in the extension \( KE/K \). Since \( KLE/K \) is a Galois extension, this assumption, by Proposition B.1.11, will also imply that no prime of \( \mathcal{V}_K \) has a relative degree one factor in the extension \( KLE/K \).

  2. Any prime of \( \mathcal{V}_K \) does not divide the discriminant of \( G_i \) for any \( i \).

• Let \( l_0 = 0, \ldots, l_s \), where \( s = pn \), be distinct natural numbers.

• Let \( \mathfrak{p}_K \) be a prime of \( K \) satisfying the following requirements:

  1. \( \mathfrak{p}_K \) must lie above an \( F \)-prime \( \mathfrak{p}_F \) not splitting in the extension \( K/F \).

  2. \( \mathfrak{p}_F \) should split completely in the extension \( FEL/F \).

  3. \( \mathfrak{p}_K \) should split completely in the extension \( EKL/K \).

  4. \( \mathfrak{p}_K \) does not divide the free term of any \( G_i \).

• Let \( \mathcal{W}_K = \mathcal{V}_K \cup \{ \mathfrak{p}_K \} \).

• Let \( \mathcal{W}_K \) be the closure of \( \mathcal{W}_K \) with respect to conjugation over \( F \).

• Let \( \mathcal{W}_{KLE} \) be the set of primes of \( KLE \) lying above the primes of \( \mathcal{W}_K \).

• Let \( r \) be defined as in Proposition 6.4.1.

• Let \( \gamma \in \mathcal{O}_K \) generate \( K \) over \( F \).

• Let \( P \) be a rational prime with all of its \( K \)-factors outside \( \mathcal{W}_K \). (Such a \( P \) can always be found by Lemma B.4.7.)

• Let \( Q \) be a rational prime below \( \mathfrak{p}_K \).

• Let \( h_K, h_F \) be the class numbers of \( K \) and \( F \) respectively.

Before we proceed with the main theorems of this section, we need to note several technical points.
7.5.2 Lemma.

The following statements are true.

1. For all \( i = 0, \ldots, n \), we have that \( G_i \) is an irreducible polynomial over \( K \).

2. For any pair \( i \neq j \), we have that \( G_i \) and \( G_j \) do not have any common roots.

3. Let \( l, h \) be positive integers. Assume also that \( l > e(P_K/Q) \), the ramification degree of \( P_K \) over \( Q \). Then for any \( x \in K \), any \( i = 0, \ldots, n \), any \( q \in \mathcal{Y}_K \), any \( j = 0, \ldots, s \), we have that \( \text{ord}_q G_i((Qx^l)^h + Ql_j) \leq 0 \).

4. \( \mathcal{V}_K \) can contain all but finitely many primes of \( K \) not splitting in the extension \( EK/K \).

5. There are infinitely many \( P_K \) satisfying the requirements listed in Notation 7.5.1.

Proof.

1. First of all, we observe that by Lemma B.3.3 and our assumption on \( p \) and \( n \), we have that \( K \) and \( E \) are linearly disjoint over \( Q \). Therefore, \([EK : K] = [E : Q] = p \) and \( G_0 \) is irreducible over \( K \). Consequently, \( G_i(T) = G_0(T + i) \) is also irreducible over \( K \) for all \( i = 1, \ldots, n \).

2. Since for all \( i, j \) we have that \( G_i \) and \( G_j \) are irreducible over \( Q \) and of the same degree, the only way they can have a common root is for \( G_i(T) = cG_j(T) \), where \( c \in Q \). But both polynomials are monic and thus would have to be equal. On the other hand, if \( G_i = G_j \), then we have that all the roots of \( G \) differ from each other by an integer and hence \( G'(\delta) \in \mathbb{Z} \), where \( 0 < \text{deg}(G') = \text{deg}(G) - 1 \). This would of course contradict the fact that \( G \) is the monic irreducible polynomial of \( \delta \) over \( Q \).

3. First of all, note that for all \( i = 0, \ldots, n \), we have that \( \delta - i \in O_{KLE} \) generates \( KLE \) over \( K \). Thus, since no prime of \( \mathcal{V}_K \) will have a degree 1 factor in the extension \( KLE/K \), by Lemma B.4.18, for all \( \Omega \in \mathcal{V}_K \), for all \( G_i \), \( i = 0, \ldots, n \), for all \( y \in K \), we know that \( \text{ord}_\Omega G_i(y) \leq 0 \). Next let \( y = (Qx^l)^h + Ql_j \) for some \( j = 0, \ldots, s \). We have to consider two cases. If \( \text{ord}_\mathcal{V}_K x < 0 \), then by our assumption on \( l \), we conclude that \( \text{ord}_\mathcal{V}_K ((Qx^l)^h + l_j) < 0 \), and since \( G_i(T) \) is monic with integral coefficients, \( \text{ord}_\mathcal{V}_K G_i((Qx^l)^h + Ql_j) < 0 \). If, on the other hand \( \text{ord}_\mathcal{V}_K x \geq 0 \), then \( \text{ord}_\mathcal{V}_K ((Qx^l)^h + Ql_j) > 0 \), and therefore, \( \text{ord}_\mathcal{V}_K G_i((Qx^l)^h + Ql_j) = 0 \), since \( P_K \) does not divide the free term of any \( G_i \).
4. This part follows from the fact that only finitely many primes can divide the discriminants of any $G_i$, $i = 0, \ldots, n$.

5. This assertion follows from Proposition 6.4.2.

We are now ready to apply the Weak Vertical Method.

7.5.3 Theorem: Applying the Weak Vertical Method to the Case of the Cyclic Extensions of Totally Real Number Fields.

Let $x_1, x_2, x_3 \in O_{K, \mathcal{W}}[\delta] \subseteq O_{K, \mathcal{W}; \delta}$ be solutions to $(6.4.1)$ such that $x_1, x_2, x_3$ are not roots of unity, let $z, c_{1,0}, \ldots, c_{1,2p-1} \in O_{K, \mathcal{W}}$, let $w_j \in O_{K, \mathcal{W}}[\delta] \subseteq O_{K, \mathcal{W}; \delta}, j = 1, \ldots, 2p - 1$ and assume that

$$
\prod_{j=1}^{2p-1} (z - \frac{x'_3 - 1}{x'_2 - 1} - c_{1,j}^{he} w_j) = 0, j = 1, \ldots, 2p - 1,
$$

(7.5.1)

where $c$ is the constant as described in Corollary 5.3.5 adjusted for $D$ equal to the discriminant of the power basis of $\gamma$,

$$
\frac{x'_3 - 1}{x'_2 - 1} \in O_{K, \mathcal{W}}[\delta],
$$

(7.5.2)

$$
x'_i = c_{1,0} + c_{1,1} \delta + \ldots + c_{1,2p-1} \delta^{2p-1},
$$

(7.5.3)

$$
\frac{c_{1,j}^{he}}{PG_u(z - Ql)} \in O_{K, \mathcal{W}}, i = 0, \ldots, s, u = 0, \ldots, n, j = 1, \ldots, 2p - 1. (7.5.4)
$$

Assume further that $z = (Qx')^{he} = \alpha/\beta, \alpha, \beta \in O_K$, and $\alpha$ and $\beta$ are relatively prime, while $l > e(\mathcal{W}/Q)$, as in Lemma 7.5.2. Then $z \in F \cap O_{K, \mathcal{W}}$.

Conversely, if $x \in \mathbb{N}$, then there exist $x_1, x_2, x_3 \in O_{K, \mathcal{W}}[\delta] \subseteq O_{K, \mathcal{W}; \delta}$, $c_{1,0}, \ldots, c_{1,2p-1} \in O_{K, \mathcal{W}}$, $w_j \in O_{K, \mathcal{W}}[\delta] \subseteq O_{K, \mathcal{W}; \delta}, j = 1, \ldots, 2p - 1$ such that $x_1, x_2, x_3$ are not roots of unity and $(6.4.1)$, and $(7.5.1) - (7.5.4)$ are satisfied.

Proof.

By Proposition 6.4.1, $x'_1, x'_2, x'_3 \in FLE$. Therefore, $c_{1,j} \in K \cap FLE = F$ for all $j = 0, \ldots, 2p - 1$. Next suppose that all the product terms in $(7.5.1)$ which are zero have $c_{1,j} = 0$. Then $z = \frac{x'_3 - 1}{x'_2 - 1} \in K \cap FLE = F$ and we are
done. Therefore, without loss of generality, we can assume that for some \( j^* \in \{1, \ldots, 2p - 1\} \) we have that \( c_{1,j^*} \neq 0 \) and

\[
z - \frac{x_j^c - 1}{x_j^e - 1} - c_{1,j^*}^h \bar{w}_{j^*} = 0 \tag{7.5.5}
\]

Since \( P \) has all of its factors outside \( \mathcal{W}_K \), all of its factors must be outside \( \mathcal{W}_K \). Indeed, if \( \tau \) is a factor of \( P \) in \( \mathcal{W}_K \setminus \mathcal{W}_K \), then \( \tau \) must have an \( F \)-conjugate \( \bar{\tau} \in \mathcal{W}_K \). But if \( \tau \) and \( \bar{\tau} \) are conjugates over \( F \), they are also conjugates over \( \bar{Q} \) and \( \bar{\tau} \) must be a factor of \( P \), contradicting the choice of \( P \). Thus \( c_{1,j^*} \) is divisible by at least one prime outside \( \mathcal{W}_K \) and therefore is not a unit of \( O_K,\mathcal{W}_K \). Hence by Corollary 5.3.5, \( c_{1,j^*}^h = y \bar{v}, y \in O_F, y \) is not divisible by any prime of \( \mathcal{W}_K \), \( \bar{v} \in F \) is divisible by primes of \( \mathcal{W}_K \) only and

\[
|N_{K/Q}(De)| < |N_{K/Q}(y)|^c, i = 0, \ldots, m - 1, \tag{7.5.6}
\]

where

\[
N_{K/Q}(\beta)z = e_0 + e_1 \gamma + \ldots + e_{m-1} \gamma^{m-1}, e_i \in F. \tag{7.5.7}
\]

Next we turn our attention to the equations in (7.5.1) and (7.5.2). First of all, let

\[
x_j^c - 1 \quad x_j^e - 1 = f_0 + f_1 \delta + \ldots + f_{2p-1} \delta^{2p-1}, f_i \in O_K,\mathcal{W}_K \cap F
\]

\[
\bar{w}_{j^*} = g_0,j^* + g_1,j^* \delta + \ldots + g_{2p-1,j^*} \delta^{2p-1}
\]

where \( g_0,j^*, \ldots, g_{2p-1,j^*} \in O_K,\mathcal{W}_K \). Then (7.5.1) can be rewritten as

\[
z - (f_0 + f_1 \delta + \ldots + f_{2p-1} \delta^{2p-1}) = c_{1,j^*}^h (g_0,j^* + g_1,j^* \delta + \ldots + g_{2p-1,j^*} \delta^{2p-1})
\]

Since \( \delta \) of degree 2p over \( K \), we can conclude that

\[
z - f_0 = c_{1,j^*}^h g_0,j^*.
\]

Further, \( N_{K/Q}(\beta)z - N_{K/Q}(\beta)f_0 = y^{c} \bar{g}, \) with \( \bar{g} \in O_K,\mathcal{W}_K \). Since \( y \in O_F \) is not divisible by any prime in \( \mathcal{W}_K \), and \( f_0 \in F \cap O_K,\mathcal{W}_K \), by the Strong Approximation Theorem, for some \( \bar{\tilde{f}} \in O_F \), we have that \( N_{K/Q}(\beta)\tilde{f} = y^{c} \bar{g}, \bar{g} \in O_K,\mathcal{W}_K \). Thus,

\[
N_{K/Q}(\beta)z - \bar{\tilde{f}} = y^{c} \bar{g}, \bar{g} \in O_K,\mathcal{W}_K.
\]

But \( \frac{N_{K/Q}(\beta)z - \bar{\tilde{f}}}{y^{c}} \) has a non-negative order at every element of \( \mathcal{W}_K \). Thus, \( \bar{g} \in O_K \). Now by the Weak Vertical Method (Theorem 7.1.2), we can conclude that \( N_{K/Q}(\beta)z \in F \). Hence, \( z \in F \).
Conversely, let \( x \in \mathbb{N} \). By Proposition 6.4.1 applied to the extension \( KLE/K \), we can find a solution \( y \in O_{KLE,W_{KLE}} \) to (6.4.1) such that \( y \) is not a root of unity and the divisor of \( y \) consists of factors of \( W_K \) only. By Corollary 6.1.5 also applied to the extension \( KLE/K \), there exists \( l_1 \in \mathbb{N} \setminus \{0\} \) such that \( x_1 = y^h \in O_{K,W_{KLE}}[\delta] \) and (7.5.4), (7.5.3) can be satisfied with \( c_{1,0}, \ldots, c_{1,2p-1} \in O_{K,W_{KLE}} \). Next, we apply Corollary 6.1.5 again to find \( l_2 \in \mathbb{N} \setminus \{0\} \) such that \( x_2 = y^h \in O_{K,W_{KLE}}[\delta] \) and \( x_2 - 1 \equiv 0 \mod \mathfrak{d} \), where \( \mathfrak{d} \) is the product of the non-\( W_K \) parts of the divisors of \( c_{1,j}^{ch} \) for all \( j = 1, \ldots, 2p-1 \) such that \( c_{1,j} \neq 0 \). Indeed, suppose that \( c_{1,1} = \ldots = c_{1,2p-1} = 0 \). Then \( x_1' = c_{1,0} \in F \) and \( 1 = n_{KLE/KE}(x_1') = x_1'^2 \), making \( x_1 \) a root of unity contrary to our assumptions. Finally, let \( x_3 = x_2^2 \). Then \( x_3 \) is also a solution to (6.4.1). On the other hand,

\[
\frac{x_3 - 1}{x_2 - 2} - z \equiv 0 \mod x_2 - 1 \equiv 0 \mod \mathbb{Z}[x_2] \subset O_{K,W_{KLE}}[\delta].
\]

Since \( x_2 - 1 \equiv 0 \mod c_{1,j}^{ch} \in O_{K,W_{KLE}}[\delta] \) for all \( j \) such that \( c_{1,j} \neq 0 \), we can find a \( j^* \in \{1, \ldots, 2p-1\} \) so that \( w_j \in O_{K,W_{KLE}}[\delta] \) satisfies (7.5.5).

### 7.5.4 Corollary.

\[ O_{K,W_{KLE}} \cap F \leq \text{Dioph } O_{K,W_{KLE}}. \]

**Proof.**

First of all we need to rewrite System (6.4.1) as a system over \( K \) with solutions in \( K \). Let \( \sigma_1 = \text{id}, \ldots, \sigma_p \) be all the elements of \( \text{Gal}(LEK/LK) \) and let \( \tau_1 = \text{id}, \tau_2 \) be all the elements of \( \text{Gal}(LEK/KE) \). Then let \( x = \sum_{i=0}^{2p-1} c_i \delta^i, c_i \in K \), and consider the system

\[
\begin{cases}
\Pi_{j=1}^{p} \left( \sum_{i=0}^{2p-1} c_i \sigma_j(\delta^i) \right) = 1, \\
\Pi_{j=1}^{2} \left( \sum_{i=0}^{2p-1} c_i \tau_j(\delta^i) \right) = 1.
\end{cases}
\]

(7.5.8)

It is pretty clear that \( x \in O_{K,W_{KLE}}[\delta] \) is a solution to System (6.4.1) if and only if \( c_0, \ldots, c_{2p-1} \in O_{K,W_{KLE}} \) are a solution to System (7.5.8).

Similarly, we can set \( x_j = \sum_{i=0}^{2p-1} c_{i,j} \delta^i, w_i = \sum_{i=0}^{2p-1} f_{i,i} \delta^i \) and rewrite the equation in (7.5.1) as

\[
\prod_{l=1}^{2p-1} \left( z - \left( \sum_{i=0}^{2p-1} c_{3,i} \delta^i \right)^{f} - 1 - c_{1,l}^{ch} \left( \sum_{i=0}^{2p-1} f_{i,i} \delta^i \right) \right) = 0.
\]

(7.5.9)
Then if we let $\Delta = \{1, \delta, \ldots, \delta^{2p-1}\}$, we can use coordinate polynomials with respect to this basis to rewrite (7.5.8) and (7.5.9) as polynomial equations with coefficients in $O_K$ and all the variables ranging over $O_K, W_K$. (See Section B.7 for a discussion of coordinate polynomials.)

Next we address the issue of making sure that $x_1, x_2, x_3$ are not roots of unity. By our choice of $r$, it is enough to make sure that $x_{r}^{j} - 1 \neq 0$. To accomplish this we can again use coordinate polynomials and the fact that $O_K, W_K$ is Dioph-regular. We leave the details to the reader.

Finally, given any $x \in O_K, W_K$ and any positive integer $l$, if we force $x^{lh}, (x+1)^{lh}, \ldots, (x+lh)^{lh}$ into $F$, then by Corollary B.10.10, we can conclude that $x \in F$. This observation completes the proof of the corollary.

We are almost ready for our main vertical result, but we need to add items to our notation list before we proceed.

### 7.5.5 Notation.

- Let $F_1, \ldots, F_r$ be all the cyclic subextensions of $K$.
- For each $j = 1, \ldots, r$, let the pair of primes $\mathfrak{p}_{F_j}, \mathfrak{p}_j$ in $F_j$ and $K$ respectively satisfy the requirements with respect to the extension $K/F_j$ in place of extension $K/F$ as listed in Notation 7.5.1.
  - Let $\mathcal{H}_{K,j} = \mathcal{V}_K \cup \{\mathfrak{p}_j\}$.
  - Let $\mathcal{H}_K = \mathcal{V}_K \cup \{\mathfrak{p}_1\} \cup \ldots \cup \{\mathfrak{p}_r\}$.

We are now ready to prove the main theorem for this section.

### 7.5.6 Theorem.

$O_{K, W_K} \cap \mathbb{Q} \leq_{\text{Dioph}} O_{K, W_K}$.

**Proof.**

By Corollary 7.5.4, we have that $O_{K, W_K,i} \cap F_i \leq_{\text{Dioph}} O_{K, W_K,j}$. Further, from Chapter 4 we also know that $O_{K, W_K,i} \leq_{\text{Dioph}} O_{K, W_K}$. Thus, by transitivity of Dioph-generation, $O_{K, W_K,i} \cap F_i \leq_{\text{Dioph}} O_{K, W_K}$. Next by the Finite Intersection Property of Dioph-generation we also have that

$$R = \left( \bigcap_{i=1}^{r} O_{K, W_K,i} \right) \cap \mathbb{Q} = \left( \bigcap_{i=1}^{r} O_{K, W_K,i} \right) \cap \left( \bigcap_{i=1}^{r} F_i \right) \leq_{\text{Dioph}} O_{K, W_K}.$$
Finally, using Dioph-regularity of $R$, which is a ring of $S$-integers of $\mathbb{Q}$ with possibly infinite $S$, together with transitivity of Dioph-generation, we get $\mathbb{Q} \leq_{\text{Dioph}} O_{K,\mathfrak{a}_K}$ and at last, by the Finite Intersection Property again, $\mathbb{Q} \cap O_{K,\mathfrak{a}_K} \leq_{\text{Dioph}} O_{K,\mathfrak{a}_K}$.

### 7.6 Consequences for Vertical Definability over Totally Real Fields.

In this section we will discuss several useful consequences of Theorem 7.5.6. We will start with a corollary which follows immediately from the Theorem 7.5.6.

#### 7.6.1 Corollary.

Let $K/\mathbb{Q}$ be a Galois extension of degree $n$ with $K$ a totally real number field. Let $E$ be a cyclic totally real extension of $\mathbb{Q}$ of degrees $p > n$. Let $\mathcal{V}_K$ be a set of primes of $K$ not splitting in the extension $EK/K$. Then there exists a set of $K$-primes $\mathcal{V}_K^{\ell}$ such that $(\mathcal{V}_K \setminus \mathcal{V}_K^{\ell}) \cup (\mathcal{V}_K^{\ell} \setminus \mathcal{V}_K)$ is a finite set and $O_{K,\mathfrak{a}_K} \cap \mathbb{Q} \leq_{\text{Dioph}} O_{K,\mathfrak{a}_K}$.

Our next step is to observe that we actually have a slightly stronger corollary.

#### 7.6.2 Corollary.

Let $K/\mathbb{Q}$ be a Galois extension of degree $n$ with $K$ a totally real number field. Let $E$ be cyclic totally real extensions of $\mathbb{Q}$ of degrees $p > n$. Let $\mathcal{V}_K$ be a set of primes of $K$ such that all but finitely many primes of $\mathcal{V}_K$ do not split in the extension $EK/K$. Then there exists a set of $K$-primes $\mathcal{V}_K^{\ell}$ containing $\mathcal{V}_K$ such that $\mathcal{V}_K \setminus \mathcal{V}_K^{\ell}$ is a finite set and $O_{K,\mathfrak{a}_K} \cap \mathbb{Q} \leq_{\text{Dioph}} O_{K,\mathfrak{a}_K}$.

The proof of this statement is very similar to the proof of Theorem 7.5.6 and we leave the details to the reader. Our next step is to drop the assumption that the field in question is Galois.

#### 7.6.3 Corollary.

Let $K/\mathbb{Q}$ be a finite extension with $K$ being a totally real number field. Let $K_G$ be the Galois closure of $K$ over $\mathbb{Q}$. Let $n = [K_G : \mathbb{Q}]$. Let $E$ be a totally
real cyclic extension of \( \mathbb{Q} \) of degree \( p > n \). Let \( \mathcal{U}_K \) be a set of primes of \( K \) such that all but finitely many of them do not split in the extensions \( EK/K \). Then there exists a set of \( K \)-primes \( \mathcal{U}_K \) containing \( \mathcal{U}_K \) such that \( \mathcal{U}_K \setminus \mathcal{U}_K \) is a finite set and \( O_{K,\mathcal{U}_K} \cap \mathbb{Q} \leq \text{Dioph} \ O_{K,\mathcal{U}_K} \).

**Proof.**

First of all, we observe that \( K_G \) is also a totally real number field. Secondly, we note that by Lemma B.3.3 and assumption on the degrees of \( E \) and \( K_G \), we have that \( K_G \) and \( E \) are linearly disjoint over \( \mathbb{Q} \), and therefore so are \( K \) and \( E \). Let \( \mathfrak{p}_K \) be a prime of \( K \) not splitting in the extension \( EK/K \). Let \( \mathfrak{p}_\mathbb{Q} \) be the prime below \( \mathfrak{p}_K \) in \( \mathbb{Q} \), and let \( \mathfrak{p}_K \) be a prime above \( \mathfrak{p}_\mathbb{Q} \) in \( K_G \). Then by Lemma B.4.7, \( \mathfrak{p}_\mathbb{Q} \) does not split in the extensions \( E/\mathbb{Q} \). Consequently, by Lemma B.4.8, \( \mathfrak{p}_K \) does not split in the extension \( EK_G/K_G \). Let \( \mathcal{W}_K \) be the set of \( K \)-primes above the primes of \( \mathcal{W}_K \). Then \( \mathcal{W}_K \) satisfies the conditions of Corollary 7.6.2. Hence, there exists a set of \( K_G \)-primes \( \bar{\mathcal{W}}_K \) containing \( \mathcal{W}_K \) such that \( \bar{\mathcal{W}}_K \setminus \mathcal{W}_K \) is a finite set and \( O_{K,\mathcal{W}_K} \cap \mathbb{Q} \leq \text{Dioph} \ O_{K,\mathcal{W}_K} \).

Let \( \bar{\mathcal{W}}_{K_G} \) be the closure of \( \bar{\mathcal{W}}_K \) with respect to conjugation over \( K \). Since \( \mathcal{W}_{K_G} \) was closed with respect to conjugation over \( K \) and \( \bar{\mathcal{W}}_K \) is larger than \( \bar{\mathcal{W}}_{K_G} \) by finitely many primes only, \( \bar{\mathcal{W}}_K \setminus \mathcal{W}_{K_G} \) is still finite. Let \( \bar{\mathcal{W}}_K \) be the set of all \( K \)-primes below the primes of \( \bar{\mathcal{W}}_K \) and observe that \( O_{K,\bar{\mathcal{W}}_K} \) is the integral closure of \( O_{K,\mathcal{W}_K} \) in \( K_G \). Note also that the set \( \bar{\mathcal{W}}_K \setminus \mathcal{W}_K \) is finite.

From Proposition 2.2.1 and from Theorem 4.2.4 we have the following:

\[
O_{K,\bar{\mathcal{W}}_K} \cap \mathbb{Q} \leq \text{Dioph} \ O_{K,\bar{\mathcal{W}}_K}, \tag{7.6.1}
\]

\[
O_{K,\bar{\mathcal{W}}_K} \leq \text{Dioph} \ O_{K,\mathcal{W}_K}, \tag{7.6.2}
\]

\[
O_{K,\mathcal{W}_K} \leq \text{Dioph} \ O_{K,\bar{\mathcal{W}}_K}, \tag{7.6.3}
\]

If we now combine the equations in (7.6.1)–(7.6.3) and use transitivity of Diophantine generation, we conclude that

\[
\mathbb{Q} \cap O_{K,\mathcal{W}_K} \leq \text{Dioph} \ O_{K,\mathcal{W}_K}, \tag{7.6.4}
\]

But \( \mathbb{Q} \cap O_{K,\mathcal{W}_K} \) is Dioph-regular by Proposition 2.2.4 and therefore by transitivity again \( \mathbb{Q} \leq \text{Dioph} \ O_{K,\mathcal{W}_K} \). Since \( O_{K,\mathcal{W}_K} \leq \text{Dioph} \ O_{K,\mathcal{W}_K} \), by Finite Intersection Property (Proposition 2.1.19),

\[
\mathbb{Q} \cap O_{K,\mathcal{W}_K} \leq \text{Dioph} \ O_{K,\mathcal{W}_K}, \tag{7.6.5}
\]

This concludes the proof of the corollary.
We can call the preceding results a “view from above”, that is from the point of view of the primes of $K$. Now we consider the same situation but from the point of view of the primes of $\mathbb{Q}$ – a “view from below”.

7.6.4 Corollary.

Let $K/\mathbb{Q}$ be a finite extension with $K$ being a totally real number field. Let $K_\mathcal{C}$ be the Galois closure of $K$ over $\mathbb{Q}$. Let $n = [K_\mathcal{C} : \mathbb{Q}]$. Let $E$ be a totally real cyclic extension of $\mathbb{Q}$ of degrees $p > n$. Let $\mathcal{W}_\mathbb{Q}$ be a set of primes of $\mathbb{Q}$ such that all but finitely many primes of $\mathcal{W}_\mathbb{Q}$ do not split in the extension $E/\mathbb{Q}$. Then there exists a set of $\mathbb{Q}$-primes $\mathcal{W}_\mathbb{Q}^o$ containing $\mathcal{W}_\mathbb{Q}$ such that $\mathcal{W}_\mathbb{Q}^o \setminus \mathcal{W}_\mathbb{Q}$ is a finite set and $O_{\mathbb{Q},\mathcal{W}_\mathbb{Q}^o}$ has a Diophantine definition over its integral closure in $K$.

Proof.

Let $\mathfrak{p}_\mathbb{Q} \in \mathcal{W}_\mathbb{Q}$ and let $\mathfrak{p}_K$ be a prime above it in $K$. Then by Lemma B.4.8, $\mathfrak{p}_K$ does not split in the extensions $EK/K$. Let $\mathcal{W}_K$ be the set of all $K$-factors of primes in $\mathcal{W}_\mathbb{Q}$. Then, by Corollary 7.6.3, there exists a set of $K$-primes $\mathcal{W}_K^o$ containing $\mathcal{W}_K$, such that $\mathcal{W}_K^o \setminus \mathcal{W}_K$ is a finite set and $O_{K,\mathcal{W}_K^o} \cap \mathbb{Q} \leq \text{Dioph} O_{K,\mathcal{W}_K^o}$. Let $\mathcal{W}_K^c$ be the closure of $\mathcal{W}_K$ under conjugation over $\mathbb{Q}$. Then, since $\mathcal{W}_K$ was closed under conjugation over $\mathbb{Q}$, we have that $\mathcal{W}_K^c \setminus \mathcal{W}_K$ is finite. Let $\mathcal{W}_\mathbb{Q}^c$ be the set of rational primes below $\mathcal{W}_K$. Then $\mathcal{W}_\mathbb{Q}^c \setminus \mathcal{W}_\mathbb{Q}$ is finite and $O_{K,\mathcal{W}_\mathbb{Q}^c}$ is the integral closure of $O_{\mathbb{Q},\mathcal{W}_\mathbb{Q}}$ in $K$. Thus, as above, we have the following relations

$$O_{K,\mathcal{W}_\mathbb{Q}} \leq \text{Dioph} O_{K,\mathcal{W}_\mathbb{Q}^c},$$

$$O_{K,\mathcal{W}_\mathbb{Q}} \cap \mathbb{Q} \leq \text{Dioph} O_{K,\mathcal{W}_\mathbb{Q}}$$

and therefore

$$O_{K,\mathcal{W}_\mathbb{Q}} \cap \mathbb{Q} \leq \text{Dioph} O_{K,\mathcal{W}_\mathbb{Q}}.$$

On the other hand, as before $\mathbb{Q} \leq \text{Dioph} O_{K,\mathcal{W}_\mathbb{Q}} \cap \mathbb{Q}$ by Proposition 2.2.4. Therefore, $\mathbb{Q} \leq \text{Dioph} O_{K,\mathcal{W}_\mathbb{Q}}$. Finally, we certainly have $O_{K,\mathcal{W}_\mathbb{Q}} \leq \text{Dioph} O_{K,\mathcal{W}_\mathbb{Q}}$. Thus by Finite Intersection Property (see Proposition 2.1.19), $O_{\mathbb{Q},\mathcal{W}_\mathbb{Q}^o} = \mathbb{Q} \cap O_{K,\mathcal{W}_\mathbb{Q}} \leq \text{Dioph} O_{K,\mathcal{W}_\mathbb{Q}}$. This concludes the proof of the corollary.

We finish with two more vertical definability results whose proofs are analogous to the proofs above and are left to the reader.
7.6.5 Corollary.
Let \( K/U \) be a finite extension of totally real number fields. Let \( K_G \) be the Galois closure of \( K \) over \( \mathbb{Q} \). Let \( n = [K_G : \mathbb{Q}] \). Let \( E \) be a totally real cyclic extension of \( \mathbb{Q} \) of degrees \( p > n \). Let \( \mathcal{W}_K \) be a set of primes of \( K \) such that all but finitely many primes of \( \mathcal{W}_K \) do not split in the extension \( EK/K \). Then there exists a set of \( K \)-primes \( \bar{\mathcal{W}}_K \) containing \( \mathcal{W}_K \) such that \( \bar{\mathcal{W}}_K \setminus \mathcal{W}_K \) is a finite set and \( O_{K, \mathcal{W}_K} \cap U \leq_{\text{Dioph}} O_{K, \bar{\mathcal{W}}_K} \).

7.6.6 Corollary.
Let \( K/U \) be a finite extension of totally real number fields. Let \( K_G \) be the Galois closure of \( K \) over \( \mathbb{Q} \). Let \( n = [K_G : \mathbb{Q}] \). Let \( E \) be a totally real cyclic extension of \( \mathbb{Q} \) of degree \( p > n \). Let \( \mathcal{W}_U \) be a set of primes of \( U \) such that all but finitely many primes of \( \mathcal{W}_U \) do not split in the extension \( EU/U \). Then there exists a set of \( U \)-primes \( \bar{\mathcal{W}}_U \) containing \( \mathcal{W}_U \) such that \( \bar{\mathcal{W}}_U \setminus \mathcal{W}_U \) is a finite set and \( O_{U, \mathcal{W}_U} \) has a Diophantine definition over its integral closure in \( K \).

7.7 Horizontal Definability for the Rings of \( \mathcal{W} \)-integers of Totally Real Number Fields and Diophantine Undecidability for These Rings.

In this section we convert the vertical definability results into a horizontal definability results and into a result asserting Diophantine undecidability of some rings of \( \mathcal{W} \)-integers. We start with an undecidability result.

7.7.1 Theorem.
Let \( K/\mathbb{Q} \) be a finite extension with \( K \) being a totally real number field. Let \( K_G \) be the Galois closure of \( K \) over \( \mathbb{Q} \). Let \( n = [K_G : \mathbb{Q}] \). Let \( E \) be a totally real cyclic extension of \( \mathbb{Q} \) of degree \( p > n \). Let \( \mathcal{W}_K \) be a set of primes of \( K \) such that all but finitely many primes of \( \mathcal{W}_K \) do not split in the extension \( EK/K \). Assume further that all but possibly finitely many primes of \( \mathcal{W}_K \) have a conjugate over \( \mathbb{Q} \) which is not in \( \mathcal{W}_K \). Then there exists a set of \( K \)-primes \( \bar{\mathcal{W}}_K \) containing \( \mathcal{W}_K \) such that \( \bar{\mathcal{W}}_K \setminus \mathcal{W}_K \) is a finite set and \( \mathbb{Z} \leq_{\text{Dioph}} O_{K, \bar{\mathcal{W}}_K} \). Thus HTP is undecidable over \( O_{K, \bar{\mathcal{W}}_K} \).
Proof.

By Corollary 7.6.3, there exists a set of $K$-primes $\mathfrak{W}_K$ containing $\mathfrak{W}_K$ such that $\mathfrak{W}_K \setminus \mathfrak{W}_K$ is a finite set and $\mathbb{Q} \cap O_K, \mathfrak{W}_K \leq \text{Dioph } O_K, \mathfrak{W}_K$. Since $\mathfrak{W}_K$ differs from $\mathfrak{W}_K$ by at most finitely many primes, all but possibly finitely many primes of $\mathfrak{W}_K$ have a $Q$-conjugate in $K$ which is not in $K$. By Lemma B.4.20, $\mathbb{Q} \cap O_K, \mathfrak{W}_K = O_{Q, V}$, where $V_Q$ is a finite, possibly empty, set. From Theorem 4.2.4 we know that $\mathbb{Z} \leq \text{Dioph } O_{Q, V}$ and the theorem now follows by transitivity of Diophantine generation.

Now we state the horizontal definability result.

7.7.2 Corollary.

Let $K/\mathbb{Q}$ be a finite extension with $K$ being a totally real number field. Let $K_G$ be the Galois closure of $K$ over $\mathbb{Q}$. Let $n = [K_G : \mathbb{Q}]$. Let $E$ be a totally real cyclic extension of $\mathbb{Q}$ of degree $p > n$ respectively. Let $\mathfrak{W}_K$ be a set of primes of $K$ such that all but finitely many primes of $\mathfrak{W}_K$ do not split in the extension $EK/K$. Assume further that all but possibly finitely many primes of $\mathfrak{W}_K$ have a conjugate over $\mathbb{Q}$ which is not in $\mathfrak{W}_K$. Then there exists a set of $K$-primes $\mathfrak{W}_K$ containing $\mathfrak{W}_K$ such that $\mathfrak{W}_K \setminus \mathfrak{W}_K$ is a finite set and $O_K \leq \text{Dioph } O_K, \mathfrak{W}_K$.

Proof.

From Theorem 7.7.1 we have that $\mathbb{Z} \leq \text{Dioph } O_K, \mathfrak{W}_K$. By Proposition 2.2.1, $O_K \leq \text{Dioph } \mathbb{Z}$. Therefore by transitivity, $O_K \leq \text{Dioph } O_K, \mathfrak{W}_K$.

7.8 Vertical Definability Results for Rings of $\mathfrak{W}$-integers of the Totally Complex Extensions of Degree 2 of Totally Real Number Fields.

In this section we will obtain results analogous to the ones we have obtained in the preceding section for totally real fields, for totally complex extensions of degree 2 of totally real fields. We obtain this extension, as in the case of the ring of integers, using the fact that a totally real field and its totally complex extensions of degree 2 have integral unit groups of the same rank. We will use this property of the fields involved in combination with the Weak Vertical Method to give a Diophantine definition of a ring of $\mathfrak{W}$-integers of a totally real field over its integral closure in a totally complex extension of degree 2. As usual, we start with a notation list to be used in this section.
7.8.1 Notation.

- Let \( K \) be a totally real field of degree \( n \) over \( \mathbb{Q} \).
- Let \( d \in K \) be such that \( M = K(\sqrt{d}) \) is a totally complex extension of \( \mathbb{Q} \).
- Let \( E \) be a totally real cyclic extension of \( \mathbb{Q} \) of odd prime degree \( p > 2n! \).
- Let \( m \in \mathbb{N} \) be as in Lemma 6.4.3.
- Let \( \delta_E \) be an integral generator of \( E \) over \( \mathbb{Q} \) (and therefore a generator of \( ME \) over \( M \)).
- Let \( D \) be the discriminant of \( \delta_E \).
- Let \( G(T) = G_0 \) be the monic irreducible polynomial of \( \delta_E \) over \( \mathbb{Q} \).
- Let \( G_i(T) = G(T + i), i = 1, \ldots, 2n \).
- Let \( \mathfrak{W}_M \) be a set of primes of \( M \) not splitting in the extension \( ME/M \) and not dividing the discriminant of \( G_i(T) \) for any \( i = 0, \ldots, 2n \).
- Let \( \mathfrak{V}_M \) be a set of primes of \( M \) containing \( \mathfrak{W}_M \) and such that the difference between the sets is finite.
- Let \( \bar{\mathfrak{W}}_M \) be the closure of \( \mathfrak{W}_M \) under conjugation over \( K \).
- Let \( c = c(d) \) be the constant from Corollary 5.3.5 applied to the extension \( M/K \) and the basis \( \{1, \sqrt{d}\} \).
- Let \( l_0 = 0, \ldots, l_z \) be distinct integers, \( z = 2pn \).
- Let \( \mathfrak{W}_K \) be the set of \( K \) primes below \( \mathfrak{W}_M \).
- Let \( h_K, h_M \) denote the class numbers of \( K \) and \( M \) respectively.
- Let \( P \) be a fixed rational prime such that all of its \( M \)-factors are outside \( \mathfrak{W}_M \). (We can again use Lemma B.4.7 to find such a \( P \).)
- \( \{\omega_1, \ldots, \omega_n\} \) be a basis of \( K \) over \( \mathbb{Q} \).
- Let \( \sigma_1 = \text{id}, \ldots, \sigma_n : K \to \mathbb{C} \) be all the embeddings of \( K \) into \( \mathbb{C} \).

Our next step is a lemma which will use norm equations to push some elements of \( M \) into \( K \).
7.8.2 Lemma.

Let $\varepsilon$ be an element of the integral closure of $O_{M,W_M}$ in $EM$ such that

$$\mathbf{N}_{ME/M}(\varepsilon) = 1,$$

and assume that $\varepsilon^m = \sum_{i=0}^{p-1} a_i \delta^i_E$, $a_i \in O_{M,W_M}$. Then $\varepsilon$ is an integral unit of $O_{EM}$ and $a_0, \ldots, a_{p-1} \in O_{M,W_M} \cap K$.

Proof.

By Lemma 6.4.3 we have that $\varepsilon \in O_{ME}$ and $\varepsilon^m \in KE$. Since $\delta_E$ also generates $KE/K$ and $[KE : K] = [ME : M]$, for some $b_i \in K$ we have that $\varepsilon^m = \sum_{i=0}^{p-1} b_i \delta^i_E$, where $b_i \in K \subseteq M$. Since $b_i$ must be equal to $a_i$, the assertion of the lemma follows.

The next lemma makes use of the norm equation to construct a Diophantine definition. As the reader no doubt will see, this lemma is very similar in flavor to Theorem 7.5.3, but some details are a bit different.

7.8.3 Lemma.

Suppose the following equations are satisfied in variables $a_{0,j}, \ldots, a_{p-1,j}, b_{0,j}, \ldots, b_{p-1,j}, x, x_r, f_{s,r,0}, \ldots, f_{s,r,z}, U_{0,r}, \ldots, U_{p-1,r}, v_{0,r}, \ldots, v_{p-1,r}$ ranging over $O_{M,W_M}$ for some $s = 1, \ldots, p - 1$, for all $r = 0, \ldots, h_M$, and all $j = 1, \ldots, h_M + 2$:

$$\nu_j = \sum_{i=0}^{p-1} a_{i,j} \delta^i_E;$$

(7.8.2)

$$\rho_j = \sum_{i=0}^{p-1} b_{i,j} \delta^i_E;$$

(7.8.3)

$$\mathbf{N}_{ME/M}(\rho_j) = 1;$$

(7.8.4)

$$\nu_j = \rho_j^m;$$

(7.8.5)

$$x_r = (x + r)^{h_M},$$

(7.8.6)

$$a_{s,1} \neq 0, a_{s,1} \equiv 0 \text{ modulo } P;$$

(7.8.7)

$$f_{s,r,i} = \frac{a_{s,1}^{h_k}}{\prod_{u=0}^{2n} G_u(x_r - l)}, i = 0, \ldots, z;$$

(7.8.8)

$$U_{0,r} + U_{1,r} \delta_E + \ldots + U_{p-1,r} \delta_E^{p-1} = \frac{\nu_{r+2}^2 - 1}{\nu_2 - 1};$$

(7.8.9)
\[ x_r - U_{0,r} - U_{1,r} \delta_E - \ldots - U_{p-1,r} \delta_E^{p-1} = a_{s,1}^{ch} (v_{s,0,r} + v_{s,1,r} \delta_E + \ldots + v_{s,p-1,r} \delta_E^{p-1}). \]  

(7.8.10)

Then \( x \in K \).

Proof.

By Lemma 7.8.2, for all \( j = 1, \ldots, h_M + 2 \) we have that \( \nu_j \) is an integral unit of \( KE \) and \( a_{i,j} \in O_{K,\mathcal{W}_K} \). Next note the following. Let \( s^* \) be the value of \( s \) for which the equations hold, and assume that \( a_{s,1} = 0 \). Then we are done because (7.8.10) in this case will force \( x_r \) into \( M \cap K(\delta_E) = K \), and Corollary B.10.10 will place \( x \) into \( K \). Thus without loss of generality we can assume that equations hold for some value of \( s \) with \( a_{s,1} \neq 0 \). We fix this value of \( s \) for the remainder of the discussion.

We now observe that by Lemma B.4.18, for all \( u = 0, \ldots, n \), for all \( x \in M \), for all \( \wp \in \mathcal{W}_M \), we have that \( \text{ord}_{\wp} G_r(x) \leq 0 \). Further by Corollary 5.3.5, we have that \( a_{s,1}^{h_0} = z_s y_s \), where \( z_s, y_s \in O_K \), \( y_s \neq 0 \), \( y_s \equiv 0 \) modulo \( P \), is a prime not lying below any prime of \( M \) in \( \mathcal{W}_M \), the \( M \)-divisor of \( y_s \) is consists of primes outside \( \mathcal{W}_M \), the \( M \)-divisor of \( z_s \) consists of primes from \( \mathcal{W}_M \), and

\[ x_r = \alpha_r / \beta_r, \alpha_r, \beta_r \in O_M; \]  

(7.8.11)

\[ N_{M/Q}(\beta_r)x_r = e_{0,r} + e_{1,r} \sqrt{d}; \]  

(7.8.12)

\[ |N_{K/Q}(de_{i,r})| < |N_{K/Q}(y_s^c)|, i = 0, 1. \]  

(7.8.13)

From (7.8.9)-(7.8.10) we get that \( x_r - U_{0,r} = a_{s,1}^{ch} y_{s,0,r} \), where \( U_{0,r} \in O_{K,\mathcal{W}_K} \).

Further,

\[ N_{M/Q}(\beta_r)x_r - N_{M/Q}(\beta_r)U_{0,r} = N_{M/Q}(\beta_r)a_{s,1}^{ch} v_{0,r} = y^c \bar{v}, \]

where \( \bar{v} \in O_{M,\mathcal{W}_M} \). Since \( y \in O_K \) is not divisible by any prime of \( \mathcal{W}_M \) and \( N_{M/Q}(\beta_r)U_{0,r} \in K \cap O_{M,\mathcal{W}_M} \), by the Strong Approximation Theorem, there exists \( \tilde{\beta}_r \in O_K \) such that \( N_{M/Q}(\beta_r)_{y^c} = \tilde{\beta}_r \in O_{M,\mathcal{W}_M} \). Hence,

\[ N_{M/Q}(\beta_r)x_r - \tilde{\beta}_r = y^c C_r, \]

where \( C_r \in O_{M,\mathcal{W}_M} \). On the other hand, \( N_{M/Q}(\beta_r)x_r - \tilde{\beta}_r \) has non-negative order at all the primes at which elements of the ring \( O_{M,\mathcal{W}_M} \) are allowed to have negative orders. Therefore, \( C_r \in O_M \) and by The Weak Vertical Method (Theorem 7.1.2), \( x_r \in K \). By Corollary B.10.10, having \( x_r \in K \) for \( r = 1, \ldots, h_M \) implies \( x \in K \) as above.
7.8.4 Lemma.

Let \( x \in \mathbb{N}, x \neq 0 \). Then all the equations (7.8.2)-(7.8.10) can be satisfied in all the other variables over \( O_{M,W} \).

Proof.

Let \( x \) be a non-zero natural number. Then for all \( r \) let \( x_r = (x + r)^{h_M} \) to satisfy (7.8.6) and note that \( x_r \) will also be a non-zero natural number. Next let \( \mu \) be an integral unit of \( K \) such that \( N_{KE/K}(\mu) = 1 \) and such that \( \mu \) is not a root of unity. Then \( N_{ME/M}(\mu) = 1 \) also. Let

\[
B = P \prod_{r=0}^{h_M} \prod_{i=0}^{z} \prod_{u=1}^{2n} G_u(x_r - l_i)
\]

By Corollary 6.1.5 applied to the extension \( KE/K \), there exists a positive natural number \( l(B) \) such that for any positive integer \( k \) we have that

\[
\mu^{k l(B)} = \sum_{i=0}^{p-1} c_i \delta_i^E, \quad c_i \in O_K,
\]

and for \( i \geq 1 \) it is the case that

\[
c_i \equiv 0 \mod P \prod_{r=0}^{h_M} \prod_{i=0}^{z} \prod_{u=1}^{2n} G_u(x_r - l_i),
\]

Let \( \rho_1 = \mu^{l(B)} \) and \( \nu_1 = \rho_1^m = \mu^{m l(B)} \). Then (7.8.2)-(7.8.5) can be satisfied for \( \nu_1 \) and \( \rho_1 \) with \( \nu_1 = \sum_{i=0}^{p-1} a_{i,1} \delta_i^E, \quad a_{i,1} \in O_K \), where by construction of \( l(B) \), for \( i \geq 1 \) we have that

\[
a_{i,1} \equiv 0 \mod P \prod_{r=0}^{h_M} \prod_{i=0}^{z} \prod_{u=1}^{2n} G_u(x_r - l_i),
\]

and for some \( i \geq 1 \) it is the case that \( a_{i,1} \neq 0 \). (Otherwise, \( \nu_1 \in K \), has \( K \)-norm 1 and thus is a root of unity.) Choose \( i \geq 1 \) such that \( a_{i,1} \neq 0 \) and set \( s = i \). Then (7.8.7) and (7.8.8) can be satisfied. Next let

\[
\rho_2 = \mu^{l(a_{s,1}^{ch_K})}, \quad \nu_2 = \rho_2^m, \quad \rho_{r+2} = \mu^{l(a_{s,1}^{ch_K})}, \quad \nu_{r+2} = \rho_{r+2}^m,
\]

where \( l(a_{s,1}^{ch_K}) \) is defined as above using Corollary 6.1.5. At this point we can also conclude that (7.8.2) - (7.8.5) will be satisfied for all \( j \). Further we see that \( \nu_{r+2} = \nu_2^{x_r} \), so that

\[
\frac{\nu_{r+2} - 1}{\nu_2 - 1} \in \mathbb{Z}[\nu_2] \subset O_K[\delta_E],
\]
and hence (7.8.9) can be satisfied with $U_{s,r} \in O_K$. Now we also note that 
$
u_2 - 1 \equiv 0$ modulo $a_{s,1}^{ch_K}$ in $O_K[\delta_E]$. Since 
$$\frac{\nu_{r+2} - 1}{\nu_2 - 1} \equiv x_r \text{ modulo } \nu_2 - 1$$
in $O_K[\delta_E]$, it is the case that 
$$\frac{\nu_{r+2} - 1}{\nu_2 - 1} \equiv x_r \text{ modulo } a_{s,1}^{ch_K} \quad (7.8.14)$$
in $O_K[\delta_E]$. Consequently, (7.8.10) is also satisfied. This concludes the proof of the lemma.

We now have all the necessary ingredients to prove the following theorem.

**7.8.5 Theorem.**

$O_{M,\mathcal{W}_M} \cap K \leq_{\text{Dioph}} O_{M,\mathcal{W}_M}$.

**Proof.**

Consider the equation

$$x = \sum \pm \frac{y_i}{y_{n+1}} \omega_i, \quad y_{n+1} \neq 0, \quad (7.8.15)$$

where for each $i = 1, \ldots, n$, we have that (7.8.2)-(7.8.10) can be satisfied for $x = y_i$ with all the other variables in $O_{M,\mathcal{W}_M}$. By Lemma 7.8.3, we know that if the equations are satisfied, then $x \in K \cap O_{M,\mathcal{W}_M}$. Further, from Lemma 7.8.4 we can conclude that every element $x$ of $K \cap O_{M,\mathcal{W}_M}$ has a representation (7.8.15), since every element of $K$ has rational coordinates with respect to the basis $\{\omega_1, \ldots, \omega_n\}$.

The only remaining task is rewriting all the equations in polynomial form and so that elements of $ME$ do not occur in the coefficients. This can be done, as before, using coordinate polynomials (see Section B.7).

We will now strengthen the result above in the same fashion as we did it for totally real number fields.

**7.8.6 Corollary.**

$O_{M,\mathcal{V}_M} \cap K \leq_{\text{Dioph}} O_{M,\mathcal{V}_M}$.

132
Proof.

The proof follows a familiar outline. As before, we have the following sequence of relations.

\[ O_M, \bar{m} \leq \text{Dioph } O_M, \bar{y}_M, \]
\[ O_M, \bar{m} \cap K \leq \text{Dioph } O_M, \bar{m}, \]
\[ K \leq \text{Dioph } O_M, \bar{m}, \]

and therefore

\[ O_M, \bar{m} \cap K \leq \text{Dioph } O_M, \bar{y}_M. \]

Now we make use of the Diophantine definitions we have constructed over totally real fields.

7.8.7 Theorem.

There exists a set of \( M \)-primes \( \bar{\mathcal{W}}_M \) containing \( \mathcal{W}_M \) such that the set \( \bar{\mathcal{W}}_M \setminus \mathcal{W}_M \) is finite and \( O_M, \bar{\mathcal{W}}_M \cap Q \leq \text{Dioph } O_M, \bar{\mathcal{W}}_M. \)

Proof.

Let \( \mathcal{W}_M \subseteq \mathcal{W}_M \) be the largest subset of \( \mathcal{W}_M \) closed under conjugation over \( K \).

Let \( \mathcal{W}_K \) be the set of primes of \( K \) below \( \mathcal{W}_M \), so that

\[ O_K, \mathcal{W}_M \cap K = O_K, \mathcal{W}_M \cap K = O_K, \mathcal{W}_K. \]

Then the primes in \( \mathcal{W}_K \) do not split in the extension \( KE/K \). (This follows from Lemma B.4.7.) Therefore, by Corollary 7.6.3 there exists a set of \( K \)-primes \( \mathcal{W}_K \), containing \( \bar{\mathcal{W}}_K \) such that \( \bar{\mathcal{W}}_K \setminus \mathcal{W}_K \) is a finite set and \( O_K, \mathcal{W}_K \cap Q \leq \text{Dioph } O_K, \mathcal{W}_K. \)

Let \( \{ \Psi_1, \ldots, \Psi_r \} = \mathcal{W}_K \setminus \bar{\mathcal{W}}_K. \) Let \( \bar{\mathcal{W}}_M \) be the result of adding to \( \mathcal{W}_M \) of all the factors of \( \{ \Psi_1, \ldots, \Psi_r \} \) in \( M \). Note that \( \bar{\mathcal{W}}_M \setminus \mathcal{W}_M \) is finite, since we added factors of finitely many primes in \( K \). Note further that \( O_M, \mathcal{W}_M \cap K = O_K, \mathcal{W}_K \) and by Corollary 7.8.6, \( O_M, \bar{\mathcal{W}}_M \cap K \leq \text{Dioph } O_M, \bar{\mathcal{W}}_M. \) Thus the assertion of the theorem follows by the transitivity of generation.

The proofs of the following results are almost identical to the proofs of the analogous results from Sections 7.6 and 7.7.

7.8.8 Corollary.

Let \( \mathcal{W}_Q \) be a set of primes of \( Q \) not splitting in the extensions \( E/Q \). Then there exists a set of \( Q \)-primes \( \bar{\mathcal{W}}_Q \) containing \( \mathcal{W}_Q \) such that \( \bar{\mathcal{W}}_Q \setminus \mathcal{W}_Q \) is a finite set and \( O_Q, \bar{\mathcal{W}}_Q \) has a Diophantine definition over its integral closure in \( M \).
7.8.9 Corollary.

Let $M/F$ be a finite extension of number fields with $M$ a totally complex extension of degree 2 of a totally real number field. Then there exists a set of $M$-primes $\mathcal{W}_M$ containing $W_M$ such that $\mathcal{W}_M \setminus W_M$ is a finite set and $O_{M,W_M} \cap F \leq_{\text{Dioph}} O_{M,W_M}$.

7.8.10 Theorem.

Assume that all but possibly finitely many primes of $W_M$ have a conjugate over $\mathbb{Q}$ that is not in $W_M$. Then there exists a set of $M$-primes $\mathcal{W}_M$ containing $W_M$ such that $\mathcal{W}_M \setminus W_M$ is a finite set and $\mathbb{Z} \leq_{\text{Dioph}} O_{M,W_M}$. Thus HTP is undecidable over $O_{M,W_M}$.

7.8.11 Corollary.

Assume that all but possibly finitely many primes of $W_M$ have a conjugate over $\mathbb{Q}$ that is not in $W_M$. Then there exists a set of $M$-primes $\mathcal{W}_M$ containing $W_M$ such that $\mathcal{W}_M \setminus W_M$ is a finite set and $O_M \leq_{\text{Dioph}} O_{M,W_M}$.

7.9 Some Consequences.

In this section we examine in detail various consequences of the theorems above. Among other things, we will analyze the maximum possible density of the prime sets which can be allowed in the denominator of the elements of our rings so that the necessary conditions for solutions of vertical and horizontal problems are satisfied. We will consider vertical definability first.

7.9.1 Theorem.

Let $K$ be any totally real field or a totally complex extension of degree two of a totally real field. Let $\mathcal{W}_K$ be any set of primes of $K$. Then for any $\epsilon > 0$ there exists a set of $K$-primes $\mathcal{W}_K$ such that $\mathcal{W}_K \setminus \mathcal{W}_K$ is contained in a set of Dirichlet density less than $\epsilon$, $\mathcal{W}_K \setminus \mathcal{W}_K$ is finite and such that $O_K,\mathcal{W}_K \cap \mathbb{Q}$ has a Diophantine definition over $O_K,\mathcal{W}_K$.

Proof.

Let $K_G$ be the Galois closure of $K$ over $\mathbb{Q}$. Let $n = [K_G : \mathbb{Q}]$. Let $p > n$ be a prime number and let $E/\mathbb{Q}$ be a totally real cyclic extensions of $\mathbb{Q}$ of degree
$p$. Let

$$\tilde{\mathcal{W}}_K = \{ p \in \mathcal{W}_K | p \text{ does not split in the extension } EK/K \}.$$ 

Then by Corollary 7.6.3 and Theorem 7.8.5 there exists a set $\tilde{\mathcal{W}}_K$ containing $\mathcal{W}_K$ such that $\mathcal{W}_K \setminus \tilde{\mathcal{W}}_K$ is a finite set and $O_{K,\tilde{\mathcal{W}}_K} \cap \mathbb{Q} \leq_{\text{Dioph}} O_{K,\mathcal{W}_K}$. Next consider the set $\mathcal{W}_K \setminus \tilde{\mathcal{W}}_K$. This is a subset of the set of all primes of $K$ splitting in the extension $KE/K$. As before, by Lemma B.3.3, $E$ and $K$ are linearly disjoint over $\mathbb{Q}$, and therefore $EK/K$ is a cyclic extension of degree $p$. The only non-ramified primes splitting in this extension are the primes with $EK$-factors whose Frobenius automorphism over $K$ is identity. (See Lemma B.4.1 for a discussion of Frobenius automorphism.) By Lemma B.5.2, the density of this set is $1/[KE:K] = 1/p$. Since $\tilde{\mathcal{W}}_K$ contains $\mathcal{W}_K$, we have that $\mathcal{W}_K \setminus \tilde{\mathcal{W}}_K$ is also contained in a set whose Dirichlet density is $1/p$. Thus, by selecting $p > \frac{1}{\varepsilon}$ we will satisfy the requirement of the theorem. (Note that a required extension exists by Lemma B.3.9.)

Using the same methodology as in Theorem 7.9.1 and Corollaries 7.6.4, 7.6.5, 7.8.8 and 7.8.9, we can also prove the following two theorems.

7.9.2 Theorem.

Let $\mathcal{W}_Q$ be any set of rational primes. Then for any $\varepsilon > 0$ and any number field $K$ that is totally real or a totally complex extension of degree 2 of a totally real field, there exists a set of rational primes $\tilde{\mathcal{W}}_Q$ such that $\mathcal{W}_Q \setminus \tilde{\mathcal{W}}_Q$ is finite, $\mathcal{W}_Q \setminus \tilde{\mathcal{W}}_Q$ is contained in a set of primes of Dirichlet density less than $\varepsilon$, and $O_{Q,\tilde{\mathcal{W}}_Q}$ has a Diophantine definition in its integral closure in $K$.

7.9.3 Theorem.

Let $K/F$ be an extension of number fields, where $K$ is totally real or a totally complex extension of degree 2 of a totally real field. Let $\mathcal{W}_F$ be any set of primes of $F$. Then for any $\varepsilon > 0$, there exists a set of $F$-primes $\tilde{\mathcal{W}}_F$ such that $\mathcal{W}_F \setminus \tilde{\mathcal{W}}_F$ is finite, $\mathcal{W}_F \setminus \tilde{\mathcal{W}}_F$ is contained in a set of primes of Dirichlet density less than $\varepsilon$, and $O_{F,\tilde{\mathcal{W}}_F}$ has a Diophantine definition in its integral closure in $K$.

Next we have some undecidability and horizontal definability results.
7.9.4 Theorem.

Let $K$ be a totally real field or a totally complex extension of degree 2 of a totally real field that is a non-trivial extension of $\mathbb{Q}$. Then for any $\varepsilon > 0$ there exists a set $\mathcal{W}_K$ of primes of $K$ whose Dirichlet density is bigger than $1 - [K : \mathbb{Q}]^{-1} - \varepsilon$ and such that $\mathbb{Z}$ has a Diophantine over $O_K, \mathcal{W}_K$. (Thus, Hilbert’s Tenth Problem is undecidable in $O_K, \mathcal{W}_K$.)

Proof.

Let $K_G$ be the Galois closure of $K$ over $\mathbb{Q}$. Let $n = [K_G : \mathbb{Q}]$. Let $p > n$ be a prime number and let $E/\mathbb{Q}$ be a totally real cyclic extension of $\mathbb{Q}$ of degree $p$. (Again we remind the reader that such an extension exists by Lemma B.3.9.) Let $\mathcal{W}_K$ be a set of primes of $K$ constructed in the following fashion. For every rational prime $p_\mathbb{Q}$ consider all the primes of $K$ above it and remove one prime with the highest possible degree. Out of the remaining set of primes remove all the primes splitting in the extension $E_K/K$. Then by Lemma B.5.5 the Dirichlet density of $\mathcal{W}_K$, denoted as before by $\delta(\mathcal{W}_K)$, exists and $\delta(\mathcal{W}_K) > 1 - [K : F]^{-1} - \frac{1}{p}$. Further by Theorems 7.7.1 and 7.8.10 there exists a set of $K$-primes $\overline{\mathcal{W}}_K$ containing $\mathcal{W}_K$ such that $\overline{\mathcal{W}}_K \setminus \mathcal{W}_K$ is a finite set and $\mathbb{Z} \leq_{\text{Dioph}} O_K, \overline{\mathcal{W}}_K$. By Proposition 4.6, Chapter IV of [37], we have $\delta(\mathcal{W}_K) = \delta(\overline{\mathcal{W}}_K)$ and the theorem holds for sufficiently large $p$.

7.9.5 Theorem.

Let $K$ be any totally real number field or a totally complex extension of degree 2 of a totally real number field, and let $\varepsilon > 0$ be given. Let $\mathcal{S}_\mathbb{Q}$ be the set of all rational primes splitting in $K$. Then there exists a set of $K$-primes $\mathcal{W}_K$ with the property that the set of rational primes $\mathcal{W}_\mathbb{Q}$ below $\mathcal{W}_K$ is such that $\mathcal{W}_\mathbb{Q} \setminus \mathcal{S}_\mathbb{Q}$ is contained in a set of Dirichlet density less than $\varepsilon$, $\mathcal{S}_\mathbb{Q} \setminus \mathcal{W}_\mathbb{Q}$ is finite and $\mathbb{Z}$ is definable over $O_K, \mathcal{W}_K$.

Proof.

Let $K_G$ be the Galois closure of $K$ over $\mathbb{Q}$. Let $n = [K_G : \mathbb{Q}]$. Let $p > n$ be a prime number and let $E/\mathbb{Q}$ be a totally real cyclic extension of $\mathbb{Q}$. Let $\mathcal{W}_K$ be a set of primes of $K$ constructed in the following fashion. For every rational prime $p_\mathbb{Q}$ consider all the primes of $K$ above it and remove one prime from the set. Out of the remaining set of primes remove all the primes splitting in the extension $E_K/K$. 

136
Note that by Lemma B.3.5, the extension $E_K/K$ is a cyclic extension of degree $p$. Next note that by Lemmas B.4.7 and B.4.8, a prime $p_Q$ splits in the extension $E/Q$ if and only if all the primes above it in $K_G$ split in the extension $E_K/G/K_G$. However, by the same lemmas, a prime of $K_G$ splits in the extension $E_K/G/K_G$ if and only if the prime below it in $K$ splits in the extension $E_K/K$. Thus, a rational prime splits in the extension $E/Q$ if and only if any prime above it splits in the extension $E_K/K$.

Let $p_Q$ be a prime splitting in the extension $K/Q$ but with no factors in $W_K$, then at least one factor of $p_Q$ in $K$ splits in the extension $E_K/K$. But by the argument above, $p_Q$ must split in the extension $E/Q$. Let $S_Q$ be the set of rational primes below $S_K$. Then $S_Q \setminus S_K$ consists of rational primes splitting in the extension $E/Q$. However, by Lemma B.5.2, the density of the set of such rational primes is less than $\frac{1}{p}$ and therefore less than $\varepsilon$ for sufficiently large $p$. Finally, by Theorems 7.7.1 and 7.8.10, there exists a set of $K$ primes $\bar{W}_K$ containing $W_K$ such that $\bar{W}_K \setminus W_K$ is a finite set of $K$-primes and $\mathbb{Z} \leq \text{Dioph} O_K,\bar{W}_K$. Let $\bar{W}_Q$ be the set of rational primes below $\bar{W}_K$. Then $\bar{W}_Q \setminus W_Q$ is finite and the assertion of the theorem holds for sufficiently large $p$.

The following corollary is an immediate consequence of Theorem 7.9.5.

7.9.6 Corollary.

Let $K$ be a totally real extension of $\mathbb{Q}$ or a degree 2 totally complex extension of a totally real number field such that $K/Q$ is Galois and not cyclic. Then for any $\varepsilon > 0$ there exists a set $\bar{W}_K$ of primes of $K$ such that $\bar{S}_Q$, the set of rational primes below $\bar{W}_K$, is of density greater than $1 - \varepsilon$ and $\mathbb{Z}$ is definable over $O_K,\bar{W}_K$.

Proof.

The only thing we need to observe here that in a Galois but not cyclic extension of number fields all primes split. (See Section 1 of Chapter III of [37].)

We finish this section with a few remarks.

7.9.7 Remark.

As in Corollary 7.3.2, the definability and undecidability results for rings of $W$-integers proved above for totally real fields and their totally complex extensions of degree 2 cover all abelian extensions of $\mathbb{Q}$.
7.9.8 Remark.

The undecidability of HTP over any ring is an interesting fact only if the ring itself is recursive. So we should say a few words about recursiveness of some of the rings mentioned in the theorems above. As it happens, if \( \mathcal{W}_K \), as constructed in Theorems 7.9.4 and 7.9.5, is as large as possible, it is computable, implying that \( \mathcal{O}_K.\mathcal{W}_k \) and consequently \( \mathcal{O}_K.\mathcal{W}_k \) are recursive by Proposition A.8.6. Indeed, by Lemma B.4.7 and B.4.8, a prime of \( K \) splits in the extension \( E/K \), where \( E \) is as above, if and only if the prime below it in \( \mathbb{Q} \) splits in the extension \( E/\mathbb{Q} \). Thus, the set of all primes of \( K \) not splitting in the extension \( E/K \) is recursive by Proposition A.8.7 and Corollary A.8.2, and so is the set of all the primes of \( K \) lying above primes of \( \mathbb{Q} \) splitting in the extension \( K/\mathbb{Q} \). Thus, the intersection of these sets is also recursive. It remains to decide how to remove a factor of the largest relative degree from each complete set of conjugates over \( \mathbb{Q} \) in this intersection. Using the presentation of primes we selected in Section A.8, this can be done by selecting primes \( p \) corresponding to the pair \( (p, \alpha(p)) \), where \( \alpha(p) \) has the least possible sequence number (under some fixed ordering of \( K \)) among all \( \alpha(p) \) with \( p \) being a factor of \( p \) of the highest relative degree over \( \mathbb{Q} \).

7.9.9 Remark.

The density results above were stated in terms of Dirichlet density. They can also be restated in terms of natural density, producing a bit stronger assertions. (See Definition B.5.9 and Proposition B.5.10 for the definition of natural density and its relation to Dirichlet density.) The only modification which would be required is the substitution of the natural density version of Chebotarev Density Theorem for the usual Chebotarev Density Theorem. (See Theorem 1 of [88]).

7.10 Big Picture for Number Fields Revisited.

We are now ready to reconsider the big picture for number fields. First we review our notations.

- \( \mathcal{P} \) is a finite set of rational primes
- \( \mathcal{W} \) is an infinite set of rational primes
- \( \mathcal{V} \) is a set of rational primes with a finite complement in the set of all primes \( \mathcal{P}(\mathbb{Q}) \).
• $K$ is a number field.

• $\mathcal{S}_K$ is a finite set of $K$-primes.

• $\mathcal{W}_K$ is an infinite set of $K$-primes

• $\mathcal{V}_K$ is a set of $K$-primes with a finite complement in the set of all $K$-primes $\mathcal{P}(K)$.

Next consider Figure 7.1. As before, arrows indicate Diophantine generation. The diagram represents the following relations.

• Let $\mathcal{U}$ be a collection of primes of $\mathbb{Q}$, let $\mathcal{W}_K$ be all the factors of $\mathcal{U}$ in $K$. Let $\mathcal{U}_K \subseteq \mathcal{W}_K$ and assume that $\mathcal{W}_K \setminus \mathcal{U}_K$ is a finite set. Then $O_K,\mathcal{U}_K \leq_{\text{Dioph}} O_{\mathbb{Q},\mathcal{W}}$. In the diagram this relation corresponds to the vertical arrows from $\mathbb{Z}$ to $O_K$, $\mathbb{Q}$ to $K$, $O_{\mathbb{Q},\mathcal{W}}$ to $O_{K,\mathcal{P}_K}$, and from $O_{\mathbb{Q},\mathcal{W}}$ to $O_K,\mathcal{W}_K$, $O_{\mathbb{Q},\mathcal{W}}$ to $O_{K,\mathcal{S}_K}$ with the assumption that $\mathcal{W}_K, \mathcal{S}_K$ contain all but possibly finitely many $K$-factors of primes in $\mathcal{W}$ and $\mathcal{V}$ respectively and no other primes. These relations are consequences of transitivity of Diophantine generation (see Theorem 2.1.15), Diophantine generation of integral closure, (see Proposition 2.2.1), Diophantine regularity of rings of $\mathcal{W}$-integers (see Proposition 2.2.4), and the fact that integrality at finitely many primes has a Diophantine definition over any ring of $\mathcal{W}$-integers of a number field (see Theorem 4.2.4).

• $K \equiv_{\text{Dioph}} O_K,\mathcal{S}_K$. This follows from existential definability of integrality at finitely many primes and Dioph-regularity of rings of $\mathcal{W}$-integers. Similarly, $O_K \leq_{\text{Dioph}} O_{K,\mathcal{S}_K}$.

• Let $K$ be a subfield of a totally real field, an extension of degree 2 of a totally real field or a field with exactly one pair of conjugate non-real embeddings. Then as we have shown earlier in this chapter, $\mathbb{Z} \leq_{\text{Dioph}} O_K$. From this Diophantine generation we can also derive the following relations:

  – Let $\mathcal{W}_K$ be any computable set of primes of $K$. (Recursive sets of primes are discussed in Section A.8.) Then $O_K,\mathcal{W}_K \leq_{\text{Dioph}} O_K$. This can be deduced from the following considerations. By Proposition A.8.4, the set

  \[ C_{\mathbb{Q}}(O_K) = \{ (a_1, \ldots, a_n) \in \mathbb{Z}^n \mid \sum_{i=1}^n a_i \omega_i \in O(\mathcal{W}_K) \}, \]

  where $O(\mathcal{W}_K)$ is the set of $K$-integers whose divisors are a product of powers of elements of $\mathcal{W}_K$, $n = [K : \mathbb{Q}]$, and $\{\omega_1, \ldots, \omega_n\}$ is an
integral basis of $K$ over $\mathbb{Q}$, is recursively enumerable. Thus $C_\mathbb{Q}(O_K)$ is Diophantine by Matiyasevich’s Theorem. Hence $O_{K,W_K} = \{ \frac{x}{y} | x, y \in O_K, y \neq 0, \exists a_1, \ldots, a_n \in C_\mathbb{Q}(O_K), \exists z \in O_K \setminus \{0\} \}$

\[ x(\sum_{i=1}^{n} a_i \omega_i) = yz \]

(7.10.1)

Since $C_\mathbb{Q}(O_K)$ is Diophantine over $\mathbb{Z}$ and $\mathbb{Z} \leq_{\text{Dioph}} O_K$, the set defined in (7.10.1) is Diophantine over $O_K$.

- $O_{Q,W} \equiv_{\text{Dioph}} O_{K,W}$. Indeed,

\[ O_{K,W} \equiv_{\text{Dioph}} O_K \equiv_{\text{Dioph}} \mathbb{Z} \equiv_{\text{Dioph}} O_{Q,W}, \]

where the first and last equivalence follow from the existential definability of the integrality at finitely many primes and Diophantine generation of the rings of $W$-integers with computable denominator sets, as described above, over the rings of integers. The middle equivalence is a combination of Diophantine definability of integers over $O_K$ and Diophantine generation of integral closure.

- Let $K$ be a subfield of a totally real field or a totally complex extension of degree 2 of a totally real field.

  - For any $\varepsilon > 0$ there exists a set $W_K$ of primes of $K$ such that the Dirichlet density of $W_K$ is greater than $1 - \varepsilon$ and $\mathbb{Q} \cap O_{K,W} \leq_{\text{Dioph}} O_{K,W}$. (See Theorem 7.9.1.)

  - For any $\varepsilon > 0$ there exists a set $W_K$ of primes of $K$ such that the Dirichlet density of $W_K$ is greater than $1 - [K : \mathbb{Q}]^{-1} - \varepsilon$ and $O_K \leq_{\text{Dioph}} O_{K,W}$. (See Theorem 7.9.4.)

### 7.11 Further results.

The results discussed in this chapter leave unanswered the big questions posed at the beginning of this book. In particular, we still do not know the Diophantine status of ring of integers in general, as well as any number field, including $\mathbb{Q}$. The issue of $\mathbb{Q}$ and some of its “large” subrings will come up again in later chapters of this book discussing Mazur’s conjectures and results of Poonen, though it will be in the context of constructing a more general Diophantine
\[ \mathcal{P}_K \text{ is a set of } K\text{-primes with a finite complement}\]

\[ \mathcal{W}_K \text{ is an infinite set of } K\text{-primes}\]

\[ \mathcal{R}_K \text{ is a finite set of } K\text{-primes}\]

\[ \mathcal{O}_{K, \mathcal{W}_K} = \mathcal{O}_{0, \mathcal{W}} \]

\[ \mathcal{W}_K \text{ contains all but possibly finitely many factors of } \mathcal{W} \text{ in } K \text{ and no other primes}\]

\[ \mathcal{E}_K \text{ consists of factors of } \mathcal{E} \text{ in } K \]

\[ \mathcal{O}_{K, \mathcal{E}_K} \]

\[ \mathcal{E}_K \text{ consists of factors of } \mathcal{E} \text{ in } K \]

\[ \mathcal{O}_{0, \mathcal{E}} \]

\[ \mathcal{E} \text{ is a set of rational primes with a finite complement}\]

\[ \mathcal{W} \text{ is an infinite set of rational primes}\]

\[ \mathcal{R} \text{ is a finite set of rational primes}\]

**Figure 7.1:** The known part of Diophantine Family of \( \mathbb{Z} \).
model of \( \mathbb{Z} \) as opposed to a Diophantine definition of integers. Unfortunately, up to this moment, the general problem of defining integrality at infinitely many primes remains intractable. There are, however, a few more things to be said about defining \( \mathbb{Z} \) over the rings of algebraic numbers before we completely abandon this subject. Recently, in [73], Bjorn Poonen proved the following theorem.

### 7.11.1 Theorem.

Let \( M/K \) be a number field extension. Suppose there exists an elliptic curve of rank 1 defined over \( K \) such that this curve retains rank 1 over \( M \). Then \( O_K \leq_{\text{Dioph}} O_K \).

The proof is partly based on the “Weak Vertical Method” and bound equations of the type described in Chapter 5. This result provided a new avenue for our investigation part of which will have to concentrate on determining exactly for which pairs of number fields such curves exist. Further extensions of this method were provided by Cornelissen, Pheidas and Zahidi in [6] and Poonen and the author independently in [72] and [92] respectively. Cornelissen, Pheidas and Zahidi showed that the conditions in Theorem 7.11.1 can be replaced by the following requirements: existence of a rank one elliptic curve over \( M \) and an abelian variety over \( K \) whose positive rank over \( K \) is the same as its rank over \( M \). Poonen and the author, on the other hand, showed that the requirement that the elliptic curve in Theorem 7.11.1 has rank one can be eliminated. In [92] the author also showed that this elliptic curve method can be adjusted for “big rings” in the same way an adjustment was made to the norm method described in this book.

In [111] the author attempted to distill the sources of difficulties of giving a Diophantine definition of \( \mathbb{Z} \) over the rings of integers of an arbitrary number field. It turns out that these difficulties are traceable to lack of good bounds on archimedean valuations over non-real number fields. The reader should be reminded that for a real number field the relationship “\( x \leq y \)” is Diophantine via the use of quadratic forms. (See Lemma 5.1.1.) However, we currently have no means of coding a relationship “\( |x| \leq |y| \)” over non-real number fields. The bounds from Chapter 5 are in some sense too rough for such a relationship and a better way is needed to enforce the bounds.
Chapter 8

Diophantine Undecidability of Function Fields.

Fields of positive characteristic do not contain integers, and therefore constructing Diophantine definitions of integers to establish Diophantine undecidability, as was done for some number rings, is not an option here. However, function fields over finite field of constants do possess Diophantine models of integers, a fact which will allow us to show that the analog of Hilbert’s Tenth Problem is undecidable over these fields. It will take us some time to arrive at the desired results and we will start with a seemingly unrelated point.

Before proceeding with our investigation we should note that the main ideas presented in this chapter are originally due to Cornelissen, Eisenträger, Pheidas, Videla, Zahidi, and the author, and can be found in [8], [23], [66], [67], [69], [102], [106] and [117].

8.1 Defining Multiplication Through Localized Divisibility.

This section contains some technical definability results which will allow us to make a transition from characteristic zero to positive characteristic. The original idea underlying this method belongs to Denef (see [17]) and Lipshitz (see [48], [49], and [50]). It was developed further by Pheidas in [67]. We reproduce Pheidas’s results below.

We start with fixing notation and a definition.
8.1.1 Notation.

In this section $p$ will denote a fixed rational prime.

8.1.2 Definition.

For $x, y \in \mathbb{N}$, define $x \mid_p y$ to mean

$$\exists f \in \mathbb{N} : y = xp^f.$$ 

8.1.3 Lemma.

Let $n, m$ be positive integers, let $s$ be a natural number. Then $m = p^s n$ if and only if

\begin{align*}
&n \mid_p m, \\
&(n + 1) \mid_p (m + p^s), \\
&(n + 2) \mid_p (m + 2p^s).
\end{align*}

Proof.

One direction of the lemma is obvious. If $m = p^s n$, then of course $n \mid_p m$ and $m + p^s = (n + 1)p^s, m + 2p^s = (n + 2)p^s$ so that $(n + 1) \mid_p (m + p^s)$, and $(n + 2) \mid_p (m + 2p^s)$.

Suppose now that $n \mid_p m, (n + 1) \mid_p (m + p^s)$, and $(n + 2) \mid_p (m + 2p^s)$. Then for some $k, l \in \mathbb{N}, \frac{m}{n} = p^k$ and $\frac{m + p^s}{n + 1} = p^l$. First assume that $n \not\equiv 0 \mod p$ and note the following.

$$\frac{m}{n} - \frac{m + p^s}{n + 1} = \frac{mn + m - mn - p^sn}{n(n + 1)} = \frac{p^k - p^s}{n + 1} = p^k - p^l.$$ 

Now we consider three cases: $k = s; k > l; l > k$. In the first case we also conclude that $l = k = s$ and we are done. In the second case, we must also have $k > s$, and further, since $p^k - p^s > p^k - p^l$, we have to conclude that $s < l$. On the other hand,

$$\text{ord}_p(p^k - p^l) = l > s \geq \text{ord}_p \frac{p^k - p^s}{n + 1} = \text{ord}_p(p^k - p^l),$$ 

144
and we have a contradiction. 
In the third case, \( \frac{1-p^s}{n+1} = 1 - p^{l-k} \) and 
\[
\frac{p^{s-k} - 1}{p^{l-k} - 1} - 1 = \frac{p^{s-k} - p^{l-k}}{p^{l-k} - 1} \equiv 0 \mod p.
\]

Thus, the condition \( n \not\equiv 0 \mod p \) together with Conditions (8.1.1) and (8.1.2) implies \( m = np^s \). On the other hand, we can rewrite Conditions (8.1.2) and (8.1.3) as
\[
n' \mid m', \quad (8.1.4)
\]
\[
(n' + 1) \mid (m' + p^s), \quad (8.1.5)
\]
where \( n' = n + 1 \) and \( m' = m + p^s \). Thus, if \( n \) is divisible by \( p \), we have that \( n' = n + 1 \not\equiv 0 \mod p \), and from Conditions (8.1.2) and (8.1.3) (or alternatively (8.1.4) and (8.1.5)) we conclude that \( m' = n'p^s \iff m + p^s = (n + 1)p^s \iff m = np^s \).

**8.1.4 Notation.**

Denote the system
\[
(n \mid_p m) \land ((n + 1) \mid_p (m + u)) \land ((n + 2) \mid_p (m + 2u))
\]
by \( PDIV(n, m, u) \). Then Lemma 8.1.3 can be stated as follows. For \( n, m, s \in \mathbb{N}, n > 0, m > 0, PDIV(n, m, p^s) \iff m = np^s \).

Below we have an easy but important corollary of Lemma 8.1.3 whose proof we leave to the reader.

**8.1.5 Corollary.**

Let \( u_1, u_2 \in \mathbb{N} \setminus \{0\} \) with
\[
1 \mid_p u_1. \quad (8.1.6)
\]

Then
\[
PDIV(u_1, u_2, u_1) \iff \exists s \in \mathbb{N}, u_2 = u_1^2 = p^{2s}. \quad (8.1.7)
\]

We also leave the proof of the following lemma to the reader.
8.1.6 Lemma.

1. Let \( l, m, r \in \mathbb{N} \). Then \((p^l - 1) \mid (p^m - 1)\) if and only if \( l \mid m \).

2. \( \frac{p^{lr} - 1}{p^l - 1} \equiv r \mod (p^l - 1) \).

The next lemma shows us how to compute squares using \( p \)-th powers.

8.1.7 Lemma.

Let \( m, n \in \mathbb{Z}_{>0} \). Then \( m = n^2 \) if and only if there exists \( r, s \in \mathbb{Z}_{>0} \) such that the following conditions are satisfied

\[
\begin{align*}
\text{(8.1.8)} & \quad n < p^s - 1 \\
\text{(8.1.9)} & \quad m < p^s - 1 \\
\text{(8.1.10)} & \quad (p^{2s} - 1) \mid (p^{2r} - 1) \\
\text{(8.1.11)} & \quad \frac{p^{2r} - 1}{p^{2s} - 1} \equiv n \mod (p^{2s} - 1) \\
\text{(8.1.12)} & \quad \frac{(p^{2r} - 1)^2}{(p^{2s} - 1)^2} \equiv m \mod (p^{2s} - 1)
\end{align*}
\]

Proof.

Suppose \( m = n^2 \). Pick an \( s \) such that \( m < p^s - 1 \). Then Inequalities (8.1.8) and (8.1.9) are satisfied. Now let \( r = sn \) to satisfy Conditions (8.1.10)–(8.1.12) via Lemma 8.1.6.

Suppose now that (8.1.8) – (8.1.12) are satisfied for some positive integers \( r \) and \( s \). First of all, we note that (8.1.8) implies that \( n^2 < (p^s - 1)(p^s + 1) = p^{2s} - 1 \). Also we obviously have that \( m < p^{2s} - 1 \). Next (8.1.10) implies by Lemma 8.1.6 that \( r = sk \) for some \( k \in \mathbb{N} \). Therefore,

\[
n \equiv \frac{p^{2r} - 1}{p^{2s} - 1} \equiv k \mod (p^{2s} - 1),
\]

while

\[
m \equiv \frac{(p^{2r} - 1)^2}{(p^s - 1)^2} \equiv k^2 \mod (p^{2s} - 1).
\]

Thus,

\[
n^2 \equiv k^2 \equiv m \mod (p^{2s} - 1)
\]
Since, $m, n^2$ are positive integers and are less than $p^{2s} - 1$, the last congruence implies $m = n^2$.

Our next step is to show that all Conditions (8.1.8) – (8.1.12) can be rewritten using variables ranging over non-negative integers, integer constants and operations “+” and “$\mid_p$”. In the listing below we provide the "translation" of each expression in the language of “+” and “$\mid_p$”. This translation provides the proof of the lemma.

### 8.1.8 Lemma.

Given $m, n \in \mathbb{Z}_{>0}$ there exists $r, s \in \mathbb{Z}_{>0}$ satisfying Conditions (8.1.8) – (8.1.12) if and only if there exists $x, y, z, z_2, w, v, v_2, w_2, v_4, w_4, t, u_1, u_2 \in \mathbb{Z}_{>0}$ satisfying the following conditions.

\[(1 \mid_p w) \wedge (1 \mid_p v)\] (8.1.13)

Translation: $\exists s \in \mathbb{N}, w = p^s$ and $\exists r \in \mathbb{N}, v = p^r$.

\[PDIV(w, w_2, w)\] (8.1.14)

Translation: $w_2 = p^{2s}$, by Corollary 8.1.5.

\[PDIV(w_2, w_4, w_2)\] (8.1.15)

Translation: $w_4 = p^{4s}$, by Corollary 8.1.5.

\[PDIV(v, v_2, v)\] (8.1.16)

Translation: $v_2 = p^{2r}$, by Corollary 8.1.5.

\[PDIV(v_2, v_4, v_2)\] (8.1.17)

Translation: $v_4 = p^{4r}$, by Corollary 8.1.5.

\[PDIV(z_2, u_2, w_4)\] (8.1.18)

Translation: $u_2 = z_2 w_4 = z_2 p^{4s}$, by Lemma 8.1.3.

\[PDIV(z_2, u_1, w_2)\] (8.1.19)

Translation: $u_1 = z_2 w_2 = z_2 p^{2s}$, by Lemma 8.1.3.

\[v_4 - 2v_2 + 1 = u_2 - 2u_1 + z_2\] (8.1.20)
Translation: \((p^{2r} - 1)^2 = z_2(p^{2s} - 1)^2\).

\[ n + x = w \quad (8.1.21) \]

Translation: \(n < p^s - 1\), since \(x \in \mathbb{Z}_{>0}\).

\[ m + y = w \quad (8.1.22) \]

Translation: \(m < p^s - 1\), since \(y \in \mathbb{Z}_{>0}\).

Translation: \(PDIV(z, v_2 - 1 + z, w_2)\) \hspace{1cm} (8.1.23)

Translation: \(p^{2r} - 1 + z = zp^{2s}, z(p^{2s} - 1) = p^{2r} - 1\), by Lemma 8.1.3.

\[ PDIV(u, z - n + u, w_2) \quad (8.1.24) \]

Translation: \(z - n + u = up^{2s}, z - n = u(p^{2s} - 1)\), by Lemma 8.1.3.

\[ PDIV(t, z_2 - m + t, w_2) \quad (8.1.25) \]

Translation: \(z_2 - m + t = tw, z_2 - m = t(p^{2s} - 1)\), by Lemma 8.1.3.

The last condition completes the “translation” of Lemma 8.1.7 into the language of “+” and “\(\mid_p\)”.

We are now ready for the main theorem of this section.

8.1.9 Theorem.

There exist linear polynomials

\[ L_1(u, z, w, x_1, \ldots, x_k), H_1(u, z, w, x_1, \ldots, x_k), \ldots, L_r(u, z, w, x_1, \ldots, x_k) \]
\[ H_r(u, z, w, x_1, \ldots, x_k), T_1(u, z, w, x_1, \ldots, x_k), \ldots, T_m(u, z, w, x_1, \ldots, x_k) \]

with coefficients in \(\mathbb{Z}\) such that for any \(z, u, w \in \mathbb{Z}_{>0}, \exists x_1, \ldots, x_k \in \mathbb{Z}_{>0}\) with

\[
\left\{ \begin{array}{l}
\bigwedge_{i=1}^{r} \left( H_i(u, z, w, x_1, \ldots, x_k) \big| L_i(u, z, w, x_1, \ldots, x_k) \right)_p \\
\bigwedge_{i=1}^{m} (T_i(u, z, w, x_1, \ldots, x_k) = 0)
\end{array} \right.
\]

if and only if \(w = uz\).

Proof.

It is enough to note that \(2uz = (u + z)^2 - u^2 - z^2\).
8.2 \textit{p-th Power Equations over Function Fields I:}
Overview and Preliminary Results.

The usefulness of Theorem 8.1.9 derives from its relationship to \(p\)-th power equations in characteristic \(p > 0\), where equations of the form \(y = x^{p^k}\) play the same fundamental role as played by Pell and other norm equations over number fields. We devote several sections below to the study of the ways these equations can be rewritten as polynomial equations over function fields over finite fields of constants. These equations together with Theorem 8.1.9 will constitute a key step in the construction of a Diophantine model of \(\mathbb{Z}\) over the function fields.

The main result concerning definability of \(p\)-th powers over global fields of positive characteristic \(p\) is the following theorem.

8.2.1 Theorem.

Let \(M\) be a function field over a finite field of constants of characteristic \(p > 0\). Then the set \(P(M) = \{(x, y) \in M^2| \exists s \in \mathbb{N}, y = x^{p^s}\}\) is Diophantine over \(M\).

The proof of this theorem is contained in Sections 8.2–8.4. In this section we start with an overview of the proof, preliminary results and notation.

8.2.2 Overview of the Proof of the Main Theorem 8.2.1.

The proof can be divided into three parts corresponding to Sections 8.2 – 8.4. In this section (Section 8.2) we lay the groundwork with some technical results. More specifically we prove that in some finite constant extension \(K\) of the given function field, there exists a special element \(t\) such that its divisor is a ratio of two primes, each of degree \(p^h\) for some natural number \(h\). The existence of this element also implies existence of a rational subfield \(F\) of \(K\) such that \(K\) is of degree \(p^h\) and separable over \(F\). Further, one can arrange for the constant field of \(K\) to be sufficiently large so that it contains a “sufficiently large” number of constants \(c\) such that the divisor of \(t + c\) in \(K\) is also a ratio of two primes, each of degree \(p^h\). The proof of existence of \(t\) and sufficiently many constants \(c\) (together with the exact definition of “sufficiently many”) is in Theorem 8.2.3. The existence of a rational subfield as described above plays a crucial technical role in the proof of Theorem 8.2.1 by helping to establish sufficient conditions for being a \(p\)-th power in \(K\). These conditions can be summarized as follows:
• Since the field of constants is perfect and in a rational function field every zero degree divisor is principal, an element of the rational subfield is a $p$-th power if and only if its divisor is a $p$-th power.

• An element of $K$ is a $p$-th power if and only if all the coefficients of its minimal polynomial over $F$ are $p$-th powers. (See Lemma 8.2.4.)

• If values of a polynomial at sufficiently many constants are $p$-th powers, then the coefficients of the polynomial are $p$-th powers. (See Lemma 8.2.5.)

• If $x \in K$, $a \in F$, then $N_{F(a)/F}(a-x)$ is the value of the minimal polynomial of $x$ over $F$ at $a$. (See Lemma 8.2.5.)

• Let $F'$ be a subfield of $K$ containing $F$ but not equal to $F$. Let $\mathfrak{p}$ be a prime of $K$ lying above a non-splitting prime of $F$, and let $\mathfrak{p}'$ be the $F'$- prime below $\mathfrak{p}$. Then $N_{F'/F}(\mathfrak{p}')$ is a $p$-th power of some prime in $F$. Thus if an element $v \in K \setminus F$ has poles and zeros of order divisible by $p$ at all the primes except possibly at primes not splitting in the extension $K/F$, then the divisor of $N_{F'(v)/F}(v)$ is a $p$-th power of a divisor in $F$. (This argument will be used in Lemma 8.3.5.)

In Section 8.3 we prove that the set $\{x \in K : \exists s \in \mathbb{N}, x = t^p^s\}$ is Diophantine over $K$. This is done in Proposition 8.3.8. In Section 8.4, using $p$-th powers of $t$, we first consider $p$-th powers of elements of $K$ that have simple zeros and poles only. (This is done in Proposition 8.3.8.) Finally, we examine the $p$-th powers of arbitrary elements. Here, due to some technical complications, we consider separately the case of even and odd characteristics. (See Proposition 8.4.8 and Proposition 8.4.10.)

We now proceed with the technical preliminaries, starting with the existence theorem discussed above.

### 8.2.3 Theorem.

Let $M$ be a function field over a finite field of constants $C_M$ of characteristic $p > 0$. Then for any $l \in \mathbb{N}$ and for any sufficiently large positive integer $h$, a finite constant extension $K$ of $M$ contains a non-constant element $t$ and constants $c_0 = 0, c_1, \ldots, c_l$ such that for all $i = 0, \ldots, l$, the divisor of $t + c_i$ in $K$ is of the form $p_i/q$, where $p_i, q$ are primes of $K$ of degree $p^h$, and for any $s \in \mathbb{N}, i \neq m, c_i^s \neq c_m$. Further, let $e(K, t)$ be the number of primes ramifying in the extension $K/C_K(t)$, where $C_K$ is the constant field of $K$. Then, for any $r \in \mathbb{N}$, we can arrange for $l$ to be greater than $2e(K, t) + r$. 

150
Proof.

Let $z$ be a non-constant element of $M$ which is not a $p$-th power. (Such an element exists by the Strong Approximation Theorem.) Then by Lemma B.1.32 the extension $M/C(z)$ is finite and separable, and therefore is simple. Thus, for some $\alpha \in M$, we have that $M = C_M(z, \alpha)$. Let $M_G$ be the Galois closure of $M$ over $C_M(z)$. Let $C$ be the constant field of $M_G$. Then $M_G/C(z)$ and, by assumption, $M_G/C(z, \alpha)$ are Galois extensions and all three fields have the same field of constants. Let $E = C(z, \alpha)$.

The following diagram describes the extensions involved.

\[
\begin{array}{c}
C(z) \\
\downarrow \\
C(z) \\
\downarrow \\
C_M(z) \\
\downarrow \\
C_M(z, \alpha) = M \\
\downarrow \\
E = C(z, \alpha)
\end{array}
\]

Fix a positive integer $h$. Let $|C| = p^r$. Then $C(z)$ has exactly $p^h$ irreducible polynomials of degree $p^h$. Indeed, $p^{rp^h} - p^{rp^h-1}$ is the number of elements of the algebraic closure of $C$ of degree $p^h$ over $C$. Each of these elements has exactly $p^h$ conjugates over $C$. Let $h_E$ be the class number of $E$. Then for any sufficiently large $h$, it is the case that $C(z)$ will contain at least $h_E + 2$ primes of degree $p^h$.

Next consider the Galois extension $M_G/C(z)$. Let $\pi$ be a prime of $C(z)$ of degree $p^h$. Assume that $\pi$ is unramified and splits completely in the extension $M_G/C(z)$. (Such a prime exists for all sufficiently large $h$ by Corollary B.4.28...
applied to \( \sigma = \text{id} \). Then, we claim, it splits completely in \( E \) and its factors in \( E \) are all of degree \( p^h \). Indeed, assume

\[
\tau = \prod_{i=1}^{[E:C(z)]} \tau_i
\]

is the factorization of \( \tau \) in \( E \). For each \( i \), the relative degree of \( \tau_i \) over \( \tau \) is equal to one. This fact together with the fact that there is no constant field extension from \( C(z) \) to \( E \) implies that \( C(z) \)-degree of \( \tau \) must be the same as the \( E \) degree of \( \tau_i \). Thus, for sufficiently large \( h \), we know that \( E \) has at least \( h_E + 2 \) primes of degree \( p^h \). Let \( b_1, \ldots, b_{h_E+2} \) be these primes. Next consider the following \( h_E + 1 \) divisors of \( E \) of degree zero: \( b_2/b_1, \ldots, b_{h_E+2}/b_1 \). At least two of these divisors belong to the same divisor class, and thus for some \( 1 < i \neq j \leq h_E + 2 \), \( b_i/b_j \) is a principal divisor. Thus, there exists \( t \in E \) such that its divisor is of the form \( p/q \), where \( p, q \) are primes of \( E \) of degree \( p^h \). Note that \( t \) is of order 1 at a prime of \( E \) and therefore is not a \( p \)-th power in \( E \). Hence, the extension \( E/C(t) \) is separable and finite by Lemma B.1.32. Let \( \wp \) be a prime of \( C(t) \) corresponding to the zero of \( t \). As we have established above, this prime remains in \( E \). Thus \( \wp \) is not ramified. Further, since the constant fields of \( C(t) \) and \( E \) are the same, \( \wp \) is of degree 1 in \( C(t) \) and \( p \) is of degree \( p^h \) in \( E \), we must conclude that the relative degree of \( p \) over \( \wp \) is \( p^h \). Therefore, by Proposition B.1.11 we have that \([E : C(w)] = p^h\).

Next from Lemma B.4.23, Corollary B.4.24 and Corollary B.4.28, we conclude that for all sufficiently large \( k \), there are primes of \( C(t) \) of degree \( k \) which remain prime in the extension \( E/C(t) \). Let \( k_1, \ldots, k_l \) be integers large enough in the sense above, and let \( \tau_1, \ldots, \tau_l \) be primes not splitting in the extension \( E/C(t) \) of degrees \( k_1, \ldots, k_l \) respectively. Assume additionally that for all \( i \neq j \), we have \((k_i, k_j) = 1\), \((k_i, p) = 1\), and \( \text{ord}_{\tau_i} t = 0 \). Let \( C_k/C \) be the extension of degree \( k_1 \ldots k_l \). Let \( K = C_kE \). Let \( C_0 = C \) and let \( C_i/C \) be the extension of degree \( \prod_{j=1}^{i} k_j \). Let \( P_i(t) \in C[t] \) be an irreducible polynomial of degree \( k_j \). We claim that the following assertions are true.

- \([C_iE : C_i(t)] = p^h\), for all \( i = 0, \ldots, l \).
- In the extension \( C_i(t)/C(t) \) primes \( \tau_1, \ldots, \tau_i \) split completely into degree 1 factors and \( \tau_{i+1}, \ldots, \tau_l \) remain prime.
- Any factor of \( \tau_j, j = 1, \ldots, n \) remains prime in the extension \( C_iE/C_i(t) \).
- Let \( c_i \in C_i \) be a root of \( P_i(t) \). Then for \( j = 1, \ldots, i - 1 \), we have that \( c_i, c_j \) are not conjugates over \( \mathbb{F}_p \), the field of \( p \) elements, and therefore for any non-negative integer \( u \) we have that \( c_i^{p^u} \neq c_j \).
We will proceed by induction. Assume the statements are for the extension $C_iE/E$ for some $i$ with $0 \leq i < l$ and consider extension $C_{i+1}E/E$. Let $t_{ij}$ be a factor of $\overline{\tau}_j$ in $C_i(t)$. Let $t_{i+1,j}$ be a factor of $t_{ij}$ in $C_{i+1}(t)$. Let $u_j$ be the prime above $\overline{\tau}_j$ in $E$, let $u_{ij}, u_{i+1,j}$ be factors of $t_{ij}$ and $t_{i+1,j}$ in $C_iE$ and $C_{i+1}E$ respectively. The following diagram describes the extensions we will consider for the inductive step.

$$
\begin{array}{ccc}
\overline{\tau}_j \subset C(t) & t_{ij} \subset C_i(t) & t_{i+1,j} \in C_{i+1}(t) \\
\end{array}
$$

First of all by Lemma B.3.4, we observe that $[C_iE : C_i(t)] = p^h$. Next consider $t_{ij}, 0 \leq j \leq i$. By induction, $t_{ij}$ is of degree 1 and therefore by Lemma B.4.16, $t_{i+1,j}$ will be the only factor of $t_{i+1,j}$ in $C_{i+1}(t)$. On the other hand, the residue field of $u_{ij}$ is of degree $p^h$ over $C_i$, since by induction $u_{ij}$ is the only factor of $t_{ij}$ in $C_iE$. Since $[C_{i+1}E : C_iE] = [C_{i+1} : C_i] = k_{i+1}$ and $(k_{i+1}, p) = 1$, by Lemma B.4.22, $u_{i+1,j}$ is the only factor of $u_{ij}$ in $C_{i+1}E$ and therefore the only factor of $t_{i+1,j}$ in $C_{i+1}E$.

Next we note that by induction hypothesis, $t_{i,i+1}$ was the only factor of $\overline{\tau}_{i+1}$ in $C_i(t)$. By Lemma B.4.21 the degree of $t_{i,i+1}$ in $C_i(t)$ is the same as the degree of $\overline{\tau}_{i+1}$ in $C(t)$, that is the degree is equal to $k_{i+1}$. Since a finite field has exactly one extension of every degree, $C_{i+1}$ is the residue field of $t_{i,i+1}$. Thus, by Lemmas B.4.15, B.4.26, in the extension $C_{i+1}(t)/C_i(t)$ we have $t_{i,i+1}$ splitting completely into degree 1 factors, and each of these factors does not split in the extension $C_{i+1}E/C_{i+1}(t)$.

Now consider $t_{ij}, u_{ij}, j > i + 1$. Their residue fields are of degrees $k_j$ and $k_jp^h$ over $C_i$ respectively. Since by assumption $(k_{i+1}, k_jp^h) = 1$ for $i + 1 < j$, we can use Lemma B.4.22 again to conclude that both primes will remain prime in the extensions $C_{i+1}(t)/C_i(t)$ and $C_{i+1}E/C_iE$ respectively.

Finally we note that for all $i$, $c_i \in C_i$ since a finite field has a unique extension of every degree and $k_i \mid [C_i : C]$. Further, suppose $c_i, c_j$ are conjugate
over \( \mathbb{F}_p \). Then for some \( \sigma \in \text{Gal}(C(c_i, c_j)/\mathbb{F}_p) \) we have that \( \sigma(c_i) = c_j \). Then \( \sigma(P_i) = \sigma(P_j) \) which impossible due to difference in degrees. This concludes the proof of the assertion above.

We now consider the divisor of \( t \) in \( K \). In \( E \), the divisor of \( t \) was \( \frac{P}{Q} \), where \( p, q \) were primes of degree \( p^h \). Therefore, as in the discussion above, neither \( p \) nor \( q \) will split in the extension \( K/E \). Similarly, the degree 1 primes below \( p, q \) in \( C(t) \) will remain prime and of degree 1 in the extension \( C_K(t)/C(t) \).

Further, consider the divisor of \( t - c_i \). This element has a unique degree one pole at \( q \). Since \( (t - c_i)|P_i(t) \), it must have a unique zero at a degree 1 factor \( T_{i,j} \) of \( T_i \).

Finally we note the following. By Proposition B.4.33 we have that \( e(K, t) \leq \deg(E) \), where \( E = \prod_{e \in \dd} e \) and \( \dd \) be the set of all the primes of \( E \) ramified in the extension \( E/C(t) \). Thus, we set \( l > \deg(\dd) + r \) to satisfy the last requirement of the theorem.

### 8.2.4 Lemma.

Let \( F/G \) be a finite separable extension of fields of positive characteristic \( p \). Let \( \alpha \in F \) be such that for some positive integer \( a \), all the coefficients of its monic irreducible polynomial over \( G \) are \( p^a \)-th powers in \( G \). Then \( \alpha \) is a \( p^a \)-th power in \( F \).

**Proof.**

Let \( a_0^p + \ldots + a_{m-1}^p T^{m-1} + T^m \) be the monic irreducible polynomial of \( \alpha \) over \( G \). Let \( \beta \) be the element of the algebraic closure of \( F \) such that \( \beta^{p^a} = \alpha \). Then \( \beta \) is of degree at most \( m \) over \( G \). On the other hand, \( G(\alpha) \subseteq G(\beta) \). Therefore, \( G(\alpha) = G(\beta) \).

### 8.2.5 Lemma.

Let \( F/G \) be a finite separable extension of fields of positive characteristic \( p \). Let \([F : G] = n \). Let \( a \) be a positive integer. Let \( x \in F \) be such that \( F = G(x) \) and for distinct \( a_0, \ldots, a_n \in G \) we have that \( N_{F/G}(a_i^{p^a} - x) = y_i^{p^a} \). Then \( x \) is a \( p^a \)-th power in \( F \).

**Proof.**

Let \( H(T) = A_0 + A_1 T + A_{n-1} T^{n-1} + T^n \) be the monic irreducible polynomial of \( x \) over \( G \). Then for \( i = 0, \ldots, n \) we have that \( H(a_i^{p^a}) = y_i^{p^a} \). Further, we...
have the following linear system of equations:

\[
\begin{pmatrix}
1 & a_0^p & \cdots & a_0^{p(n-1)} & a_0^{p^n} \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
1 & a_n^p & \cdots & a_n^{p(n-1)} & a_n^{p^n}
\end{pmatrix}
\begin{pmatrix}
A_0 \\
\vdots \\
1
\end{pmatrix}
= 
\begin{pmatrix}
y_0^p \\
\vdots \\
y_n^p
\end{pmatrix}
\]

Using Cramer’s rule to solve the system, it is not hard to conclude that for \( i = 0, \ldots, n \) it is the case that \( A_i \) is a \( p^a \)-th power in \( G \). Then, by Lemma 8.2.4, \( x \) is a \( p^a \)-th power in \( F \).

### 8.2.6 Lemma.

Let \( F \) be a function field. Let \( w \in F \), let \( a_1, \ldots, a_r \) be primes of \( K \) and let \( a_1, \ldots, a_{r+1} \) be a set of distinct constants of \( F \). Then the set \( \{w + a_1, \ldots, w + a_{r+1}\} \) contains at least one element of \( F \) having no zero at any of the primes \( a_1, \ldots, a_r \).

**Proof.**

The lemma follows from the fact that each prime \( a_i \) can be a zero of at most one element of the set \( \{w + a_1, \ldots, w + a_{r+1}\} \).

### 8.2.7 Lemma.

Let \( w \) be a non-constant element of a function field \( K \), and let \( b, c \in C \) – the constant field of \( K \). Then all the zeros of \( \frac{w+c}{w+b} \) are zeros of \( w + c \) and all the poles of \( \frac{w+c}{w+b} \) are zeros of \( w + b \). Further, the height of \( \frac{w+c}{w+b} \) is equal to the height of \( w \). (Here by height we mean the degree of zero or pole divisor of an algebraic function. See Definition B.1.25.)

**Proof.**

Let \( p \) be a prime of \( K \). Then \( p \) is a pole \( w \) if and only if \( p \) is a pole of \( w + c \) and a pole of \( w + b \). Moreover, the order of the pole at all the three functions will be the same. On the other hand, any zero of \( \frac{w+c}{w+b} \) will come from zeros of \( w + c \) or poles of \( w + b \). So let \( p \) be a pole of \( w + b \). Then \( \operatorname{ord}_p(w+c) = \operatorname{ord}_p(w+b) \) and therefore \( \operatorname{ord}_p \frac{w+c}{w+b} = 0 \). A similar argument shows that \( \frac{w+c}{w+b} \) is a unit at any valuation which is a pole of \( w + c \). Consequently, all zeros of \( \frac{w+c}{w+b} \) are zeros of \( w + c \) and all the poles of \( \frac{w+c}{w+b} \) are zeros of \( w + b \).
Finally, note that $\frac{w+c}{w+b} = 1 + \frac{c-b}{w+b}$. Let $H_K(\frac{w+c}{w+b})$ denote the $K$-height of $\frac{w+c}{w+b}$. Then by Remark B.1.26 we have the following equalities.

$$H_K\left(\frac{w+c}{w+b}\right) = H_K\left(1 + \frac{c-b}{w+b}\right) = H_K\left(\frac{c-b}{w+b}\right) = H_K(w+b) = H_K(w).$$

The last equality follows from the fact, mentioned above, that the pole divisors of $w+b$ and $w$ are the same.

We leave of the proof of the following lemma to the reader.

### 8.2.8 Lemma.

Let $K$ be a function field. Let $m > 1$ be an integer. Let $x \in K$. Then for any prime $p$ of $K$ we have that $p$ is a pole of $x^m - x$ if and only if it is a pole of $x$. If $\text{ord}_p x < 0$ then $\text{ord}_p (x^m - x) \equiv 0 \mod m$.

In the remainder of this section and Sections 8.3 and 8.4 we will use the following notation and assumptions.

### 8.2.9 Notation and Assumptions.

- $M$ will denote a function field over a finite field of constants of characteristic $p > 0$.
- Let $a = 1$ if $p > 2$, and let $a = 2$ if $p = 2$.
- $K$ will denote a finite separable constant field extension of $M$.
- $C_K$ will denote the finite constant field of $K$.
- There exist $c_0 = 0, \ldots, c_l \in C_K \setminus \{\pm 1\}$ such that for some $t \in K$, for all $i = 0, \ldots, l$, the divisor of $t + c_i$ is of the form $p_i/q$, where $p_i, q$ are primes of $K$.
- Let $C(K) = \{c_0, \ldots, c_l\}$.
- $r_i$ will denote the smallest positive integer such that $c_i^{p_{r_i}} = c_i$.
- For any $0 < j \leq r_i, m \neq i$, we have that $c_i^{p_j} \neq c_m$.
- Let $d_{ij} = c_i^{p_j}, j \in \mathbb{N}$.
- $[K : C_K(t)] = p^h = n$ for some $h \in \mathbb{N}$. 156
Let $\mathcal{E}(K, t)$ be the set of all primes of $K$ ramifying in the extension $K/C_K(t)$ together with primes $p$ and $q$.

$e(K, t) = |\mathcal{E}(K, t)|$ will denote the number of primes ramifying in the extension $K/C_K(t)$.

$I > (p^h + 2e(K, t)) + 2$

For any $w \in K$, let

$C_w = \{ c \in C(K) : (\forall j \in \mathbb{N})(\forall p \in \mathcal{E}(K, t))(\text{ord}_p(w - c^p) \leq 0)\}$.

For any $b \in \mathbb{N}, w \in K$, let $B(b, w, u, v)$ denote the system of equations

\begin{align*}
y - t &= u^{p^b} - u \tag{8.2.1} \\
y^{-1} - t^{-1} &= v^{p^b} - v \tag{8.2.2}
\end{align*}

For $i, k \in \{1, \ldots, l\}, j_i \in \{1, \ldots, r_i\}, j_k \in \{1, \ldots, r_k\}, w, u_{i,j_i,j_k}, v_{i,j_i,j_k} \in K$, let $C(i, k, j_i, j_k, w, u_{i,j_i,j_k}, v_{i,j_i,j_k})$ denote the system of equations

\begin{align*}
w_{i,j_i,j_k,k,j_k} &= \frac{w - d_{i,j_i}}{w - d_{k,j_k}} \tag{8.2.3} \\
t_{i,k} &= \frac{t - c_i}{t - c_k} \tag{8.2.4} \\
w_{i,j_i,j_k,k,j_k} - t_{i,k} &= u_{i,j_i,j_k}^{p^e} - u_{i,j_i,j_k} \tag{8.2.5} \\
\frac{1}{w_{i,j_i,j_k,k,j_k}} - \frac{1}{t_{i,k}} &= v_{i,j_i,j_k}^{p^e} - v_{i,j_i,j_k} \tag{8.2.6}
\end{align*}

For $s \in \mathbb{N}, i, k \in \{1, \ldots, l\}, j_i \in \{1, \ldots, r_i\}, j_k \in \{1, \ldots, r_k\}, e = -1, 1, m = 0, 1, u, v, \mu_{i,j_i,j_k,e,m}, \sigma_{i,j_i,j_k,e}, \nu_{i,j_i,e} \in K$, let

$D(s, i, j_i, k, e, m, j_k, u, v, \mu_{i,j_i,j_k,e,m}, \sigma_{i,j_i,j_k,e}, \nu_{i,j_i,e})$

be the following system of equations.

\begin{align*}
u_{i,j_i,k,j_k} &= \frac{u + c_i}{u + c_k} \tag{8.2.7} \\
v_{i,j_i,j_k} &= \frac{v + d_{i,j_i}}{v + d_{k,j_k}} \tag{8.2.8} \\
v_{i,j_i,j_k,k,j_k}^{2e} t_{i,j_i,j_k}^{mp^e} - u_{i,k}^{2e} t^{mp} &= \mu_{i,j_i,j_k,e,m} - \mu_{i,j_i,j_k,e,m} \tag{8.2.9} \\
v_{i,j_i,j_k}^{e} - u_{i,k}^{e} &= \sigma_{i,j_i,j_k,e}^{p^e} - \sigma_{i,j_i,j_k,e} \tag{8.2.10}
\end{align*}
Let \( j, r, s \in \mathbb{N} \), \( u, \tilde{u}, v, \tilde{v}, x, y \in K \). Let \( E(u, \tilde{u}, v, \tilde{v}, x, y, j, r, s) \) denote the following system of equations

\[
\begin{align*}
v &= u^{p^r} \\
\tilde{v} &= \tilde{u}^{p^j} \\
u &= \frac{x^p + t}{x^p - t} \\
\tilde{u} &= \frac{x^p + t^{-1}}{x^p - t^{-1}} \\
v &= \frac{y^p + t^p s}{y^p - t^p s} \\
\tilde{v} &= \frac{y^p + t^{-p s}}{y^p - t^{-p s}}
\end{align*}
\]

As will become clear in the following section, it will be important to be able to assume that the "important" variables do not have poles or zeros at primes ramifying in the extension \( K/C(t) \). The next lemma assures us, that, under our assumptions, we have enough constants to replace a variable by its sum with a constant from a fixed set, if necessary, to make sure the non-ramification condition is satisfied.

\textbf{8.2.10 Lemma.}

For any \( u, w \in K \), we have that \(|C_w|\) and \(|C_w \cap C_u|\) contain more than \(n + 2\) elements.
Proof.

Consider the following table.

\[
\begin{bmatrix}
  w - c_1 & w - c_1^p & \ldots & w - c_1^{p^i} & \ldots \\
  \ldots & \ldots & \ldots & \ldots & \ldots \\
  w - c_l & w - c_l^p & \ldots & w - c_l^{p^j} & \ldots
\end{bmatrix}
\]

Observe that by assumption on the elements of \( C(K) \) no two rows share an element, and the difference between any two elements of the table is constant. Thus, by Lemma 8.2.6, elements of \( l - e(K, t) \) rows have no zero at any element of \( \mathcal{E}(K, t) \) and consequently, \( |C_w| \geq n + 2 + e(k, t) \). Next consider a table

\[
\begin{bmatrix}
  u - b_1 & u - b_1^p & \ldots & u - b_1^{p^i} & \ldots \\
  \ldots & \ldots & \ldots & \ldots & \ldots \\
  u - b_{|C_w|} & u - c_{|C_w|}^p & \ldots & u - c_{|C_w|}^{p^j} & \ldots
\end{bmatrix}
\]

where \( b_i \in C_w \). By an analogous argument, at least \( |C_w| - e(K, t) \) rows of this table contain no element with a zero at any valuation of \( \mathcal{E}(K, t) \). Thus, at least \( |C_w| - 2e(K, t) = n + 2 \) elements are contained in \( C_w \cap C_u \).

The final lemma of this section is a technical result which will help us to eliminate a case in a later section.

8.2.11 Lemma.

Let \( \sigma, \mu \in K \). Assume that all the primes that are poles of \( \sigma \) or \( \mu \) do not ramify in the extension \( K/C_K(t) \). Further, assume the following equality is true.

\[
t(\sigma^{p^a} - \sigma) = \mu^{p^a} - \mu \quad \tag{8.2.23}
\]

Then \( \sigma^{p^a} - \sigma = \mu^{p^a} - \mu = 0 \).

Proof.

Let \( \mathfrak{a}, \mathfrak{b} \) be integral divisors of \( K \), relatively prime to each other and to \( p \) and \( q \), such that the divisor of \( \sigma \) is of the form \( \frac{\mathfrak{a}}{\mathfrak{b}} p^i q^k \), where \( i, k \) are integers. Then it is not hard to see that for some integral divisor \( \mathfrak{c} \), relatively prime to \( \mathfrak{b}, p \) and \( q \), some integers \( j, m \), the divisor of \( \mu \) is of the form \( \frac{\mathfrak{c}}{\mathfrak{b}} p^j q^m \). Indeed, let \( t \) be a pole of \( \mu \) such that \( t \neq p \) and \( t \neq q \). Then

\[
0 > p^3 \text{ord}_t \mu = \text{ord}_t (\mu^{p^a} - \mu) = \text{ord}_t (t(\sigma^{p^a} - \sigma)) = \text{ord}_t (\sigma^{p^a} - \sigma) = p^3 \text{ord}_t \sigma.
\]
Conversely, let \( t \) be a pole of \( \sigma \) such that \( t \neq p \) and \( t \neq q \). Then

\[ 0 > p^a \text{ord}_t \sigma = \text{ord}_t(\sigma^{p^a} - \sigma) = \text{ord}_t(t(\sigma^{p^a} - \sigma)) = \text{ord}_t(\mu^{p^a} - \mu) = p^a \text{ord}_t \mu. \]

By the Strong Approximation Theorem (see Theorem B.2.1), there exists \( b \in K \) such that the divisor of \( b \) is of the form \( \mathfrak{a} \mathfrak{b}/q^c \), where \( \mathfrak{b} \) is an integral divisor relatively prime to \( \mathfrak{a} \), \( c \), \( p \), \( q \) and \( c \) is a natural number. Then \( b \sigma = s_1 t^i, b \mu = s_2 t^j \), where \( s_1, s_2 \) are integral over \( C_K[t] \) and have zero divisors relatively prime to \( p \) and \( \mathfrak{b} \). Indeed, consider the divisors of \( b \sigma \):

\[
\frac{\mathfrak{b} \mathfrak{d} \mathfrak{A}}{q^k} p^i q^k = \mathfrak{A} p^i q^{k-c} = \mathfrak{A} q^{k-c} p^i q^c
\]

Thus the divisor of \( s_1 \) is of the form \( \mathfrak{A} q^{k-c+i} \) and therefore, \( q \) is the only pole of \( s_1 \), making it integral over \( C_K[t] \). Further, by construction \( \mathfrak{a} \) and \( \mathfrak{d} \) are integral divisors relatively prime to \( p \) and \( \mathfrak{b} \). A similar argument applies to \( s_2 \).

Multiplying through by \( b^{p^a} \) we will obtain the following equation.

\[ t(s_1^{p^a} t^{ip^a} - b^{p^a-1} s_1 t^i) = s_2^{p^a} t^{ip^a} - b^{p^a-1} s_2 t^j. \]  

(8.2.24)

Suppose \( i < 0 \). Then the left side of (8.2.24) has a pole of order \( ip^a + 1 \) at \( p \). This would imply that \( j < 0 \) and the right side has a pole of order \( jp^a \) at \( p \). Thus, we can assume that \( i, j \) are both non-negative. We can now rewrite (8.2.24) in the form

\[ (s_1^{p^a} t^{ip^a+1} - s_2^{p^a} t^{ip^a}) = b^{p^a-1}(s_1 t^{i+1} - s_2 t^j). \]  

(8.2.25)

Let \( t \) be any prime factor of \( \mathfrak{b} \) in \( K \). Then \( t \) does not ramify in the extension \( K/C_K(t) \) and since \( p^a > 2 \), we know that \( \text{ord}_t(s_1^{p^a} t^{ip^a+1} - s_2^{p^a} t^{ip^a}) \geq 2 \). Further, since \( t \) is not a \( p \)-th power in \( K \), the global derivation with respect to \( t \) is defined by Proposition B.9.3, and by Corollary B.9.7 we also have

\[
\text{ord}_t \frac{d(s_1^{p^a} t^{ip^a+1} - s_2^{p^a} t^{ip^a})}{dt} > 0.
\]

Finally,

\[
\text{ord}_t \frac{d(s_1^{p^a} t^{ip^a+1} - s_2^{p^a} t^{ip^a})}{dt} = \text{ord}_t(s_1^{p^a} t^{ip^a}).
\]

Therefore, since \( t \), by assumption is not a zero of \( t \), \( s_1 \) has a zero at \( t \). This, however is impossible. Consequently, \( \mathfrak{b} \) is a trivial divisor, and in (8.2.23) all the functions are integral over \( C_K[t] \), i.e they can have poles at \( q \) only. Assuming \( \mu \) is not a constant and thus has a pole at \( q \), we note that the left side has a pole at \( q \) of order equivalent to 1 modulo \( p \), while the right side has the pole \( q \) of order equivalent to 0 modulo \( p \). Thus, \( \mu \) is a constant. But the only
way the product of $t$ and a function integral over $C_K[t]$ can be a constant is for that function to be equal to zero.

In the following sections we prove a sequence of lemmas which will describe the equations constituting a Diophantine definition of $p$-th powers in $K$. Occasionally we will have to separate out the cases of $p > 2$ and $p = 2$. We start with $p$-th powers of $t$.

### 8.3 $p$-th Power Equations over Function Fields II: $p$-th Powers of a Special Element.

We start this section with observing in the first two lemmas that in the equations below, under some circumstances, we can replace the “the most important” variable by its $p$-th root.

#### 8.3.1 Lemma.

Suppose $B(b, w, u, v)$ holds for some $w, u, v \in K$ and $\tilde{w}^p = w$. Then for some $\tilde{u}, \tilde{v} \in K, B(b, \tilde{w}, \tilde{u}, \tilde{v})$ holds.

**Proof.**

Set $\tilde{u} = u - \tilde{w}, \tilde{v} = v - \tilde{w}^{-1}$ and observe that the following equations hold.

$$\tilde{w} - t = (u - \tilde{w})^p - (u - \tilde{w})$$

$$\tilde{w}^{-1} - t^{-1} = (v - \tilde{w}^{-1})^p - (v - \tilde{w}^{-1})$$

#### 8.3.2 Lemma.

Suppose $w, u_{i,j,k}, v_{i,j,k}, i, k = 0, \ldots, l, j_i = 1, \ldots, r_i, j_k = 1, \ldots, r_k$ are elements of $K \setminus C(t)$ such that

$$\left( \bigwedge_{i=0, j_i \in \{1, \ldots, r_i\}} \bigvee_{k=0, k \neq j_k \in \{1, \ldots, r_k\}} C(i, k, j_i, j_k, w, u_{i,j,k}, v_{i,j,k}) \right)$$

holds. Suppose $w = \tilde{w}^p$ for some $\tilde{w} \in K$. Then $K$ contains elements $\tilde{u}_{i,j,k}, \tilde{v}_{i,j,k}, i, k = 0, \ldots, l, j_i = 1, \ldots, r_i, j_k = 1, \ldots, r_k$ such that

$$\left( \bigwedge_{i=0, j_i \in \{1, \ldots, r_i\}} \bigvee_{k=0, k \neq j_k \in \{1, \ldots, r_k\}} C(i, k, j_i, j_k, \tilde{w}, \tilde{u}_{i,j,k}, \tilde{v}_{i,j,k}) \right)$$
holds.

**Proof.**

Observe the following.

\[ w_{i,j,k,j} = w - d_{i,j} = w - c_{i,j}^{p_i} = \left( \tilde{w} - c_{j,k}^{p_j} \right)^p, \]

where \( m_i = j_i - 1, m_k = j_k - 1 \), if \( j_k, j_i > 1 \) and \( m_i = r_i, m_k = r_k \), if \( j_k = 1, j_i = 1 \). Note that since for all \( k \), we have that \( j_k \) took all values \( 1, \ldots, r_k \), the same will be true of \( m_k \). Thus equations (8.2.5) and (8.2.6) can be rewritten in the following manner.

\[ \tilde{w}_{i,m_i,k,m_k} - t_{i,k} = (u_{i,j,k,j} - \tilde{w}_{i,m_i,k,m_k}) - (u_{i,j,k,j} - \tilde{w}_{i,m_i,k,m_k}), \quad (8.3.1) \]

\[ \frac{1}{\tilde{w}_{i,m_i,k,m_k}} - \frac{1}{t_{i,k}} = (v_{i,j,k,j} - \frac{1}{\tilde{w}_{i,m_i,k,m_k}}) - (v_{i,j,k,j} - \frac{1}{\tilde{w}_{i,m_i,k,m_k}}), \quad (8.3.2) \]

where \( 1 \leq m_i \leq r_i, 1 \leq m_k \leq r_k \).

The next lemma and its corollary treat the case of a rational function.

**8.3.3 Lemma.**

Let \( u, v \in K \), let \( y \in C(t) \), and assume \( y \) does not have zeros or poles at any valuation of \( K \) ramifying in the extension \( K/C_K(t) \), and \( y \) is not a \( p^a \)-th power. Assume further that \( B(a, y, u, v) \) holds. Then \( y = t \).

**Proof.**

First of all, note that all the poles of \( v^{p^a} - v \) and \( u^{p^a} - u \) in \( K \) are of orders divisible by \( p^a \) by Lemma 8.2.8. Since the zero and the pole of \( t \) are of orders equal to \( \pm 1 \), we must conclude from (8.2.1) and (8.2.2) that the divisor of \( y \) is of the form \( u^{p^a} p^{b_1} q^{b_2} \). Indeed, let \( i \) be a prime which is not equal to \( p \) or \( q \). Without loss of generality assume \( i \) is a pole of \( y \). Then, since \( \text{ord}_t t = 0 \),

\[ 0 > \text{ord}_t y = \text{ord}_t (t - y) = \text{ord}_t (u^{p^a} - u) \equiv 0 \mod p^a. \]

Now consider the order at \( q \). We have

\[ \text{ord}_q (y - t) = \text{ord}_q (u^{p^a} - u). \]
Therefore, either $\text{ord}_q y < -1$ and $\text{ord}_q y \equiv 0 \mod p^a$, or $\text{ord}_q y = \text{ord}_q t = -1$. Similarly, either $\text{ord}_p y > 1$ and $\text{ord}_p y \equiv 0 \mod p^a$, or $\text{ord}_p y = \text{ord}_p t = 1$. Further, since the divisor of $y$ must be of degree 0, the orders at $p$ and $q$ must be equivalent modulo $p^a$. If $\text{ord}_q y \equiv \text{ord}_p y \equiv 0 \mod p^a$, taking into account the fact that no prime which is a pole or zero of $y$ ramifies in the extension $K/C_K(t)$, we can conclude that the divisor of $y$ in the rational field is also a $p^a$-th power of another divisor. Thus, since in the rational field every zero degree divisor is principal and the field of constants is perfect, $y$ is a $p^a$-th power. Therefore, we must conclude $|\text{ord}_q y| = |\text{ord}_p y| = 1$. Then we can deduce, using an argument similar to the one above, that $yt^{-1}$ is a $p^a$-th power in the rational field. Thus, $(8.2.1)$ can be rewritten as

$$t(f - 1)^{p^a} = u^{p^a} - u,$$

where $f \in C_K(t)$. Since $f - 1$ is a rational function in $t$, we can further rewrite $(8.3.3)$ as

$$t(f_1^{p^a} / f_2^{p^a}) = u^{p^a} - u,$$

where $f_1, f_2$ are relatively prime polynomials in $t$ over $C$ and $f_2$ is monic. From this equation it is clear that any valuation that is a pole of $u$, is either a pole of $t$ or a zero of $f_2$. Further, the absolute value of the order of any pole of $u$ at any valuation which is a zero of $f_2$, must be the same as the order of $f_2$ at this valuation. Therefore, $s = f_2 u$ will have poles only at the valuations which are poles of $t$. Thus we can rewrite $(8.3.4)$ in the form

$$-tf_1^{p^a} + s^{p^a} = sf_2^{p^a-1}.$$

Let $\epsilon$ be a zero of $f_2$. Then, since $f_2$ is a polynomial in $t$, $\epsilon$ is not a pole of $t$. Since, $p^a - 1 \geq 2$ and $s$ is integral over $C_K[t]$, we have that $\text{ord}_\epsilon(s^{p^a} - tf_1^{p^a}) \geq 2$.

Now observe that by Proposition B.9.3

$$d(-tf_1^{p^a} + s^{p^a})/dt = -f_1^{p^a},$$

and since, by assumption $f_2$ does not have any zeros at valuations ramifying in the extension $K/C_K(t)$, by Corollary B.9.7,

$$\text{ord}_\epsilon(-f_1^{p^a}) = \text{ord}_\epsilon(d(-tf_1^{p^a} + s^{p^a})/dt) > 0.$$

Thus, $f_1$ has a zero at $\epsilon$. But $f_1$ and $f_2$ are supposed to be relatively prime polynomials. Hence, $f_2$ does not have any zeros, and thus is equal to 1. Therefore, $y$ is a polynomial in $t$. Similarly, we can show that $1/y$ is a polynomial in $1/t$. Hence, $y$ is a power of $t$, and more specifically, unless $y = t$, $y$ must be a power of $t$ divisible by $p^a$. If $y = t$ we are done. Otherwise, we have shown that $y$ is a $p^a$-th power of another rational function in $t$ over $C_K$, contradicting our assumptions.
8.3.4 Corollary.

Let \( u, v, y \) be as in Lemma 8.3.3 with the exception that we will now allow \( y \) to be a \( p^a \)-th power in \( K \). Then for some non-negative integer \( s \) we have that \( y = t^{p^a s} \).

Proof.

First of all, observe the following. Either \( y \) is a constant or for some non-negative integer \( k \) it is the case that \( y = w^{p^a k} \), where \( w \in C_K(t) \), \( w \) is not a \( p^a \)-th power of any element and by Lemma 8.3.1 and induction, there exist \( \bar{u}, \bar{v} \in K \) such that \( B(a, w, \bar{u}, \bar{v}) \) holds. Now, it is not hard to see that \( y \) cannot be a constant. Indeed, if \( y \in C_K \), then \( \text{ord}_q(t - y) = -1 \), while, as discussed above, the degrees of all the poles of the right side of (8.2.1) are divisible by \( p^a \). Thus, there exist \( \bar{u}, \bar{v} \in K \) such that \( B(a, w, \bar{u}, \bar{v}) \) holds. Note further that since \( K/C(t) \) is separable, \( w \in C(t) \). Hence, we can apply Lemma 8.3.3 to \( w, t, \bar{u}, \bar{v} \) in place of \( y, t, u, v \) to conclude that \( w = t \). But in this case \( y = w^{p^a k} = t^{p^a k} \) and the corollary holds.

We now proceed to eliminate the assumption that the function in question is rational.

8.3.5 Lemma.

Let \( w \) be an element of \( K \setminus C_K(t) \), let \( u, v, u_{i,j}, k_{j_1}, v_{i,j}, k_{j_2}, i, k = 0, \ldots, l, j_1 = 1, \ldots, r_1, j_2 = 1, \ldots, r_2 \) be elements of \( K \) satisfying

\[
\bigwedge_{i=0}^l \bigvee_{j_1 \in \{1, \ldots, r_1\}} \bigwedge_{k=0}^k \bigvee_{j_2 \in \{1, \ldots, r_2\}} C(i, k, j_1, j_2, w, u_{i,j}, k_{j_1}, v_{i,j}, k_{j_2}). \tag{8.3.5}
\]

Then \( w \) is a \( p \)-th power of some element of \( K \).

Proof.

By Corollary 8.2.10, we can choose distinct natural numbers

\[
i, k_1, \ldots, k_{n+1} \in \{1, \ldots, l\}
\]

such that \( \{c_i, c_{k_1}, \ldots, c_{k_{n+1}}\} \subset C_w \). Fix the indices \( i, k_1, \ldots, k_{n+1} \). By assumption of the lemma, (8.2.3)–(8.2.6) hold for quadruples

\[
(i, j_1, k_1, j_1), \ldots, (i, j_l, k_{n+1}, j_{n+1})
\]
for some index $j_i$ with $1 \leq j_i \leq r_i$, and indices $j_{k_1}, \ldots, j_{k_{n+1}}$ with $1 \leq j_{k_m} \leq r_{k_m}$.

Next consider $w_{i,j,k_m,j_{k_m}} = \frac{w - d_{i,j}}{w - d_{i,j}}$ for $m = 1, \ldots, n + 1$. Note that neither numerator, nor denominator of this fraction has a zero at a valuation ramifying in the extension $K/C_K(t)$. Thus, by Lemma 8.2.7, for all $m = 1, \ldots, n + 1$, we have that $w_{i,j,k_m,j_{k_m}}$ has no zeros or poles at any valuation ramifying in the extension $K/C_K(t)$.

By assumption, $w \notin C_K(t)$. This implies that for all $m = 1, \ldots, n + 1$ we also have that $w_{i,j,k_m,j_{k_m}} \notin C_K(t)$. Further, by an argument similar to the one used in the proof of Lemma 8.3.3, for all $m = 1, \ldots, n + 1$, equations (8.2.5) and (8.2.6) imply that the divisor of $w_{i,j,k_m,j_{k_m}}$ is of the form $\mathfrak{p}_{km}^{b_1} \mathfrak{p}_r^{b_2}$, where $b_1$ is either -1 or 0 and $b_2$ is either 1 or 0.

Let $w = C_K(w, t)$, and note that for all $m = 1, \ldots, n + 1$ we have that $w_{i,j,m,j_n} \in K_w$ and $[K_w : C_K(t)] = p^\delta$, where $0 < \delta \leq h$. (The left inequality is strict due to our assumption that $w \notin C_K(t)$). Further, since $w_{i,j,k_m,j_{k_m}}$ does not have any zeros or poles ramifying in the extension $K/C_K(t)$, the divisor of $w_{i,j,k_m,j_{k_m}}$ will be of the form $\mathfrak{p}_w^{\bar{p}_w} \mathfrak{p}_s^{b_1} \mathfrak{p}_t^{b_2}$ in $K_w$, where $\mathfrak{p}_w$ is the $K_w$-divisor below the divisor $\mathfrak{a}$, and for all $s$ we have that $\mathfrak{p}_s^{\bar{p}_w}$ denotes the prime below $p_s$ in $C_K(t, w)$. Next we note that by Proposition B.4.2, the divisor of

$$ N_{K_w/C_K(t)}(w_{i,j,k_m,j_{k_m}}) $$

is equal to the norm of the divisor of $w_{i,j,k_m,j_{k_m}}$. On the other hand,

$$ N_{K_w/C_K(t)}(\bar{p}_s^{\bar{p}_w}) = \bar{p}_s^{\bar{p}_w} \bar{p}_s^{p_\delta} = \bar{p}_s^{p_\delta}. $$

Thus the divisor of the norm of $w_{i,j,k_m,j_{k_m}}$ in $C_K(t)$ is a $p$-th power of some other divisor of $C_K(t)$. Since in $C_K(t)$ every zero degree divisor is principal, we must conclude that for all $m = 1, \ldots, n + 1$, the $K/C_K(t)$ norm of $w_{i,j,k_m,j_{k_m}}$ is a $p$-th power of some element of $C_K(t)$. Further,

$$ w_{i,j,k_m,j_{k_m}}^{-1} = \frac{w - d_{k_m,j_{k_m}}}{w - d_{i,j}} = 1 + \frac{d_{i,j} - d_{k_m,j_{k_m}}}{w - d_{i,j}} = \left( d_{i,j} - d_{k_m,j_{k_m}} \right) \left( \frac{1}{d_{i,j} - d_{k_m,j_{k_m}}} - \frac{1}{d_{i,j} - w} \right). $$

Thus, we can conclude that for $m = 1, \ldots, n + 1$ it is the case that

$$ N_{K_w/C_K(t)} \left( \frac{1}{d_{i,j} - d_{k_m,j_{k_m}}} - \frac{1}{d_{i,j} - w} \right) $$

is a $p$-th power. Then, by Lemma 8.2.5, taking into account our assumption that for all natural numbers $s$, for $m \neq j$, we have that $c_{m}^{p_r} \neq c_j$, we can conclude that $w - d_{i,j}$ is a $p$-th power in $K$. Consequently, $w$ is a $p$-th power in $K$. 

165
8.3.6 Corollary.

Let \( w, u, v, u_i, j_k, v_i, j_k, i, k = 0, \ldots, l, j_i = 1, \ldots, r_i, j_k = 1, \ldots, r_k \) be as above. Then \( w \in C_K(t) \).

Proof.

Unless \( w \) is a constant and consequently is in \( C_K \subseteq C_K(t) \), for some natural number \( m \), there exists \( \bar{w} \) such that \( w = \bar{w}^p \) and \( \bar{w} \) is not a \( p \)-th power. By Lemma 8.3.2 and induction, there exist \( \bar{u}, \bar{v}, \bar{u}_i, j_k, \bar{v}_i, j_k, i, k = 0, \ldots, l, j_i = 1, \ldots, r_i, j_k = 1, \ldots, r_k \) such that

\[
\bigwedge_{i=0}^l \bigvee_{j_i \in \{1, \ldots, r_i\}} \bigvee_{k=0, k \neq j_k \in \{1, \ldots, r_i\}} C(i, k, j_i, j_k, \bar{w}, \bar{u}_i, j_k, \bar{v}_i, j_k, k)
\]

Since \( \bar{w} \) is not \( p \)-th power, we conclude that \( \bar{w} \in C_K(t) \). Thus for some \( s \), we have that \( w^p \in C_K(t) \). But the extension \( K/C_K(t) \) is separable. Thus, \( w \in C_K(t) \).

8.3.7 Corollary.

Let \( w, u, v, u_i, j_k, v_i, j_k, i, k = 0, \ldots, l, j_i = 1, \ldots, r_i, j_k = 1, \ldots, r_k \) be elements of \( K \) satisfying

\[
\left( \bigwedge_{i=0}^l \bigvee_{j_i \in \{1, \ldots, r_i\}} \bigvee_{k=0, k \neq j_k \in \{1, \ldots, r_i\}} C(i, k, j_i, j_k, w, u_i, j_k, v_i, j_k) \right) \bigwedge (B(a, w, u, v))
\]

Then for some \( s \in \mathbb{N} \) we have that \( w = t^{p^s} \).

Proof.

From Corollary 8.3.6 we conclude that \( w \in C_K(t) \). Therefore we can apply Corollary 8.3.4 to conclude that \( w = t^{p^s} \) for some non-negative integer \( s \).

Finally we prove the main result of this section.

8.3.8 Proposition.

The set \( \{ w \in K \mid \exists s \in \mathbb{N} : w = t^{p^s} \} \) is Diophantine over \( K \).
Proof.

First of all observe that for any \( x \in K \) and any \( s \in \mathbb{N} \)
\[
\begin{align*}
    x^{p^a s} - x &= (x^{p^a (s-1)} + x^{p^a (s-2)} + \ldots + x)^p - (x^{p^a (s-1)} + x^{p^a (s-2)} + \ldots + x) \\
    x^{p^a s} - x &= (x^{p^a (s-1)} + x^{p^a (s-2)} + \ldots + x)^p - (x^{p^a (s-1)} + x^{p^a (s-2)} + \ldots + x)
\end{align*}
\] (8.3.6)

Next we want to show that assuming \( w = t^{p^a s} \), (8.3.5) is true over \( K \). In view of equality (8.3.6), it is enough to show that for some \( 1 \leq j_i \leq r_i \) and \( 1 \leq k_j \leq r_j \),
\[
    w_{i,j} = (t_{i,k})^{p^a}
\]

Choose \( j_i \equiv a_i \mod r_i \). (Such a \( j_i \) exists since the set of all possible values of \( j_i \) contains a representative of every class modulo \( r_i \).) Then for some integer \( m \)
\[
    c_{p^a} = (c_{p^a})^{p^m} = c_{p^a}.
\]
Similarly, choose \( j_k \equiv a_k \mod r_k \) so that \( c_{p^a} = c_{p^a} \). Now we conclude, that the set
\[
    \{ w \in K | \exists s \in \mathbb{N} : w = t^{p^a} \}
\]
is Diophantine over \( K \) for \( p > 2 \). Finally in the case \( p = 2 \) and \( a = 2 \), we note that there exists a non-negative \( r \) such that \( w = t^{2^r} \) if and only if either there exists a non-negative \( s \) such that \( w = t^{4^s} \) or \( w = (t^{4^s})^2 \).

8.4 \( p \)-th Power Equations over Function Fields


In this section we will use \( p \)-th powers of \( t \) to construct \( p \)-th powers of arbitrary elements. We will start with a lemma which is a slightly different version of an idea we have already used in Section 8.3.

8.4.1 Lemma.

Let \( m \) be a positive integer. Let \( v \in K \) and assume that for some distinct \( a_0 = 0, a_1, \ldots, a_n \in C_K \), the divisor of \( v + a_0, \ldots, v + a_n \) is a \( p^m \)-th power of some other divisor of \( K \). Then, assuming for all \( i \) we have that \( v + a_i \) does not have any zeros or poles at any prime ramifying in the extension \( K/C_K(t) \), it is the case that \( v \) is a \( p^m \)-th power in \( K \).

Proof.

First assume \( v \in C_K(t) \). Since \( v + a_i \) does not have any zeros or poles at primes ramifying in the extension \( K/C_K(t) \), the divisor of \( v + a_i \) in \( C_K(t) \) is a \( p^m \)-th power of another \( C_K(t) \) divisor. Since in \( C_K(t) \) every zero degree divisor is principal and the constant field is perfect, \( v \) is a \( p \)-th power in \( C_K(t) \) and therefore in \( K \). Next assume \( v \notin C_K(t) \). Note that no zero or pole of \( v + a_i \)
is at any valuation ramifying in the extension $K/C_K(t, v)$. Hence, in $C_K(t, v)$ the divisor of $v + a_i$ is also a $p^m$-th power of another divisor. Finally note that $N_{C_K(t, v)/C_K(t)}(v + a_i)$ will be a $p^n$-th power in $C_K(t)$ and apply Lemma 8.2.5.

Before we produce a Diophantine definition of $p$-th powers of arbitrary elements of $K$, we will carry out the construction for elements with simple zeros and poles. The next two lemmas deal with the construction of such elements. We will use a global derivation with respect to $t$ to verify that an element has simple poles at certain valuations. A discussion of global and local derivations and their relationship to the order of zeros can be found in Section B.9 of the Number Theory Appendix.

8.4.2 Lemma.

Let $p > 2$. Let $x \in K$. Let $u = \frac{x^p + t}{x^p - t}$. Let $a \in C_K, a \neq \pm 1$. Then all zeros and poles of $u + a$ are simple except possibly for zeros or poles at $p, q$ or at primes ramifying in in the extension $K/C_K(t)$.

Proof.

It is enough to show that the proposition holds for $u$. The argument for $u^{-1}$ follows by symmetry. First of all we note that the global derivation with respect to $t$ is defined over $K$, and the derivative follows the usual rules by Definition B.9.2 and Proposition B.9.4. So consider

$$
\frac{d(u + a)}{dt} = 2x^p \frac{2x^p}{(x^p - t)^2}.
$$

If $\iota$ is a prime of $K$ such that $\iota$ does not ramify in the extension $K/C_K(t)$ and is not a pole or zero of $t$, then by Corollary B.9.7 we have that

$$
\text{ord}_\iota(u + a) = \text{ord}_\iota \frac{(1 + a)x^p + (1 - a)t}{x^p - t} > 1
$$

if and only if $\iota$ is a common zero of $u + a$ and $\frac{d(u + a)}{dt}$. If $\text{ord}_\iota \frac{2x^p}{(x^p - t)^2} > 0$, then $\iota$ is either a zero of $x$ or a pole of $x^p - t$. Any zero of $x$, which is not a zero of $t$, is not a zero of $u + a$ for $a \neq 1$. Further, any pole of $x$ is also not a zero of $u + a$. Thus all zeros of $u + a$ at primes not ramifying in the extension $K/C_K(t)$ and different from $p$ and $q$ are simple. Next we note that poles of $u + a$ are zeros of $u^{-1}$. Further

$$
\frac{du^{-1}}{dt} = \frac{-2x^p}{(x^p + t)^2},
$$

168
and by a similar argument $u^{-1}$ and $\frac{du}{dt}$ do not have any common zeros at any primes not ramifying in the extension $K/C_K(t)$ and not being a pole or a zero of $t$.

We leave to the reader a proof of a similar lemma below dealing with the case of $p = 2$.

**8.4.3 Lemma.**

Let $p = 2$. Let $x \in K$. Let $u = \frac{x^2 + x + t}{x^2 + t}$. Let $a \in C_K, a \neq 1$. Then all zeros and poles of $u + a$ are simple except possibly for zeros or poles at $p, q$ or at primes ramifying in in the extension $K/C_K(t)$.

Our next task is to note that equations we are going to be using for this case (the case of a function with simple zeros or poles) can be reproduced if we take the $p$-th root of the “main” variable, just as it happened in the case of Lemma 8.3.2. The proof is also analogous to the proof of Lemma 8.3.2 and we omit it.

**8.4.4 Lemma.**

Let $s \in \mathbb{N}, s > 0$. Let $x, v \in K \setminus \{0\}$ and assume that for some $\tilde{v} \in K$ we have that $\tilde{v}^p = v$. Let $u = \frac{x^p + t}{x^p - t}$ if $p > 2$ and let $u = \frac{x^2 + x + t}{x^2 + t}$, if $p = 2$. Further, assume that

$$
\exists \mu_{i,j,k,j,k,m,e} \in K
\forall i \exists j \forall (k \neq i) \exists j \forall m \forall v : D(s, i, j, k, j, k, m, e, u, v, \mu_{i,j,k,j,k,m,e}, \nu_{i,j,e})
$$

holds. Then

$$
\exists \tilde{\mu}_{i,j,k,j,k,m,e} \in K
\forall i \exists j \forall (k \neq i) \exists j \forall m \forall v : D(s - 1, i, j, k, j, m, e, u, v, \tilde{\mu}_{i,j,k,j,k,m,e}, \tilde{\nu}_{i,j,e})
$$

holds.

**8.4.5 Lemma.**

Let $s \in \mathbb{N}, x, v \in K \setminus \{0\}$. Let $u = \frac{x^p + t}{x^p - t}$, if $p > 2$, and let $u = \frac{x^2 + x + t}{x^2 + t}$, if $p = 2$. Further, assume that (8.4.1) holds. Then for some natural number $d$, we have that $v = u^d$.  

169
Proof.

First of all, we claim that for all $i, k$, it is the case that $u_{i,k}$ has no multiple zeros or poles except possibly at the primes ramifying in $K/C_K(t)$, $p$ or $q$. Indeed, by Lemma 8.2.7, all the poles of $u_{i,k}$ are zeros of $u + c_k$ and all the zeros of $u_{i,k}$ are zeros $u + c_i$. However, by Lemma 8.4.2 and by assumption on $c_i$ and $c_k$, all the zeros of $u + c_k$ and $u + c_i$ are simple, except possibly for zeros at $p$, $q$, or primes ramifying in the extension $K/C_K(t)$. For future use, we also note that $u$ is not a $p$-th power in $K$, assuming $x \neq 0$. (This can be established by computing the derivative of $u$, which is not 0, if $x$ is not 0.)

We will show that if $s > 0$ then $v$ is a $p^s$-th power in $K$, and if $s = 0$ then $u = v$. This assertion together with Lemma 8.4.4 will produce the desired conclusion.

Note that by Corollary 8.2.10, we can choose distinct natural numbers $i, k, 1, \ldots, k_{n+1} \in \{0, \ldots, l\}$ such that $\{c_i, c_k, \ldots, c_{k_{n+1}}\} \subset C_v \cap C_u$ and for all $1 \leq j_i \leq r_i, 1 \leq j_{k_f} \leq r_{k_f}$, with $f = 1, \ldots, n+1$, we have that $u_{i,k_f,1}$ and $v_{i,j_i,j_{k_f},1}$ have no zeros or poles at the primes of $K$ ramifying in the extension $K/C(t)$, or $p$ or $q$. Note also that for thus selected indices, all the poles and zeros of $u_{i,k_f,1}$ are simple. Thus, we can pick natural numbers $i, k, 1, \ldots, k_{n+1}, j_1, j_2, \ldots, j_{n+1}$ such that the equations in (8.2.7) - (8.2.10) are satisfied for these values of indices, and $u_{i,k_1}$, $v_{i,j_1,j_{k_1},1}$, $\ldots$, $u_{i,k_{n+1}}$, $v_{i,j_1,j_{k_1},j_{k_{n+1}}}$ have no poles or zeros at primes ramifying in the extension $K/C(t)$, or at $p$ or $q$.

Now assume $s > 0$, and let $f$ range over the set $\{1, \ldots, n+1\}$. First let $e = \pm 1$, while $m = 0$, and consider the two versions of the equation in (8.2.9) with these values of $e$ and $m$.

\[
\begin{align*}
    v^2_{i,j_i,j_{k_f},1} - u^2_{i,k_f} &= \mu^{p^s}_{i,j_i,j_{k_f},1,0} - \mu_{i,j_i,j_{k_f},1,0}, \quad (8.4.3) \\
    v^{-2}_{i,j_i,j_{k_f},1} - u^{-2}_{i,k_f} &= \mu^{p^s}_{i,j_i,j_{k_f},-1,0} - \mu_{i,j_i,j_{k_f},-1,0}. \quad (8.4.4)
\end{align*}
\]

By an argument similar to the one used in the proof of Lemma 8.3.3, either for all $f = 1, \ldots, n+1$, the divisor of $v_{i,j_i,j_{k_f}}$ in $K$ is a $p^s$-th power of another divisor, or for some $f$ and some prime $i$ not ramifying in $K/C(t)$ and not equal to $p$ or to $q$, we have that $\text{ord}_i v_{i,j_i,j_{k_f}} = \pm 1$.

In the first case, given the assumption that $v_{i,j_i,j_{k_f}}$’s do not have poles or zeros at ramifying primes and Lemma 8.4.1, we have that $v$ is a $p^s$-th power in $K$. So suppose the second alternative holds. In this case, without loss of generality, assume $i$ is a pole of $v_{i,j_i,j_{k_f}}$ for some $f$. Next consider the following equations

\[
\begin{align*}
    v^2_{i,j_i,j_{k_f},1} t^{p^s} - u^2_{i,k_f} t &= \mu^{p^s}_{i,j_i,j_{k_f},1,1} - \mu_{i,j_i,j_{k_f},1,1}, \quad (8.4.5)
\end{align*}
\]

170
\[ v_{i,j,k_r,j_y}^2 - u_{i,k_r}^2 = \mu_{i,j,k_r,j_y,0,1}^p - \mu_{i,j,k_r,j_y,0,1}, \quad (8.4.6) \]

obtained from (8.2.9) by first making \( e = 1, m = 1 \) and then \( e = 1, m = 0 \). (If \( i \) were a zero of \( v_{i,j,k_r,j_y} \), then we would set \( e \) equal to \(-1\) in both equations.) Since \( t \) does not have a pole or zero at \( i \) and \( p^a > 2 \), we must conclude that

\[ \text{ord}_t(v_{i,j,k_r,j_y}^2 - u_{i,k_r}^2, t) = \text{ord}_t(\mu_{i,j,k_r,j_y,1,1}^p - \mu_{i,j,k_r,j_y,1,1}) \geq 0 \]

and

\[ \text{ord}_t(v_{i,j,k_r,j_y}^2 - u_{i,k_r}^2, t) = \text{ord}_t(\mu_{i,j,k_r,j_y,0,1}^p - \mu_{i,j,k_r,j_y,0,1}) \geq 0 \]

Thus,

\[ \text{ord}_t(v_{i,j,k_r,j_y}^2 - u_{i,k_r}^2)(t^{p^a} - t) \]

\[ = \text{ord}_t(\mu_{i,j,k_r,j_y,1,1}^p - \mu_{i,j,k_r,j_y,1,1} - t\mu_{i,j,k_r,j_y,0,1}^p + t\mu_{i,j,k_r,j_y,0,1}) \geq 0. \]

Finally, we must deduce that \( \text{ord}_t(t^{p^a} - t) \geq 2|\text{ord}_t v| \). But in \( \mathbb{C}_K(t) \) all the zeros of \( (t^{p^a} - t) \) are simple. Thus, this function can have multiple zeros only at primes ramifying in the extension \( K/C_K(t) \). By assumption \( i \) is not one of these primes and thus we have a contradiction, unless \( \nu \) is a \( p^a \)-th power.

Suppose now that \( s = 0 \). Set \( g = 1 \) again and let \( i, k_1, \ldots, k_{n+1} \) be selected as above. Then from (8.4.5) and (8.4.6) we obtain for \( k_r \in \{ k_1, \ldots, k_{n+1} \} \),

\[ \mu_{i,j,k_r,j_y,1,1}^p - \mu_{i,j,k_r,j_y,1,1} - t\mu_{i,j,k_r,j_y,0,1}^p + t\mu_{i,j,k_r,j_y,0,1} \geq 0. \]

Note here that all the poles of \( \mu_{i,j,k_r,j_y,1,1} \) and \( \mu_{i,j,k_r,j_y,0,1} \) are poles of \( u_{i,k_r} \), \( v_{i,j,k_r,j_y} \), or \( t \), and thus are not at any valuation ramifying in the extension \( K/C_K(t) \). By Lemma 8.2.11 we can then conclude that for all \( k_r \in \{ k_1, \ldots, k_{n+1} \} \)

\[ v_{i,j,k_r,j_y}^2 - u_{i,k_r}^2 = 0. \]

Thus, \( v_{i,j,k_r,j_y} = \pm u_{i,k_r} \). Since all the poles of \( u_{i,k_r} \) are simple, (8.2.10) with \( e = 1 \) rules out "-". Therefore,

\[ v_{i,j,k_r,j_y} = u_{i,k_r}. \quad (8.4.7) \]

Rewriting (8.4.7) we obtain

\[ \frac{d_{i,j} - d_{k_r,j_y}}{v + d_{k_r,j_y}} = \frac{c_i - c_{k_r}}{u + c_{k_r}}, \]

or

\[ v = au + b, \quad (8.4.8) \]

where \( a, b \) are constants. However, unless \( b = 0 \), we have a contradiction with (8.2.10) with \( e = -1 \) because unless \( b = 0 \), we have that \( v^{-1} \) and \( u^{-1} \)
have different simple poles. Finally, if \( a \neq 1 \), then we have a contradiction with (8.2.10) with \( e = 1 \) again, because the difference, unless it is 0 (and therefore \( a = 1 \)), will have simple poles.

The following corollary completes the construction for the “simple pole and zero” case.

8.4.6 Corollary.
Let \( x \in K \), and let \( u = \frac{x^p + t}{x^q - t} \) if \( p > 2 \) and let \( u = \frac{x^2 + x + t}{x^2 + t} \). Then the set \( \{ w \in K | \exists s \in \mathbb{N} : w = u^{p^s} \} \) is Diophantine over \( K \).

Proof.
Given Lemma 8.4.5, as in Proposition 8.3.8, it is enough to show that if \( w = u^{p^s} \) for some natural number \( s \), then (8.4.1) can be satisfied in the remaining variables over \( K \). This assertion can be shown to be true in the the same way as the analogous statement in Proposition 8.3.8.

8.4.7 Remark.
The reader should note that in all Propositions 8.4.2 - 8.4.6 we can systematically replace \( t \) by \( t^{-1} \) without changing the conclusions.

We are now ready for the last sequence of propositions before the main theorem. We will have to separate the case of \( p = 2 \) again. We start with the case of \( p > 2 \).

8.4.8 Proposition.
Let \( p > 2 \). Let \( x, y \in K \). Then there exist \( v, \bar{v}, u, \bar{u}, v_1, \bar{v}_1, u_1, \bar{u}_1 \in K \), \( s, r, j, r_1, j_1 \in \mathbb{N} \) such that
\[
\begin{align*}
E(u_1, \bar{u}_1, v_1, \bar{v}_1, x + 1, y + 1, j_1, r_1, s) \\
E(u, \bar{u}, v, \bar{v}, x, y, j, r, s)
\end{align*}
\]
hold if and only if \( y = x^{p^s} \).
Proof.

Suppose (8.4.9) is satisfied over $K$. Then using the fact that $E(u, \bar{u}, v, \bar{v}, x, y, j, r, s)$ holds, from (8.2.11), (8.2.13) and (8.2.15) we obtain
\[
\frac{x^{p^{r+1}} - t^{p^r}}{x^{p^{r+1}} + t^{p^r}} = \frac{y^p - t^{p^r}}{y^p + t^{p^r}}
\]
and
\[y = x^{p^r} t^{q^s - 1 - p^r - 1}.
\]

Similarly, from (8.2.12), (8.2.14) and (8.2.16)
\[y = x^{p^j} t^{-p^s - 1 + j - 1}.
\]

Thus, $x^{p^r - p^s} = t^{2p^s - 1 - p^j - 1 - p^r - 1}$. From $E(u_1, \bar{u}_1, v_1, \bar{v}_1, x + 1, y + 1, j_1, r_1, s)$ we similarly conclude
\[(y + 1) = (x + 1)^{p^1} t^{q^s - 1 - p^j - 1},
\]
and
\[(x + 1)^{p^1 - p^s} = t^{2p^s - 1 - p^j - 1 - p^r - 1}.
\]

If $x$ is a constant, then $s = r = s = j_1 = r_1$ and $y = x^{p^s}$. Suppose $x$ is not a constant. If $2p^s - 1 - p^j - 1 - p^r - 1 > 0$, then $x$ has a zero at $p$ and a pole at $q$. Further, we also conclude that $x + 1$ has a pole at $q$, $2p^s - 1 - p^j - 1 - p^r - 1 > 0$ and $x + 1$ has a zero at $p$, which is impossible. We can similarly rule out the case of $2p^s - 1 - p^j - 1 - p^r - 1 < 0$. Thus, $2p^s - 1 - p^j - 1 - p^r - 1 = 0$, $s = r = s = j_1 = r_1$, and $y = x^{p^s}$. On the other hand if $y = x^{p^s}$ and we set $s = r = s = j_1 = r_1$ we can certainly find $v, \bar{v}, u, \bar{u}, v_1, \bar{v}_1, u_1, \bar{u}_1 \in K$ to satisfy (8.4.9).

The following propositions treat the characteristic 2 case.

**8.4.9 Lemma.**

Let $p = 2$. Then for $x, y = y^2 \in K, j, r, s \in \mathbb{N} \setminus \{0\}, u, \bar{u} \in K$ there exist $v, \bar{v} \in K$ such that
\[E2(u, \bar{u}, v, \bar{v}, x, y, j, r, s) \quad (8.4.10)
\]
holds if and only if there exist $v_1, \bar{v}_1 \in K$ such that
\[E2(u_1, \bar{u}_1, v_1, \bar{v}_1, x, y, j - 1, r - 1, s - 1) \quad (8.4.11)
\]
holds.
Proof.

Suppose that for some \( x, y = \tilde{y}^2 \in K, j, r, s \in \mathbb{N} \setminus \{0\}, u, \tilde{u} \in K, \) (8.4.10) holds. Then from (8.2.21) we derive

\[
v = \frac{\tilde{y}^4 + t^{2s+1} + t^{2s}}{\tilde{y}^4 + t^{2s}} = \left( \frac{\tilde{y}^2 + t^{2s} + t^{2s-1}}{\tilde{y}^2 + t^{2s-1}} \right)^2.
\]  

(8.4.12)

Thus, if we set

\[
v_1 = \frac{\tilde{y}^2 + t^{2s} + t^{2s-1}}{\tilde{y}^2 + t^{2s-1}},
\]

(8.4.13)

we conclude that \( v_1 = u^{2^{s-1}} \). Similarly, if we set

\[
\tilde{v}_1 = \frac{\tilde{y}^2 + t^{-2s} + t^{-2s-1}}{\tilde{y}^2 + t^{-2s-1}},
\]

(8.4.14)

the \( \tilde{v}_1 = \tilde{u}^{2^{s-1}} \). Thus, (8.4.11) holds. On the other hand, it is clear that if for some \( x, y = \tilde{y}^2 \in K, j, r, s \in \mathbb{N} \setminus \{0\}, u, \tilde{u} \in K \) there exist \( v_1, \tilde{v}_1 \in K \) such that (8.4.11) holds, then by setting \( v = v_1^2, \tilde{v} = \tilde{v}_1^2 \) we will insure that (8.4.10) holds.

8.4.10 Proposition.

Let \( p = 2 \). Then for \( x, y \in K, s \in \mathbb{N} \) there exist \( j, r \in \mathbb{N}, u, \tilde{u}, v, \tilde{v} \in K \) such that (8.4.10) holds if and only if \( y = x^{2^s} \).

Proof.

Since \( E2(u, \tilde{u}, v, \tilde{v}, x, y, j, r, s) \) holds, from (8.2.17), (8.2.19) and (8.2.21) we conclude that

\[
y^2 = (x^{2^{j+1}} t^{2^{r+1}} + t^{2^r+2^{j+1}} + t^{2^r+2^{j+1}}) t^{-2^{r+1}}.
\]  

(8.4.15)

Similarly, from (8.2.17), (8.2.19) and (8.2.21) we conclude that

\[
y^2 = (x^{2^{j+1}} t^{-2^{j+1}} + t^{-2^j-2^{r+1}} + t^{-2^j-2^{r+1}}) t^{2^{j+1}}.
\]

(8.4.16)

Thus to show that (8.4.10) implies \( y = x^{2^s} \) it is enough to show that \( s = r \) or \( s = j \).

By Lemma 8.4.9 it is enough to consider two cases: one of \( r, j, s \) is equal to zero or \( y \) is not a square. First suppose that \( s = 0 \). Then \( v = \frac{v^2 + t^{2s+1}}{y^2 + t} \) and \( v \) is not a square since \( \frac{dv}{dt} = \frac{t^2}{y^2 + t} \neq 0 \). But \( v = u^{2^r} \) and therefore \( r = 0 = s \).
Suppose now that \( r = 0 \). Then \( v = u \) and therefore \( v \) is not a square by an argument similar to the one above. On the other hand, if \( s > 0 \) the \( v \) is a square. Thus, to avoid contradiction we must conclude that \( s = 0 \).

Finally if \( j = 0 \), then \( \tilde{v} = \tilde{u} \) is not a square and \( s = 0 \) again. Thus we have reduced the problem to the case where \( y \) is not a square and \( r, s, j \) are positive. In this case, from (8.4.15), taking the square root of both sides of the equation we obtain

\[
y = \left(x^{2r}t^{2s} + t^{2r-1+2s} + t^{2r+2s-1}\right)t^{-2r},
\]

implying that, unless \( r = 1, s > 1 \) or \( s = 1, r > 1 \), \( y \) is a square.

Similarly, from (8.4.16), taking the square root we obtain,

\[
y = \left(x^{2j}t^{-2s} + t^{-2j-1-2s} + t^{-2j-2s-1}\right)t^{2j},
\]

implying that, unless \( j = 1, s > 1 \) or \( s = 1, j > 1 \), \( y \) is a square again.

Thus, either \( s = 1, r > 1, j > 1 \) or \( r = j = 1, s > 1 \), or \( y \) is a square.

First suppose \( s = 1 \). Then eliminating \( y \) from (8.4.17) and (8.4.18) and substituting 1 for \( s \) yields

\[
\left(x^{2r}t^{2} + t^{2r-1+2} + t^{2r+1}\right)t^{-2r} = \left(x^{2j}t^{-2} + t^{-2j-1-2} + t^{-2j-1}\right)t^{2j},
\]

\[
x^{2r}t^{2-2r} + t^{2r-1+2} + t = x^{2j}t^{2j-2} + t^{2j-1-2} + t^{-1},
\]

Then \( t + \frac{1}{t} \) is a square in \( K \). This is impossible, since this element is not a square in \( C_K(t) \) and the extension \( K/C_K(t) \) is separable.

Suppose now that \( r = j = 1, s > 1 \). Eliminating \( y \) from (8.4.17) and (8.4.18) and substituting 1 for \( j \) and \( r \) produces

\[
t^{2s-2}x^2 + t^{2-2s}x^2 = t^{2s-1} + t^{2s-1} + t^{1-2s} + t^{-2s-1}.
\]

This equation implies that \( t^{2s-1} + t^{1-2s} \) is a square in \( K \). But

\[
\text{ord}_p(t^{2s-1} + t^{1-2s}) = \text{ord}_p(t^{1-2s}) = 1 - 2^s
\]

is odd and \( p \) is not ramified in the extension \( K/C_K(t) \). Thus we have a contradiction again.

Hence, if \( y \) is not a square, \( r = s = j = 0 \). Thus, we have shown that (8.4.10) implies \( y = x^{2s} \). Conversely, if \( y = x^{2s} \), we can set \( j = r = s \) and (8.4.10) will be satisfied.
**The Proof of Theorem 8.2.1 Completed.**

To complete the proof of Theorem 8.2.1 we note the following. Let $M$ be any function field over a finite field of constants. Let $K$ be a finite constant extension of $M$ satisfying the conditions listed in Notation and Assumptions 8.2.9. Such an extension exists by Theorem 8.2.3. Then the set $P(K)$ is Diophantine over $K$. On the other hand, $P(M) = P(K) \cap K^2$, and therefore by the “Going up and then down” method, $P(M)$ is Diophantine over $M$.

We end this section with two corollaries we will use in the chapter on Diophantine classes of function fields.

**8.4.11 Lemma.**

Let $t \in K \setminus \{0\}$. Let $a$ be a fixed natural number different from zero. Let $\mathcal{W}$ be any set of primes of $K$. Then the set

$$\{(x, y) \in O_K^2_{\mathcal{W}} | \exists r \in \mathbb{N} : x = t^p^r \land y = t^{p^r} \}$$

is Diophantine over $O_{K, \mathcal{W}}$.

**Proof.**

We will proceed by induction. Suppose we can write down a set of polynomial equation specifying that $x = t^{p^r}$ and $y = t^{p^r}$. Next consider the following set of equations.

$$w_a = t(ty_{a-1} + 1) \quad (8.4.20)$$

$$\exists s \in \mathbb{N}, z_a = w_s^{p^r} \quad (8.4.21)$$

$$\text{ord}_p z_a = \text{ord}_p x \quad (8.4.22)$$

$$y_a = ((z_a/x) - 1)/x \quad (8.4.23)$$

It is clear, that given our inductive assumptions, equations (8.4.20) - (8.4.23) will have solutions in $K$ if and only if $y_a = t^{p^r}$. Furthermore, by discussion above and Theorem 4.2.4, equations (8.4.21) and (8.4.22) can be rewritten in a polynomial form.

**8.4.12 Corollary.**

Let $x, t \in K$. Then the set $\{(x, y, w, t) \in K^4 | \exists r \in \mathbb{N} : y = x^{p^r}, w = t^{p^r} \}$ is Diophantine over $K$. (The proof is similar to the proof of Lemma 8.4.11).
8.5 Diophantine Model of $\mathbb{Z}$ over Function Fields over Finite Fields of Constants.

Using $p$-th power equations and the fact that we can assert integrality at finitely many primes using polynomial equations, we now show Diophantine undecidability of algebraic function fields over finite fields of constants by constructing a Diophantine model of $\mathbb{Z}$ over such fields. The construction we present here is based on the results by Zahidi and Cornelissen from [8]. We also remind the reader that a definition of models and their relation to Diophantine undecidability can be found in Definition 3.4.3 and Proposition 3.4.4. We start with introducing notations for this section.

8.5.1 Notation.

- Let $M$ be a function field over a finite field of constants of characteristic $p > 0$.
- Let $P(M) = \{ (x, y) : \exists s \in \mathbb{N}, y = x^{p^s} \}$.
- Let $p$ be any prime of $M$.
- Let $INT(p) = \{ x \in M : \text{ord}_p x \geq 0 \}$.
- Let $DIV(p) = \{ (x, y) \in K^2 : \text{ord}_p x \mid \text{ord}_p y \}$
- Let $MULT(M) = \{ (x, y, z) \in M^3 : \text{ord}_p x)(\text{ord}_p y) = \text{ord}_p z \}$.
- Let $ADD(M) = \{ (x, y, z) \in M^3 : (\text{ord}_p x) + (\text{ord}_p y) = \text{ord}_p z \}$.

8.5.2 Proposition.

$DIV(p)$ is Diophantine over $M$.

Proof.

For any $(x, y) \in M^2$ we have $(x, y) \in DIV(p)$ if and only if there exists $z \in M$ such that $(x, z) \in P(M)$ and $\{y/z, z/y\} \subset INT(p)$. Now $P(M)$ is Diophantine over $M$ by Theorem 8.2.1. $INT(p)$ is Diophantine over $M$ by Theorem 4.3.4. Thus the proposition holds.

8.5.3 Proposition.

$MULT(M)$ and $ADD(M)$ are Diophantine over $M$. 

177
Proof.

Note that \((x, y, z) \in ADD(M)\) if and only if \(\{xy/z, z/xy\} \subset INT(p)\). Thus \(ADD(M)\) is Diophantine over \(M\). Now by Theorem 8.1.9, the fact that \(ADD(M), INT(p)\) and \(DIV(p)\) are Diophantine over \(M\) implies that

\[
MULT^+(M) = MULT(M) \cap INT(p)^3
\]

is Diophantine over \(M\). We need to take care of elements which have negative orders at \(p\). Observe that for any \((x, y, z) \in M^3\), we have that \((x, y, z) \in MULT(M)\) if and only if one of the following statements is true: \((x, y, z) \in MULT^+(M)\) or \((\frac{1}{x}, y, \frac{1}{z}) \in MULT^+(M)\), or \((x, \frac{1}{y}, \frac{1}{z}) \in MULT^+(M)\), or \((\frac{1}{x}, \frac{1}{y}, z) \in MULT^+(M)\).

8.5.4 Corollary.

Let \(A \subset \mathbb{Z}^k\) be a Diophantine subset of \(\mathbb{Z}^k\). Then \(\{(z_1, \ldots, z_k) \in M^k : (\text{ord}_p z_1, \ldots, \text{ord}_p z_k) \in A\}\) is a Diophantine subset of \(M^k\).

Proof.

The inductive argument necessary to prove this corollary is similar to the argument used to prove Proposition 3.4.7 and Lemma 3.2.2.

8.5.5 Theorem.

\(M\) has a Diophantine model of \(\mathbb{Z}\).

Proof.

First of all we observe that by Corollary A.7.8, it is the case that \(M\) is recursive. Therefore, by Proposition 3.4.7, it is enough to construct a map from \(\mathbb{Z}\) into \(M\) making the image of the graph of multiplication and addition Diophantine. Consider a map \(\phi : \mathbb{Z} \rightarrow M\) defined by \(\phi(k) = t^{\rho^k}\) if \(k \geq 0\) and \(\phi(k) = t^{-\rho^{-k}}\) otherwise. From Section 8.3, we know that \(\phi(\mathbb{Z})\) is a Diophantine subset of \(M\). Next consider a subset of \(\mathbb{Z}\) consisting of the following pairs of integers \(A = \{(k, \rho^k) : k \geq 0\} \cup \{(k, -\rho^{-k}) : k < 0\}\). By Corollary A.1.6, \(A\) is recursive and therefore, it is r.e. by Lemma A.2.2. Thus by Theorem 1.2.2, \(A\) is Diophantine. Hence by Corollary 8.5.4 the set

\[
M(A) = \{(u, v) \in M^2 : (\text{ord}_p u, \text{ord}_p v) \in A\}
\]
is Diophantine over $M$. Next consider the following sets:

$$B_\times = \{(x, y, z) \in \phi(\mathbb{Z})^3 : \exists x_1, y_1, z_1, \{(x_1, x), (y_1, y), (z_1, z)\} \subset M(A), (x_1, y_1, z_1) \in MULT(M)\},$$

and

$$B_+ = \{(x, y, z) \in \phi(\mathbb{Z})^3 : \exists x_1, y_1, z_1, \{(x_1, x), (y_1, y), (z_1, z)\} \subset M(A), (x_1, y_1, z_1) \in ADD(M)\}.$$

Observe that the sets $B_\times$ and $B_+$ are both Diophantine subsets of $M^3$ with $B_\times$ being the $\phi$-image of the graph of multiplication, while $B_+$ is the $\phi$-image of the graph of addition.
Chapter 9

Bounds for Function Fields.

In this chapter we will discuss some bound equations specialized for function fields. These bounds will be used in the next chapter in discussion of Diophantine classes of function fields. Some of the methods used below should be familiar to the reader from Chapter 5.

9.1 Height Bounds.

In this section we will discuss how to obtain some information about the height of a function, given some information on the height of a polynomial evaluated at this function. We also compare the height of the coordinates of a field element with respect to a chosen basis to the height of the element itself. (The reader is reminded that the definition of height of a function field element can be found in B.1.25.)

9.1.1 Lemma.

Let $K$ be a function field, and let $F(T) \in K[T]$ be a polynomial of degree greater or equal to 1. Let $H_K(x)$ denote the height of $x$ in $K$. Then there exists a positive constant $C_F$, depending only on $F(T)$, such that for all $x \in K$ we have that $H_K(x) \leq C_F \cdot (H_K(F(x))).$

Proof.

Since the case of degree of $F(T)$ being equal to 1 is obvious, we will assume that degree of $F(T)$ is greater than 1. Let

$$F(T) = A_0 + A_1 T + \ldots + A_n T^n, \quad n > 1.$$
Let $C_{1F}$ be the maximum of the height $s$ of the coefficients of $F(T)$. Let $p$ be a pole of $x$, such that $p$ is not a zero or a pole of any coefficient of $F$ or $\vert \text{ord}_p x \vert > 2C_{1F}$. Then $\vert \text{ord}_p F(x) \vert \geq \vert \text{ord}_p x \vert$, with $p$ being the pole of both $x$ and $F(x)$. Indeed, in this case, for any $i = 1, \ldots, n - 1$ we have that

$$\vert \text{ord}_p A_n x^n \vert > \vert \text{ord}_p A_{n-i} x^{n-i} \vert.$$  

This is true because

$$\vert \text{ord}_p A_n x^n \vert \geq n \vert \text{ord}_p x \vert - \vert \text{ord}_p A_n \vert \geq n \vert \text{ord}_p x \vert - C_{1F},$$  

while

$$\vert \text{ord}_p A_{n-i} x^{n-i} \vert \leq (n - i) \vert \text{ord}_p x \vert + \vert \text{ord}_p A_{n-i} \vert \leq (n - i) \vert \text{ord}_p x \vert + C_{1F}.$$  

Thus,

$$\vert \text{ord}_p A_n x^n \vert - \vert \text{ord}_p A_{n-i} x^{n-i} \vert \geq \vert \text{ord}_p x \vert - 2C_{1F} > 0.$$  

Therefore,

$$\vert \text{ord}_p F(x) \vert \geq \vert \text{ord}_p x \vert - C_{1F} \geq \vert \text{ord}_p x \vert.$$  

Let $\mathcal{P}$ be the set of primes of $K$ satisfying conditions described above. That is, if $p \in \mathcal{P}$ then $p$ is a pole of $x$ such that it is not a zero or a pole of any coefficient of $F(T)$ or the absolute value of the order of the pole is greater than $2C_{1F}$. Note that the number of primes of $K$ which are not in $\mathcal{P}$ but are poles of $x$ is less or equal to $2(n + 1)C_{1F}$ and their degrees are also bounded by $C_{1F}$. Then we have the following inequality

$$H_K(x) = \left\lvert \sum_{p \text{ is a pole of } x} \text{deg}(p) \text{ord}_p x \right\rvert = \sum_{p \in \mathcal{P}} \text{deg}(p) \text{ord}_p x + \sum_{p \text{ is a pole of } x, p \notin \mathcal{P}} \text{deg}(p) \text{ord}_p x \leq \sum_{p \in \mathcal{P}} \text{deg}(p) \text{ord}_p F(x) + \sum_{p \text{ is a pole of } x, p \notin \mathcal{P}} 2(C_{1F})^2 \leq H_K(F(x)) + 4(n + 1)(C_{1F})^3 \leq 4(n + 1)(C_{1F})^3 H_K(F(x)) = C_F H_K(F(x)).$$

### 9.1.2 Lemma.

Let $C_1(t)/C_2(t)$ be a constant field extension of rational function fields over finite fields of constants. Let $r = [C_1(t) : C_2(t)]$. Let $w \in C_1(t)$ be of $C_1(t)$-height $h$. Then $w = f/g$, where $g \in C_2(t)$, $H_{C_1(t)}(f) \leq rh$, and $H_{C_2(t)}(g) = H_{C_1(t)}(g) \leq rh$.
Proof.

First of all, we note that since the constant extension is separable, by Lemma B.4.21, the $C_1(t)$ and $C_2(t)$ height $s$ of an element of the smaller field will be the same. Next write $w = u/v$ where $u$ and $v$ are relatively prime polynomials in $t$. Then

\[ \max(H_{C_1(t)}(u), H_{C_1(t)}(v)) \leq H_{C_1(t)}(w) = h. \]

Let $v = v_1, \ldots, v_r$ be all the conjugates of $v$ over $C_2(t)$. Then $\prod_{i=1}^r v_i \in C_2(t)$, and for all $i$, we have that $H_{C_1(t)}(v) = H_{C_1(t)}(v_i)$. On the other hand, $H_{C_1(t)}(uv_2 \ldots v_r) \leq rh$ and $H_{C_1(t)}(vv_2 \ldots v_r) \leq rh$.

The following lemma is quite similar to Corollary 5.2.2. We leave the proof to the reader.

9.1.3 Lemma

Let $K/L$ be a finite separable extension of function fields. Let $K_N$ be the Galois closure of $K$ over $L$. Let $h \in K$, let $h = h_1, \ldots, h_k \in K_N$ be all the conjugates of $h$ over $L$. Let $\Omega = \{\omega_1, \ldots, \omega_k\}$ be a basis of $K$ over $L$ and assume $h = \sum_{i=0}^{k-1} f_i \omega_i$, where $f_i \in L$ for $i = 0, \ldots, k - 1$. Then $H_{K_N}(f_i) \leq a H_{K_N}(h)$, where $a = a(\Omega)$ is a positive constant depending on the basis elements only.

9.2 Using $p$-th Powers to Bound the Height.

9.2.1 Lemma.

Let $\mathcal{W}$ be a collection of primes of a function field $K$ such that in some finite extension $M$ of $K$ only finitely many primes of $\mathcal{W}$ have relative degree one factors. Let $F(T)$ be a polynomial over $K$ as described in Lemma B.4.19. Let $t \in K$ be such that all the poles of $t$ are among the primes of $\mathcal{W}$. Let $x \in K$. Let $k, m$ be arbitrary non-negative integers. Then the following statements are true.

1. $\left(\frac{t^{pk} - t}{F(t)}\right)^m \in O_{K, \mathcal{W}}$ implies that all the poles of $\frac{t^{pk} - t}{F(t)}$ are poles of $t$, and all the zeros of $F(x)$ are among the zeros of $t^{pk} - t$.

2. For every $x \in K$ there exists $k, m \in \mathbb{N}$ such that $\left(\frac{t^{pk} - t}{F(t)}\right)^m \in O_{K, \mathcal{W}}$.

3. If $\frac{t^{rk} - t}{F(t)} \in O_{K, \mathcal{W}}$ then $H_K(x) \leq C_F p^{(k+m)} H_K(t)$. 

182
Proof.

1. Any pole of \( \frac{(t^p - t)^m}{F(x)} \) is either a pole of \( t \) or a zero of \( F(x) \). But by Lemma B.4.18, none of the zeros of \( F(x) \) is in \( \mathcal{W} \), while the quotient \( \frac{(t^p - t)^m}{F(x)} \in \mathcal{O}_K \), and thus must have poles at primes of \( \mathcal{W} \) only. Therefore, all the poles of the quotient must come from poles of \( t \).

2. If \( p \) is a prime of \( K \) which is not a pole of \( t \), then for some \( k \in \mathbb{N} \) it is the case that \( p \) is a zero of \( t^p - t \).

3. By Lemma 9.1.1,

\[
H_K(x) \leq C_F H_K(F(x)) \leq C_F H_K(t^p - t)^m = C_F p^{(m+k)} H_K(t).
\]

9.2.2 Corollary.

Let \( K \) be a function field over a finite field of constants of characteristic \( p > 0 \). Let \( \mathcal{W}_K \) be a set of primes of \( K \) without relative degree 1 factors in some finite separable extension of \( K \). Let \( a, b \in \mathbb{N} \) and assume \( t \in \mathcal{O}_{K, \mathcal{W}_K} \). Then there exists a set \( A \subset \mathcal{O}_{K, \mathcal{W}_K} \) such that the following statements are true.

1. \( A \) is Diophantine over \( \mathcal{O}_{K, \mathcal{W}_K} \).

2. \((x, y) \in A \Rightarrow \exists r \in \mathbb{N}, y = t^r \) and \( H_K(y) > aH_K(x) + b \).

3. For every \( x \in \mathcal{O}_{K, \mathcal{W}} \) there exists \( y \in \mathcal{O}_{K, \mathcal{W}} \) such that \((x, y) \in A \).

Proof.

Let \( p \in \mathcal{W}_K \) be a pole of \( t \). Let \( s \in \mathbb{N} \) be such that \( p^s > C_F H_K(t) \), where \( F(T) \) is as defined in Lemma B.4.19 and \( C_F \) is as defined in Lemma 9.1.1. Next let \( A \) be a set of pairs \((x, y) \in \mathcal{O}_{K, \mathcal{W}}^2 \) such that there exist \( k, m \in \mathbb{Z}_{>0}, z \in \mathcal{O}_{K, \mathcal{W}} \) satisfying the following equations:

\[
z = \frac{(t^p - t)^m}{F(x^a + b)} \quad (9.2.1)
\]

\[
y = t^{k+m+s} \quad (9.2.2)
\]

Suppose equations (9.2.1) and (9.2.2) are satisfied over \( \mathcal{O}_{K, \mathcal{W}} \). Then

\[
H_K(F(x^a + b)) \leq H_K((t^p - t)^m) = H_K(t^{p^k + m}),
\]

and by Lemma 9.1.1,

\[
aH_K(x) + b \leq (a + b)H_K(x) = H_K(x^{a+b}) \leq C_F H_K(t^{p^k + m}) = C_F p^{(k+m)} H_K(t) < p^{(k+m)} p^s < H_K(y).
\]

Finally we note that \( A \) is Diophantine over \( \mathcal{O}_{K, \mathcal{W}_K} \) by Lemma 8.4.12.
Chapter 10

Diophantine Classes over Function Fields.

Having resolved the issues of Diophantine decidability over global function fields, we turn our attention to Diophantine definability over these fields. Our goal for this chapter is to produce vertical and horizontal definability results for “large” rings of functions, as we did for “large” number rings. The original results discussed in this chapter can be found in [97], [104] and [107].

We start with a function field version of the Weak Vertical Method.

10.1 The Weak Vertical Method Revisited.

In this section we revisit the Weak Vertical Method and adjust it for function fields. As you will see below very little “adjusting” will be required.

10.1.1 Theorem: The Weak Vertical Method For Function Fields.

Let $K/L$ be a finite separable extension of function fields over finite fields of constants, and let $K_N$ be the normal closure of $K$ over $L$. Let $\{\omega_1 = 1, \ldots, \omega_k\}$ be a basis of $K$ over $L$. Let $z \in K$. Further, let $\mathcal{V}$ be a finite set of primes of $K$ satisfying the following conditions.

1. Each prime of $\mathcal{V}$ is unramified over $L$ and is the only $K$-factor of the prime below it in $L$.
2. $z$ is integral at all the primes of $\mathcal{V}$.
3. For each \( p \in \mathcal{V} \) there exists \( b(p) \in C_L \) (the constant field of \( L \)) such that
\[
z - b(p) \equiv 0 \pmod{p}.
\]
4. \( \{\omega_1, \ldots, \omega_k\} \) is a local integral basis with respect to every prime of \( \mathcal{V} \).
5. \( |\mathcal{V}| > ka(\Omega)H_{K_n}(z) \), where \( a(\Omega) \) is a constant defined as in the Lemma 9.1.3.

Then \( z \in L \).

**Proof.**

Write \( z = \sum_{i=1}^k f_i \omega_i \), where for all \( i = 1, \ldots, k \), we have that \( f_i \in L \). By assumption, \( \{\omega_1, \ldots, \omega_k\} \) is a local integral basis for all the primes in \( \mathcal{V} \). By the Strong Approximation Theorem (see Theorem B.2.1), there exists \( f \in L \) such that for every \( p \in \mathcal{V} \), we have that \( f \equiv b(p) \pmod{p} \). Thus, \( z - f \) will be zero modulo every prime of \( \mathcal{V} \). On the other hand, \( z - f = (f_1 - f) + f_2 \omega_2 + \ldots + f_k \omega_k \). By Lemma B.4.12, for \( i = 2, \ldots, k \), for all \( p \in \mathcal{V} \) we have that \( \text{ord}_p f_i > 0 \). Furthermore, by Lemma 9.1.3 we have that
\[
H_K(f_i) \leq H_{K_n}(f_i) \leq akH_{K_n}(z) < |\mathcal{V}|.
\]

Thus, unless \( f_2 = \ldots = f_k = 0 \), we have a contradiction. But if \( f_2 = \ldots = f_k = 0 \), then \( z \in L \).

Using the Weak Vertical Method we will prove the following theorem concerning vertical Diophantine definability.

**10.1.2 Theorem.**

Let \( K/L \) be a finite separable extension of global fields. Then the following statements are true.

1. For any \( \varepsilon > 0 \) there exists a set \( \mathcal{W}_K \) of primes of \( K \) of density greater than \( 1 - \varepsilon \) such that \( L \cap O_{K, \mathcal{W}_K} \leq_{\text{Dioph}} O_{K, \mathcal{W}_K} \).

2. For any \( \varepsilon > 0 \) there exists a set \( \mathcal{W}_L \) of primes of \( L \) of density greater than \( 1 - \varepsilon \) such that \( O_{L, \mathcal{W}_L} \) has a Diophantine definition in its integral closure in \( K \).

The proof of the theorem is contained in Sections 10.2 – 10.4. The overall plan for the proof is very similar to the plan we used for number fields.
Essentially, as over number fields, it is enough to take care of the cyclic case. The only difference here is that we will have two kinds of cyclic extensions: non-constant cyclic extensions (with no change in the constant field) and constant extensions (which will automatically be cyclic).

10.2 The Weak Vertical Method Applied to Non-Constant Cyclic Extensions.

In this section we will consider a cyclic extension of global function fields over the same field of constants. We will start with fixing notation for this section.

10.2.1 Notation.

- $G$ will denote an algebraic function field of positive characteristic $p > 0$.
- Let $\mathcal{P}(G)$ be the set of all primes of $G$.
- Let $\mathcal{W}_G \subset \mathcal{P}(G)$ be such that in some finite separable extension of $G$ all but possibly finitely many primes of $\mathcal{W}_G$ have no factors of relative degree 1.
- Let $F$ be a subfield of $G$ such that
  - both $G$ and $F$ have the same field constants $C$ which is of size $p^r$ for some positive integer $r$;
  - $G/F$ is a cyclic extension.
- $t$ will denote a non-constant element of $F$ such that $t$ is not a $p$-th power and $t \in \mathcal{O}_{G,\mathcal{W}_G}$.
- Let $\mathcal{D}(t)$ be the set of all $G$-primes occurring in the divisor of $t$.
- Let $d = [G : C(t)]$
- Let $\Omega = \{1, \alpha, \ldots, \alpha^{m-1}\}$ be a basis of $G$ over $F$.
- Let $q \neq p$ be a rational prime, assume $q > d$, $(q, r) = 1$, $(q, m) = 1$.
- Let $\beta$ be an element of the algebraic closure of $C$ such that $[C(\beta) : C] = q$.
- Let $n(\alpha)$ be the constant defined as in Lemma B.4.34. This constant depends on $\alpha$ and $K$ only.
Let $a(\Omega)$ be the constant computed as in Lemma 9.1.3. This constant depends on the power basis of $\alpha$ only.

Let $g_F, g_G$ be the genuses of $F$ and $G$ respectively.

Let $b$ be a fixed positive integer such that

$$b > 2 \log_p 2(m + 4g_G + 3mg_F + 1 + 2dm).$$

Next we prove an easy lemma which makes the construction work.

**10.2.2 Lemma.**

Let $f \in C[t]$. Let $l$ be a positive integer such that $l \equiv 0 \mod r$. Then $\frac{f^{pl} - f}{t^{pl} - t} \in C[t]$.

**Proof.**

Let $f(t) = \sum_{i=0}^{k} a_i t^i, a_i \in C$. Then, since $l \equiv 0 \mod r \Rightarrow a_i^{pl} = a_i$, and

$$f^{pl} - f = \sum_{i=0}^{k} a_i^{pl} t^{ipl} - \sum_{i=0}^{k} a_i t^i = \sum_{i=0}^{k} a_i (t^{ipl} - t^i)$$

$$= (t^{pl} - t) \sum_{i=0}^{k} a_i \left(\frac{t^{ipl} - t^i}{t^{pl} - t}\right).$$

Thus the lemma holds.

**10.2.3 Lemma.**

Suppose the following equations and inequalities are satisfied for some $x \in G$ and some $u \in \mathbb{N} \setminus \{0\}$.

$$x_j = tx^q + x^j, j = 0, 1, \quad (10.2.1)$$

$$H_G(t^{pu}) > \max \{2mH_G(t)(ma(\Omega)(qH_G(x) + H_G(t)) + 2d + n(\alpha)), H_G(t^{pb})\} \quad (10.2.2)$$

$$l = (qu + 1)r, \quad (10.2.3)$$

$$\text{ord}_q \left(\frac{x_j^{pl} - x_j}{t^{pl} - t}\right) \equiv 0 \mod q, \quad (10.2.4)$$
or
\[
\text{ord}_\mathfrak{p} \left( \frac{x_j^{p} - x_j}{t^{p} - t} \right) \geq 0,
\]
for all \( G \)-primes \( \mathfrak{p} \) not splitting in the extension \( G(\beta)/G \). Then \( x \in F \).

**Proof.**

Suppose the (10.2.1) - (10.2.5) are satisfied as indicated in the statement of the lemma. Then from (10.2.1) we conclude that for all \( p \in \mathcal{P}(G) \setminus \mathcal{Z}(t) \) such that \( \text{ord}_p x_j < 0 \) we have that \( \text{ord}_p x_j \equiv 0 \) modulo \( q \). Further, observe that in \( G \) all the zeros of \( t^p - t \) are of order at most \( d < q \) by Proposition B.1.11. Similarly, \( |\mathcal{Z}(t)| \leq 2d \), by Lemma B.4.21 taking into account that in \( C(t) \) both the zero and the pole divisors of \( t \) have degree 1.

Next consider a prime \( p \in \mathcal{P}(G) \setminus \mathcal{Z}(t) \) such that it does not split in the extension \( G(\beta)/G \) and is a zero of \( t^p - t \). If \( p \) is a pole of \( x_j \) or if \( x_j^{p} - x_j \) is a unit at \( p \), then
\[
\text{ord}_p \left( \frac{x_j^{p} - x_j}{t^{p} - t} \right) \equiv -\text{ord}_p (t^{p} - t) \not\equiv 0 \text{ modulo } q.
\]

Therefore from (10.2.4) and (10.2.5) we can conclude that \( x_j^{p} - x_j \) has a zero at every \( p \) such that \( p \notin \mathcal{Z}(t) \), \( \text{ord}_p (t^{p} - t) > 0 \) and \( p \) does not split in the extension \( G(\beta)/G \).

Next let \( C_l \) be the splitting field of the polynomial \( X^{p} - X \). Note that by (10.2.3), we have that \( l \equiv 0 \) mod \( r \) and therefore \( C \subset C_l \). Let \( \mathcal{Z}_l(t) \) be the set of \( C_lG \) primes lying above the primes of \( \mathcal{Z}(t) \). Observe that \( |\mathcal{Z}_l(t)| < 2d \) also, by Lemma B.4.21. Further, \( (l, q) = 1 \), and since \( p^u > p^b \) by (10.2.2), we also have that
\[
1 > u > \log_p (2 \log_p (2m + 4g_G + 3mg_F + 1 + 2dm)).
\]

Therefore, the following statements are true.

1. There are more than \( p^l/2m \) degree 1 primes of \( C_lF \) which do not split in the extension \( C_l(\beta)G/C_lF \), by Proposition B.4.31.

2. For any prime \( p_{C_lG} \) of \( C_lG \), it is the case that \( p_{C_lG} \) lies above a degree one \( C_lF \) prime which is not a pole of \( t \) if and only if \( \text{ord}_{p_{C_lG}} (t^{p} - t) > 0 \).

3. Let \( p_{C_lG} \) be a prime of \( C_lG \) lying above a degree one \( C_lF \) prime not splitting in the extension \( C_l(\beta)G/C_lF \). Let \( p_G \) be the \( G \)-prime below \( p_{C_lG} \). Then \( p_G \) does not split in the extension \( C(\beta)G/G \), by Proposition B.4.31.
Therefore, in $C_lG$, we have that $x_j^{p^l} - x_j$ has a zero at every prime $p_{C_lG}$ such that $p_{C_lG} \not\in \mathcal{Z}(t)$, $\text{ord}_p(t^{p^l} - t) > 0$ and $p_{C_lG}$ lies above a degree one prime of $C_lF$ that does not split in the extension $C_l(\beta)G/C_lF$. But this means, that for at least $p^l/2m - 2d$ distinct primes $p$ of $C_lG$ lying above non-splitting primes of $C_lF$,

$$\text{ord}_p(x_j - a(p)) > 0,$$

for some constant $a(p) \in C_l \subset C_lF$. Now going back to (10.2.2) and (10.2.3) we observe that

$$p^l/2m > p^n/2m > a(\Omega)m(qH_G(x) + H_G(t)) + 2d + n(\alpha) = a(\Omega)mH_G(x_j) + n(\alpha) + 2d$$

so that by the Weak Vertical Method for function fields (Theorem 10.1.1), $x_j \in C_lF$. Since $x_j \in G$, we must conclude that $x_j \in C_lF \cap G = F$, as in the extension $F/G$ the constant field remains the same. Finally if $x^q t, x^q t + x \in F$, then $x \in F$.

10.2.4 Theorem.

$O_{G,\mathcal{W}_G} \cap F \leq \text{Dioph} O_{G,\mathcal{W}_G}$. 

Proof.

First of all we observe the following. Let $x \in C_F[t]$. Then by Corollary 9.2.2, for some $u$, (10.2.2) is satisfied. Now by Lemma 10.2.2, $x_j^{p^l} - x_j$ is a polynomial of degree $p^l(q \deg(x) + 1) - p^l = p^l q \deg(x)$. Therefore, (10.2.4), (10.2.5) are satisfied. Next let $\gamma$ be a generator of $F$ over $C_F(t)$. Then $x \in O_{G,\mathcal{W}_G} \cap F$ if and only if $x \in O_{G,\mathcal{W}_G}$ and $x = \sum_{i=0}^{d-1} z_i \gamma^i$, where $z_i, v_i \in C_F(t)$ and $v_i \neq 0$.

The only remaining task is to rewrite (10.2.1)–(10.2.5) in a Diophantine fashion. We can rewrite (10.2.2) using Corollary 9.2.2. Next given $x$, by Lemmas 8.4.11 and 8.4.12, $\{(t^{p^l}, t^{p^l}, x_j^{p^l}), l = (qu + 1)r, u \in \mathbb{N}\}$ is a set Diophantine over $G$. Finally, (10.2.4) and (10.2.5) can be transformed using Theorem 4.5.2.

10.3 The Weak Vertical Method Applied to Constant Field Extensions.

In this section we will consider finite constant extensions of rational function fields. We will again start with describing notation for the section.
10.3.1 Notation.

- Let $C$ be a finite field of characteristic $p$.
- Let $t$ be transcendental over $C$.
- Let $\mathcal{W}_{C(t)}$ be a set of primes of $C(t)$ such that in some finite separable extension $M$ of $C(t)$ only finitely many primes of $\mathcal{W}_{C(t)}$ have relative degree one factors. Assume also that the prime which is the pole of $t$ is included in $\mathcal{W}_{C(t)}$.
- Let $q \neq p$ be a rational prime.
- Let $r = [C : \mathbb{F}_p]$.
- Let $\beta$ be an element of the algebraic closure of $C$ such that $[C(\beta) : C] = q$.
- Let $p_t$ be the zero of $t$ in $C(t)$.

10.3.2 Lemma.

Suppose equations and inequalities below are satisfied over $O_{C(t),\mathcal{W}_{C(t)}}$ for some $x \in O_{C(t),\mathcal{W}_{C(t)}}$ and some $u \in \mathbb{N}$. Then $x \in O_{C(t),\mathcal{W}_{C(t)}} \cap \mathbb{F}_p(t)$.

\[ \text{ord}_p, x \geq 0, \quad (10.3.1) \]
\[ x_j = tx^q + x^j, j = 0, 1, \quad (10.3.2) \]
\[ H_{C(t)}(t^{p^j}) > 2(r + 1) \cdot H_{C(t)}(x_j), \quad (10.3.3) \]
\[ l = 2qru + 1, \quad (10.3.4) \]
\[ \text{ord}_p \left( \frac{x_j^{p^j} - x_j}{t^{p^j} - t} \right) \equiv 0 \mod q, \quad (10.3.5) \]

or
\[ \text{ord}_p \left( \frac{x_j^{p^j} - x_j}{t^{p^j} - t} \right) \geq 0, \quad (10.3.6) \]

for all zeros $p$ of $t^{p^j} - t$ in $C[t]$ such that $p$ does not split in the extension $C(\beta, t)/C(t)$. 

190
Proof.

Suppose the equations and inequalities above have a solution with $l \in \mathbb{N}$ and all the other variables in $O_{C(t), W_{C(t)}}$. Then by Lemma 9.1.2, we have that $x_j = f/g$, where $g \in \mathbb{F}_p(t)$ and $H_{C(t)}(f) \leq rH_{C(t)}(x_j)$. From (10.3.5), (10.3.6) and from Lemma B.4.32 we conclude in the same fashion as in Lemma 10.2.3 that $x_j^{p^l} - x_j$ has zeros at all the primes which are zeros of $t^{p^l} - t$. Thus,

$$f^{p^l} g - f g^{p^l}$$

is divisible by $t^{p^l} - t$ in $C[t]$. Since, $g \in \mathbb{F}_p[t]$, we have that $g^{p^l} - g \equiv 0$ modulo $t^{p^l} - t$ in $C[t]$, and thus $g(f^{p^l} - f) \equiv 0$ modulo $t^{p^l} - t$. On the other hand, let $f_0$ be the polynomial obtained from $f^{p^l}$ by replacing $t^{p^l}$ by $t$. Clearly, $f_0$ is of the same degree as $f$ and $f_0 \equiv f^{p^l}$ modulo $t^{p^l} - t$, and thus, $g(f_0 - f) \equiv 0$ modulo $t^{p^l}$. Therefore, unless $f_0 = f$, degree of $fg$ is greater or equal to $p^l$. But by (10.3.3), we know that $\text{deg}(gf) < p^l$. Thus, $f_0 = f$. That means, that every coefficient of $f$ raised to the power $p^l$ is equal to itself. On the other hand, since $C$ is of degree $r$ over $\mathbb{F}_p$, every coefficient of $f$ raised to the power $p^{ru}$ is equal to itself. Thus, every coefficient of $f$ raised to the $p$-th power is equal to itself, and therefore belongs to $\mathbb{F}_p$.

We can now prove the theorem below following the same plan as in the proof of Theorem 10.2.4.

10.3.3 Theorem.

$$\mathbb{F}_p(t) \cap O_{C(t), W_{C(t)}} \subseteq_{\text{Dioph}} O_{C(t), W_{C(t)}}.$$  

10.4 Vertical Definability for Large Subrings of Global Function Fields.

In this section we put together Theorems 10.2.4 and 10.3.3 to obtain vertical definability for large subrings of function fields and complete the proof of Theorem 10.1.2. As in the case of number fields, these vertical results will later lead to a way to define integrality at infinitely many primes in the function field case. We start as usual with a notation list for this section.

10.4.1 Notation.

- Let $K/L$ be a separable extension of global function fields.
Let $S_K$ be a finite set of primes of $K$.

Let $C_K, C_L$ be the constant fields of $K$ and $L$ respectively.

Let $t \in L$ be such that it is not a $p$-th power in $K$.

Let $N$ be the Galois closure of $K$ over $C_K(t)$ and let $C_N$ be the constant field of $N$.

Let $\mathcal{P}(K)$ be the set of all the primes of $K$.

Let $\mathcal{W}_K \subset \mathcal{P}(K)$ be such that $t \in O_K, \mathcal{W}_K \cap L \leq \Dioph O_K, \mathcal{W}_K$.

Let $\mathcal{W}_N$ be the set of primes of $N$ lying above $\mathcal{W}_K$. (We remind the reader that this assumption implies that $O_N, \mathcal{W}_N$ is the integral closure of $O_K, \mathcal{W}_K$ in $N$ by Proposition B.1.22.)

Let $\mathcal{W}_{C_N(t)}$ be the set of all the primes of $C_N(t)$ such that all of their $N$-factors are in $\mathcal{W}_N$.

Let $\mathcal{W}_L$ be the set of all the primes of $L$ such that all of their $N$-factors are in $\mathcal{W}_N$.

Assume that in some finite separable extension $F$ of $N$ all but finitely many primes of $\mathcal{W}_N$ have no factors of relative degree 1.

Let $\{E_i, i = 1, \ldots, l\}$ be the set of all the fields satisfying the following conditions: $C_N(t) \subset E_i \subset N; N/E_i$ is a cyclic extension.

We now prove a more general vertical definability result. A reader might recognize the similarities with the number field case.

### 10.4.2 Theorem.

$O_K, \mathcal{W}_K \cap L \leq \Dioph O_K, \mathcal{W}_K$.

**Proof.**

First of all we observe the following. Since $N/C_K(t)$ is Galois, we also have that $N/C_N(t)$ is Galois. Next let $\sigma \in \Gal(N/C_N(t))$ and observe that the fixed field of $\sigma$ is one of finitely many cyclic subextensions of $N$ containing $C_N(t)$. Thus, if $x \in \cap_{i=1}^l E_i$, we have that $x$ is fixed by all the elements of the Galois group and therefore must be in $C_N(t)$. Further, since for all $i$ it is the case that $C_N(t) \subset E_i$ and $C_N$ is the constant field of $N$, it follows that the
constant field of $E_i$ is also $C_N$. Thus, by Theorem 10.2.4, for all $i = 1, \ldots, l$, we have that $O_{N,W_N} \cap E_i \leq_{Dioph} N$.

Using the intersection property of Diophantine Generation, we immediately conclude that $O_{N,W_N} \cap C_N(t) \leq_{Dioph} O_{N,W_N}$. Next, note that $O_{N,W_N} \cap C_N(t) = O_{C(t),W_N(t)}$. Furthermore, in the extension $FN/C(t)$, none of the primes of $W_C(t)$ has a relative degree one factor. Thus, by Theorem 10.3.3 we have that $O_{W_C(t)} \cap F_p(t) \leq_{Dioph} O_{W_C(t)}$. Using transitivity of Generation, we now conclude that $O_{N,W_N} \cap F_p(t) \leq_{Dioph} O_{N,W_N}$.

Since $t \in O_{K,W_K} \subset O_{N,W_N}$, using Diophantine generation of fraction field and extensions, we now have

$$L \leq_{Dioph} F_p(t) \leq_{Dioph} O_{N,W_N} \cap F_p(t) \leq_{Dioph} O_{N,W_N}.$$

Using the fact that $O_{N,W_N} \leq_{Dioph} O_{N,W_N}$ and the intersection property again, we get

$$L \cap O_{N,W_N} \leq_{Dioph} O_{N,W_N}.$$

Finally, by Diophantine generation of integral closure,

$$L \cap O_{K,W_K} = L \cap O_{N,W_N} \leq_{Dioph} O_{K,W_K}.$$

As before we can give an estimate on the “size” of the rings to which our results are applicable.

10.4.3 Theorem.

Let $G/F_p(t)$ be a cyclic extension of prime degree $q$ such that $(q, [N : F_p(t)]) = 1)$. Let $W_L$ be the set of all $L$-primes not splitting in the extension $LG/L$. Let $W_K$ be the set of all $K$-primes lying above primes of $W_L$. Then

$$O_{L,W_L} = O_{K,W_K} \cap L \leq_{Dioph} O_{K,W_K}.$$

and Dirichlet density of both prime sets is $1 - \frac{1}{q}$.

Proof.

Let $W_N$ be the set of $N$-primes above the primes of $W_L$. By Lemmas B.4.7 and B.4.8, we have that $W_N$ and $W_K$ consist of all the primes of $N$ and $K$ respectively not splitting in the extensions $GN/N$ and $KG/K$, plus or minus a finite set of primes. Therefore, we can apply Theorem 10.4.2 to conclude that $O_{K,W_K} \cap L \leq_{Dioph} O_{K,W_K}$. On the other hand, by Chebotarev Density Theorem, the density of $K$-primes and the density of $L$-primes not splitting in the extensions $KG/K$ and $LG/L$ is $1 - \frac{1}{q}$. 193
10.4.4 Remark

Since \( q \) can be made arbitrarily large, Theorem 10.4.2 implies Theorem 10.1.2.

Finally we note that the vertical definability results certainly apply to the rings of \( \mathcal{S} \)-integers since the conditions on the prime sets in Theorem 10.4.2 must hold up to a finite set of primes. Thus we also have the following result.

10.4.5 Theorem.

\[ O_{K,\mathcal{S}} \cap L \leq_{\text{Dioph}} O_{K,\mathcal{S}}. \]

10.5 Integrality at Infinitely Many Primes over Global Function Fields.

In this section we convert our vertical definability results into horizontal definability results using the same methods as over the number fields. The main result which will be proved in this section is stated below.

10.5.1 Theorem.

Let \( K \) be a function field over a finite field of constants. Let \( \mathcal{S} \) be a finite collection of primes of \( K \). Then for any \( \varepsilon > 0 \) there exists a set of \( K \)-primes \( \mathcal{W} \), containing \( \mathcal{S} \) and of Dirichlet density greater than \( 1 - \varepsilon \), such that \( O_{K,\mathcal{S}} \) has a Diophantine definition over \( O_{K,\mathcal{W}} \).

The proof of this theorem is derived from a technical result contained in Proposition B.5.6, which is the function field analog of Lemma B.5.5, and Proposition 10.5.3 below. Before we proceed, as usual, we need to describe the objects under consideration.

10.5.2 Notation.

- Let \( K \) be a function field of characteristic \( p > 0 \) over a finite field of constants \( C \).
- Let \( \mathcal{S}_K \) be a finite collection of primes of \( K \).
- Let \( t \in K \) be such that \( t \) has poles at all the elements of \( \mathcal{S}_K \), has no other poles and is not a \( p \)-th power. (Such a \( t \) exists by the Strong Approximation Theorem - Theorem B.2.1.)
• Let $\varepsilon$ be a positive real number.
• Let $s$ be a natural number not divisible by $p$ and such that $s > \frac{2}{\varepsilon}$.
• Let $E = C(t^s)$.
• Let $M$ be a constant extension of $E$ of prime degree $r > \frac{2}{\varepsilon}$ and such that $r$ does not divide $[K : C(t^s)]!$.
• Let $K_G$ be the Galois closure of $K$ over $E$.
• Let $\mathcal{V}_{K,1}$ be the set of primes of $K$ splitting completely in the extension $MK_G/K$.
• Let $\mathcal{W}_{K,1}$ be the set of all the $K$- primes lying above $E$-primes splitting completely in the extension $K/E$.
• Let $\mathcal{Z}_{K,1} = \mathcal{W}_{K,1} \setminus \mathcal{V}_{K,1}$.
• Let $\mathcal{Z}_{E,1}$ be the set of $E$-primes below the primes $\mathcal{Z}_{K,1}$.
• Let $\mathcal{G}_{K,1}$ be a set of $K$-primes such that it contains exactly one prime above each prime in $\mathcal{Z}_{E,1}$.
• Let $\mathcal{V}_{K,2}$ be the set of all the primes of $K$ of relative degrees greater than or equal to 2 over $E$.
• Let $\mathcal{V}_K = \mathcal{V}_{K,1} \cup \mathcal{G}_{K,1} \cup \mathcal{V}_{K,2}$.
• Let $\mathcal{W}_K = \mathcal{P}(K) \setminus \mathcal{V}_K$.
• Let $\mathcal{H}_K = \mathcal{W}_K \cup \mathcal{G}_K$.

The diagram below shows all the fields under consideration.
10.5.3 Proposition.

\[ O_{K, \mathcal{K}} \leq_{\text{Dioph}} O_{K, \overline{W}_K} \text{ and } \delta(\overline{W}_K) > 1 - \varepsilon. \]

Proof.

First of all we observe the following. Since \( t \) is not a \( p \)-th power in \( K \) and \( s \not\equiv 0 \mod p \), we have that \( t^s \) is not a \( p \)-th power in \( K \). Therefore, the extension \( K/C(t^s) \) is separable by Lemma B.1.32. Next, by Proposition B.5.6 and construction, we know that \( \overline{W}_K \) satisfies the requirements of Theorem 10.4.2. Further by Proposition B.5.6 and construction of \( \overline{W}_K \) again, \( O_{K, \overline{W}_K} \cap E = C[t^s] \). Thus, by Theorem 10.4.2, we have that \( C[t^s] \) has a definition over \( O_{K, \overline{W}_K} \) or \( C[t^s] \leq_{\text{Dioph}} O_{K, \overline{W}_K} \). On the other hand, since \( O_{K, \mathcal{K}} \) is the integral closure of \( C[t^s] \) in \( K \), by Proposition 2.2.1 we have that \( O_{K, \mathcal{K}} \leq_{\text{Dioph}} C[t^s] \). Thus, by transitivity of Dioph-genereation we have that \( O_{K, \mathcal{K}} \leq_{\text{Dioph}} O_{K, \overline{W}_K} \). Finally, by Theorem B.5.6,

\[ \delta(\overline{W}_K) = \delta(W_K) > 1 - 1/[K : E] - 1/[M : E] > 1 - \varepsilon. \]

10.6 The Big Picture for Function Fields Revisited.

In this section we go back to the Diophantine family of a polynomial ring over a finite field of constants to review what we have learned about Diophantine Generation and Diophantine classes within the family. With this plan in mind, consider Diagram 10.1. It illustrates the facts listed in Proposition 10.6.2 below, most of which we have already established. As before, the arrows signify Diophantine Generation. In our cataloging of facts we will proceed from right to left, starting with the lower level. First, however, we review the notation and assumptions.

10.6.1 Notation and Assumptions.

- Let \( \mathbb{F}_p \) be a finite field of \( p \) elements.
- Let \( t \) be transcendental over \( \mathbb{F}_p \).
- Let \( K \) be a finite separable extension of \( \mathbb{F}_p(t) \).
$\mathbb{F}_p(t)$ is a finite field of characteristic $p > 0$.

$\mathbb{O}_K, \mathfrak{p}_K \cap \mathbb{F}_p(t) = \mathbb{O}_{\mathbb{F}_p(t)}, \mathfrak{p}$

$\mathfrak{p}_K$ contains primes of $K$ without relative degree 1 factors in some finite and separable extension. $\mathbb{O}_K$ is the integral closure of $\mathbb{F}_p[t]$ in $K$.

Figure 10.1: Horizontal and Vertical Problems for the Diophantine Family of $\mathbb{F}_p[t]$ revisited.
• Let $\mathcal{P}(K), \mathcal{P}(\mathbb{F}_p(t))$ be the sets of all the primes of $K$ and $\mathbb{F}_p(t)$ respectively.

• Let $\mathcal{W} \subset \mathcal{P}(K), \mathcal{W}' \subset \mathcal{P}(\mathbb{F}_p(t))$ be prime sets containing all the poles of $t$ in $K$ and $\mathbb{F}_p(t)$ respectively. Assume further that for some separable subextension $U$ of $K$, every element of $\mathcal{W}'$ has a conjugate over $U$ which is not in $\mathcal{W}$. Similarly, for some separable subextension $U$ of $\mathbb{F}_p(t)$, every element of $\mathcal{W}'$ has a conjugate over $U$ which is not in $\mathcal{W}'$. We should note that by Riemann-Hurwitz formula, $U$ must be a rational function field.

• Let $\mathcal{W} \subset \mathcal{P}(K), \mathcal{W} \subset \mathcal{P}(\mathbb{F}_p(t))$ be such that $\mathcal{W} \subset \mathcal{W}'$ and $\mathcal{W}' \subset \mathcal{W}$. Further, for some finite separable extension $M$ of $K$, all but finitely many primes of $\mathcal{W}$ have no relative degree 1 factors in $M$. Similarly, for some finite separable extension $M$ of $\mathbb{F}_p(t)$, all but finitely many primes of $\mathcal{W}'$ have no relative degree 1 factors in $M$. Finally, $\mathcal{O}_{\mathbb{F}_p(t), \mathcal{W}} = \mathcal{O}_{\mathbb{F}_p(t), \mathcal{W}}$.

• Let $\mathcal{V} \subset \mathcal{P}(\mathbb{F}_p(t))$ be such that $\mathcal{P}(\mathbb{F}_p(t)) \setminus \mathcal{V}$ is a finite set. Similarly, let $\mathcal{V} \subset \mathcal{P}(K)$ be such that $\mathcal{P}(K) \setminus \mathcal{V}$ is a finite set.

### 10.6.2 Proposition.

The following statements are true.

• $\mathcal{O}_K \leq_{\text{Dioph}} \mathbb{F}_p[t]$ (and $\mathcal{O}_{K, \mathcal{W}} \leq_{\text{Dioph}} \mathcal{O}_{K, \mathcal{W}}$). This follows from Diophantine generation of integral closure. (See Proposition 2.2.1.)

• $\mathbb{F}_p[t] \leq_{\text{Dioph}} \mathcal{O}_{\mathbb{F}_p(t), \mathcal{W}}$. (10.6.1)

This assertion "almost" follows from Theorem 10.4.2. Indeed, let $U$ be the Galois closure of $F_p(t)$ over $U$. To apply Theorem 10.4.2 we need to know that all the $N$-factors of primes in $\mathcal{W}'$ have no relative degree 1 factors in some finite separable extension of $N$. This in fact is implied by the assumption that in some finite separable extension of $F_p(t)$ all the primes in $\mathcal{W}' \cup \mathcal{W}$ do not have relative degree one factors. Unfortunately, the proof of this fact is outside the scope of this book, but it can be found in [94]. Now Theorem 10.4.2 gives us the fact that

$$\mathcal{O}_{F_p(t), \mathcal{W}} \cap U \leq_{\text{Dioph}} \mathcal{O}_{F_p(t), \mathcal{W}}.$$ 

Let $\mathcal{W}_U$ be the set of all primes of $U$ with all their $F_p(t)$-factors in $\mathcal{W}'$. Then by assumption $\mathcal{W}_U$ is a finite set and $\mathcal{O}_{F_p(t), \mathcal{W}} \cap U = \mathcal{O}_{U, \mathcal{W}_U}$. Let
\( \mathcal{O}_{F_p(t), \mathcal{S}'} \) be the integral closure of \( \mathcal{O}_{U, \mathcal{W}_U} \) in \( F_p(t) \). Then \( \mathcal{S}' \) is a finite set and it contains the pole of \( t \). Thus using Diophantine generation of integral closure, and the fact that we can define integrality at finitely many primes, we can conclude that \((10.6.1)\) holds.

- The Diophantine class of \( \mathcal{O}_{F_p(t), \mathcal{W}} \) (or \( \mathcal{O}_{K, \mathcal{W}_K} \)) does not change if we add or remove finitely many primes from \( \mathcal{W} \) (or \( \mathcal{W}_K \)). This assertion is new and requires an (easy) argument. It is enough to carry out an argument for the case where we remove or add one prime. We will describe the argument for \( \mathcal{W} \). The identical argument will also work for \( \mathcal{W}_K \). So let \( q \in \mathcal{W} \) and let \( \mathcal{W}' = \mathcal{W} \setminus \{q\} \). Since we know how to define integrality at finitely many primes in any global function field (see Theorem 4.3.4), and holomorphy rings of global function fields are Dioph-regular (see Note 2.2.5), \( \mathcal{O}_{F_p(t), \mathcal{W}} \leq \text{Dioph} \mathcal{O}_{F_p(t), \mathcal{W}'} \). Thus, the only assertion that requires proof is the assertion that

\[
\mathcal{O}_{F_p(t), \mathcal{W}} \leq \text{Dioph} \mathcal{O}_{F_p(t), \mathcal{W}'}. \tag{10.6.2}
\]

By the Strong Approximation Theorem (see Theorem B.2.1) there exists an element \( x \in \mathcal{O}_{F_p(t), \mathcal{W}} \) such that \( x \) has only one zero at \( q \). Let \( y \in \mathcal{O}_{F_p(t), \mathcal{W}} \). Then for some \( k \in \mathbb{N} \), \( z = x^{p^k}y \in \mathcal{O}_{F_p(t), \mathcal{W}} \) and \( y = \frac{z}{x^{p^k}} \). Thus,

\[
\mathcal{O}_{F_p(t), \mathcal{W}} = \left\{ \frac{z}{w}, z, w \in \mathcal{O}_{F_p(t), \mathcal{W}} \land \exists k \in \mathbb{N}, w = x^{p^k} \right\}.
\]

Since by Theorem 8.2.1 and Dioph-regularity of holomorphy rings we can rewrite \( \exists k \in \mathbb{N}, w = x^{p^k} \) in a Diophantine fashion, we can conclude that in fact \((10.6.2)\) holds.

- \( F_p[t] \leq \text{Dioph} \mathcal{O}_K \). This follows from Theorem 10.4.5

- \( \mathcal{O}_K \leq \text{Dioph} \mathcal{O}_{K, \mathcal{W}'} \). Here we can use an argument similar to the argument used to show \((10.6.1)\).

- \( \mathcal{O}_{F_p(t), \mathcal{W}} \leq \text{Dioph} \mathcal{O}_{K, \mathcal{W}_K} \). This assertion follows by Theorem 10.4.2 again with the same caveat as in \((10.6.1)\).
Chapter 11

Mazur’s Conjectures and Their Consequences.

In this chapter we explore two conjectures due to Barry Mazur. These conjectures, which are a part of a series of conjectures made by Mazur concerning the topology of rational points, had a very important influence on the development of the subject. The conjectures first appeared in [55], and later in [56], [57], and [58]. They were explored further among others by Colliot-Thélène, Skorobogatov, and Swinnerton-Dyer in [4], Cornelissen and Zahidi in [71], Pheidas in [70], and by the author in [112]. Perhaps the most spectacular result which came out of attempts to prove or disprove the conjectures is a theorem of Poonen which will be discussed in detail in the next chapter. Unfortunately, up to this moment the conjectures are still unresolved.

The first of the conjectures we are going to discuss states the following.

11.1.1 Conjecture.

Let $V$ be any variety over $\mathbb{Q}$. Then the topological closure of $V(\mathbb{Q})$ in $V(\mathbb{R})$ possesses at most a finite number of connected components. ([58][Conjecture 2.])

11.1.2 Remark.

Let $W$ be an algebraic set defined over a number field. Then $W = V_1 \cup \ldots \cup V_k$, $k \in \mathbb{N}$, where $V_i$ is a variety and $\bar{W} = \bar{V}_1 \cup \ldots \cup \bar{V}_k$, with $\bar{W}, \bar{V}_1, \ldots, \bar{V}_k$ denoting the topological closure of $W, V_1, \ldots, V_k$ respectively in $\mathbb{R}$ if $K$ is a real field and in $\mathbb{C}$, otherwise. Further, if $n_W, n_1, \ldots, n_k$ are the numbers
of connected components of $\bar{W}, \bar{V}_1, \ldots, \bar{V}_k$ respectively and $n_i < \infty$ for all $i = 1, \ldots, k$, then $n_W \leq n_1 + \ldots + n_k$. Thus, without changing the scope of the conjecture we can apply Conjecture 11.1.1 to algebraic sets instead of varieties.

This conjecture has an implication (the second Mazur’s conjecture) whose importance should be clear to a reader of this book.

11.1.3 Conjecture.

There is no Diophantine definition of $\mathbb{Z}$ over $\mathbb{Q}$.

Instead of proving this implication right away, we will first restate the first conjecture for a wider variety of objects and consider this implication in an extended setting.

11.2 A Ring Version of Mazur’s Conjecture.

11.2.1 Notation.

- For a number field $K$, let $\mathcal{P}(K)$ denote the set of all finite primes of $K$.
- Let $V \subset \mathbb{C}^n$ be an algebraic set defined over a field $K$. Let $A \subseteq K$. Then let $V(A) = \{\bar{x} = (x_1, \ldots, x_n) \in V \cap A^n\}$.

11.2.2 Question

Let $K$ be a number field and let $\mathcal{W}_K$ be a set of primes of $K$. Let $V$ be any affine algebraic set defined over $K$. Let $\overline{V(O_K, \mathcal{W}_K)}$ be the topological closure of $V(O_K, \mathcal{W}_K)$ in $\mathbb{R}$ if $K \subset \mathbb{R}$ or in $\mathbb{C}$, otherwise. Then how many connected components does $\overline{V(O_K, \mathcal{W}_K)}$ have?

We start with the following simple observations.

11.2.3 Proposition.

Let $T_1, T_2$ be topological spaces. Consider $T = T_1 \times T_2$ under the product topology. Let $\pi : T \rightarrow T_1$ be a projection. Let $S \subset T$ be such that the topological closure $\overline{\pi(S)}$ of $\pi(S)$, has infinitely many components. Then the topological closure $\overline{S}$ of $S$ has infinitely many components.
Proof.

First of all, observe that \( \pi(\bar{S}) \subseteq \pi^{-1}(\pi(S)) \), since a projection maps limit points to limit points. Thus, \( \bar{S} \subseteq \pi^{-1}(\pi(S)) \). By assumption \( \pi(S) = \bigcup_{i \in I} C_i \), where \( I \) is infinite and \( C_i \) are closed and pairwise disjoint. Further, infinitely many \( C_i \)'s will have points of \( \pi(S) \). Indeed suppose not. Let \( C_1, \ldots, C_l \) be all the \( C_i \)'s containing points of \( \pi(S) \). Let \( a \in C_i \). Then \( a \notin \pi(S) \subseteq C_1 \cup \ldots \cup C_l \). Let \( a \notin \pi(S) \subseteq C_1 \cup \ldots \cup C_l \), but every neighborhood of \( a \) has a point of \( C_i \) for some \( i = 1, \ldots, l \). Therefore, for some \( i = 1, \ldots, l \), we have that \( a \) is a limit point of \( C_i \). Indeed suppose not. Then for each \( i \), there is a neighborhood of \( a \), where \( C_i \) has no points. The intersection of all such neighborhoods is a neighborhood where \( C_1 \cup C_2 \cup \ldots \cup C_l \) has no points, and we have a contradiction. Since \( C_i \)'s are are closed, \( a \in C_i \) for some \( i = 1, \ldots, l \). Thus we have a contradiction. Consequently, \( \bar{S} = \bigcup_{i \in I} (\bar{S} \cap \pi^{-1}(C_i)) \), where infinitely many elements of the union are non-empty and all elements are closed. Hence, \( \bar{S} \) is a union of infinitely many pairwise disjoint closed sets.

From this observation we immediately derive several easy but useful corollaries concerning connected components.

11.2.4 Corollary.

Suppose that for some ring \( R \) contained in a number field, for some affine algebraic set \( V \) defined over the fraction field of \( R \), we have that \( V(\bar{R}) \) has infinitely many connected components. Assume also that \( R \) has a Diophantine definition over a ring \( \bar{R} \supset R \), where the fraction field of \( \bar{R} \) is a number field \( K \). Then for some affine algebraic set \( W \) defined over \( K \), we have that \( W(\bar{R}) \) has infinitely many connected components.

Proof.

Let \( V \) be an algebraic set as described in the statement of the proposition with infinitely many components of \( \bar{V}(R) \). Let \( g(t, \bar{y}) \) be a Diophantine definition of \( R \) over \( \bar{R} \). Let \( \{ f_i(\bar{x}), \bar{x} = (x_1, \ldots, x_n), i = 1, \ldots, m \} \) be polynomials defining \( V \). Then consider the following system.

\[
\begin{align*}
g(x_i, \bar{y}_i) &= 0, i = 1, \ldots, n \\
f_i(\bar{x}) &= 0, j = 1, \ldots, m
\end{align*}
\]  

(11.2.1)

Let \( W \) be the algebraic set defined by this system in \( K \). Note that projection of \( W(\bar{R}) \) on \( \bar{x} \)-coordinates is precisely \( V(\bar{R}) \) and therefore the topological closure of \( W(\bar{R}) \) in \( \mathbb{R} \) or \( \mathbb{C} \) will have infinitely many connected components.
11.2.5 Corollary.

Let $\mathcal{W}, \mathcal{I}$ be finite sets of primes of $\mathbb{Q}$, with $\mathcal{I} = \mathcal{P}(\mathbb{Q}) \setminus \mathcal{W}$. Suppose that Conjecture 11.1.1 holds over $\mathbb{Q}$. Let $V$ be any variety defined over $\mathbb{Q}$. Then the real topological closure of $V(O_{\mathbb{Q}, \mathcal{W}})$ has finitely many connected components.

Proof.

Since by Theorem 4.2.4 we know how to define integrality at finitely many primes over number fields, $O_{\mathbb{Q}, \mathcal{W}}$ has a Diophantine definition over $\mathbb{Q}$. Therefore we can apply Corollary 11.2.4 to reach the desired conclusion.

We can specialize Corollary 11.2.4 to obtain the following proposition which will account for Mazur’s second conjecture.

11.2.6 Proposition.

Let $R$ be a subring of a number field $K$ such that for any affine algebraic set $V$ defined over $K$, the topological closure of $V(R)$ has finitely many connected components. Then no infinite discrete (in the archimedean topology) subset of $R$ has a Diophantine definition over $R$. In particular, no infinite subset of $\mathbb{Z}^n$, where $n$ is a positive integer, has a Diophantine definition over $R$.

On the other hand, using definability of integrality at finitely many primes we can obtain another easy consequence of Corollary 11.2.4 and Proposition 11.2.6.

11.2.7 Corollary.

Let $\mathcal{I}$ be defined as in Corollary 11.2.5. Then there exists an affine algebraic set $U$ such that the real closure of $U(O_{\mathbb{Q}, \mathcal{I}})$ will have infinitely many components.

Proof.

By Theorem 4.2.4, $\mathbb{Z}$ has a Diophantine definition over $O_{\mathbb{Q}, \mathcal{I}}$. Therefore we can apply Proposition 11.2.6 to reach the desired conclusion.

Thus if we allow finitely many primes in the denominator, in the closure, we will have algebraic sets over the resulting ring with infinitely many connected
components. Similarly, if Conjecture 11.1.1 is true and we remove a finite number of primes from the denominator, all the varieties over the resulting rings will have finitely many components only, in the closure. The natural question is then how many primes we can remove from the denominator before we see algebraic sets with infinitely many components in the topological closure over the resulting rings. We will answer this question partially in this chapter. A more comprehensive answer will be provided in the chapter on Poonen’s results.

11.3 First Counterexamples.

In this section we will describe some counterexamples to the ring version of Mazur’s conjecture using norm equations. First we state a lemma whose proof follows from Part (5) of Proposition 6.2.1.

11.3.1 Lemma.

Let $K$ be a number field. Let $\mathcal{W}_K \subset \mathcal{P}(K)$ be such that for some finite extension $M$ of $K$ all the primes of $\mathcal{W}_K$ remain prime in the extension $M/K$. Let $\mathcal{W}_M$ be the set of all the $M$-primes above the primes of $\mathcal{W}_K$. Then all the solutions $x \in O_{M,\mathcal{W}_M}$ to the equation

$$N_{M/K}(x) = 1 \quad (11.3.1)$$

are integral units.

Equipped with the lemma above, we can now produce an equation with an infinite set of integer solutions over a “large” subring of $\mathbb{Q}$.

11.3.2 Lemma.

Let $M$ be any finite extension of $\mathbb{Q}$ of degree $n > 2$. Let $\mathcal{W}_Q \subset \mathcal{P}(\mathbb{Q})$ be a set of $\mathbb{Q}$-primes not splitting in the extension $M/\mathbb{Q}$. Let $\{\omega_1, \ldots, \omega_n\} \subset O_M$ be an integral basis of $M$ over $\mathbb{Q}$. Let $\{\omega_{i,j}, j = 1, \ldots, n\}, \omega_{i,1} = \omega_i$ be all the conjugates of $\omega_i$ over $\mathbb{Q}$. Then all the solutions $(a_1, \ldots, a_n) \in O_{\mathbb{Q},\mathcal{W}_Q}$ to the equation in (11.3.2)

$$\prod_{j=1}^{n} \sum_{i=1}^{n} a_i \omega_{i,j} = 1 \quad (11.3.2)$$

are actually in $\mathbb{Z}$. Furthermore the set of these solutions is infinite.
Proof. 

Let $\mathcal{W}_M$ contain all the $M$-primes lying above primes of $\mathcal{W}_Q$. Then $x = \sum_{i=1}^{n} a_i \omega_i \in O_{M,\mathcal{W}_M}$. Further the set $\{x_i = \sum_{i=0}^{n} a_{i,j}, j = 1, \ldots, n\}$ contains all the conjugates of $x = x_1$ over $Q$. Thus, the equation in (11.3.2) is equivalent to the equation in (11.3.1), with $K = Q$. Therefore, if $x = \sum_{i=1}^{n} a_i \omega_i$ is a solution to the equation in (11.3.2) then $x$ is an integral unit of $M$. Since $\{\omega_1, \ldots, \omega_n\}$ is an integral basis, we must conclude that $a_i \in \mathbb{Z}$.

Conversely, if $x = \sum_{i=0}^{n} a_i \omega_i$ is a square of any integral unit of $M$, then $(a_1, \ldots, a_n)$ are solutions to this equation. Since we assumed the degree of the extension to be greater than 2, we can conclude that by Dirichlet Unit Theorem (see [37], Chapter I, Section 11, Theorem 11.19), the unit group of $M$ is of rank at least 1 and the solution set of the equation in (11.3.2) is infinite in $\mathbb{Z}^n$.

We can now state our first counterexample for a subring of $\mathbb{Q}$.

11.3.3 Proposition.

For any $\epsilon > 0$ there exists a set of rational primes $\mathcal{W}_Q$ such that Dirichlet density of $\mathcal{W}_Q$ is greater than $1 - \epsilon$ and there exists a variety $V$ defined over $\mathbb{Q}$ such that the topological closure of $V(O_{Q,\mathcal{W}_Q})$ in $\mathbb{R}$ has infinitely many connected components.

Proof.

It is enough to take $M$ to be a cyclic extension of prime degree greater than $\epsilon^{-1}$. Then by Lemma B.5.2 the set of primes splitting in the extension $M/Q$ has density less than $\epsilon$ and we can apply Corollary 11.3.2 and Proposition 11.2.6.

We will now prove analogous results for totally real number fields and their totally complex extensions of degree 2 using what we know about vertical Diophantine definability for these extensions.

11.3.4 Theorem.

Let $K$ be a totally real field or a totally complex extension of degree 2 of a totally real field. Then for any $\epsilon > 0$ there exists a set of primes $\mathcal{W}_K \subset \mathcal{P}(K)$ such that Dirichlet density of $\mathcal{W}_K$ is greater $1 - \epsilon$ and there exists an
affine algebraic set $V$ defined over $K$ such that $\overline{V(O_K,,W_K)}$ has infinitely many connected components.

**Proof.**

Since we have dealt with the case of $K = \mathbb{Q}$ already, we can assume that $K$ is a non-trivial extension of $\mathbb{Q}$. We consider the case of totally real fields first. First let $E, K_G$ be as described in Corollary 7.6.3 with the additional assumption that 

$$\frac{1}{p} > \varepsilon^{-1}$$

and $W_K$ contains all the primes of $K$ not splitting in the extension $E/K$. Observe that under this assumption, by Lemma B.5.2, the density of the set of all $K$ primes not splitting in the extension $E/K$ is greater than $1 - \varepsilon$. Adding finitely many primes to $W_K$ to form $\bar{W}_K$ as in Corollary 7.6.3, will not change the density. Let $W_Q$ be the set of all the rational primes below the primes of $W_K$ such that for every $q \in W_Q$, we have that $W_K$ contains all the factors of $q$ in $K$, and note that due to our assumption on $p$, by Lemmas B.4.7 and B.4.8, primes of $W_Q$ do not split in the extension $E/\mathbb{Q}$. Note also that $O_K, W_K \cap \mathbb{Q} = O_Q, W_Q$.

Now let $\bar{W}_Q$ be the set of all the rational primes below the primes of $W_K$ such that for every $q \in \bar{W}_Q$, we have that $W_K$ contains all the factors of $q$ in $K$. Again we observe that $\mathbb{Q} \cap O_K, W_K = O_Q, W_Q$. By construction, $\bar{W}_Q$ can differ from $W_Q$ by finitely many primes only. Therefore, we claim that the following statements are true by Corollary 7.6.3, definability of integrality at finitely many primes and transitivity of Dioph-generation:

$$O_Q, W_Q \leq_{\text{Dioph}} O_K, W_K,$$

$$O_Q, W_Q \leq_{\text{Dioph}} O_Q, \bar{W}_Q,$$

$$O_Q, W_Q \leq_{\text{Dioph}} O_K, \bar{W}_K.$$

On the other hand, by Corollary 7.5.4, there exists an infinite set of rational integers Diophantine over $O_Q, W_Q$ and thus over $O_K, W_K$.

The case of $K$ being a totally complex extension of degree 2 of a totally real field is handled in a similar manner using Theorem 7.8.7.

We now turn out attention to extensions with one pair of non-real conjugate embeddings. There we do not have results analogous to Corollary 7.6.3 and Theorem 7.8.7, but we do know that rational integers have a Diophantine definition over the rings of integers of these fields (see Section 7.2). We
will use an approach utilized in the above cited result to prove the following theorem.

11.3.5 Theorem.

Let \( K \) be a non-real number field with exactly one pair of non-real conjugate embeddings. Then there exists a set \( \mathcal{W}_K \subset \mathcal{P}(K) \) such that the Dirichlet density of \( \mathcal{W}_K \) is \( 1/2 \) and for some affine variety \( V \) defined over \( K \) we have that \( V(O_K,\mathcal{W}_K) \) has infinitely many connected components.

Proof.

Let \( a \in O_K \) be as described in Notation 6.3.3 for the case of \( K \) with exactly one pair of conjugate non-real embeddings. Let \( M = K(\sqrt{a^2 - 1}) \) be a totally complex extension of degree 2 of \( K \). Note that the density of the set of \( K \)-primes not splitting in the extension \( M/K \) is exactly \( 1/2 \) by Lemma B.5.2. So let \( \mathcal{W}_K \subset \mathcal{P}(K) \) be the set of primes not splitting in the extension \( M/K \). Let \( \mathcal{W}_M \) be the set of \( M \)-primes above the primes of \( W_K \) and observe that by Proposition 11.3.1 all the solutions to \( N_{M/K}(z) = 1 \) in \( O_{M,\mathcal{W}_M} \) are algebraic integers. However in this case we can say a little bit more. By Lemma 6.3.5, we know that solutions to this norm equation form a multiplicative group of rank 1 and modulo roots of unity are powers of \( \mu = a - \sqrt{a^2 - 1} \). Note that either \( \mu \) or \( \mu^{-1} \) is of absolute value greater than 1 by Lemma 6.3.4.

Assume without loss of generality that \( |\mu| > 1 \) and let \( \mu^{r^k} = x_k - \sqrt{a^2 - 1}y_k \) for some sufficiently large \( r \) such that \( |\mu^{r^k}| > 2^k \). Then \( |x_k| = |\frac{\mu^{r^k} + \mu^{-r^k}}{2}| > 2^k \). Therefore, for any \( l \in \mathbb{N} \), any neighborhood \( U \) of \( x_l \), there exist only finitely many \( m \in \mathbb{N} \) such that \( x_m \in U \). In other words, the set

\[
\{ x \in O_K, \mathcal{W}_K | \exists x_0, y_0, y \in O_K, W_K, x - \sqrt{a^2 - 1}y = (x_0 - \sqrt{a^2 - 1}y_0)' , x_0^2 - (a^2 - 1)y_0^2 = 1 \}
\]

is discrete and the assertion of the theorem follows from Corollary 11.2.6.

11.4 Consequences for Diophantine Models.

As we have seen in the first section of this chapter, the truth of the first Mazur’s conjecture implies that there is no Diophantine definition of \( \mathbb{Z} \) over \( \mathbb{Q} \). However, we know that Diophantine definitions are only one type of elements in a large class of objects called Diophantine models. From Corollary 3.4.6 we also know that it would be enough to show that \( \mathbb{Q} \) has a Diophantine
model of \( \mathbb{Z} \) to assert Diophantine undecidability of \( \mathbb{Q} \). Therefore, we would like to know if the above mentioned Mazur’s conjecture precludes existence of a Diophantine model of \( \mathbb{Q} \) over \( \mathbb{Z} \). Cornelissen and Zahidi showed that this was indeed the case in [8] using a more restrictive definition of a Diophantine model. Under their assumptions the image of a Diophantine set was a Diophantine set in the target ring. We can call this kind of Diophantine models tight. We reproduce below a slightly generalized version of their proof.

11.4.1 Proposition.

Let \( K \) be a number field, let \( \mathcal{W}_K \) be a computable set of primes of \( K \) and assume that for any affine algebraic set \( V \) defined over \( K \) we have that \( V(O_K, \mathcal{W}_K) \) has finitely many connected components. Then \( O_K, \mathcal{W}_K \) does not have a tight Diophantine model of \( \mathbb{Z} \). (We remind the reader that a definition of a computable set of primes can be found in Section A.8.)

Proof.

Let \( P(x_1, \ldots, x_k, t_1, \ldots, t_m) \) be a Diophantine definition of a set \( D = \phi(\mathbb{Z}) \) over \( (O_K, \mathcal{W}_K)^k \). Let

\[
V = \{(x_1, \ldots, x_k, t_1, \ldots, t_m) \in O_K^{k+m} : P(x_1, \ldots, x_k, t_1, \ldots, t_m) = 0\}
\]

and consider the map

\[
f : V(O_K, \mathcal{W}_K) \to (O_K, \mathcal{W}_K)^k
\]

implemented by projection on the first \( k \) coordinates. Note that \( f(V) = D \).

By assumption and by Proposition 11.2.3 we have that \( \bar{D} \), the closure of \( D \) in \( \mathbb{R} \) if \( K \) is a real field, or \( \mathbb{C} \), otherwise, will have finitely many connected components. Since \( \phi(\mathbb{Z}) = D \) has infinitely many points, for at least one connected component \( C \) of \( \bar{D} \), it is the case that \( C \cap \phi(\mathbb{Z}) \) must have more than one point, and projection of \( C \) onto one of the coordinates if \( K \) is real, or on the imaginary or real part of one of the coordinates, if \( K \) is not real, will contain a non-trivial interval whose end points are rational numbers. (This is so because the only connected subsets of the real line containing more than one point are intervals.) Let \( a \) be the left endpoint of this interval and let \( l \) be its length. Let \( d_n = s \circ \phi(n) \), where \( s \) is either the projection on the coordinate described above, or the real part or the imaginary part of the projection, as necessary, and let

\[
\tilde{Z} = \{n \in \mathbb{Z} | a + \frac{l}{2j+1} \leq d_n \leq a + \frac{l}{2j}, j \in \mathbb{Z}_{>0}\}.
\]

208
Since \( \phi \) is computable, and by Proposition A.8.8 we can compute effectively decimal expansions for real and (if necessary) imaginary parts of all the elements of \( K \), we conclude that \( \tilde{Z} \) is recursively enumerable and therefore \( \tilde{Z} \) is a Diophantine subset of \( \mathbb{Z} \) by the result of Matiyasevich, Robinson, Davis and Putnam. Further, \( s(\phi(\mathbb{Z})) \cap [a, a + l] \) is dense in \( [a, a + l] \). Indeed, \( [a, a + l] \subseteq s(C) \subset s(\phi(\mathbb{Z})) = s(\bar{D}) \). Since \( D \) is dense in \( \bar{D} \) and projection maps dense subsets into dense subsets, our claim is true. Thus, any interval \([a + \frac{l}{2j+1}, a + \frac{l}{2j}]\) will have infinitely many points from \( s(D) \) and therefore elements \( d_n \), with \( n \in \tilde{Z} \) by definition of \( \tilde{Z} \). Let \( \tilde{D} = \{ \phi(n) | n \in \tilde{Z} \} \). Then \( \tilde{D} \) has a Diophantine definition over \((O_K)^k\) as the \( \phi \)-image of a Diophantine subset of \( \mathbb{Z} \). Let \( \tilde{P}(x_1, \ldots, x_k, t_1, \ldots, t_m) \) be a Diophantine definition of \( \tilde{D} = \phi(\tilde{Z}) \), and let \( \tilde{V} \) be the algebraic set defined by \( \tilde{P}(x_1, \ldots, x_k, t_1, \ldots, t_m) = 0 \). Then \( s \circ f \), the projection from \( \tilde{V} \) on the first \( k \) coordinates combined with projection onto a real or imaginary part of a coordinate chosen as above will produce a projection of \( \tilde{V} \) onto set whose closure has infinitely many components. Thus, \( \tilde{V} \) will have to have infinitely many components in contradiction of our assumptions for this proposition.
Chapter 12

Results of Poonen.

Poonen’s Theorem is arguably the most important development in the subject since Matiyasevich completed the proof of the original HTP in the late sixties. One could say that for the first time the solution of HTP for $\mathbb{Q}$ has become visible over the distant horizon, though we still have to traverse an “infinite” distance, as will be explained below.

The result came out of the attempts to falsify the ring version of Mazur’s conjecture (Conjecture 11.1.1) for a ring of rational $\mathcal{S}$-integers where $\mathcal{S}$ had natural density equal to 1. In the process of constructing a counterexample to the conjecture, Poonen constructed a (tight) Diophantine model of $\mathbb{Z}$ over such a ring. Thus, this result has moved us “infinitely” far away from where we started ($\mathbb{Z}$ and rings of rational $\mathcal{S}$-integers with finite $\mathcal{S}$), but since the set of allowed denominators in Poonen’s Theorem still misses an infinite set of primes (though of natural density 0), we still have “infinitely” far to go.

In this chapter we will go over Poonen’s proof, which appeared originally in [74], in some detail. We will start with the overall plan and then will try to sort out the rather challenging technical details.

12.1 A Statement of the Main Theorem and an Overview of the Proof.

A good place to start is a precise statement of the theorem which is presented below.

12.1.1 Theorem.

There exist recursive sets of rational primes $\mathcal{R}_1$ and $\mathcal{R}_2$, both of natural density zero and with an empty intersection, such that for any set $\mathcal{S}$ of rational primes
containing \( \mathcal{T}_1 \) and avoiding \( \mathcal{T}_2 \), the following hold:

1. There exists an affine curve \( E \) over \( \mathbb{Q} \) such that the topological closure of \( E(\mathbb{Q}) \) in \( E(\mathbb{R}) \) is an infinite discrete set.

2. \( \mathbb{Z} \) has a (tight) Diophantine model over \( \mathbb{Q} \).

3. Hilbert's Tenth Problem is undecidable over \( \mathbb{Q} \). (Computability of \( \mathcal{T}_2 \) implies that \( \mathcal{S} = \mathcal{P}(\mathbb{Q}) \setminus \mathcal{T}_2 \) is computable, and therefore by Proposition A.8.6 we have that \( \mathbb{Q} \) is computable. Thus over such a ring it makes sense to talk about undecidability of HTP.)

The proof of the theorem will rely on the existence of an elliptic curve \( E \) defined over \( \mathbb{Q} \) such that the following conditions are satisfied.

1. \( E(\mathbb{Q}) \) is of rank 1.

2. \( E(\mathbb{R}) \cong \mathbb{R}/\mathbb{Z} \) as topological groups.

3. \( E \) does not have complex multiplication.

(An example of such a curve is given in Proposition B.6.2.)

Denote an infinite order point of \( E(\mathbb{Q}) \) by \( P \). For a non-zero integer \( n \), let \( (x_n(P), y_n(P)) \) be the affine coordinates of \( [n]P \) given by a (from now on fixed) Weierstrass equation of \( E \) of the form \( y^2 = x^3 + a_2 x^2 + a_4 x + a_6 \) (see Chapter III, Section 1 of [113]), where \( [n] \) denotes the \( n \)-th multiple of \( P \) under the addition on \( E \). We note for future reference, that given this form of Weierstrass equation, for a non-zero point \( Q \in E \) with affine coordinates \((x, y)\), we have that \((x, -y)\) are the affine coordinates of \(-Q\). (See Chapter III, Section 2 of [113] for more details on group law.)

The proof of the theorem will consist of the following steps.

1. Show that there exists a computable sequence of rational primes \( l_1 < \ldots < l_n < \ldots \) such that \([l_j]P = (x_{l_j}, y_{l_j})\) and for all \( j \in \mathbb{N} \), we have that \( |y_{l_j} - j| < 10^{-j} \).

2. Prove the existence of infinite sets \( \mathcal{T}_1 \) and \( \mathcal{T}_2 \), as described in the statement of the theorem, such that for any set \( \mathcal{S} \) of rational primes containing \( \mathcal{T}_1 \) and disjoint from \( \mathcal{T}_2 \), we have that \( E(\mathcal{S}) = \{[l_j]P\} \cup \{ \text{ finite set } \} \).

3. Note that \( \{y_{l_j}\} \) is an infinite discrete set and thus is a counterexample to Mazur's conjecture for the ring \( \mathbb{Q} \).
4. Show that \( \{y_j\} \) is a (tight) Diophantine model of \( \mathbb{Z} \) over \( \mathbb{Q} \).

To carry out the steps outlined above, and, especially, to show that the sets \( \mathscr{T}_1 \) and \( \mathscr{T}_2 \) have the required densities, we will have to use a fair amount of material concerning elliptic curves. We tried to separate out the properties of general nature (which can be found in the Number Theory Appendix, Section B.6) and properties more or less unique to the situation at hand (which are discussed in this chapter). We will use notation from Section B.6: Notation B.6.1 with \( \mathbb{Q} \) replacing an arbitrary number field \( K \). We will also use additional notation described below.

An attentive reader will note that the statement of the theorem refers to the natural density of the prime sets. The density we have used so far was the Dirichlet density. For the definition of the natural density and its relation to the Dirichlet density, we refer the reader to Definition B.5.9 and Proposition B.5.10.

Finally, before taking the plunge, we remind the reader that everything we need to know about elliptic curves (and much, much more, of course) can be found in [113] and [114].

### 12.1.2 Notation.

- For each prime number \( l \), let \( a_l(P) \) be the smallest positive integer such that \( \mathscr{I}_{a_l(P)}(P) \setminus \mathscr{I}_1(P) \neq \emptyset \). Such an \( a_l(P) \) exists for every \( l \) and is equal to 1 for all but finitely many \( l \)’s by Siegel’s Theorem since \( \mathscr{I}_0(\mathbb{Q}) \cup \mathscr{I}_1(P) \) is a finite set. ("\( \mathscr{I}_l(P) \)" and "\( \mathscr{I}_0(\mathbb{Q}) \)" are defined in Notation B.6.1.)

- Let \( \mathcal{L}(P) = \{ l \in \mathcal{P}(K) : a_l(P) > 1 \} \).

- Let \( p_l(P) = \max \mathscr{I}_l(P) \setminus \mathscr{I}_1(P) \).

- For rational prime numbers \( l, p \), let \( p_{lp} = \max(\mathscr{I}_{lp} \setminus (\mathscr{I}_l \cup \mathscr{I}_p)) \), if the set difference is not empty. By Proposition 12.2.2 for sufficiently large \( \max(l, p) \), the set difference will be non-empty.

- Let

\[
\mu_l(P) = \sup_{X \in \mathbb{Z}, X \geq 2} \frac{\# \{ p \in \mathscr{I}_l(P) : p \leq X \}}{\# \{ p \in \mathcal{P}(\mathbb{Q}) : p \leq X \}}.
\]

- For \( X \in \mathbb{R} \) let \( \pi_\mathbb{Q}(X) = \# \{ p \in \mathcal{P}(\mathbb{Q}) : p \leq X \} \).

By the denominators of points we mean the denominators of the affine coordinates of non-zero multiples of $P$ under our fixed Weierstrass equation, where the numerator and the denominator of the coordinates are relatively prime. We should note here that since the affine Weierstrass equation is monic in $x$ and $y$, the set of primes which occur in the denominator of $x$ is the same as the set of primes occurring in the denominator of $y$. The goal is to understand what primes to ban from denominators to eliminate the "extraneous" points from the solution set in the constructed ring.

The primes are divided into sets $\mathcal{I}_i$ we already mentioned above. One can think of $\mathcal{I}_0$ as a set of generally inconvenient primes such as primes where $E$ does not have a good reduction, and $\mathcal{I}_i(P)$, for $i > 0$ can be thought of as a set of the "relevant" primes appearing in the denominator of $[\pm i]P$.

The first proposition below deals with the primes two different point denominators can have in common.

12.2.1 Proposition.

For any $m, n \in \mathbb{Z} \setminus \{0\}$, we have that $\mathcal{I}_m(P) \cap \mathcal{I}_n(P) = \mathcal{I}_{(m,n)}(P)$, where $(m, n)$ is the GCD of $m$ and $n$.

Proof.

Let $q \in \mathcal{I}_m(P) \cap \mathcal{I}_n(P)$. Then

$$\{m, n\} \subseteq \mathcal{I}_l = \{\text{non-zero } l \in \mathbb{Z} : q \mid b_l(P)\} \cup \{0\},$$

a subgroup of $\mathbb{Z}$ by Corollary B.6.5. Thus, $(m, n) \in \mathcal{I}_l$ or in other words $q \in \mathcal{I}_{(m,n)}$. Hence $(\mathcal{I}_m \cap \mathcal{I}_n) \subseteq \mathcal{I}_{(m,n)}$. On the other hand, by Corollary B.6.7, we have that $\mathcal{I}_{(m,n)} \subseteq \mathcal{I}_m \cap \mathcal{I}_n$. Thus, the proposition holds.

The next proposition shows when we can expect new primes to appear in a point denominator.

12.2.2 Proposition.

If $l, m \in \mathcal{P}(\mathbb{Q})$, then for sufficiently large $\max(l, m)$ we have that $\mathcal{I}_m \setminus (\mathcal{I}_l \cup \mathcal{I}_m) \neq \emptyset$. 

213
Proof.

First of all we note that without loss of generality we can assume that \( l \geq 2, m \geq 2 \). Next suppose \( \mathcal{S}_{lm} \setminus (\mathcal{S}_l \cup \mathcal{S}_m) = \emptyset \). We want to evaluate \( \text{ord}_q d_{lm} \) for \( q \in \mathcal{S}_l \cup \mathcal{S}_m = \mathcal{S}_{lm} \). ("\( d_{lm} \)" is defined in Notation B.6.1.) Without loss of generality assume that \( q \in \mathcal{S}_l \). Then by Proposition B.6.6 we have that \( \text{ord}_q d_{lm} = \text{ord}_q d_l \) if \( q \nmid m \) and \( \text{ord}_q d_{lm} = \text{ord}_q d_l + 2 \) if \( q \mid m \). Thus, \( d_{lm} \mid d_l m^2 \) and by Lemma B.6.9 it follows that

\[
h_0(d_{lm}) \leq h_0(d_l) + h_0(d_m) + 2l + 2m. \tag{12.2.1}
\]

("\( h_0 \)" is defined in Notation B.6.1 also.)

Together, Lemma B.6.8 and (12.2.1) imply that for some positive constant \( c \) we have that

\[
h_0(d_{lm}) = (c - o(1))l^2 m^2, h_0(d_l) = (c - o(1))l^2, h_0(d_m) = (c - o(1))m^2. \tag{12.2.2}
\]

Given \( \varepsilon > 0 \), let \( C(\varepsilon) \) be such that for any \( n > C(\varepsilon) \), it is the case that \( h(d_n) = (c - o(1))n^2 \) with \( |o(1)| < \varepsilon \). Also let \( C \in \mathbb{R} \) be such that \( h(d_n) < Cn^2 \) for all \( n \in \mathbb{N} \setminus \{0\} \). Choose \( \varepsilon \) small enough so that \( c > 3\varepsilon \).

Next consider two cases: \( m > C(\varepsilon) \) and \( m < C(\varepsilon) \). In the first case choose \( l > C(\varepsilon) \) and large enough so that

\[
c > 3\varepsilon + \frac{4}{l}.
\]

Then our assumptions and (12.2.2) imply

\[
(c - o(1))l^2 m^2 \leq (c - o(1))l^2 + (c - o(1))m^2 + 2l + 2m,
\]

and

\[
(c - \varepsilon)l^2 m^2 \leq (c + \varepsilon)l^2 + (c + \varepsilon)m^2 + 2l + 2m,
\]

which after division by \( l^2 m^2 \) becomes

\[
(c - \varepsilon) \leq (c + \varepsilon)m^{-2} + (c + \varepsilon)l^{-2} + \frac{2}{lm^2} + \frac{2}{l^2 m} < \frac{c + \varepsilon}{2} + \frac{2}{l}
\]

contradicting the choice of \( l \) and \( m \).

Suppose now that \( m < C(\varepsilon) \). Now choose \( l > C(\varepsilon) \) and large enough so that

\[
l > \frac{CC(\varepsilon)^2 + 2C(\varepsilon) + 2}{(3c - 5\varepsilon)}
\]

214
Now (12.2.1), (12.2.2) and our assumptions imply

\[ 4(c - \epsilon)^2 \leq (c + \epsilon)^2 + CC(\epsilon)^2 + 2C(\epsilon) + 2l, \]

\[ (3c - 5\epsilon)l \leq CC(\epsilon)^2 + 2C(\epsilon) + 2, \]

and we have a contradiction with our choice of \( l \).

12.2.3 Remark.

The denominators of the affine coordinates of the points of \( E \) form what is called an “elliptic divisibility sequence”, and the properties listed above are characteristic for such sequences. For more information on such sequences we refer the reader to [31].


In this section we will discuss probably the most difficult part of the proof – the part which will be crucial in showing that \( \mathscr{S}_2 \) can have natural density zero. As we have observed from the section above, except possibly for finitely many primes \( l \), it is the case that \( \mathscr{S}_l \) contains a prime which is not in any \( \mathscr{S}_q \) with \( q \) prime and \( q \neq l \). Further, from Proposition 12.2.1 we know that \( \mathscr{S}_l \subset \mathscr{S}_{kl} \) for any \( k \in \mathbb{Z} \setminus \{0\} \). Thus, if we banned a prime unique to \( \mathscr{S}_l \) from the denominators of the points in our ring, we will eliminate all the multiples of \( \mid l \mid P \) from the solution set over the ring. Therefore, it is important to know what the density of the set of the largest “unique to \( \mathscr{S}_l \)” primes is. Our first task is to establish a relationship between a prime \( p_l \in \mathscr{S}_l \setminus \mathscr{S}_1 \) and a prime \( l \). Our hope is that \( p_l \) is going to be “on the average” large compared to \( l \). (This will help with making density of \( p_l \)’s small.) We start with the following observation.

12.3.1 Lemma.

Let \( l \in \mathscr{P}(\mathbb{Q}) \) and suppose \( p \in \mathscr{S}_{p_l(p)}(P) \setminus \mathscr{S}_1(P) \). Then \( \mid l \mid \# E(\mathbb{F}_p) \).

Proof.

If \( p \in \mathscr{S}_{p_l(p)}(P) \setminus \mathscr{S}_1(P) \), then \( p \) does not divide the discriminant of our Weierstrass equation, \( E \) has a good reduction at \( p \) (and thus \( \tilde{E} \) is non-singular) with all the coefficients of our chosen affine Weierstrass equation integral
at \( p \). Further, \( x_1(P) \), \( y_1(P) \) are integral at \( p \), while \( \text{ord}_p x_1([l^a(P)]P) < 0 \), \( \text{ord}_p y_1([l^a(P)]P) < 0 \). Therefore, under reduction mod \( p \), the image of \( P \) is not \( \bar{O} - \) the image of \( O \), while \([l^d]\bar{P} = \bar{O} \). By definition of \( a_1(P) \), we must conclude that \( E(\mathbb{F}_p) \) has an element of order \([l^a(P)] \) and therefore \( l | \#E(\mathbb{F}_p) \).

The lemma provides us with some information about the relationship of \( l \) and \( p_i \), but to estimate the density of the set of \( p_i \)'s we need more. From a theorem of Hasse we know that \( \#E(\mathbb{F}_p) \leq Cp \), where \( C \) is a constant independent of \( p \) (see [113], Chapter V, Section 1, Theorem 1.1). Thus we could hope that “on the average” \( \#E(\mathbb{F}_p) \) has a lot of small factors, and therefore \( l \) is “much” smaller than \( \#E(\mathbb{F}_p) \). The next two proposition will show just that. They are based on two results: the natural density version of the Chebotarev Density Theorem (Theorem 1 of \cite{113}) and on the relationship between the action of the Galois group and the automorphism groups of torsion elements of the curve (Proposition B.6.14). The first of these propositions relates \( E(\mathbb{F}_p) \) having a point of order \( l \) and the action of Frobenius automorphism of \( p \).

### 12.3.2 Proposition.

Let \( p \neq l \) be rational prime numbers. Let \( \mathbb{F}_p \) be a field of \( p \) elements. Let \( M \) be a Galois extension of \( \mathbb{Q} \) containing all the elements of \( E(\bar{\mathbb{Q}})[l] \), where \( \bar{\mathbb{Q}} \) is the algebraic closure of \( \mathbb{Q} \). Let \( G(M/\mathbb{Q}) \) be the Galois group of \( M \) over \( \mathbb{Q} \). Assume \( p \notin \mathcal{S}_0(M)(\mathbb{Q}) \) (see Notation B.6.1). Then \( E(\mathbb{F}_p) \) has an element of order \( l \) if and only if for some \( \sigma \in \text{Gal}(M/\mathbb{Q}) \) and some \( Q \in E(\bar{\mathbb{Q}})[l] \setminus \{O\} \), we have that \( \sigma(Q) = Q \) and \( \sigma \) is the Frobenius automorphism for some factor of \( p \) in \( M \).

**Proof.**

Let \( p_M \) be a factor of \( p \) in \( M \) and let \( \mathbb{F}_{p_M} \) be the residue field of \( p_M \). Let \( \bar{\sigma} \) be the Frobenius automorphism of \( \mathbb{F}_p \), i.e. \( \bar{\sigma}(x) = x^p \) for all \( x \in \mathbb{F}_p \). Then for any point \( \bar{Q} \in E(\mathbb{F}_{p_M}) \) of order \( l \), we have that \( \bar{\sigma}(\bar{Q}) = \bar{Q} \) if and only if \( \bar{Q} \in E(\mathbb{F}_p) \). On the other hand, let \( Q \in E(M) \setminus \{O\} \) be of order \( l \) with

\[
\sigma(Q) \neq Q, \tag{12.3.1}
\]

where \( \sigma \) is the Frobenius automorphism of \( p_M \) over \( \mathbb{Q} \). If we reduce \((12.3.1) \mod p_M \), we will obtain \( \bar{\sigma}(\bar{Q}) \neq \bar{Q} \), by Corollary B.6.12. Further, since by Corollary B.6.12, reduction modulo \( p_M \) is an isomorphism of \( E(M)[l] \) onto \( E(\mathbb{F}_{p_M})[l] \), every \( \bar{P} \in E(\mathbb{F}_{p_M}) \) of order \( l \) is the image of an order \( l \) point in \( E(M)[l] \). Thus, \( \bar{\sigma} \) fixes an element of order \( l \) if and only if \( \sigma \) fixes an element of order \( l \) and the assertion of the proposition follows.
12.3.3 Remark.

If $l = p$ and the Frobenius automorphism of a factor of $p$ fixes some point of order $p$, then under reduction modulo a factor of $p$, the image of this point will remain fixed. However we are no longer assured of the converse. That is if a point is fixed after the reduction, we don’t know if it was fixed before the reduction.

In the next proposition we will examine directly the set of $p$’s for which $\#E(\mathbb{F}_p)$ has “few” factors.

12.3.4 Proposition.

For a prime $p \not\in \mathcal{I}_0(\mathbb{Q})$ and a positive constant $C$, define

$$A(p, C) = \{ l \in \mathcal{P}(\mathbb{Q}) \setminus \mathcal{I}(\mathbb{Q}), l | \#E(\mathbb{F}_p), l < C \},$$

$$f(p, C) = |A(p, C)|.$$

Then for any $t \geq 1$, the upper natural density of

$$\mathcal{B}(C, t) = \{ p \in \mathcal{P}(\mathbb{Q}) : f(p, C) \leq t \}$$

tends to 0 as $C \to \infty$. (See Proposition B.6.14 for definition of $\mathcal{I}(\mathbb{Q})$.)

Proof.

Fix $t, C$. Let $M$ be any Galois extension of $\mathbb{Q}$ such that $M$ contains $E(\overline{\mathbb{Q}})[l]$ for all $l \leq C$. Next consider the natural homomorphism:

$$\Lambda_{M,C} : \text{Gal}(M/\mathbb{Q}) \rightarrow \prod_{l \in \mathcal{P}(\mathbb{Q}) \setminus \mathcal{I}(\mathbb{Q}), l \leq C} \text{Aut}(E(\overline{\mathbb{Q}})[l])$$

and note that by Proposition B.6.14, this map is onto. Let $\sigma \in \text{Gal}(M/\mathbb{Q})$ and let $\Lambda_{M,C}(\sigma) = (\sigma_1, \ldots, \sigma_n)$, where $\{l_1, \ldots, l_n\}$ are all the prime numbers less than $C$ and not in $\mathcal{I}(\mathbb{Q})$. Let $\Sigma(C, t)$ denote the set

$$\{\sigma \in \text{Gal}(M/\mathbb{Q}), \Lambda_{M,C}(\sigma) \text{ has at most } t \text{ components with a fixed point } Q \neq O\}$$

We want to determine

$$R(C, t) = \frac{|\Sigma(C, t)|}{|\text{Gal}(M/\mathbb{Q})|}. \quad (12.3.2)$$
Denote \((\sigma_1, \ldots, \sigma_n) : \sigma_i \in \text{Aut}(E(\overline{\mathbb{Q}})[l])\) by \(\overline{\sigma}\). Since \(\Lambda_{M,C}\) is a surjective homomorphism, the ratio in (12.3.2) is equal to
\[
\frac{\#\{\overline{\sigma} : \text{at most } t \text{ components have a fixed point } Q \neq O\}}{\#\{\overline{\sigma}\}}.
\] (12.3.3)

The ratio in (12.3.3) in turn gives us
\[
\sum_{j=1}^{t} \frac{\#\{\overline{\sigma} : \text{exactly } j \text{ components have a fixed point } Q \neq O\}}{\#\{\overline{\sigma}\}}.
\] (12.3.4)

Given \(i, j \in \{1, \ldots, n\}\) and a \(j\)-element subset \(l_j \subseteq \{1, \ldots, n\}\), let
\[
F_{i, l_j} = \{\overline{\sigma} : \forall i \in l_j, \exists Q \in E(\overline{\mathbb{Q}})[l] \setminus \{O\}, \sigma_i(Q) = Q\}
\]
and let
\[
G_{i, l_j} = \{\overline{\sigma} : \forall i \notin l_j, \forall Q \in E(\overline{\mathbb{Q}})[l] \setminus \{O\}, \sigma_i(Q) \neq Q\}
\]
Then sum in (12.3.4) is equal to
\[
\sum_{j=1}^{t} \sum_{l_j} |F_{i, l_j} \cap G_{i, l_j}| \frac{1}{\#\{\overline{\sigma}\}}.
\] (12.3.5)

where \(l_j\) ranges over all the \(j\)-element subsets of \(\{1, \ldots, n\}\). Continuing further, we observe that the sum from (12.3.5) is equal to
\[
\sum_{j=1}^{t} \sum_{l_j} \left(\prod_{i \in l_j} \alpha_i\right) \left(\prod_{i \notin l_j} (1 - \alpha_i)\right) = \sum_{j=1}^{t} \sum_{l_j} \left(\prod_{i \in l_j} \frac{\alpha_i}{1 - \alpha_i}\right) \prod_{i=1}^{n} (1 - \alpha_i).
\] (12.3.6)

where for each \(i = 1, \ldots, n\) we have that
\[
\alpha_i = \frac{\#\{\tau \in \text{Aut}(E(\overline{\mathbb{Q}})[l]) : \exists Q \in E(\overline{\mathbb{Q}})[l] \setminus \{O\}, \tau(Q) = Q\}}{|\text{Aut}(E(\overline{\mathbb{Q}})[l])|} = \frac{1}{l_i} + o\left(\frac{1}{l_i^2}\right),
\]
by Proposition B.6.13. Now by Proposition B.10.2, if we fix \(t\) and let \(C \to \infty\) (or, alternatively, let \(n \to \infty\)), then \(R(C, t) \to 0\).

Next we observe that \(\Sigma(C, t)\) is closed under conjugation. In other words, if \(\sigma \in \Sigma(C, t)\), then all of the conjugates of \(\sigma\) in \(\text{Gal}(M/\mathbb{Q})\) are also in \(\Sigma(C, t)\), since for any point \(P \in E(M)\), and any \(\tau, \sigma \in \text{Gal}(M/\mathbb{Q})\), we have that \(\tau^{-1}\sigma\tau\left(\tau^{-1}(P)\right) = \tau^{-1}(P) \leftrightarrow \sigma(P) = P\). Thus, since the order of the point is preserved by any action of the Galois group, for any natural number \(r\), \(\Lambda_{M,C}(\sigma)\) has exactly \(r\) components with non-\(O\) fixed points if and only if the same is true of \(\Lambda(M, C)(\tau\sigma\tau^{-1})\). Therefore by the natural density version of
Chebotarev Density Theorem (see Theorem 1 of [88]), the density of primes of \( \mathbb{Q} \) whose factors have Frobenius automorphism in \( \Sigma(C, t) \) is \( R(C, t) \).

Next suppose \( p \in \mathcal{B}(C, t) \) and no factor of \( p \) is in \( \mathcal{A}_0(M) \). \( \left( \mathcal{A}_0(M), \text{ defined in Notation B.6.1, will contain all the factors of primes in } \mathcal{A}_0(\mathbb{Q}) \text{ together with primes ramifying in the extension } M/\mathbb{Q} \right) \). Then we consider two cases: \( p \mid \#E(\mathbb{F}_p) \) and \( p \nmid \#E(\mathbb{F}_p) \). In the first case, exactly \( t_0 \leq t \) primes \( l \not\in \mathcal{A}(\mathbb{Q}), l \neq p, l \leq C \) divide \( E(\mathbb{F}_p) \). Therefore by Sylow Theorem, for exactly \( t_0 \leq t \) primes \( l \not\in \mathcal{A}(\mathbb{Q}), l \neq p, l \leq C \), a Frobenius automorphism \( \sigma \) of a factor of \( p \) fixes a point of order \( l \) not equal to \( O \). Therefore, \( p \) has a factor in \( M \) with a Frobenius automorphism \( \sigma \) such that \( \Lambda_{M,C}(\sigma) \) has exactly \( t_0 \leq t \) components \( \sigma_i \) with fixed points different from \( O \). Thus, \( p \in \Sigma(C, t) \).

Similarly, if \( p \mid \#E(\mathbb{F}_p) \), we have exactly \( t_0 < t \) primes \( l \not\in \mathcal{A}(\mathbb{Q}), l \neq p, l \leq C \) divide \( E(\mathbb{F}_p) \). Since Proposition 12.3.2 does not cover the case \( l = p \) (see Remark 12.3.3), it is possible that \( p \in \Sigma(C, t - 1) \). However, since \( \Sigma(C, t - 1) \subseteq \Sigma(C, t) \), we reach the same conclusion in both cases. Thus, in any case \( p \) belongs to the set whose natural density is \( R(C, t) \).

Finally, let \( t \) be given and choose \( C \) large enough so that \( R(C, t) < \epsilon \). Note that we can do this before we choose field \( M \) by using (12.3.6). We just need to arrange that \( n \) which is the number of primes not in \( \mathcal{A}(\mathbb{Q}) \) and less than \( C \) is large enough. Then we can choose \( M \) as above and conclude that \( \mathcal{B}(C, t) \) without primes with factors in \( \mathcal{A}_0(M) \) has upper density less than \( \epsilon \).

Since \( \mathcal{A}_0(M) \) is finite, we conclude that \( \mathcal{B}(C, t) \) has upper density less than \( \epsilon \).

**12.3.5 Proposition.**

The set \( \mathcal{W}(P) = \{ p_l(P), l \in \mathcal{P}(\mathbb{Q}) \} \) has natural density 0.

**Proof.**

We will show that for every \( \epsilon > 0 \), the set \( \mathcal{W}(P) \) has upper natural density less than \( \epsilon \). So let \( \epsilon \) be given. Choose an integer \( t \) such that \( 2^{2^{-t}} < \epsilon/2 \). Choose \( C > 0 \) such that the set \( \mathcal{B}(C, t) \) (defined in Proposition 12.3.4) has the upper natural density less than \( \epsilon/2 \). Such a \( C \) exists by Proposition 12.3.4. It remains to show that the set

\[
\mathcal{W} \cap \overline{\mathcal{B}(C, t)} = \{ p_l : l \in \mathcal{P}(\mathbb{Q}) \wedge f(p_l, C) > t \}
\]

has upper natural density less or equal to \( \epsilon/2 \). Suppose \( p_l \in \overline{\mathcal{B}(C, t)} \). Then by Lemma 12.3.1 we have that \( l \mid \#E(\mathbb{F}_p) \) and \( \#E(\mathbb{F}_p) \) is divisible by at least
t other primes. Hence \(2^t l \leq \#E(\mathbb{F}_p)\). Further, by a theorem of Hasse mentioned above,

\[
\#E(\mathbb{F}_p) \leq p_l + 1 + 2\sqrt{p_l} \leq 4p_l.
\]

Thus, \(l \leq 2^{2-t}p_l \leq \epsilon p_l/2\). Consequently, for each \(p_l \in \mathcal{B}(C, t)\) there exists a distinct \(l \in \mathcal{P}(Q)\) such that \(l \leq \epsilon p_l/2\). Therefore, by the Prime Number Theorem ([46], Theorem 4, Chapter XV, Section 5),

\[
\#\{p_l \in \mathcal{B}(C, t) : p_l \leq X\} \leq \pi_Q\left(\frac{\epsilon X}{2}\right) = \frac{\epsilon X}{2 \log \frac{\epsilon X}{2}} + o\left(\frac{X}{\log X}\right)
\]

as \(X \to \infty\). Therefore, the upper natural density of \(\mathcal{U} \cap \mathcal{B}(C, t)\) is less or equal to \(\epsilon/2\). Consequently, the natural density of \(\mathcal{U}\) is 0.

### 12.4 Properties of Elliptic Curves III: Finite Sets Looking Big.

In this section we will prove a technical proposition which will allow us to make sure that \(\mathcal{R}_1\) is of natural density zero. The proposition considers certain properties of the “denominator” sets \(\mathcal{R}_i\). Since these sets are finite, their natural density is, of course, 0. We are, however, interested in how big the ratio computing density gets for most primes. It turns out, not very surprisingly, that “on the average” this ratio is always arbitrarily close to 0.

#### 12.4.1 Proposition.

For any \(\epsilon > 0\), the natural density of the set \(\{l : \mu_l(P) > \epsilon\}\) is zero.

**Proof.**

If \(l \in \mathcal{P}(Q)\) and \(\mu_l(P) > \epsilon\), then there exists \(X_l(P, \epsilon) \geq 2\) in \(\mathbb{Z}\) such that

\[
\frac{\#\{p \in \mathcal{R}_1(P) \setminus \mathcal{R}_1(P) : p \leq X_l(P, \epsilon)\}}{\pi_Q(X_l(P, \epsilon))} > \epsilon.
\]

For \(M \in \mathbb{Z}, M \geq 2\), let

\[U_M(P, \epsilon) = \{l \in \mathcal{P}(Q) : \mu_l(P) > \epsilon \land X_l(P) \in [M, 2M]\}.
\]

Then if \(l \in U_M(P, \epsilon)\), we have that

\[
\#\{p \in \mathcal{R}_1(P) \setminus \mathcal{R}_1(P) : p \leq 2M\} \geq \#\{p \in \mathcal{R}_1(P) \setminus \mathcal{R}_1(P) : p \leq X_l(P, \epsilon)\} >
\]
\[ \varepsilon \pi_Q(\mathcal{X}_l(P, \varepsilon)) \geq \varepsilon \pi_Q(M). \]

Since by Proposition 12.2.1, for \( l \neq p \in \mathcal{P}(Q) \), we have that \( \mathcal{I}_i \cap \mathcal{I}_p = \mathcal{I}_1 \), it is also the case that

\[ \pi_Q(2M) \geq \sum_{l \in U_M(P, \varepsilon)} \#\{\mathcal{I}_l \cap \mathcal{I}_1 : p \leq 2M\} \geq \varepsilon \pi_Q(M) \#\{l \in U_M(P, \varepsilon)\}. \]

Thus, by the Prime Number Theorem, \( \#\{l \in U_M(\varepsilon, P)\} = O(1) \) as \( M \to \infty \).

Next suppose \( N \) is an integer such that \( 2^k - 1 \leq N < 2^k \). Then

\[ \#\{l \in \mathcal{P}(Q) : \mu_l(P) > \varepsilon \land \mathcal{X}_l(P, \varepsilon) \leq N\} \leq \sum_{i=1}^{k-1} \#\{l \in \mathcal{P}(Q) : \mu_l > \varepsilon \land 2^i \leq \mathcal{X}_l(P, \varepsilon) < 2^{i+1}\} \quad (12.4.1) \]

On the other hand, if \( \mu_l(P) > \varepsilon \), then by definition of \( \mathcal{X}_l(P, \varepsilon) \) we have that

\[ \pi_Q(\mathcal{X}_l(P, \varepsilon)) < \frac{\#\{l \in \mathcal{I} \setminus \mathcal{I}_1\}}{\varepsilon} \leq \frac{\log_2 d_l}{\varepsilon} = O(2^l), \]

by Lemma B.6.8, as \( l \to \infty \). By the Prime Number Theorem, \( \pi_Q(\mathcal{X}_l(P, \varepsilon)) = O(\frac{\mathcal{X}_l}{\log \mathcal{X}_l}) \), as \( l \to \infty \). Further, by Lemma B.10.1,

\[ \mathcal{X}_l < C l^2 \log l, \quad (12.4.2) \]

for some positive constant \( C \) as \( l \to \infty \). Combining the equations in (12.4.1) and (12.4.2), we obtain the following equation for \( Y \in \mathbb{R} \).

\[ \#\{l \in \mathcal{P}(Q) : (l \leq Y) \land (\mu_l(P) > \varepsilon)\} \leq \#\{l \in \mathcal{P}(Q) : (\mu_l(P) > \varepsilon) \land (\mathcal{X}_l(P, \varepsilon) \leq CY^2 \log Y)\} \leq \bar{C} \log(Y^2 \log Y) = o(\pi_Q(Y)), \]

where \( \bar{C} \) is a positive constant and \( Y \to \infty \).

12.4.2 Remark.

Note that the supremum \( \mu_l(P) \) is attained for some \( X \leq \max \mathcal{I}_i(P) \), and therefore \( \mu_l(P) \) is computable for each \( l \), given \( P \).

12.5 Properties of Elliptic Curves IV: Consequences of a Result of Vinogradov.

Below we state a result of Vinogradov which will allow the \( y \)-coordinates of certain multiples of a chosen point of infinite order to get arbitrarily close to integers.
12.5.1 Proposition.

Let $\alpha \in \mathbb{R} \setminus \mathbb{Q}$. Let $J \subseteq [0, 1]$ be an interval. Then the natural density of the set of primes $\{l \in \mathcal{P}(\mathbb{Q}) : (l\alpha \mod 1) \in J\}$ is equal to the length of $J$. (See [118], Chapter XI.)

From this result we derive the following corollary for our elliptic curve.

12.5.2 Corollary.

Let $E$ be an elliptic curve defined over $\mathbb{Q}$ such that $E(\mathbb{R}) \cong \mathbb{R}/\mathbb{Z}$ as topological groups. Let $P$ be any point of infinite order. Then for any interval $J \subset \mathbb{R}$ whose interior is non-empty, the set $\{l \in \mathcal{P}(\mathbb{Q}) | y_1([l]P) \in J\}$ has positive density.

Proof.

Under our assumptions we have an isomorphism of $E(\mathbb{R}) \rightarrow \mathbb{R}/\mathbb{Z}$ as topological groups. Under this isomorphism a point of infinite order must be mapped into an irrational number. Since every real number occurs as a $y$-coordinate of some point in $E(\mathbb{R})$, the set of all points of $E(\mathbb{R})$ projecting $y$-coordinates onto $J$ is non-empty and open. Finally this open subset of $E(\mathbb{R})$ will correspond under the above-mentioned isomorphism to a non-empty open subset of $\mathbb{R}/\mathbb{Z}$.

12.6 Construction of Sets $\mathcal{T}_1(P)$ and $\mathcal{T}_2(P)$ and Their Properties.

In this section we construct (in an effective manner) the sets $\mathcal{T}_1$ and $\mathcal{T}_2$ and make sure that they live up to expectations.

12.6.1 Lemma: Construction of the Sequence $\{l_i(P)\}$.

We define a sequence of rational prime numbers $\{l_i\} = \{l_i(P)\}$ in the following inductive manner. Assume $l_1, \ldots, l_{i-1}$ have already been defined. Then define $l_i$ to be the smallest rational prime number satisfying the following conditions.

1. $l_i \notin \mathcal{L}(P)$.
2. $\forall j = 1, \ldots, i-1$, we have that $l_i > l_j$. 

222
3. $\mu_i(P) \leq 2^{-i}$.

4. $\forall j = 1, \ldots, i$, we have that $p_{ij} > 2^j$. (This condition includes the requirement that $l_i$ is large enough so that $p_{ij}$ is defined for all $j = 1, \ldots, i$.)

5. $\forall l \in \mathcal{L}(P)$, it is the case that $p_{il} > 2^l$. (This condition also includes the requirement that $l_i$ is large enough so that $p_{il}$ is defined for all $l \in \mathcal{L}(P)$.)

6. $y_1([l]P) = y_l(P)$ is such that $|y_l(P) - i| \leq \frac{1}{10^i}$.

Then $\{l_i\}$ is well-defined and computable.

**Proof.**

To prove the lemma, it is enough to show that $l_i$ exists, and can be found effectively for each $i$. Let

$$\mathcal{C}_{i,j}(P) = \{l \in \mathcal{P}(\mathbb{Q}) : l \text{ satisfies Requirement (j) at Stage (i)}\}.$$

First of all, we note that by Lemma 12.5.1, we have that $\mathcal{C}_{i,6}(P)$ has positive natural density. Secondly, note that $\mathcal{C}_{i,3}(P)$ has natural density equal to 1 by Proposition 12.4.1. Thus, $\mathcal{C}_{i,6}(P) \cap \mathcal{C}_{i,3}(P)$ has the same natural density as $\mathcal{C}_{i,6}(P)$, by Proposition B.5.11, and therefore $\mathcal{C}_{i,6}(P) \cap \mathcal{C}_{i,3}(P)$ is an infinite set. Next that the sets $\mathcal{C}_{i,4}(P)$ and $\mathcal{C}_{i,5}(P)$ contain all sufficiently large prime numbers by Proposition 12.2.2. This is also obviously true for sets $\mathcal{C}_{i,1}(P)$ and $\mathcal{C}_{i,2}(P)$. Therefore, the intersection $\mathcal{C}_{i,4}(P) \cap \mathcal{C}_{i,5}(P) \cap \mathcal{C}_{i,1}(P) \cap \mathcal{C}_{i,2}(P)$ contains all sufficiently large prime numbers. Thus, $\bigcap_{j=1}^{6} \mathcal{C}_{i,j}(P) \neq \emptyset$ for all positive integers $i$.

Finally, we observe that $\mathcal{C}_{i,j}(P)$ is recursive for all $j = 1, \ldots, 6$. First of all we note that given the finite set $\mathcal{L}(P) \cup \mathcal{I}(\mathbb{Q})$ and affine coordinates of $P$ corresponding to our chosen Weierstrass equation, we can compute $\mathcal{I}_{n}(P)$ as a recursive function of $n$. Thus we can effectively compute $p_l(P), p_{lm}(P)$ for any prime numbers $l$ and $m$. Further, for each prime number $l$, it is the case that $\mu_i(P)$ can also be computed effectively by Remark 12.4.2.

We are now ready to define $\mathcal{I}_1$ and $\mathcal{I}_2$.

**12.6.2 Definition of $\mathcal{I}_1(P)$ and $\mathcal{I}_2(P)$.**

- Let $\mathcal{I}_1(P) = \bigcup_{i=1}^{\infty} \mathcal{I}_i(P) \cup \mathcal{I}_0(\mathbb{Q})$. (Note that $\mathcal{I}_1$ is automatically included in the union as a subset of every $\mathcal{I}_i$.)

223
Let $T_2(P) = T_{2a} \cup T_{2b} \cup T_{2c}$, where

- Let $T_{2a}(P) = \{p_l : l \in \mathcal{P}(\mathbb{Q}) \setminus \{l_i, i \in \mathbb{N}^+\}\}$.
- Let $T_{2b}(P) = \{p_{ij} : i, j \in \mathbb{N}^+, 1 \leq j \leq i\}$.
- Let $T_{2c}(P) = \{p_{li} : l \in \mathcal{L}(P), i \in \mathbb{N}^+\}$.

The next three propositions will describe the important properties of the sets $T_1(P)$ and $T_2(P)$: the sets are disjoint, computable and have natural density 0.

12.6.3 Proposition.

$T_1(P)$ and $T_2(P)$ are disjoint.

Proof.

Let $q \in T_1(P)$. Then for some positive integer $i$ we have $q \in \mathcal{I}_i(P)$ or $q \in \mathcal{I}_0(\mathbb{Q})$. Next we consider three cases.

- $q \in T_{2a}(P)$: Then $q = p_l \in \mathcal{I}_{p_l}(P) \setminus \mathcal{I}_1(P)$ for some prime number $l \neq l_i$. Since for any $i > 1$, by definition, $\mathcal{I}_i(P) \cap \mathcal{I}_0(\mathbb{Q}) = \emptyset$ and

$$\mathcal{I}_i(P) \cap \mathcal{I}_{p_l}(P) = \mathcal{I}_{(l,l)}(P) = \mathcal{I}_1(P),$$

this case cannot occur.

- $q \in T_{2b}(P)$: Then for some positive integers $k, j$ we have that

$$q = p_{kl} \in \mathcal{I}_{kl}(P) \setminus (\mathcal{I}_k(P) \cup \mathcal{I}_j(P)).$$

Thus, $i \neq j$ and $i \neq k$. On the other hand,

$$\mathcal{I}_{kl}(P) \cap \mathcal{I}_i(P) = \mathcal{I}_{(kl,i)}(P) = \mathcal{I}_1(P),$$

as $l_i, l_j, l_k$ are distinct prime numbers. However, since $\mathcal{I}_1(P) \subseteq \mathcal{I}_k(P)$, this case cannot occur either.

- $q \in T_{2c}(P)$: In this case, $q = p_{lj} \in \mathcal{I}_{lj}(P) \setminus \mathcal{I}_j(P)$ for some $l \in \mathcal{L}(P)$ and some positive integer $j$. Thus, $i \neq j$. By construction, $l_i \neq l$. Next observe that since $l, l_j$ are prime numbers distinct form the prime number $l_i$, it is also the case that

$$\mathcal{I}_{lj}(P) \cap \mathcal{I}_i(P) = \mathcal{I}_{(lj,i)}(P) = \mathcal{I}_1(P) \subset \mathcal{I}_j(P).$$

Therefore this case cannot occur either.
12.6.4 Proposition.
\( \mathcal{T}_1(P) \) and \( \mathcal{T}_2(P) \) are computable.

Proof.
Observe that \( p \in \mathcal{T}_1(P) \) if and only if \( p \in \mathcal{S}_0(Q) \lor \exists i \in \mathbb{Z}_{>0}: p \in \mathcal{I}_i(P) \). Since \( \mathcal{S}_0(Q) \cup \mathcal{I}_1(P) \) is finite, it is enough to produce an effective procedure to decide if \( \exists i \in \mathbb{Z}_{>0}: p \in \mathcal{I}_i(P) \setminus \mathcal{S}_1(P) \). On the other hand,
\[
\exists i \in \mathbb{Z}_{>0}: p \in \mathcal{I}_i(P) \setminus \mathcal{S}_1(P) \iff [l_i]P = \tilde{O} \mod p
\]
or in other words the order of \( P \) modulo \( p \) is \( l_i \). Thus, since the set \( \{l_i\} \) is recursive, it is enough to compute the order of \( P \) modulo \( p \) and ascertain whether this order belongs to \( \{l_i\} \).

As before we need to consider separately the three sets comprising \( \mathcal{T}_2(P) \).

- \( \mathcal{T}_{2a}(P) \) is computable. If \( p \in \mathcal{T}_{2a}(P) \), then \( p = p_i \) for some \( i \not\in \{l_i\} \). Thus, as above it is enough to compute the order of \( P \) modulo \( p \) and establish that \( i \not\in \{l_i\} \).

- \( \mathcal{T}_{2b}(P) \) is computable. If \( p \in \mathcal{T}_{2b}(P) \), then \( p = p_{ij} \), where \( i, j \) are positive integers, \( 1 \leq j \leq i < \log_2 p \) by Requirement (4) of Lemma 12.6.1. Thus it is enough to determine largest element of each set \( \mathcal{I}_{ij} \setminus (\mathcal{I}_i \cup \mathcal{I}_j) \) for \( 1 \leq j \leq i < \log_2 p \).

- \( \mathcal{T}_{2c}(P) \) is computable. The proof of this assertion is similar to the proof above but this time using Requirement (5) of Lemma 12.6.1.

12.6.5 Proposition.
Both \( \mathcal{T}_1(P) \) and \( \mathcal{T}_2(P) \) are of natural density 0.

Proof.
We start with \( \mathcal{T}_1(P) \). The upper natural density of this set is equal to
\[
\limsup_{X \to \infty} \frac{\#\{p \in \mathcal{S}_0(Q) \cup (\bigcup_{i=1}^{\infty} \mathcal{I}_i(P)) : p \leq X\}}{\#\{p \in \mathcal{P}(Q) : p \leq X\}} \leq
\]
\[
\limsup_{X \to \infty} \frac{\#\{p \in \mathcal{S}_0(Q) : p \leq X\}}{\#\{p \in \mathcal{P}(Q) : p \leq X\}} + \sum_{i=1}^{\infty} \frac{\#\{p \in \mathcal{I}_i(P) : p \leq X\}}{\#\{p \in \mathcal{P}(Q) : p \leq X\}}
\]
where $r$ is any positive integer. Thus the density must be zero.

Next we consider the upper natural density of $T_2b(P)$. Note that by Requirement (4) of Lemma 12.6.1, for each $q \in T_2b(P)$, we can find a distinct pair of natural numbers $(i, j)$ with $j \leq i \leq \log q$. Thus for any positive real number $X$,

$$\#\{q \in T_2b : q \leq X\} \leq \#\{(i, j), i, j \in \mathbb{N}, 1 \leq i, j \leq \log X\}.$$ 

Consequently, the upper natural density of $T_2b(P)$ is equal to

$$\limsup_{X \to \infty} \frac{\#\{q \in T_2b : q \leq X\}}{\#\{p \in \mathcal{P}(\mathbb{Q}) : p \leq X\}} \leq \limsup_{X \to \infty} \frac{\#\{(i, j), i, j \in \mathbb{N}, 1 \leq j \leq i \leq \log X\}}{\#\{p \in \mathcal{P}(\mathbb{Q}) : p \leq X\}}$$

$$= \limsup_{X \to \infty} \frac{O(\log^2 X)}{O(X/\log X)} = 0.$$

By Requirement (5) of Lemma 12.6.1, the upper natural density of $T_{2c}(P)$ is similarly equal to

$$\limsup_{X \to \infty} \frac{\#\{p_{li} \leq X, i \in \mathbb{N}, i \geq 1, l \in \mathcal{L}(P)\}}{\#\{p \in \mathcal{P}(\mathbb{Q}) : p \leq X\}}$$

$$\leq \limsup_{X \to \infty} \frac{|\mathcal{L}(P)|\#\{i \in \mathbb{N}, 1 \leq i \leq \log X\}}{\#\{p \in \mathcal{P}(\mathbb{Q}) : p \leq X\}} = \limsup_{X \to \infty} \frac{O(\log X)}{O(X/\log X)} = 0.$$

Finally, $T_{2a}(P) \subset \mathcal{U}(P)$, where $\mathcal{U}(P)$ was defined in Proposition 12.3.5. Since by this proposition the natural density of $\mathcal{U}(P)$ is zero, the natural density of $T_{2a}(P)$ is also zero.

The next two propositions will show that if we exclude all primes from $T_2$ and allow all primes from $T_1$ in the denominators, the only points of $E$ which will "survive" will be points of the form $[\pm li]P$ together with a finite set of points.

**12.6.6 Proposition.**

Let $\mathcal{U} \subset \mathcal{P}(\mathbb{Q})$ be such that $T_1(P) \subset \mathcal{U}$ and $T_2(P) \cap \mathcal{U} = \emptyset$. Then there exists a finite set $A$ of natural numbers such that for any $m \in \mathbb{Z}$ we have $[m]P \in E(\mathcal{O}_{\mathbb{Q}, \mathcal{U}})$ only if $\exists i \in \mathbb{Z}_{>0} : m = \pm li$ or $m \in A$. 

226
Proof.

Let

\[ m = \pm \left( \prod_{l \in \mathcal{P}(Q)} l^{b(l)} \right), \]

where \( b(l) = 0 \) for all but finitely many primes. Suppose \( [m]P \in E(O_K, \mathcal{W}) \)
and for some \( i \in \mathbb{Z}_{>0} \) it is the case that \( b(l_i) \neq 0 \). We claim, that in this case,
\( b(l_i) = 1 \), and for all \( j \neq i \), we have that \( b(l_j) = 0 \). Indeed, suppose \( b(l_i) > 1 \).
Then \( p_{l_i} | d_m \), and by Corollary B.6.7, and construction of \( \{l_i\}, \mathcal{T}_1(P), \) and \( \mathcal{T}_2(P) \), we have to conclude that

\[ p_{l_i} \in (\mathcal{I}_{p_{l_i}} \setminus \mathcal{T}_1) \subseteq (\mathcal{I}_m \setminus \mathcal{T}_1) \subseteq \mathcal{W} \cap \mathcal{T}_2(P) = \emptyset. \]

Thus, if \( b(l_i) \neq 0 \), then \( b(l_i) = 1 \). Next we note that a similar argument excludes the case of \( b(l_i) = b(l_j) = 1 \) simultaneously for some \( i, j \in \mathbb{Z}_{>0} \).

Suppose now that for some \( l \in \mathcal{P}(Q) \setminus \{l_i, i \in \mathbb{Z}_{>0}\} \) we have that \( b(l) \neq 0 \).
We claim that in this case \( b(l) \leq a_i(P) - 1 \). Indeed, if \( b(l) \geq a_i(P) \), then

\[ p_l \in (\mathcal{I}_{p_l} \setminus \mathcal{T}_1) \subseteq (\mathcal{I}_m \setminus \mathcal{T}_1) \subseteq \mathcal{W} \cap \mathcal{T}_2(P) = \emptyset. \]

Since Notation 12.1.2 tell us that \( a_i(P) > 1 \) for \( l \in \mathcal{L} \) only, from the discussion above we can now conclude that
\( m = l_i^{b(l_i)} \prod_{l \in \mathcal{L}} l^{b(l)} \), where \( i \in \mathbb{Z}_{>0} \),
\( b(l_i) = 0,1 \), and \( b(l) \leq a(l) - 1 \) for \( l \in \mathcal{L} \). Now it suffices to show that if \( b(l) > 0 \) for some \( l \in \mathcal{L} \) then \( b(l_i) = 0 \). Suppose not, then, just as above, we have

\[ p_{l_i} \in (\mathcal{I}_{p_{l_i}} \setminus \mathcal{T}_1) \subseteq (\mathcal{I}_m \setminus \mathcal{T}_1) \subseteq \mathcal{W} \cap \mathcal{T}_2(P) = \emptyset. \]

Now the assertion of the proposition follows from the fact that \( \mathcal{L} \) is a finite set.

It is also clear from the definition of \( \mathcal{W} \) and \( \mathcal{T}_1(P) \) that the following statement is true.

12.6.7 Proposition.

For all \( i \in \mathbb{Z}_{>0} \), we have that \( [\pm l_i]P \in E(O_K, \mathcal{W}) \), where \( \mathcal{W} \) is defined as in Proposition 12.6.6.

We are almost ready to proceed with the final part if the proof of Theorem 12.1.1. We need just one more proposition and corollary to deal with the torsion elements of \( E \).
12.6.8 Proposition.

Let $E/\mathbb{Q}$ be a curve as in Proposition B.6.2. Let $r \geq 1$ be the size of the torsion group of $E$. Let $Q \in E(\mathbb{Q})$ be a generator of $E(\mathbb{Q})$ modulo the torsion group. Let $P = [r]Q$. Let $\mathcal{W}$ be defined as in Proposition 12.6.6. Then the set $\{y_{\pm i}(P) | i \in \mathbb{N}, i \geq 1\}$ is Diophantine over $E(O_{\mathbb{Q}, \mathcal{W}})$.

Proof.

First of all we note that $\{(x, y) \in [r]E(\mathbb{Q})\}$ is a Diophantine subset of $\mathbb{Q}$. Secondly, let $T \in [r]E(\mathbb{Q})$. Then $T = [r]T'$, where $T' = [k]Q + _E V$, where $k \in \mathbb{Z}$, “+_E” is the addition on $E$, and $V$ is an element of the torsion group. Then $T = [k](rQ) = [k]P$. On the other hand, it is clear that every multiple of $P$ is in $[r]E(\mathbb{Q})$. Next we observe that since $O_{\mathbb{Q}, \mathcal{W}}$ is Dioph-regular, $\mathbb{Q} \leq _{Dioph} O_{\mathbb{Q}, \mathcal{W}}$ and therefore, $[r]E(\mathbb{Q}) \cap O_{\mathbb{Q}, \mathcal{W}}$ is Diophantine over $O_{\mathbb{Q}, \mathcal{W}}$ by “Going up and then down method”. Finally, by Propositions 12.6.6 and 12.6.7, it follows that $[r]E(\mathbb{Q}) \cap O_{\mathbb{Q}, \mathcal{W}} = \{\pm [l]P, i \in \mathbb{Z}_{>0}\} \cup \{\text{finite set}\}$. Since we can eliminate the points from the finite set by explicitly listing several “not” equalities, we conclude that the assertion of the proposition is true.

12.6.9 Corollary.

Let $P, E$ as in Proposition 12.6.8. Then the set $\{y_{i}(P) | i \in \mathbb{Z}_{>0}\}$ is Diophantine over $E(O_{\mathbb{Q}, \mathcal{W}})$.

Proof.

To show that the corollary is true, it is enough to note that we just need to select positive elements of the sets $\{y_{\pm i}(P) | i \in \mathbb{N}, i \geq 1\}$. As before this can be done in a Diophantine manner by Corollary 5.1.2.

12.7 Proof of Poonen’s Theorem.

Let $\mathcal{W}$ be again defined as in Proposition 12.6.6. We will show that the conditions of Theorem 12.1.1 are satisfied over $O_{\mathbb{Q}, \mathcal{W}}$.

1. Since $|y_{i}(P) - i| < \frac{1}{10i}$, the set $D = \{y_{i}(P), i \in \mathbb{Z}_{>0}\}$ is clearly discrete and therefore provides a counterexample for the first Mazur’s conjecture for the ring $O_{\mathbb{Q}, \mathcal{W}}$.

2. By Proposition 3.4.7, to show that $O_{\mathbb{Q}, \mathcal{W}}$ has Diophantine model of $\mathbb{Z}$, it is enough to show that under the proposed computable mapping of $\mathbb{Z}$
into the ring, the graphs of addition and multiplication are Diophantine. To accomplish this, we will first show that the sets

\[ D^+ = \{(y_i, y_j, y_k) \in D^3 : k = i + j, i, j \in \mathbb{Z}_{>0}\} \]

and

\[ D_2 = \{(y_i, y_k) \in D^2 : k = i^2, i \in \mathbb{Z}_{>0}\} \]

are Diophantine over \( O_{Q, \mathcal{W}} \). To see that \( D^+ \) is a Diophantine subset of \( O_{Q, \mathcal{W}} \) observe that for \( i, j, k \in \mathbb{Z}_{>0} \) it is true that

\[ k = i + j \iff |y_i + y_j - y_k| < 1/3. \]

Indeed suppose \( k = i + j \), then

\[
|y_i + y_j - y_k| = |y_i - i + y_j - j - y_k + k| \leq \\
|y_i - i| + |y_j - j| + |k - y_k| < \frac{1}{10i} + \frac{1}{10j} + \frac{1}{10k} < 1/3.
\]

Conversely, suppose

\[ |y_i + y_j - y_k| < 1/3. \tag{12.7.1} \]

Then

\[
|y_i - i + i + y_j + j - j - k + k - y_k| < 1/3 \\
|i + j - k| < 1/3 + |y_i - i| + |y_j - j| + |k - y_k| < 2/3.
\]

Since \( i, j, k \in \mathbb{Z} \), we must conclude that \( i + j - k = 0 \). Next we want to show that for \( i \in \mathbb{Z}_{>0} \) it is the case that

\[ k = i^2 \iff |y_i^2 - y_k| < 2/5. \]

So suppose \( k = i^2 \). Then

\[
|y_i^2 - i^2 + k - y_k| < \frac{1}{10i} |2i + \frac{1}{10i}| + \frac{1}{10k} < 2 \cdot \frac{1}{10} + \frac{1}{100} + \frac{1}{10} < \frac{2}{5}.
\]

Conversely, suppose that

\[ |y_i^2 - y_k| < 2/5. \tag{12.7.2} \]

Then, by an argument similar to the one used above,

\[
|i^2 - k| \leq \frac{2}{5} + |y_i^2 - i^2| + |y_k - k| < \\
\frac{2}{5} + |y_i + i| \frac{1}{10i} + \frac{1}{10k} \leq \frac{2}{5} + (2i + \frac{1}{10i}) \frac{1}{10i} + \frac{1}{10k}
\]

229
\[ \leq \frac{2}{5} + \frac{1}{5} + \frac{1}{5} = \frac{4}{5} < 1 \]

Thus, we conclude that \( i^2 - k = 0 \). Finally, we note that by Corollary 5.1.2, inequalities in (12.7.1) and (12.7.2) are Diophantine over \( \mathbb{Q} \) and consequently over \( O_{Q, \mathcal{W}} \). Thus, both \( D+ \) and \( D_2 \) are Diophantine. As in the case of function fields, if squares and sums form Diophantine sets, so do products since \( xy = \frac{1}{2}((x + y)^2 - x^2 - y^2) \).

What we have constructed so far is really a Diophantine model of \((\mathbb{Z}_{>0}, +, \cdot)\) over \( O_{Q, \mathcal{W}} \). To obtain a Diophantine model of \((\mathbb{Z}, +, \cdot)\) we can adopt one of the following two strategies:

1. Extend the model of \( \mathbb{Z}_{>0} \) to a model of \( \mathbb{Z} \). Here we need to select images for 0 and negative integers. Note that \( y_{-l} = -y_l \), given the form of our Weierstrass equation. Therefore, it is natural to send \(-i\) to \(-y_l\), and 0 to 0.

2. Construct a model of \((\mathbb{Z}, +, \cdot)\) over \((\mathbb{Z}_{>0}, +, \cdot)\) by, for example, using pairs of positive integers to represent arbitrary integers: for \( a > 0 \), let \((1, a)\) represent \( a \), let \((2, a)\) represent \(-a\) and let \((3, 1)\) represent 0.

We leave the details of these constructions to the reader.

### 12.7.1 Remark.

We finish our discussion by mentioning two papers which attempt different approaches to Diophantine problem of \( \mathbb{Q} \). The first paper ([70]) is by Pheidas and attempts to use points on elliptic curve to construct a Diophantine model of \( \mathbb{Z} \), but in a manner different from Poonen’s. Given a rank 1 elliptic curve over \( \mathbb{Q} \) and a generator \( P \), Pheidas proposes to map \( n \) to \([n]P\). Here the difficulty lies in showing that such a map will make the image of the multiplication graph Diophantine. In fact it is not at all clear that it is.

Taking a different route Cornelissen and Zahidi in [7] revisit first-order definability results by Julia Robinson and attempt to update them.
Chapter 13

Beyond Global Fields.

The questions and problems raised by the solution of Hilbert’s Tenth Problem extend to many other objects besides the global fields which are the subject of this book. In particular, the questions we raised are just as relevant for infinite algebraic extensions of global fields, for fields of positive characteristic of transcendence degree greater than one and for function fields of characteristic 0. A detailed and substantial discussion of existential definability and decidability over these object is beyond the scope of this book, but in this chapter we will briefly survey extensions of Hilbert’s Tenth Problem to some of the objects mention above so that an interested reader can be directed to the original sources. Before proceeding we would like to note that many detailed surveys of the subjects discussed in this chapter can be found in [20].

13.1 Function Fields of Positive Characteristic of Higher Transcendence Degree or over Infinite Fields of Constants.

The most general result concerning concerning rational function fields of positive characteristic has been obtained by H. Kim and F.Roush in [42]. They proved the following proposition.

13.1.1 Theorem.

Let $K$ be a rational function field over a field $C$ of constants of characteristic $p > 0$. Assume that $C$ does not contain the algebraic closure of finite field . Then HTP is undecidable over $K$. 
The proof of the theorem followed essentially the same line as the proof of the Diophantine undecidability of function fields over finite field of constants described in Chapter 10. Thus the two main ingredients of this proof were the Diophantine definability of $p$-th power equations and Diophantine definability of integrality at a single prime. The proof of existential definability of $p$-th power equations in Pheidas’ paper ([69]) applies to any rational function field, but Kim and Roush had to come up with a new existential definition of integrality at a single prime. For that proof they used Hasse Strong Norm Principle and a function field version of Hilbert Class Field. While the original idea to use the strong Hasse Norm Principle to define integrality at finitely many primes probably belongs to Rumely who used it in [85] in the context of first order definability questions, Kim and Roush were the first to use Hasse Norm Principle explicitly for Diophantine definability.

The result of Kim and Roush was partially lifted to non-rational function fields by the Eisenträger and the author in [23], [106], [108] and [91]. We would like to mention here that ideas of Prunescu from [77] played an important role in the proofs of [108]. Perhaps the most general results concerning non-rational function fields are in [91] and can be stated in the following manner.

13.1.2 Theorem.
Let $M$ be any function field of characteristic $p > 0$ such that the algebraic closure $C$ of a finite field in $M$ has an extension of degree $p$. Let $L$ be any field finitely generated over $C$ and linearly disjoint from $M$ over $C$. Let $K = ML$. Then Diophantine problem of $K$ is undecidable.

This theorem has an important corollary.

13.1.3 Corollary.
Let $M$ be a field finitely generated over a finite field. Then HTP is undecidable over $M$.

We would like to finish this section with two related questions which have eluded so far researchers in the area.

13.1.4 Question.
Is it possible to give a Diophantine definition of order at a single prime over a function field of positive characteristic over a field of constants which is
algebraically closed?

13.1.5 Question.

Is HTP undecidable over a function field of positive characteristic over a field of constants which is algebraically closed?

If we are to pursue the second question along the road we have travelled before with respect to function fields of positive characteristic, then we will have to answer Question 13.1.4 first. However, it is quite conceivable that Question 13.1.4 has a negative answer, while HTP is still undecidable over function fields over algebraically closed fields of constants. So perhaps a different approach is warranted here.

13.2 Algebraic Extensions of Global Fields of Infinite Degree.

Since HTP clearly becomes decidable over the field of all algebraic numbers (the algebraic closure of $\mathbb{Q}$), as we consider infinite algebraic extensions, we might expect the situation to change, as indeed it does. We do have decidability in some sufficiently large extensions. First, however, we describe the few Diophantine undecidability results that we have for infinite algebraic extensions of $\mathbb{Q}$.

Perhaps the first person to consider in print the problem of showing that HTP is undecidable in some rings whose quotient fields are infinite extensions of $\mathbb{Q}$ was Denef in [18]. He pointed out that if one could find an elliptic curve defined over $\mathbb{Q}$ such that it had the same positive rank over $\mathbb{Q}$ as over some infinite totally real extension of $\mathbb{Q}$, then one could use such a curve to give a definition of $\mathbb{Z}$ over the ring of algebraic integers of this totally real infinite extension. We do have examples of such elliptic curves, though the complete picture concerning the phenomenon of elliptic curves keeping the same rank under infinite extensions is far from clear. For more information on the subject see, for example, [59] and [54].

Using a refinement of the methods developed for finite extensions, the author constructed Diophantine definitions of $\mathbb{Z}$ in “small” and “large” rings of algebraic numbers whose fraction fields were totally real infinite extensions of $\mathbb{Q}$. (See [106] and [93] for more details.)
When one considers HTP as a problem of determining decidability of some existential theory, it is clear that proving existential undecidability of some ring implies that the full theory of this ring is also undecidable. Of course the reverse happens in the case of decidability. There, clearly one gets a stronger result by showing that the full theory of a ring is decidable. Thus, in many cases, some of them listed below, the decidability of Hilbert’s Tenth Problem over a ring is a consequence of the fact that the ring’s full first order theory is decidable.

Perhaps the most famous decidability result concerning HTP is due to Rumely. In [86], he showed that HTP was decidable in the ring of all algebraic integers. The proof relied on what became known as Rumely’s Local-Global Principle stating that a variety has a smooth integral point in the algebraic closure of \( \mathbb{Q} \) if and only if it has a smooth point in every localization of the ring of all algebraic integers. This result was a generalization of a more restricted version of local-global principle obtained by Cantor and Roquette in [2]. A similar result was obtained by Moret-Bailly in [61] but using completely different methods.

Rumely’s results were later strengthened in different ways. In particular, van den Dries showed in [115] that the first order theory of the ring of all algebraic integers is decidable. Van den Dries and Macintyre extended this decidability result to many localizations of the ring of all algebraic integers and ring of all integral functions in [116]. A similar result was also obtained by Prestel and Schmid in [75].

In [61], Moret-Bailly, and in [35], Green, Pop and Roquette showed that Rumely’s results apply to smaller (though still large) fields. Additional versions of both local and global principle and decidability results were later obtained by Moret-Bailly (see [62] and [63]), by Jarden and Razon (see [38], [39]), by Darniè re (see [11] and [10]), by Prestel and Schmid (see [76]) and by Ershov (see, for example, [27], [28], [29], [30]).

Using different methods, Fried, Haran, and Völklein showed that the field of totally real numbers has a decidable first order theory in [32]. This result is made more remarkable by the fact that Julia Robinson proved that the first order theory of the ring of the totally real integers is not decidable (see [83]).

As we said above, this list of results is far from being exhaustive and is just supposed to serve as a guide for further reading. We also would like to mention a very nice survey article on the subject by Darniè re (see [9]) which we recommend to the interested reader.
13.3 Function Fields of Characteristic 0.

The issues of existential definability proved to be much harder to understand over the function fields of characteristic 0 than over function fields of positive characteristic. One of the problems which was solved over large classes of function fields of positive characteristic and which remains elusive for many function fields is the problem of Diophantine definability of order at finitely many primes. Before we state the main results concerning Diophantine undecidability over function fields of characteristic 0, we need to state a definition.

13.3.1 Definition.

Let $K$ be a field of characteristic 0. Then it is called formally real if $-1$ is not a sum of squares. If it is also the case that every odd degree polynomial has a root in $K$, then $K$ is called real closed.

The first result concerning function fields is due to Denef who proved in [16] that HTP is undecidable over rational function fields over formally real fields of constants. Note that this result covers rational function fields of any finite transcendence degree over any subfield of $\mathbb{R}$ since a rational function field over a formally real field of constants is itself formally real. This result was important not only for what it said about Diophantine problem of a large class of rational function fields but also because its proof introduced an elliptic curve

$$(T^3 + aT + b)Y^2 = X^3 + aX + b, a, b \in \mathbb{Q},$$

(later named “Manin-Denef”) as a tool for constructing Diophantine models of integers. The proof used the fact that, assuming that the elliptic curve $y^2 = x^3 + ax + b$ had no complex multiplication, Manin-Denef curve was of rank one over $K(T)$ for any field $K$ of characteristic 0. The other part necessary, under Denef’s method, for a construction of a Diophantine model was the existential definition of order at any one prime. (This was where the "formally real" condition was used.)

The results of Denef were extended by Kim and Roush who showed in [43] Diophantine unsolvability of any rational function field whose constant field could be embedded in a $p$-adic field. As Denef, Kim and Roush constructed a Diophantine model of integers over the fields in question using the Manin-Denef elliptic curve, but they devised a different method for defining existentially integrality at a single prime using quadratic forms. Kim and Roush also proved in [41] that HTP was undecidable over $\mathbb{C}(t_1, t_2)$. This proof also constructed a Diophantine model of $\mathbb{Z}$ with a help of an elliptic curve of rank
one. A very nice exposition of their method can be found in [71].

The next step was taken by Karim Zahidi who showed in [120] that integers have a Diophantine definition in hyperelliptic function fields over real closed fields of constants. The proof of this result was obtained via a sophisticated refinement of the argument used by Denef. For a while further progress over function fields was stalled by the lack of knowledge concerning elliptic curves of rank 1 over function fields which were not rational. This obstacle was surmounted by Moret-Bailly who showed in [60] that every function field of characteristic 0 has an elliptic curve of rank 1. This result allowed Moret-Bailly to show that HTP is undecidable over any function field over formally real field of constants or over a constant field which is a subfield of a p-adic field. (The last result was also independently obtained by Kirsten Eisenträger in [22].) Finally, Moret-Bailly’s result on elliptic curves also served as a foundation for the proof by Eisenträger in [24] extending Kim and Roush results on \( C(t_1, t_2) \) to any function field over \( C \) in two or more variables.

Unfortunately, the case of an arbitrary function field of transcendence degree 1 over \( \mathbb{Q} \) remains open with the difficulty centered on the existential definition of the order. In particular, we still don’t know the Diophantine status of \( C(t) \) and its algebraic extensions. (As a matter of fact, the status of the first-order theory is unknown for these fields.)

When it comes to the rings of functions the situation is better since over the rings there is a natural way to define order using the primes which were not inverted. In particular, Moret-Bailly also showed in [60] that HTP is undecidable in any semilocal holomorphy ring of functions of characteristic zero. (Zahidi proved the analogous result in [121] for rational function fields.) The author proved that \( \mathbb{Z} \) has a Diophantine definition in any ring of \( S \)-integers of a function field of characteristic 0 in [96] and also in bigger rings in [100] and [109].
Appendix A

Recursion Theory.

This appendix contains some basic information on recursive functions, recursive sets, recursively enumerable sets and relativized versions of these concepts. We also briefly discuss the recursiveness of some algebraic objects. We use [84] and [33] as our main references for the material below.

Before proceeding we would like to note the following concerning terminology in this section. During the past ten years the terms “Recursion Theory”, “recursive functions”, “recursive sets”, and “recursively enumerable sets” have fallen out of fashion and have been partially supplanted by “Computability Theory”, “computable functions”, “computable sets” and “computably enumerable sets” respectively. We will use both types of terms interchangeably.

A.1 Computable Functions.

We will use the definition of computable functions from [33]. First, however, we need to define the “least” operator.

A.1.1 Definition.

Let $R(x_1, \ldots, x_m, y)$ be a relation on $\mathbb{N}$ such that for each $m$-tuple $\bar{x} = (x_1, \ldots, x_m) \in \mathbb{N}^m$, there exists $y \in \mathbb{N}$ for which $R(x_1, \ldots, x_m, y)$ is true. Then for any $\bar{x} \in \mathbb{N}^m$, define $(\mu y)R(x_1, \ldots, x_m, y)$ to be the smallest natural number $y$ such that $R(x_1, \ldots, x_m, y)$ is true.
A.1.2 Definition.

Let \( F_n \) be the set of all functions from \( \mathbb{N}^n \) to \( \mathbb{N} \). Let \( F = \bigcup_{n=1}^{\infty} F_n \). Then the set of recursive functions is the smallest subset of \( F \) containing the following functions, which we will call the basic functions:

1. \( f(x) = 0 \),
2. The successor function \( f(x) = x + 1 \),
3. The projection function \( \pi_i(x_1, \ldots, x_n) = x_i \), where \( n \in \mathbb{N}, i \in \{1, \ldots, n\} \),

and closed under the following operations:

1. Composition. For recursive functions \( g \in F_m, h_1, \ldots, h_m \in F_n \), the function \( h \in F_n \) defined by
   \[
   h(x_1, \ldots, x_n) = g(h_1(x_1, \ldots, x_n), \ldots, h_m(x_1, \ldots, x_n))
   \]
   is also recursive.
2. Inductive definition. For recursive functions \( f_0 \in F_n, g \in F_{n+2} \), the function \( f \in F_{n+1} \) defined by
   \[
   f(x_1, \ldots, x_n, 0) = f_0(x_1, \ldots, x_n),
   f(x_1, \ldots, x_n, y + 1) = g(x_1, \ldots, x_n, y, f(x_1, \ldots, x_n, y))
   \]
   is also recursive.
3. Minimization. Let \( R(x_1, \ldots, x_m, y) \) be a relation with a recursive characteristic function and such that for all \( (x_1, \ldots, x_m) \in \mathbb{N}^m \), there exists \( y \in \mathbb{N} \) with \( R(x_1, \ldots, x_m, y) \). Then the function \( f \in F_m \) defined by
   \[
   f(x_1, \ldots, x_m) = (\mu y)R(x_1, \ldots, x_m, y)
   \]
   is also recursive.

There are other equivalent definitions of recursive functions using Turing machines and rudimentary programming languages. (See for example [14].) In practice, however, the definition given above as well as alternative definitions are cumbersome to use. For that reason a proof that a given function or set is computable or recursive is often rendered informally by appealing to Church’s Thesis which states that the set of recursive functions is precisely the set of functions whose values can be computed algorithmically. For a discussion of Church’s Thesis see [84], Section 1.7, among others. In this book we attempted to provide wherever feasible formal proofs of computability using our definition of computable functions. We produced informal versions of the argument along the lines of Church’s Thesis when formalization of the proof was straightforward but labor intensive.
A.1.3 Definition.
Let \( A \subset \mathbb{N}^m \) be a set whose characteristic function is recursive (computable). Then \( A \) will be called recursive or computable.

A.1.4 Lemma.
The following functions from natural numbers to natural numbers and the following subsets of natural numbers are computable.

1. Addition \( f(x, y) = x + y \) and multiplication \( f(x, y) = xy \).
2. The minimum function \( \min(x, y) \).
3. The maximum function \( \max(x, y) \).
4. The exponential function \( H(x_1, x_2) = x_1^{x_2} \).
5. The sign function: \( \text{sgn}(0) = 0 \) and \( \text{sgn}(x + 1) = 1 \).
6. The absolute value function \( |x - y| \).
7. Predecessor function \( \text{Pr}(x) = \max(0, x - 1) \).
8. Truncated difference \( \text{TD}(x, y) = \max(0, x - y) \).
9. Summation
\[
F(x_1, \ldots, x_m, a, y) = \sum_{i=a}^{y} f(x_1, \ldots, x_m, i),
\]
and product
\[
H(x_1, \ldots, x_m, a, y) = \prod_{i=a}^{y} f(x_1, \ldots, x_m, i),
\]
assuming \( f(x_1, \ldots, x_m, i) \) is computable.
10. Bounded minimization defined as follows. Let \( R(x_1, \ldots, x_m, y) \) be a relation with a recursive characteristic function. Then the function
\[
f(x_1, \ldots, x_m, a, z) = \mu_{a < y \leq z} R(x_1, \ldots, x_m, y)
\]
is defined to be equal to the smallest \( y \) such that \( a < y \leq z \) and \( R(x_1, \ldots, x_m, y) = 1 \) if such a \( y \) exists and to \( z \) otherwise.

See Sections 8.3 and 8.4 of [33] for proof.
A.1.5 Remark.

We will also use bounded minimization with $a \leq y \leq z$, $a < y < z$, and $a \leq y < z$. It is not hard to show that the slightly different bounds for the variable do not change the recursive status of bounded minimization.

Using closure under composition, one can easily show that the following functions are recursive.

A.1.6 Corollary.

1. Sum and product of two computable functions are computable.
2. All polynomial functions are computable.
3. If $f, g$ are computable functions, then $F(x_1, \ldots, x_n) = f(x_1, \ldots, x_n)g(x_1, \ldots, x_n)$ is computable.

With a slight effort we also obtain the following corollary of Lemma A.1.4.

A.1.7 Corollary.

1. Let $f(x_1, \ldots, x_n)$ be a computable function. Then the relation $R(x_1, \ldots, x_n, y) = 1 \iff f(x_1, \ldots, x_n) = y$ is computable.
2. Let $\{R_i(z_1, \ldots, z_l), i = 1, \ldots, k\}$ be a finite collection of recursive relations. Then a relation $R(z_1, \ldots, z_l) = \bigwedge_{i=1}^{k} R_i(z_1, \ldots, z_l)$ is also recursive.

Proof.

1. Define the characteristic function $\chi(x_1, \ldots, x_n, y)$ for $R$ in the following manner. Let $\chi(x_1, \ldots, x_n, y) = 1 - \text{sgn}|f(x_1, \ldots, x_n) - y|$. This function is computable by Lemma A.1.4 and by Corollary A.1.6.
2. This part follows from the fact that a product of computable functions is computable from Corollary A.1.6.

The next lemma tells us that computable sets are closed under simple set operations.
A.1.8 Lemma.

The unions, intersections, cartesian products and complements of recursive sets are recursive.

Proof.

Let $A, B$ be recursive sets with characteristic functions $\chi_A$ and $\chi_B$ respectively. Then $\chi_{A \cap B}(n) = \chi_A(n)\chi_B(n)$ is a characteristic function of the intersection, while $\chi_{A \cup B}(n) = \chi_A(n) + (1 - \chi_A(n))\chi_B(n)$ is the characteristic function of the union. Both functions are recursive by Corollary A.1.6. Further, if $(x, y) \in A \times B$, then we can define $\chi_{A \times B}(x, y) = \chi_A(x)\chi_B(y)$. Thus $\chi_{A \times B}(x, y)$ is recursive by Corollary A.1.6 also. Finally, if $\chi_A(n)$ is a characteristic function of $A$, then $1 - \chi_A(n)$ is the characteristic function of the complement.

Next we observe that functions defined by recursive clauses are computable.

A.1.9 Lemma.

Let $A_1, \ldots, A_n \subset \mathbb{N}^m$ be computable sets constituting a partition of $\mathbb{N}^m$. Let $f_1, \ldots, f_n \in \mathcal{F}_m$ be computable functions. Then the following function is computable.

$$h(x_1, \ldots, x_m) = f_i(x_1, \ldots, x_m), \text{ if } (x_1, \ldots, x_m) \in A_i$$

Proof.

Let $\chi_{A_i}$ be the characteristic function of $A_i$ and define

$$h(x_1, \ldots, x_m) = \sum_{i=1}^{n} \chi_{A_i}(x_1, \ldots, x_m)f_i(x_1, \ldots, x_m).$$

Next we note that the function $h(x_1, \ldots, x_m)$ is computable by Corollary A.1.6.

A.1.10 Lemma.

Finite sets are recursive.
Proof.
First we show that the set consisting of one element is recursive. Let $A = \{ a \}$. Then $\chi_A(x) = 1 - \text{sgn}(|x - a|)$ which is clearly recursive by Definition A.1.2 and Lemma A.1.4. Next we proceed by induction. Let $\chi_{\{a_1, \ldots, a_{n-1}\}}$ be a recursive characteristic function of a set of $n-1$ elements and let $\chi_{\{a_n\}}$ be the characteristic function of $\{a_n\}$. Then $\max(\chi_{\{a_1, \ldots, a_{n-1}\}}(x), \chi_{\{a_n\}}(x)) = \chi_{\{a_1, \ldots, a_n\}}(x)$ is recursive by Lemma A.1.4 also.

It is a bit more difficult to show that the following proposition holds.

A.1.11 Proposition.
The following sets and functions are computable.

1. The set of pairs of positive integers $(m, n)$ such that $m|n$.
2. The set of prime numbers.
3. The function $\phi(n)$ computing the $n$-th prime number in the ascending list of all prime numbers. Set $\phi(0) = 0$.
4. The function $\rho(n, m)$ computing the exponent of the $n$-th prime number in the prime factorization of a given positive integer $m$. We set $\rho(n, 0) = \rho(0, m) = 0$.
5. The function $\mu(n)$ computing the largest prime dividing a given integer $n \geq 2$. We let $\mu(0) = 0$ and $\mu(1) = 1$.
6. The function $\nu(n)$ computing the number of distinct prime factors of a positive integer. We set $\nu(0) = \nu(1) = 0$.
7. The function $g(n)$ defined as follows: $g(n) = 0$ if $n$ is not a prime number, and $g(n)$ is the sequence number of $n$ in the ascending sequence of all prime numbers, if $n$ is a prime number.
8. The function computing $(m, n) –$ the GCD of $m$ and $n$ for $m \geq 1, n \geq 1$. We set $(m, 0) = 0, (0, n) = 0$.
9. The set $\{(m, n) | m < n\}$
10. The function computing the result of integer division: $n \div m = q$, where $m \neq 0, n = mq + r, 0 \leq r < m$. We set $n \div 0 = 0$. 

242
Proof.

1. Assuming $m \geq 1, n \geq 1$, we can let

$$\chi(m, n) = \text{sgn}(n + 1 - \mu_{1 \leq y < n + 1}(my = n)).$$

Then $\chi(m, n) = 1$ if and only if $m \mid n$. By Lemmas A.1.4, A.1.8, A.1.9, A.1.10, and Remark A.1.7, $\chi(m, n)$ is computable.

2. Let $\chi_{\text{primes}}(n) = \text{sgn}(n - \mu_{2 \leq y < n}(y \mid n))$ for $n \geq 2$. Set $\chi_{\text{primes}}(0) = \chi_{\text{primes}}(1) = 0$. Then $\chi(n)$ is computable by Lemmas A.1.4, A.1.8, A.1.9, A.1.10, and Part 1 of this lemma.

3. We construct an inductive definition for $\phi$: let $\phi(1) = 2$, and let

$$\phi(n) = \mu m(\max(m, \phi(n - 1) + 1) = m \wedge m \text{ is a prime number}).$$

Note that $\phi(n)$ is recursive by Definition A.1.2, Lemma A.1.4, Corollary A.1.7 and Part 2 of this lemma.

4. Define $\rho(n, m) = \mu_{1 \leq z \leq m}(\phi(n)^{m-z}\mid m)$, where $\phi(n)$, as above, is the $n$-th prime in the ascending sequence of primes. Observe that $\rho(n, m)$ is computable by Lemmas A.1.4, A.1.8, A.1.9, A.1.10, and Parts 1 and 3 of this lemma.

5. For $n > 1$ define

$$\mu(n) = n - \mu_{0 \leq z < n + 1}(n - z \text{ is a prime number} \wedge (n - z)\mid n).$$

As above, $\mu(n)$ is computable by Lemmas A.1.4, A.1.8, A.1.9, A.1.10, Corollary A.1.7 and Parts 1 and 3 of this lemma.

6. For $n > 1$ define $\nu(n) = \sum_{i=2}^{n} \chi_{\text{primes}}(i)\chi(i, n)$, where for $i \geq 1$ we have that $\chi(i, n) = 1$ if $i \mid n$, and $\chi(i, n) = 0$ otherwise. Now $\nu(n)$ is computable by Lemmas A.1.4, A.1.8, A.1.9, A.1.10, and Parts 1, 2 of this lemma.

7. Let $g(n) = \chi_{\text{primes}}(n)\mu_{1 \leq k \leq n}(n = \phi(k))$. Then $g(n)$ is computable by Lemma A.1.4 and Part 2 of this lemma.

8. For $m \neq 0, n \neq 0$ define

$$(m, n) = (m + n) - \mu_{1 \leq k < m + n}([(m + n - k)\mid m] \wedge [(m + n - k)\mid n]).$$

Then $(m, n)$ is recursive by Lemmas A.1.4, A.1.8, A.1.9, A.1.10, Corollary A.1.7 and Part 1 of this lemma.
Since $m < n$ is equivalent to $m = \min(m, \Pr(n))$, the recursiveness of this relation follows from Lemma A.1.4 and Corollary A.1.6.

For $m \neq 0$ let $n \div m = \mu(q)([mq < n \vee mq = n] \wedge [n - mq < m])$. Then $n \div m$ is recursive by Lemmas A.1.4, A.1.8, A.1.9, A.1.10, Corollary A.1.7, and Part 9 of this lemma.

A.1.12 Lemma.

Let $G(X_1, \ldots, X_m)$ be a computable function. Then for any $A \in \mathbb{N}$,

$$G(X_1, \ldots, X_{i-1}, A, X_{i+1}, \ldots, X_m)$$

is computable.

Proof.

This lemma is easily proved by induction starting with basic functions.

Next we expand the definition of computable functions to functions whose range is the set of all the finite sequences of non-negative integers. To be more formal, let $\mathcal{N} = \bigcup_{i=1}^{\infty} \mathbb{N}^i$ and consider the following definition.

A.1.13 Definition.

Let $g : \mathbb{N} \to \mathcal{N}$ be such that the following conditions are satisfied.

- Let $h : \mathbb{N} \to \mathbb{N}$ be defined by $h(n) = \mu m(g(n) \in \mathbb{N}^m)$. Then $h$ is computable.

- For $n \in \mathbb{N}$, for $1 \leq i \leq h(n)$ let $f(i, n)$ be the $i$-th coordinate of $g(n)$. For $i > h(n)$, define $f(i, n) = f(i_0, n)$, where $1 \leq i_0 \leq h(n)$ and $i \equiv i_0 \mod h(n)$. Then $f(i, n)$ is computable.

Then call $g$ computable.

Given an expanded definition of computable functions, one can now state the following lemma whose proof we leave to the reader.
A.1.14 Lemma.

1. For \( n > 1 \) let \( \bar{F}(n, m) = (a_1, \ldots, a_m) \), where \( a_i \geq 0, n = p_1^{a_1} \cdots p_l^{a_l} \), and \( p_1 = 2 \leq \ldots \leq p_l \) is the listing of the first \( l \) prime numbers in order such that \( l \geq m \) and is as small as possible subject to this condition. Set \( \bar{F}(0, m) = 0, \bar{F}(1, m) = 1 \).

2. Let \( G_m: \mathbb{N}^m \rightarrow \mathbb{N} \) be defined by \( G_m(a_1, \ldots, a_m) = \prod_{i=1}^m p_i^{a_i} \), where \( p_1 = 2, \ldots, p_m \) are the first \( m \) prime numbers in order.

Then \( \bar{F} \) and \( G_m \) for all \( m \), are computable. Further,
\[
\bar{F}(G_m(a_1, \ldots, a_m), m) = (a_1, \ldots, a_m),
\]
and
\[
G_m \circ \bar{F}(n, m) = n,
\]
for all \( n \) whose largest prime factor is less or equal to \( p_m \).

A.2 Recursively Enumerable Sets.

We now define recursively or computably enumerable sets abbreviated as r.e. or c.e. sets.

A.2.1 Definition.

Let \( A \subseteq \mathbb{N}^k, k \in \mathbb{Z}_{>0} \). Then we will call \( A \) recursively or computably enumerable if it is empty or \( A \) is the range of some computable function.

Next we observe that it is not hard to show the following.

A.2.2 Lemma.

A recursive set is a c.e. set. Further, in the case of an infinite set it can be enumerated in strictly ascending order.

Proof.

If \( A \) is an empty recursive set, then it is a c.e. set by definition of c.e. sets. Now let \( A \) be a finite recursive set \( \{a_1 < \ldots < a_n\} \). For \( i \in \{1, \ldots, n\} \), let \( \chi_i \) be the characteristic function of the set \( \{m \in \mathbb{N} : m \equiv i \mod n\} \). Then \( \chi_i \)
is recursive by Proposition A.1.11. Next let $\xi_A(m) = \sum a_i \chi_i(m + 1)$. Then $\xi_A(m)$ is recursive by Corollary A.1.6 and lists $A$.

Suppose now that $A$ is an infinite recursive set with a computable characteristic function $\chi_A(n)$. We construct inductively a computable function $\xi_A(n)$ to list $A$ in the ascending order. Let $\xi_A(0) = \mu k(\chi_A(k) = 1)$. Let

$$\xi_A(n) = \mu k (k > \xi_A(n - 1) \land \chi_A(k) = 1).$$

Thus $\xi_A(n)$ is recursive by Corollary A.1.7 and lists $A$ in the ascending order.

The converse of Lemma A.2.2 is not true and its negation is the logical foundation for the proof of unsolvability of Hilbert’s Tenth Problem.

### A.2.3 Proposition.

There exist r.e. sets which are not recursive. (See [84], Section 1.9 for the proof.)

Further we have the following property of r.e. sets.

### A.2.4 Lemma.

Let $A \subset \mathbb{N}^k$ be an r.e. set. Let $a_1, \ldots, a_l \in \mathbb{N}$. Let $i_1, \ldots, i_l \in \{1, \ldots, k\}$. Then $B = \{(x_1, \ldots, x_k) \in A : x_{i_1} = a_1 \land \ldots \land x_{i_l} = a_l\}$ is also an r.e. set.

**Proof.**

We have to consider two cases: $B$ is finite, possibly empty, and $B$ is infinite. In the former case $B$ is recursive and therefore r.e. by Lemma A.2.2. In the latter case let $\xi_A : \mathbb{N} \rightarrow A$ be a recursive function listing $A$. Then define $\xi_B : \mathbb{N} \rightarrow B$ in the following manner.

$$\xi_B(0) = \xi_A(\mu s(\pi_{i_1}(\xi_A(s)) = a_1, \ldots, \pi_{i_l}(\xi_A(s)) = a_l)),$$

$$\xi_B(n) = \xi_A(\mu s (s \geq n \land \pi_{i_1}(\xi_A(s)) = a_1 \land \ldots \land \pi_{i_l}(\xi_A(s)) = a_l)),$$

where $\pi_i$, a projection on the $i$-th coordinate, is one of the basic functions from Definition A.1.2. As in many cases above, $\xi_B$ is recursive by Corollary A.1.7.
A.3 Turing and Partial Degrees.

We will now relativize the notion of computability and enumerability.

A.3.1 Definition.

Let \( A \subset \mathbb{N}^m, B \subset \mathbb{N}^l \) for some positive integers \( m \) and \( l \). Let \( \chi_B \) be the characteristic function of \( B \). Suppose that \( \chi_A \) – the characteristic function of \( A \), can be constructed from the basic functions and \( \chi_B \) by finite number of applications of composition, induction and minimization. Then we will say that \( A \) is Turing reducible to \( B \) and write \( A \leq_T B \).

A.3.2 Definition.

Let \( A \subset \mathbb{N}^m, B \subset \mathbb{N}^l \) for some positive integers \( m \) and \( l \). Suppose also that for any function \( \tilde{f} : \mathbb{N} \rightarrow B \) enumerating \( B \), there exists a function \( \tilde{g} : \mathbb{N} \rightarrow A \) enumerating \( A \), constructed from the basic functions and \( \tilde{f} \) by finite number of applications of composition, induction and minimization. Then we will say that \( A \) is enumerably reducible to \( B \) and write \( A \leq_e B \).

It is clear that both Turing reducibility and enumeration reducibility are transitive and reflexive and therefore can be used to form equivalence relations. The equivalence classes corresponding to Turing reducibility are called Turing degrees while the classes corresponding to enumeration reducibility are called partial degrees. We should also note here that neither reducibility implies the other. See Section 9.7 of [84] for more information on the matter.

A.3.3 Proposition.

There exist infinitely many partial degrees.

Proof.

Suppose there were finitely many partial degrees only. Let \( A_1, \ldots, A_n \) be sets representing each of these degrees and let \( \xi_1, \ldots, \xi_n \) be functions listing \( A_1, \ldots, A_n \) respectively. Consider all the functions that can be constructed from \( \xi_1, \ldots, \xi_n \) using rules described in Definition A.1.2. Then there are only countably many of these functions. Let \( \{f_i, i \in \mathbb{N}\} \) be a listing of all such functions. Let \( \xi(n) = f_n(n) + 1 \). Then \( \xi(n) \) is not on the list and thus cannot be constructed from \( \xi_1, \ldots, \xi_n \) using rules from Definition A.1.2. Thus, \( \xi(n) \) is listing a set that is not relatively enumerable with respect to any of \( A_i \)'s.
Consequently, this set cannot belong to the same partial degree as any of $A_i$’s.

### A.4 Degrees of Sets of Indices, Primes and Products.

Given these definitions of Turing and enumeration reducibilities we now obtain the following proposition.

#### A.4.1 Proposition.

Let $A \subset \mathbb{Z}_{>0}$ and let $p_i$ be the $i$-th prime number in the ascending list of all prime numbers. Finally, let

$$\mathcal{P} = \{n \in \mathbb{N} | \exists i \in A, n = p_i\}.$$ 

Then $A$ and $P$ are Turing and enumeration equivalent.

**Proof.**

Without loss of generality we can assume that both sets are not empty. Next let $g(n)$ be a recursive function defined in Proposition A.1.11. Then we can set $\chi_{\mathcal{P}}(m) = \chi_A(g(m))$, since $0 \notin A$. Further, $\chi_A(n) = \chi_{\mathcal{P}}(\phi(n))$, where $\phi(n) = p_n$, is also a recursive function defined in Proposition A.1.11. Thus $P \equiv_T A$.

Now let $\xi_A(n)$ be the function enumerating $A$. Then $\phi(\xi_A(n))$ will produce an effective listing of $\mathcal{P}$. Conversely, let $\xi_{\mathcal{P}}(n)$ be a function listing $\mathcal{P}$. Then $g(\xi_{\mathcal{P}}(n))$ will list $A$. Consequently, $\mathcal{P} \equiv_e A$.

We will now relate sets of primes to sets of their products.

#### A.4.2 Proposition.

Let $\mathcal{P}$ be a set of prime numbers. Let $U$ consist of all the finite products of elements of $\mathcal{P}$. Then $U \equiv_T \mathcal{P}$ and $U \equiv_e \mathcal{P}$.

**Proof.**

First of all, without loss of generality we can assume that both sets are not empty. Next let the functions $\mu(m)$, $g(m)$, $\rho(n, m)$, $\phi(n)$, and $\mu(m)$, be
defined as in Proposition A.1.11, and let the function $\text{sgn}(x)$ be defined as in Proposition A.1.4. Now consider the following function:

$$\chi_U(m) = \frac{g(\mu(m))}{\prod_{i=1}^{\rho(1,m)} (\chi_P(\phi(i))\text{sgn}(\rho(i,m)) + (1 - \text{sgn}(\rho(i,m))))}$$ \hspace{1cm} (A.4.1)

Suppose that all the factors of $m$ are elements of $\mathcal{P}$. Then for each term in the product one of the following statements will be true:

1. $\phi(i)$ occurs in the factorization of $m$ with a non-zero exponent and therefore, by assumption, $\phi(i) \in \mathcal{P}$. Then $\rho(i,m) > 0$, $\text{sgn}(\rho(i,m)) = 1$, $\chi_P(\phi(i))\text{sgn}(\rho(i,m)) = 1$, $1 - \text{sgn}(\rho(i,m)) = 0$.

2. $\phi(i)$ does not occur in the factorization of $m$. Then $\rho(i,m) = 0$, $\text{sgn}(\rho(i,m)) = 0$, $\chi_P(\phi(i))\text{sgn}(\rho(i,m)) = 0$, and $1 - \text{sgn}(\rho(i,m)) = 1$.

Thus in either case, each term in the product is equal to one and $\chi_U(m) = 1$.

Suppose now that for some $j \in \mathbb{N}^+$, the prime $p_j$ occurs with a non-zero exponent in the factorization of $m$, while $\chi_P(p_j) = 0$. In this case $j \leq g(\mu(m))$ and thus the product contains a term with $i = j$. Note that in this case $\rho(j,m) > 0$, $\text{sgn}(\rho(j,m)) = 1$, $\chi_P(p_j)\text{sgn}(\rho(j,m)) = 0$, while at the same time $1 - \text{sgn}(\rho(j,m)) = 0$. Thus the $j$-th term in the product is equal to zero and therefore the product is equal to zero. Hence, the function $\chi_U(m)$ defined in (A.4.1) is actually the characteristic function of $U$ and we conclude that $U \leq T_A$.

Conversely, let $\chi_{\text{primes}}(m)$ be, as before, the characteristic function of the set of all prime numbers. Then, by Proposition A.1.11, $\chi_{\text{primes}}(m)$ is a recursive function. Hence, it is not difficult to see that $\chi_A(m) = \chi_U(m)\chi_{\text{primes}}(m)$.

Now let $\xi_{\mathcal{P}}(n)$ be any function listing $\mathcal{P}$. Then let

$$\xi_U(m) = \prod_{i=1}^{\rho(1,m) - 1} \xi_{\mathcal{P}}(i)^{\rho(i+1,m)}.$$ 

As $m$ runs through $\mathbb{N}$, we have that $(\rho(2,m), \ldots, \rho(1,m) + 1, m))$ runs through all the finite sequences of natural numbers. Indeed, let $(a_1, \ldots, a_l)$ be a finite sequence. Then if we let $m = 2^l \prod_{i=2}^{l+1} p_i^{a_i - 1}$, we see that

$$(\rho(2,m), \ldots, \rho(1,m) + 1, m)) = (a_1, \ldots, a_l).$$

Thus, $\xi_U(m)$ will run through all the elements of $U$. Consequently, $U \leq_e \mathcal{P}$.

Conversely, let $\xi_U(n)$ be any function listing elements of $U$ and let $p_0 \in \mathcal{P}$. Then let $\xi_{\mathcal{P}}(m) = \xi_U(m)\chi_{\text{primes}}(m) + p_0(1 - \chi_{\text{primes}}(m))$ and we can conclude that $\mathcal{P} \leq_e U$. 

249
A.5  Computable Algebra.

In this section we will extend the notions of recursive sets and functions to algebraic objects.

A.5.1  Definition.

Let $\mathbb{R}$ be a countable ring (field). Let $J : \mathbb{R} \rightarrow \mathbb{N}$ be an injective function such that $J(\mathbb{R})$ is recursive and the functions translating addition, multiplication, and subtraction are recursive (in case of a field, division is also translated by a recursive function). Then $J$ will be called a recursive presentation of $\mathbb{R}$.

Let $A \subseteq \mathbb{R}$. Then $A$ will be called recursive (r.e) if $J(A)$ is recursive (r.e.) under some recursive presentation of $\mathbb{R}$. Similarly for $A, B \subseteq \mathbb{R}$, we will say that $A \cong_T B$ ($A \cong_e B$) if $J(A) \cong_T J(B)$ ($J(A) \cong_e J(B)$) under some recursive presentation $J$ of $\mathbb{R}$.

Let $f : \mathbb{R}^n \rightarrow \mathbb{R}$ be a function. Then $f$ will be called recursive if under some recursive presentation of $\mathbb{R}$, the translation of $f$ is recursive.

A.5.2  Proposition.

Let $\mathbb{R}, J$ be as in Definition A.5.1. Then translations of all polynomial functions in case $\mathbb{R}$ is a ring, and the translation of all rational functions in case $\mathbb{R}$ is a field are recursive.

Proof.

The proof of this proposition is analogous to the proof of Proposition 3.2.2.

A.6  Recursive Presentation of $\mathbb{Q}$.

In this section we will describe a recursive presentation of $\mathbb{Q}$ in some detail. We will start with a presentation of $\mathbb{Z}$ though.

A.6.1  Proposition.

Consider the following map $J : \mathbb{Z} \rightarrow \mathbb{N}$ defined by $J(m) = 2^a3^{|m|}$, where $a = 0$ if $m \geq 0$ and $a = 1$ otherwise. Then the following statements are true:

1. $J$ is a recursive presentation of $\mathbb{Z}$.

2. For any $A \subseteq \mathbb{N}$ we have that $J(A) \equiv_T A$ and $J(A) \equiv_e A$. 

250
3. The absolute value function is a recursive function on \( \mathbb{Z} \).

4. Let \( A \subset \mathbb{N} \). Let \( B \subset \mathbb{Z} \) be defined by \( B = \{ x \in \mathbb{Z} \mid |x| \in A \} \). Then \( J(B) \equiv_T J(A) \) and \( J(B) \equiv_e J(A) \).

**Proof.**

1. First of all, the Unique Factorization Theorem assures us that \( J \) is injective. To see that \( J(\mathbb{Z}) \) is a recursive subset of \( \mathbb{N} \), note that

\[
J(\mathbb{Z}) = \{ m \in \mathbb{N} : m = 1 \lor [(4 \nmid m) \land (\mu(m) = 3)]\},
\] (A.6.1)

where \( \mu(m) \) is a function defined in Proposition A.1.11. In other words we can describe an element of \( J(\mathbb{Z}) \) in the following manner: either it is equal to 1 or it is a natural number not divisible by 4, and 3 is the largest prime dividing it. Using propositions from Section A.1 we easily deduce that (A.6.1) is a recursive set.

Next we need to show that addition, subtraction and multiplication are recursive under \( J \). Let

\[
A_{o,o}, A_{o,e}, A_{e,o}, A_{e,e}, A_{o,e,1}, A_{o,e,2}, A_{e,o,1}, A_{e,o,2} \subset \mathbb{N}^2
\]

be defined as follows.

\[
A_{o,o} = \{ (m,n), \ 2 \nmid m, 2 \nmid n \},
\]  
\[
A_{e,e} = \{ (m,n), \ 2 \mid m, 2 \mid n \},
\]  
\[
A_{o,e} = \{ (m,n), \ 2 \nmid m, 2 \mid n \},
\]  
\[
A_{e,o} = \{ (m,n), \ 2 \mid m, 2 \nmid n \},
\]  
\[
A_{o,e,1} = \{ (m,n) \in A_{o,e}, 2m \geq n \},
\]  
\[
A_{o,e,2} = \{ (m,n) \in A_{o,e}, 2m < n \},
\]  
\[
A_{e,o,1} = \{ (m,n) \in A_{e,o}, m > 2n \},
\]  
\[
A_{e,o,2} = \{ (m,n) \in A_{e,o}, m \leq 2n \}.
\]

Using Section A.1 again, we conclude that these sets are recursive. Further, it is easy to see that

\[
\{ A_{o,o}, A_{e,e}, A_{o,e,1}, A_{o,e,2}, A_{e,o,1}, A_{e,o,2} \}
\]
is a partition of \( \mathbb{N}^2 \). Therefore Corollary A.1.9 tells us that we can define the following recursive function:

\[
P_+(m, n) = \begin{cases} 
2 \cdot 3^{\rho(2, m) + \rho(2, n)}, & \text{if } (m, n) \in A_{e,e}, \\
3^{\rho(2, m) + \rho(2, n)}, & \text{if } (m, n) \in A_{o,o}, \\
3^{\rho(2, m) - \rho(2, n)}, & \text{if } (m, n) \in A_{o,e,1} \cup A_{e,o,2}, \\
2 \cdot 3^{\rho(2, m) - \rho(2, n)}, & \text{if } (m, n) \in A_{e,o,1} \cup A_{o,e,2}. 
\end{cases}
\]

where \( \rho(2, n) \) is the exponent of 3 in the prime factorization of \( n \). It is clear that \( J(x + y) = P_+(J(x), J(y)) \). Next let

\[
\text{Minus}(m) = \begin{cases} 
2m, & \text{if } 2 \nmid m, \\
m/2 & \text{if } 2|m.
\end{cases}
\]

Then \( \text{Minus}(m) \) is a recursive function by Section A.1. Also, by construction, \( \text{Minus}(J(x)) = J(-x) \). Now define \( P_x \) by

\[
P_x(m, n) = \begin{cases} 
3^{\rho(2, m) + \rho(2, n)}, & \text{if } (m, n) \in A_{e,e} \cup A_{o,o}, \\
2 \cdot 3^{\rho(2, m) + \rho(2, n)}, & \text{if } (m, n) \in A_{o,e,1} \cup A_{e,o,2},
\end{cases}
\]

By the same considerations as above, it is clear that \( P_x \) is a recursive function and, by construction,

\[
P_x(J(x), J(y)) = J(xy)
\]

for \( x, y \in \mathbb{Z} \). Thus, the first assertion of the proposition holds.

2. Next we note that \( J(\mathbb{N}) = \{ m \in \mathbb{N} : (m = 1) \lor [(2 \nmid m) \land (\mu(m) = 3)] \} \)

and, therefore, \( J(\mathbb{N}) \) is recursive.

Now let \( A \subseteq \mathbb{N} \) and let \( \chi_A \) be a characteristic function of \( A \subseteq \mathbb{N} \). Also let \( \chi_{J(A)} \) be the characteristic function of \( J(\mathbb{N}) \) and observe that it is recursive by the argument above. Then \( \chi_{J(A)}(n) = \chi_{J(\mathbb{N})}(n) \chi_A(\rho(2, n)) \). Conversely, if \( \chi_{J(A)} \) is the characteristic function of \( J(A) \), then \( \chi(A)(n) = \chi_{J(A)}(3^n) \). Further, let \( \xi_A(n) \) be a function listing \( A \), then \( \xi_{J(A)} = 3^{\xi_A(n)} \) will list \( J(A) \). Conversely, let \( \xi_{J(A)}(n) \) be a function listing \( J(A) \). Then \( \rho(2, \xi_{J(A)}(n)) \) will list \( A \).

3. Let \( J(x) = n \). We set \( \text{abs}(n) = 3^{\rho(2, n)} \). Note that \( \text{abs}(n) \) is a recursive function by Section A.1, and it is clear that \( \text{abs}(J(x)) = J(|x|) \).

4. Here we note that

\[
\chi_{J(B)}(n) = \chi_{J(A)}(\text{abs}(n))
\]

252
\[ \chi_{J(A)}(n) = \chi_{J(B)}(n) \chi_{J(N)}(n), \]

where \( \chi_{J(A)}, \chi_{J(B)}, \chi_{J(N)} \) are the characteristic functions of \( J(A), J(B), \) and \( J(N) \) respectively. Thus we have Turing equivalence.

Now let \( \xi_{J(A)}(n) \) be a function listing \( J(A) \). Then define \( \xi_{J(B)}(2m) = \xi_{J(A)}(m) \) and \( \xi_{J(B)}(2m+1) = 2\xi_{J(A)}(m) \). Using Section A.1 we can ascertain that \( \xi_{J(B)}(n) \) can be constructed from \( \xi_{J(A)}(n) \) and basic functions by the rules stipulated in Definition A.1.2. Finally, given a function \( \xi_{J(B)}(n) \) enumerating \( J(B) \), we can obtain \( \xi_{J(A)}(n) \) – a function enumerating \( J(A) \), by setting \( \xi_{J(A)}(n) = \text{abs}(\xi_{J(B)}(n)) \).

We now expand our recursive presentation to \( \mathbb{Q} \).

**A.6.2 Definition.**

Define \( J_Q : \mathbb{Q} \rightarrow \mathbb{N} \) as follows. For \( m \in \mathbb{Z} \setminus \{0\}, n \in \mathbb{N} \setminus \{0\}, (m, n) = 1 \), set \( J_Q(m/n) = J(m) \cdot 5^{n-1} \). Also set \( J_Q(0) = J(0) = 1 \).

**A.6.3 Proposition.**

\( J_Q \) is a recursive presentation of \( \mathbb{Q} \) extending the map \( J : \mathbb{Z} \rightarrow \mathbb{N} \) defined in Proposition A.6.1.

**Proof.**

First of all we note that \( J_Q \) is injective by the Fundamental Theorem of Arithmetic. The fact that \( J_Q \) extends \( J \) from A.6.1 is clear since \( J_Q(m/1) = J(m) \).

Next observe that

\[ J_Q(\mathbb{Q}) = \{ m \in \mathbb{N} : (m = 1) \lor [(3 \mid m) \land (4 \nmid m) \land (\mu(m) \leq 5)] \} \]

and this set is recursive by propositions from Section A.1 as before.

Next we need to show that the field operations are also recursive. We will start with functions that can produce the reduced numerator and denominator of an element of \( \mathbb{Z} \). Define recursive functions

\[ \text{Num}(n) = 2^{\rho(1,n)}3^{\rho(2,n)} \]

and

\[ \text{Denom}(n) = 3^{\rho(3,n)+1}. \]
Note that the image of both functions is clearly in $J(\mathbb{Z})$ and if $n \in J_Q(\mathbb{Q})$ then

$$J_Q(J^{-1}(\text{Num}(n))/J^{-1}(\text{Denom}(n))) = n.$$  

Further, observe that for $m \in J_Q(\mathbb{Q})$ we have that $m \leq 2 \cdot 5^{\rho(2, N) + \rho(2, D)}$, where $N = \text{Num}(m), D = \text{Denom}(m)$. Now given $n_1, n_2$, let

$$N_+ = \text{Num}_+(n_1, n_2) = P_+(P_x(\text{Num}(n_1), \text{Denom}(n_2)), P_x(\text{Num}(n_2), \text{Denom}(n_1))).$$  

Let

$$D_+ = \text{Denom}_+(n_1, n_2) = P_x(\text{Denom}(n_1), \text{Denom}(n_2)).$$

Here $P_+, P_x$ are translations of addition and multiplication under $J$. Next let

$$P_{+,Q}(n_1, n_2) = \mu_{1 \leq m \leq 2 \cdot 5^{\rho(2, N_+) + \rho(2, D_+)}}(m \in J_Q(\mathbb{Q}) \land P_x(N_+, \text{Denom}(m)) = P_x(D_+, \text{Num}(m))).$$

Next let

$$\text{Minus}_Q(n) = 2^{\rho(1, \text{Minus}(\text{Num}(n)))}3^{\rho(2, n)}5^{\rho(3, n)}.$$  

Let

$$N_x = \text{Num}_x(n_1, n_2) = P_x(\text{Num}(n_1), \text{Num}(n_2)),$$  

let

$$D_x = \text{Denom}_x(n_1, n_2) = P_x(\text{Denom}(n_1), \text{Denom}(n_2)).$$

Let

$$P_{x,Q}(n_1, n_2) = \mu_{1 \leq m \leq 2 \cdot 5^{\rho(2, N_x) + \rho(2, D_x)}}(m \in J_Q(\mathbb{Q}) \land P_x(N_x, \text{Denom}(m)) = P_x(D_x, \text{Num}(m))).$$

Our last task is to define the reciprocals. Define

$$\text{Oneover}(n) = 2^{\rho(1, n)}3^{\rho(3, n)}15^{\rho(2, n)-1},$$

and note that for $n \in J_Q(\mathbb{Q})$ we always have that $\rho(2, n) \geq 1$ since $3 | n$.

We can now continue the discussion we started with Propositions A.4.1 and Proposition A.4.2.

**A.6.4 Proposition.**

Let $I \subseteq \mathbb{N}$. Let $\mathcal{A}_I = \{p_i, i \in I\}$. Let $U_I$ be the set of natural numbers with prime factors in $\mathcal{A}_I$. Then $J_Q(O_Q, U_I) \cong_e I$ and $J_Q(O_Q, U_I) \cong_T I$. 

254
Proof.

Since \( U_i \cong_T \emptyset_i \cong_T I \) and \( U_i \cong_e \emptyset_i \cong_e I \) by Propositions A.4.1 and A.4.2, it is enough to show that \( U_i \) is Turing and enumeration equivalent to \( O_{Q,U_i} \). Let \( \chi_U \) be the characteristic function of \( U_i \). Then \( \chi_{O_{Q,U_i}}(n) = \chi_U(\rho(3,n) - 1) \) is the characteristic function of \( J_Q(O_{Q,U_i}) \). Conversely, let \( \chi_{J_Q(O_{Q,U_i})}(n) \) be the characteristic function of \( J_Q(O_{Q,U_i}) \). Then \( \chi_U(n) = \chi_{J_Q(O_{Q,U_i})}(3 \cdot 5^{n-1}) \).

One of the most important properties of the recursive presentation above is that it preserves all the Turing and enumeration degrees of subsets of \( N \). This fact is not accidental. As a matter of fact, this will be true of any recursive presentation of \( \mathbb{Z} \) and \( \mathbb{Q} \). Since this fact will play an important role in our discussion of undecidability of HTP, we prove below that a general version of this phenomenon holds.

A.6.5 Proposition.

Let \( R \) (\( F \)) be a finitely generated ring (field). For \( i = 1, 2 \), let \( J_i : R \rightarrow \mathbb{N} \) (\( J_i : F \rightarrow \mathbb{N} \)) be two recursive presentations of \( R \) (\( F \)). Then there exists a computable function \( g : \mathbb{N} \rightarrow \mathbb{N} \) such that \( g \circ J_1 = J_2 \).

Proof.

We will sketch a proof for the case of a finitely generated ring of characteristic 0. The positive characteristic case and the case of a finitely generated field are similar. Let \( x_1, \ldots, x_n \) be a set of generators of \( R \). Let \( m \in J_1(R) \) be given. Then by systematically iterating ring operations on \( x_1, \ldots, x_n \) we will construct a polynomial \( f(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n] \) such that \( J_1(f)(J_1(x_1), \ldots, J_1(x_n)) = m \). Then we can set

\[
g(m) = J_2(f)(J_2(x_1), \ldots, J_2(x_n)).
\]

If we apply Proposition A.6.5 to \( R = \mathbb{Z} \) and \( F = \mathbb{Q} \), we obtain the following.

A.6.6 Corollary.

Let \( J : \mathbb{Z} \rightarrow \mathbb{N} \) be a recursive presentation of \( \mathbb{Z} \). Then for any subset \( A \subset \mathbb{N} \), \( A \equiv_T J(A) \) and \( A \equiv_e J(A) \). Further under any recursive presentation \( J \) of \( \mathbb{Q} \), we have that \( J(\mathbb{Z}) \) is recursive.
A.7 Recursive Presentation of Other Fields.

Having dealt in great detail with a recursive presentation of \( \mathbb{Q} \) we will present a more abbreviated account of a construction of recursive presentations of other fields.

A.7.1 Proposition.

Let \( F \) be a countable field, let \( j : F \to \mathbb{N} \) be a recursive presentation of \( F \). Let \( t \) be transcendental over \( F \). Then there exists a recursive presentation \( J : F[t] \to \mathbb{N} \) such that \( J|_F = \psi \circ j \), where \( \psi : \mathbb{N} \to \mathbb{N} \) is recursive. Further, under \( J \), there exist the following recursive functions:

- \( \text{deg} : \mathbb{N} \to \mathbb{N} \) such that for any \( P(t) \in F[t] \), we have that \( \text{deg} \circ J(P(t)) = \text{deg}(P(t)) \).
- \( C : \mathbb{N} \times \mathbb{N} \to \mathbb{N} \) such that for any \( a_0, \ldots, a_n \in F \), we have that \( C(J(\sum_{i=0}^{n} a_i t^i))(a_m) = J(a_m) \), where \( a_m = 0 \) for \( m > \text{deg}(\sum_{i=0}^{n} a_i t^i) \).
- \( \text{GCD} : \mathbb{N} \times \mathbb{N} \to \mathbb{N} \), where for any \( P_1(t), P_2(t) \in F[t] \), we have that \( \text{GCD}(J(P_1(t)), J(P_2(t))) = J((P_1(t), P_2(t))) \).

Proof.

Let \( P(t) = \sum_{i=0}^{n} a_i t^i \in F[t] \). Then define \( J(t) = \prod_{i=0}^{n} p_i^{\text{deg}(a_i)} \), where \( p_1 = 2 < p_2 < \ldots < p_{n+1} \) are the first \( n + 1 \) rational primes. By Proposition A.1.11, since \( j(F) \) is recursive, \( J(F[t]) \) is a recursive set and functions \( \text{deg} \) and \( C \) are computable. Defining ring operations and the greatest common divisor of two polynomials is a straightforward but rather tedious process requiring use of Proposition A.1.11 again and again. We will leave the details as an exercise for an interested reader.

A.7.2 Corollary.

Let \( F \) be a countable field, let \( j : F \to \mathbb{N} \) be a recursive presentation of \( F \). Let \( t \) be transcendental over \( F \). Then there exists a recursive presentation \( \bar{J} : F(t) \to \mathbb{N} \) such that \( \bar{J}|_F = \psi \circ j \), where \( \psi : \mathbb{N} \to \mathbb{N} \) is recursive. Further, under \( \bar{J} \), there exist the following recursive functions: \( \text{Num} : \mathbb{N} \to \mathbb{N} \), \( \text{Denom} : \mathbb{N} \to \mathbb{N} \) such that for any \( f \in F(t) \) we have that

- \( \bar{J}^{-1}(\text{Num}(\bar{J}(f))), \bar{J}^{-1}(\text{Denom}(\bar{J}(f))) \in F[t] \).
- \( \bar{J}^{-1}(\text{Denom}(\bar{J}(f))) \) is monic.
Proof.

Let \( f \in F(t) \), then \( f \) has a unique representation as \( P(t)/Q(t) \) where \( P(t), Q(t) \in F[t] \), are relatively prime in the polynomial ring, and \( Q(t) \neq 0 \) is monic. Thus, we can define \( \bar{J}(f) = 2^{J(P(t))}3^{J(Q(t))} \), where \( J \) is the presentation of \( F[t] \) defined in Proposition A.7.1. Again, we leave the straightforward but lengthy proof that the resulting presentation satisfies all the conditions stated in the corollary to the interested reader.

We will next prove a general proposition about constructing a recursive presentation of a fraction field, given a recursive presentation of a ring. First we need a new definition.

A.7.3 Definition.

Let \( R \) be a countable ring. We will call \( R \) strongly recursive if \( R \) is recursive and under some recursive presentation of \( R \) we have that the set \( D = \{(x, y) : \exists z \in R, x = yz\} \) is recursive. Such a presentation of \( R \) will also be called strongly recursive. (Observe that \( D \) is a Diophantine subset of \( R^2 \).

By virtue of the division algorithm, it is clear that \( \mathbb{Z} \) and any polynomial ring over a recursive field are strongly recursive. This property is in general enough for construction of a recursive presentation of the fraction field while preserving recursive status of the ring.

A.7.4 Proposition.

Let \( R \) be a recursive ring under a presentation \( j \). Let \( F \) be its fraction field. Then there exists a recursive presentation \( J \) of \( F \) such that \( J(R) \) is also recursive if and only if \( R \) is strongly recursive. Further, if \( R \) is strongly recursive then under some recursive presentation \( J \) of its fraction field \( F \) there exist recursive functions \( \Lambda_1, \Lambda_2 : \mathbb{N} \rightarrow \mathbb{N} \) such that for all \( x \in F \)
\[
x = \frac{J^{-1}(\Lambda_1(J(x)))}{J^{-1}(\Lambda_2(J(x)))}, \Lambda_1(J(x)), \Lambda_2(J(x)) \in J(R), \Lambda_2(J(x)) \neq 0.
\]
Proof.

We will first show that if $R$ is strongly recursive then the required presentation of $F$ exists. The construction we present here is in some sense the usual construction of the fraction field of the ring using the equivalence classes of fractions. To simplify the discussion, instead of constructing a map $J : F \rightarrow \mathbb{N}$, we will construct a map $J : F \rightarrow \mathbb{N}^2$ satisfying all the requirements. We remind the reader that we can always move back and forth from $\mathbb{N}^k$ to $\mathbb{N}$ via recursive functions with recursive inverses using Lemma A.1.14.

So let $\phi : \mathbb{N} \rightarrow j(R)^2$ be a recursive listing of $j(R)^2$. (It exists by Lemma A.2.2 and Lemma A.1.8.) We will denote $\phi(n)$ by $(a_n, b_n)$. Below we list steps that will result in construction of $J$. We will define a recursive function $H : \mathbb{N} \rightarrow j(R^2)$ which essentially will be the presentation of $F$.

1. Let $H(1) = (a_1, b_1)$.

2. Assume $H(1), \ldots, H(n)$ have already been defined. If $b_{n+1} = j(0)$ then set $H(n+1) = (j(0), j(0))$. Otherwise check if for some $i = 1, \ldots, n$, we have that $P_x(a_i, b_{n+1}) = P_x(a_n b_i)$, where $P_x$ is, as usual, the translation of multiplication over $R$ under $j$. If such an $i$ is found, then set $H(n+1) = H(i)$. If such an $i$ is not found then check whether $(a_n, b_n) \in j(D)$. If this is the case, then find $c$ such that $P_x(c, b_n) = a_n$ and set $H(n) = (c, j(1))$. Finally, if $(a_n, b_n) \notin j(D)$ set $H(n+1) = (a_{n+1}, b_{n+1})$.

We claim that $H$ is recursive (by the construction above) and there exists a map $J : F \rightarrow H(\mathbb{N})$ such that $J$ is a recursive presentation of $F$. Let $z \in F$. Then $z = x/y, y \neq 0, x, y \in R$. Let $(a_n, b_n) = (j(x), j(y))$. Then define $J(z) = H(n)$. Construction above implies that $J$ is well-defined. (We leave the details of the proof of this claim to the reader.) Next observe that $J(R)$ is recursive. Indeed, given $(m, k) \in \mathbb{N}^2$, we can determine effectively whether $(m, k) \in J(R)$. First of all we determine whether $(m, k) \in j(R)^2$ and if so determine $n \in \mathbb{N}$ such that $(m, k) = (a_n b_n)$. If $(m, k) \notin j(R)^2$, then $(m, k) \notin J(F)$. Next we compute $H(n)$ and check whether $H(n) = (m, k)$. If the answer is “yes” and $k \neq j(0)$, then $(m, k) \in J(F)$, and the answer is “no” otherwise. Further, note that $J(R)$ is also recursive. Indeed, given a pair $(m, k) \in J(F)$, it is enough to check whether $k = j(1)$ to determine whether $(m, k) \in J(R)$. Also, by construction, for each $z \in F$, we have $J(z) = (\Lambda_1(J(z)), \Lambda_2(J(z)))$.

Next we need to show that all the operations over $F$ are recursive. We will show that this is true for addition and the reader can produce analogous proofs for the remaining field operations. Given $(m_1, k_1), (m_2, k_2)$, do the the
following to compute the sum. Let

\[ I = P_+(P_x(m_1, k_2), P_x(m_2, k_1)), u = P_x(k_1, k_2), \]

where \( P_+, P_x \) are the translation of addition and multiplication over \( R \) under \( j \). Note that \((I, u) \in j(R)^2\). So we can find \( n \) such that \((a_n, b_n) = (I, u)\). Then set the sum of \((m_1, k_1)\) and \((m_2, k_2)\) to be \( H(n)\).

Suppose now that \( R \) is an arbitrary recursive ring and there exists a recursive presentation \( J : F \rightarrow \mathbb{N} \) such that \( J(R) \) is recursive. Then let \((m, k) \in J(R)^2\). We can determine whether \((m, k) \in J(D)\) by checking whether \( P/(m, k) \in J(R)\).

### A.7.5 Remark.

In the proof above we presented the algorithm informally. We remind the reader that informal descriptions of algorithms and their relation to the formal descriptions of algorithms are discussed immediately following Definition A.1.2.

### A.7.6 Remark.

While the proposition above plays a role in tying together generation and Diophantine undecidability, it, in general, does not provide enough information about the recursive presentation of the fraction field. For this reason we chose to construct the recursive presentations of rational numbers and rational functions directly.

Our next task is to discuss a presentation of finite field extensions.

### A.7.7 Proposition.

Let \( F \) be a countable field, let \( j : F \rightarrow \mathbb{N} \) be a recursive presentation of \( F \). Let \( G \) be a finite extension of \( F \) of degree \( n \). Let \( \Omega = \{\omega_1, \ldots, \omega_n\} \) be a basis of \( G \) over \( F \). Then there exists a recursive presentation \( J : G \rightarrow \mathbb{N} \) such that \( J \) restricted to \( F \) is equal to \( \psi \circ j \), where \( \psi : \mathbb{N} \rightarrow \mathbb{N} \) is recursive, and there exist recursive coordinate functions \( C_1, \ldots, C_n : \mathbb{N} \rightarrow \mathbb{N} \) such that for any element \( x \in G \), we have that \( x = \sum_{i=1}^{n} J^{-1}(C_i \circ J(x))\omega_i \), and \( C_i \circ J(x) \in J(F) \) for all \( i = 1, \ldots, n \).
Proof.
This proposition can be proved utilizing a construction we used to extend weak presentations in Proposition 3.2.4.

As an immediate corollary of Proposition A.6.3, Corollary A.7.2 and Proposition A.7.7, we get the following result.

A.7.8 Corollary.
Global fields are recursive.

A.7.9 Remark.
From now on we will assume that number fields are given under a recursive presentation $J$ described in Proposition A.7.7 with respect to some integral basis $\Omega$ of the field over $\mathbb{Q}$. (Such a basis always exists. See Definition B.1.29 and Proposition B.1.30.)

Proposition A.7.7 has another useful corollary.

A.7.10 Corollary.
Let $F, G, J$ be as in Proposition A.7.7. Given $x \in F$, let $A_0(x), \ldots, A_n(x)$ be the coefficients of the characteristic polynomial of $x$ over $G$. Then each $A_i(x)$ is a computable function under $J$, depending on the chosen basis of $F$ over $G$ only.

Proof.
Indeed, let $x \in G, x = \sum_{i=1}^{n} a_i \omega_i$, where $\Omega = \{\omega_1, \ldots, \omega_n\}$. Then for each $i$, we have that $A_i(x)$ is a fixed polynomial in $a_1, \ldots, a_n$. Since $J(a_i) = C_i(J(x))$, where $C_i$ are recursive functions defined in Proposition A.7.7 and all the polynomial functions are translated by recursive functions by Proposition A.5.2, the assertion holds.

We will now deal with a case of countable transcendence degree.
A.7.11 Proposition.

Let \( F \) be a countable field, let \( j : F \to \mathbb{N} \) be a recursive presentation of \( F \). Let \( \{ t_i, i \in \mathbb{N} \} \) be a set of variables algebraically independent over \( F \). Then \( F(t_1, \ldots, t_k, \ldots) \) also has a recursive presentation.

Proof.

We will describe the encoding and we will leave it to the reader to prove that the resulting presentation is recursive. Let \( f = \frac{P}{Q} \), where

\[
P = \sum_{(i_1, \ldots, i_k)} A_{i_1, \ldots, i_k} t_1^{i_1} \cdots t_k^{i_k},
\]

\[
Q = \sum_{(i_1, \ldots, i_k)} A_{i_1, \ldots, i_k} t_1^{i_1} \cdots t_s^{i_s},
\]

where \((P, Q)\) are relatively prime in the polynomial ring \( F[t_1, \ldots] \). Assume that if we sort the terms of \( Q \) in a lexicographical order using powers of \( t_i \)'s, then the first term has coefficient 1. Clearly, every element of the field has a unique representation of this form. For a monomial \( A_{i_1, \ldots, i_k} t_1^{i_1} \cdots t_k^{i_k} \), let

\[
J_1(A_{i_1, \ldots, i_k} t_1^{i_1} \cdots t_k^{i_k}) = 2^{i(A_{i_1, \ldots, i_k})} 3^{i_1} \cdots p_{k+1}^{i_k}.
\]

For a polynomial \( P = \sum_{r=1}^u M_r \), where \( M_r \) is a monomial, let \( J_2(P) = \prod_{r=1}^u p_r^{J(M_r)} \). Finally, let \( J(f) = 2^{J_2(P)} 3^{J_2(Q)} \).

A.7.12 Proposition.

Let \( K \) be a recursive field. Then there exists an algebraic closure of \( K \) which is recursive. (See [[78], Theorem 7.])

A.7.13 Proposition.

Let \( G \) be a countable field. Then \( G \) is a subfield of a recursive field.

Proof.

We have to consider two possibilities: \( G \) has characteristic 0 or \( G \) has positive characteristic. First assume \( G \) has characteristic 0. Then \( G \) contains \( \mathbb{Q} \) and consequently \( G \) is a subfield of the algebraic closure of \( \mathbb{Q}(t_1, \ldots) \), which is computable by Proposition A.7.11 and Proposition A.7.12.

If \( G \) is of characteristic \( p > 0 \), then the argument above applies with \( \mathbb{Q} \) replaced by a finite field of \( p \) elements.
A.8 Representing Sets of Primes and Rings of \( S \)-integers in Number Fields.

In this section we will address the issue of representing recursive prime sets in number fields. We have already discussed these sets when the field in question is \( \mathbb{Q} \). We will now do it for other number fields.

Let \( K \) be a number field. Let \( \Omega = \{\omega_1, \ldots, \omega_n\} \) be an integral basis of \( K \) over \( \mathbb{Q} \). (See Definition B.1.29 for a definition of integral basis.) Let \( J : K \to \mathbb{N} \) be a presentation described in Proposition A.7.7 with respect to basis \( \Omega \), with \( \mathbb{Q} \) being the field below under presentation from Proposition A.6.3. Fix a recursive enumeration of \( J(K) \), i.e. a computable bijection \( \Phi : \mathbb{N} \to J(K) \). (For example, using an ordering of integers 0, 1, 2, 3, ..., one can order the elements of \( K \) using the lexicographical ordering with respect to \( \Omega \)-coordinates of the field elements.) For each prime \( p \) fix the smallest (under the chosen ordering) element \( \alpha \) of \( K \) satisfying the following conditions.

- \( \text{ord}_p \alpha = 1 \)
- \( \text{ord}_q \alpha = 0 \) for any conjugate \( q \) of \( p \) over \( \mathbb{Q} \).
- \( \alpha = \sum_{i=1}^n a_i \omega_i, a_i \in \mathbb{Z}, |a_i| < p^2 \), where \( p \) is the rational prime below \( p \).

Such an \( \alpha \) exists for every \( p \) by Proposition B.2.4. We will represent each prime \( p \) by a pair \( (\alpha(p), p) \), where \( \alpha(p) \) satisfies the conditions above and \( p \) is the rational prime below it in \( \mathbb{Q} \). Now call a set of \( K \)-primes \( \mathcal{W}_K \) computable (r.e.) if the corresponding set of pairs is recursive (r.e. respectively). This identification has several desirable properties described below.

A.8.1 Proposition.

Let \( K, J \) be as above. For a rational prime \( q \) let

\[
S(q) = 2^{J(\alpha(q_1))}3^{J(\alpha(q_2))} \cdots p_k^{J(\alpha(q_k))},
\]

where \( q_1, \ldots, q_k \) are all the distinct factors of \( q \) in \( K \) and \( p_1 = 2, \ldots, p_k \) are the first \( k \) rational primes. For \( n \) not equal to a prime, let \( S(n) = 1 \). Then \( S : \mathbb{N} \to \mathbb{N} \) is a recursive function.
Proof.

We will present an informal algorithm to compute $S(n)$. Let $\omega_1, \ldots, \omega_n$ be an integral basis of $K$ over $\mathbb{Q}$. For each expression of the form $\sum_{i=1}^{n} a_i \omega_i$ with $a_i \in \mathbb{Z}$ and $|a_i| < p^2$, do the following.

1. Compute the $\mathbb{Q}$-norm of this sum. (This a recursive operation by Corollary A.7.10.)

2. If the norm is divisible by $q$, set the sum aside.

Now let $B = \{\beta_1, \ldots, \beta_k\}$ be the set of all the elements set aside. Now repeat the following procedure until $B$ is empty.

1. Choose elements of $B$ whose norm has the lowest order at $q$. Among the elements with norms of the lowest order, choose the element with the lowest sequence number under the chosen ordering of $K$. Denote this element by $\gamma$.

2. For every element $\beta_i \neq \gamma$ currently in the set, compute the norm of $\gamma + \beta_i$.

3. If the norm is divisible by $q$, then remove $\beta_i$ from the set.

4. Remove $\gamma$ from $B$ and put into a set which we will denote by $F$.

We claim that at the end of this process, $F$ will contain exactly

$$\alpha(q_1), \alpha(q_2), \ldots, \alpha(q_k),$$

where $q_1, \ldots, q_k$ are all the factors of $q$ in $K$. Indeed, by Proposition B.2.4, we know that $B$ contains $\alpha(q_i)$ for each factor of $q$. Further, any element of $B$ which is divisible by at least two distinct factors of $q$ or by a square of a factor of $q$ will have a norm of bigger order at $q$ than at least one $\alpha(q_i)$ at any stage of the process. Further, the norm of $\gamma + \beta_i$ is divisible by $q$ if and only if both $\gamma$ and $\beta_i$ are both divisible by the same factor of $q$. Thus elements of $B$ divisible by at least two distinct factors of $q$ or by a square of a factor of $q$ will be removed from $B$ at some point. Elements of $B$ having exactly one factor of $q$ in their divisors but not having the lowest sequence number will also be removed from $B$ when the element with a lower sequence number and the same factor of $q$ in the divisor is chosen.

As an immediate corollary of the proposition above we have the following statement.
A.8.2 Corollary.

Let \( \mathcal{W}_Q \) be a set of rational primes, and let \( \mathcal{W}_K \) be the set of all \( K \)-primes above \( \mathcal{W}_Q \). Then \( \mathcal{W}_K \equiv_T \mathcal{W}_Q \) and \( \mathcal{W}_K \equiv_e \mathcal{W}_Q \).

A.8.3 Remark.

In what follows we will continue to use presentation \( J \) of the number field \( K \) we have discussed above.

A.8.4 Proposition.

Let \( K \) be a number field of degree \( n \) over \( \mathbb{Q} \). Let \( \omega_1, \ldots, \omega_n \) be an integral basis of \( K \) over \( \mathbb{Q} \). Let \( \mathcal{W}_K \) be a recursive (r.e.) set of \( K \)-primes. Then the following sets are also recursive (r.e.).

1. The set of \( K \)-integers whose divisors are a product of powers of elements of \( \mathcal{W}_K \). (We will denote this set by \( O(\mathcal{W}_K) \).)
2. \( \mathcal{C}_\mathbb{Q}(O(\mathcal{W}_K)) = \{(a_1, \ldots, a_n) \in \mathbb{Z}^n | \sum_{i=1}^n a_i \omega_i \in O(\mathcal{W}_K)\} \).

Proof.

As above, we present an informal algorithm computing the listing or characteristic function of the sets involved.

1. We will consider the case of computable \( \mathcal{W}_K \) first. Given \( \alpha \in O_K \) do the following.
   
   (a) Compute the norm of \( \alpha \). Determine what primes divide the norm. Let \( q_1, \ldots, q_m \) be the list of these primes.
   
   (b) For each \( q_i \), compute \( \alpha(q_{i,j}) \) for each factor \( q_{i,j} \) of \( q_i \) in \( K \).
   
   (c) Use the characteristic function of the set \( \{(q_i, \alpha(q_{i,j}))\} \) to determine for each \( j \) whether \( q_{i,j} \in \mathcal{W}_K \).
   
   (d) If for some \( i \), no factor of \( q_i \) is in \( \mathcal{W}_K \), then \( \alpha \not\in O(\mathcal{W}_K) \).
   
   (e) Otherwise for each \( i,j \), compute the \( \mathbb{Q} \)-norm of \( \alpha + \alpha(q_{i,j}) \). If for some \( i,j \) we have that \( q_{i,j} \not\in \mathcal{W}_K \), but \( \mathbb{Q} \)-norm of \( \alpha + \alpha(q_{i,j}) \) is divisible by \( q_i \), then \( \alpha \not\in O(\mathcal{W}_K) \).
   
   (f) Conclude that \( \alpha \in O(\mathcal{W}_K) \).
Now assume that $\mathcal{W}_K$ is r.e. and let $f(n)$ be a recursive function listing pairs $(p, \alpha(p))$, where $p \in \mathcal{W}_K$. Given an element $\alpha \in O_K$ use the procedure described above to compute all pairs $(q, \alpha(q))$ such that $q$ occurs in the divisor of $\alpha$. Next check if all the pairs have been listed, then $\alpha$ should be included in listing of $O(\mathcal{W}_K)$. Otherwise, it should be stored in a “waiting” list.

2. Given $(a_1, \ldots, a_n)$, check to see if $\sum_{i=1}^n a_i \omega_i \in O(\mathcal{W}_K)$ when $\mathcal{W}_K$ is recursive and check to see if $\sum_{i=1}^n a_i \omega_i$ has been listed already if $O(\mathcal{W}_K)$ is r.e.

A.8.5 Remark.

Using the same approach as in the proof above we can show that $O(\mathcal{W}_K)$ and $C_\mathbb{Q}(O(\mathcal{W}_K))$ are actually Turing and enumerably equivalent to $\mathcal{W}_K$.

We are now ready for the following assertions.

A.8.6 Proposition.

Let $K$ be a number field of degree $n$ over $\mathbb{Q}$. Let $\mathcal{W}_K$ be a set of primes of $K$. Then $O_{K,\mathcal{W}_K}$ is computable (r.e) if and only if $\mathcal{W}_K$ is computable (r.e.).

Proof.

First assume $\mathcal{W}_K$ is computable (r.e.). Given $\alpha \in K$, compute the coefficients $A_r(\alpha), r = 0, \ldots, n - 1$ of the characteristic polynomial of $\alpha$ over $\mathbb{Q}$ and determine the rational primes $q_1, \ldots, q_l$ dividing the denominators of these coefficients. (This can be done effectively by A.7.10.) For each prime $q_i$ compute $\alpha(q_{i,j})$ for each $K$-factor $q_{i,j}$ of $q_i$. (This part is computable by A.8.1.) Further for $i = 1, \ldots, l$ compute $a_i = -\min_{0 \leq r < n}\{\text{ord}_q A_r(\alpha)\}$. For each pair $(i,j)$, let $\beta_{i,j}(\alpha) = \prod_{k \neq j} \alpha(q_{i,k})$. Next for all $i,j$, we compute the coefficients $A_r(\beta^{n_a}_{i,j} \alpha)$ of the characteristic polynomial of $\beta^{n_a}_{i,j} \alpha$ over $\mathbb{Q}$. Note that if $\text{ord}_{q_{i,j}} \alpha < 0$, then $\text{ord}_{q_{i,j}} \beta^{n_a}_{i,j} \alpha < 0$ and for some $r$ we will have $\text{ord}_{q_{i,j}} A_r(\beta^{n_a}_{i,j} \alpha) < 0$. Conversely, for $k \neq j$, we have that $\text{ord}_{q_{i,k}} \alpha > -n a_i$ and therefore $\text{ord}_{q_{i,k}} \alpha \beta^{n_a}_{i,j} > 0$. Thus, $\alpha \beta^{n_a}_{i,j}$ is integral at $q_i$ if and only if $\alpha$ is integral at $q_{i,j}$. Hence, by following this effective procedure we will be able to establish which $q_{i,j}$ occur in the denominator of the divisor of $\alpha$. Once this is done, if $\mathcal{W}_K$ is recursive, for each $(i,j)$ we can check to see if the pair $(q_i, \alpha(q_{i,j})) \in \mathcal{W}_K$. If $\mathcal{W}_K$ is r.e. we can wait for the pair to be listed.
Now suppose $O_{K,W_K}$ is computable (c.e.). Then given a prime $p$ of $K$, we can conduct a systematic search of the field until we find an integral element $\beta$ whose divisor is a power of $p$ only. Such an element exists since the divisor $p^{h_K}$, where $h_K$ is the class number of $K$ is principal. We can recognize such an element, since $p -$ the prime below $p$, will be the only prime dividing its norm, all the coefficients of the characteristic polynomial of $\beta$ over $\mathbb{Q}$ will be integral, and the $\mathbb{Q}$-norm of $\beta + \alpha(q)$, where $q$ is any other factor of $p$ in $K$, will not be divisible by $p$. Next we can check whether $\frac{1}{\beta}$ is in $O_{K,W_K}$ (or has already been listed).

Finally, we note that as above, one can adjust this proof to show that $O_{K,W_K}$ and $W_K$ are and enumerably equivalent.

A.8.7 Proposition.

Let $K$ be a number field. Let $\mathcal{W}$ be a set of rational primes with a factor of relative degree $d$ in $K$ and let $\mathcal{W}_K$ be the set of $K$ primes of relative degree $d$ over $\mathbb{Q}$. Then $\mathcal{W}$ and $\mathcal{W}_K$ are both recursive sets of primes.

Proof.

Given a rational prime $p$, do the following.

• Compute $\alpha(p_i)$ for each factor $p_i$ of $p$.

• Compute $N_{K/Q}(\alpha(p_i))$ and determine $f_i = \text{ord}_p N_{K/Q}(\alpha(p_i)) = f(p_i/p)$ for all $i$. If for some $i$ we have $f_i = d$, then $p \in \mathcal{W}$, otherwise it is not.

The procedure for determining whether a pair $(p, \alpha(p_i))$ is in the set representing $\mathcal{W}_K$ is analogous.

A.8.8 Proposition.

Let $K$ be a number field. Then, if $K$ is real, there exists a recursive function $f : K \times \mathbb{N} \rightarrow \mathbb{N}$ producing a decimal expansion of the elements of the field. If $K$ is not real, there are recursive functions $f_i : K \times \mathbb{N} \rightarrow \mathbb{N}, i = 1, 2$, producing the decimal expansions of the real and imaginary parts of the elements of the field.

Proof.

Let $\omega \in \Omega$ (an integral basis of $K$ over $\mathbb{Q}$). Let $h(T)$ be its monic irreducible polynomial over $\mathbb{Q}$. If $\omega$ is real, then let $a_1 < b_1 \in \mathbb{Q}$ be such that $\omega \in (a_1, b_1)$,
and $[a, b]$ contains no other real root of $h$. If $\omega$ is not real, let $a_1 < b_1, a_2 < b_2 \in \mathbb{Q}$ be such that $\omega \in B = \{z \in \mathbb{C} \mid \Re z \in (a_1, b_1), \Im z \in (a_2, b_2)\}$ and the topological closure $\bar{B}$ of $B$ contains no other root of $h$. Let $r$ be a positive rational number greater than the distance from any other root of $h(x)$ to the boundary of the region. Next let $g(x) = \frac{f(x)}{x-\omega}$. Then for any $c$ in the chosen region, $|g(c)| > r^{d-1}$, where $d = \deg f$. Finally note that

$$|\omega - c| = \left| \frac{f(c)}{g(c)} \right| < r^{1-d} |f(c)|.$$ 

Thus by systematic search of the rational elements of the region, we can effectively construct the decimal expansion of $\omega$ if it is real, or decimal expansions of its real and imaginary parts.

Since for every element of $K$, we can produce effectively its rational coordinates with respect to $\Omega$, knowing the decimal expansions of the elements of the basis is enough to produce the decimal expansions for all the elements of the field.
Appendix B

Number Theory.

This appendix contains the algebraic and number theoretic facts which we use in this book.

B.1 Global Fields, Valuations and Rings of \( W \)-integers.

We start with a definition of a global field.

B.1.1 Definition.

A global field is a finite extension of \( \mathbb{Q} \) (a number field) or a finite extension of a rational function field over a finite field of constants.

We remind the reader that throughout the book we assume that all the number fields are subfields of \( \mathbb{C} \), and for each \( p > 0 \) we have fixed an algebraic closure for a rational function field over a constant field of \( p \) elements. Thus any two global fields of the same characteristic in the book are assumed to be subfields of the same algebraically closed field.

In the function field case we need a couple more definitions.

B.1.2 Definition.

Let \( C \) be a field, let \( t \) be transcendental over \( C \), and let \( K \) be a finite extension of \( C(t) \). Then the algebraic closure of \( C \) in \( K \) is called the constant field of \( K \) or the field of constants of \( K \).
B.1.3 Remark.

In general a function field is a finite extension of a rational function field. What makes a function field “global” is the fact that the constant field is finite.

We will distinguish a special class of function field extensions.

B.1.4 Definition.

Let $K$ be a function field over a constant field $C$. Let $C_1$ be an algebraic extension of $C$. Then the field $K_1 = C_1K$ will be called a constant field extension of $K$. (Here we also remind the reader that, as we stated in the introduction, whenever we use a compositum of fields, they are assumed to be subfields of some algebraically closed field. In this case the compositum is simply the smallest field containing all the fields in the compositum.)

Next we define a non-archimedean valuation of a global field.

B.1.5 Definition.

Let $K$ be a global field. Then let $\nu : K \to \mathbb{Z} \cup \{\infty\}$ be a map satisfying the following properties.

1. $\nu : K^* \to \mathbb{Z}$ is a homomorphism from the multiplicative group of $K$ into $\mathbb{Z}$ as a group under addition.
2. $\nu(0) = \infty$.
3. For all $x, y \in K$ we have that $\nu(x + y) \geq \min(\nu(x), \nu(y))$.
4. If $K$ is a function field, then for any constant $c$ we have that $\nu(c) = 0$.
5. There exists $x \in K$ such that $\nu(x) \neq 0$.

Then $\nu$ is called a (non-trivial) discrete or non-archimedean valuation of $K$ or a prime of $K$. If $x \in K$, then $\nu(x)$ is also denoted by $\text{ord}_x x$. For a general discussion of valuations and primes of global fields the reader can be referred to [37] (Chapters 1 and 2), [47] (Chapters 1–3), [33] (Chapters 2 and 3), and [3] (Chapter 1).

Next we list some important properties of the valuations. We will leave the proof to the reader.
B.1.6 Proposition.
Let $K$ be a global field and let $v$ be a valuation of $K$. Let
\[ R(v) = \{ x \in K, v(x) \geq 0 \}. \]
Then $R(v)$ is a discrete valuation ring (i.e. a local PID) whose fraction field is $K$, and
\[ M(v) = \{ x \in R(v) | v(x) > 0 \} \]
is its unique maximal ideal. (The identification of $v$ with $M(v)$ explains the dual terminology.) $R(v)$ is called the valuation ring of $v$.

Conversely, let $R \subset K$ be a ring such that for every $x \in K$ either $x \in R$ or $x^{-1} \in R$. Then $R$ is a discrete valuation ring such that for some valuation $v$ of $K$, we have that $R(v) = R$. (For a discussion of discrete valuation rings see, for example, [37], Chapter 1, Section 3.)

From this proposition we immediately derive the following property of non-archimedean valuations.

B.1.7 Corollary.
Let $K$ be a global field, $v$ a non-archimedean valuation. Let $a, b \in K$ be such that $v(a) < v(b)$. Then $v(a + b) = v(a)$.

The definition below tells us when two valuations are essentially the same.

B.1.8 Definition.
Let $K$ be a global field. Then two valuations $v_1$ and $v_2$ of $K$ will be called equivalent if $M(v_1) = M(v_2)$. (Note that since $R(v)$ is a local ring for all $v$, $M(v_1) = M(v_2) \Leftrightarrow R(v_1) = R(v_2)$.)

The next definition introduces us to an important object associated with valuations.

B.1.9 Definition.
Let $K$, $v$, $M(v)$, $R(v)$ be as in Proposition B.1.6. Then the field $F(v) = R(v)/M(v)$ is called the residue field of $v$.

The two propositions below constitute a starting point for our investigation of extensions of valuations. The first one tells us that every valuation above
comes from below. The second proposition lists several properties connecting valuations above to valuations below.

**B.1.10 Proposition.**

Let $M/K$ be a finite extension of global fields. Let $w$ be a non-archimedean valuation of $M$ and let $v$ be its restriction to $K$. Then $v$ is a valuation of $K$.

**Proof.**

The only way $v$ can fail to be a valuation, as defined above, is for $v(x)$ to be identically zero on $K$. This case is excluded by Statement C, Section 4.1 of [80].

**B.1.11 Proposition.**

Let $M/K$ be a finite extension of global fields. Let $v$ be a valuation of $K$. Then there exists a valuation $w$ of $M$ extending a valuation of $K$ equivalent to $v$. Let $\bar{v}$ be the restriction of $w$ to $K$. Then the following statements are true.

1. $F(v)$ is isomorphic to a subfield of $F(w)$ and under this isomorphism $[F(w) : F(v)]$ is finite. This degree is called the relative degree of $w$ over $v$ and it is denoted by $f(w/v)$.

2. $\bar{v}(K^*) \subseteq w(M^*)$ and the index of $\bar{v}(K^*)$ in $w(M^*)$ is finite. This index is called the ramification of $w$ over $v$ and is denoted by $e(w/v)$.

3. For any valuation $v$ there are only finitely many valuations $w$ in $M$ such that the restriction of $w$ to $K$ is a valuation equivalent to $v$. Let $w_1, \ldots, w_k$ be all such valuations of $M$. Then $\sum_{i=1}^k e(w_i/v)f(w_i/v) = [M : K]$. Further, if the extension is Galois, for all $i, j = 1, \ldots, k$ we have that $e(w_i/v) = e(w_j/v)$ and $f(w_i/v) = f(w_j/v)$, implying that for all $i$ it is the case that $f(w_i/v) [M : K], e(w_i/v) [M : K]$, and $k [M : K]$.

4. The integral closure $R_M(v)$ of $R(v)$ in $M$ is equal to $\bigcap_{i=1}^k R(w_i)$.

5. $R_M(v) M(v) = \prod_{i=1}^k (M(w_i) \cap R_M(v))^{e(w_i/v)}$.

For the proof of this proposition see Lemma 6.5 and Corollary 6.7 in Chapter 1, Section 6 of [37], Theorem 2 in Chapter 4, Section 4.2 of [80], and Theorem 1 in Chapter IV, Section 1 of [3].
It is not hard to show that relative degrees and ramification degrees also have the following properties whose proof we leave to the reader.

**B.1.12 Proposition.**

Let \( K \subset E \subset F \) be a finite extension of global fields. Let \( w_F \) be a non-archimedean valuation of \( F \) and let \( w_E \) and \( w_K \) be its restrictions to \( E \) and \( K \) respectively. Then \( e(w_F/w_K) = e(w_F/w_E)e(w_E/w_K) \) and \( f(w_F/w_K) = f(w_F/w_E)f(w_E/w_K) \).

**B.1.13 Alternative Terminology.**

The discussions above can be rephrased in terms of ideals rather than valuations since we can “reconstruct” \( v \) from its ideal \( M(v) \). For any \( x \in K^* \cap M(v) \), set \( \bar{v}(x) = \{ \min n : x \in M(v)^n \setminus M(v)^{n+1} \} \). For all \( x \in R(v) \cap K^* \setminus M(v) \), set \( \bar{v}(x) = 0 \). For any \( x \in K \setminus R(v) \) define \( \bar{v}(x) = -\bar{v}(x^{-1}) \). Finally, let \( \bar{v}(0) = \infty \). Then \( \bar{v} \) is equivalent to \( v \). We will usually denote \( M(v) \) by characters “\( p \)”, “\( q \)”, or “\( \Omega \)”. Instead of writing “\( v(x) \)” we will normally write “ord\( p \)\( x \)” (or “ord\( q \)\( x \)”, “ord\( q \)\( x \)”, “ord\( \Omega \)\( x \)” respectively).

Given an extension \( M/K \) of global fields, instead of saying that a valuation \( w \) of \( M \) is an extension of a valuation \( \bar{v} \) of \( K \) equivalent to a given valuation \( v \) of \( K \), we will say that a prime \( p_M \) of \( M \) is a factor or lies above a given prime \( p_K \) of \( K \). We will also say that \( p_K \) lies below \( p_M \) in \( K \).

If an \( M \)-prime \( p_M \) lies above a \( K \)-prime \( p_K \) and \( e(p_M/p_K) > 1 \), then we will say that \( p_M \) is “ramified over” \( p_K \) or \( K \), and we will say that \( p_K \) is “ramified” in the extension \( M/K \). If \([M : K] > 1 \) and the ramification degree is equal to the degree of the extension, we will say that \( p_K \) and \( p_M \) are “totally ramified” in the extension. If a \( K \)-prime \( p_K \) has only one prime \( p_M \) of \( M \) above it in \( M \) and \( p_M \) is unramified over \( p_K \), we will say that \( p_K \) “does not split” in the extension or that \( p_K \) is “inert” in the extension, otherwise we will say that \( p_K \) “splits in the extension”. Finally, if for every \( M \)-prime \( p_M \) lying above a \( K \)-prime \( p_K \), the relative degree is 1, we will say that \( p_K \) “splits completely”. If, furthermore, \( p_K \) is unramified in the extension, we will say that \( p_K \) “splits completely into distinct factors”.

To facilitate further discussion we introduce several more terms.

**B.1.14 More Terminology.**

If \( K \) is a global field, \( v \) - a non-archimedean valuation of \( K \) and \( x \in K \), then we will say that \( x \) has a zero at \( v \) if \( v(x) > 0 \). We will say that \( v(x) \) has a
pole at \( v \) if \( v(x) < 0 \). Finally we will say that \( x \) is a unit at \( v \) if \( v(x) = 0 \). If 
\[ v(x) = \{ \min n : x \in M(v)^n \setminus M(v)^{n+1} \} \text{ as above, and } v(x) = n > 0, \]
we will say that \( x \) has a zero of order \( n \). If \( v(x) = -n < 0 \), we will say that \( x \) has a 
pole of order \( n \) at \( v \).

This terminology is standard for function fields only but for the sake of 
brevity we will use it for number fields also.

The next two propositions will identify all the discrete valuations of a global 
field, starting with the case of rational numbers and rational functions.

**B.1.15 Proposition.**

Let \( a \in \mathbb{Z}, a \neq 0 \). Let \( p \) be a rational prime. Let \( b \in \mathbb{Z} \) be such that 
\( a = p^m b \) and \( (p,b) = 1 \). Then define \( v_p(a) = \text{ord}_p(a) = m \). For a non-zero rational 
number \( x = \frac{a_1}{a_2} \), with \( a_2 \neq 0, (a_1, a_2) = 1 \), define \( v_p(x) = v_p(a_1) - v_p(a_2) \). 
Then \( v_p \) is a valuation of \( \mathbb{Q} \). Conversely, if \( v \) is a discrete valuation of \( \mathbb{Q} \), then 
\( v \) is equivalent to \( v_p \) for some \( p \). (See Theorem 1 in Chapter 1, Section 1.3 
of [80].)

**B.1.16 Proposition.**

Let \( C \) be a field. Let \( t \) be transcendental over \( C \). Let \( h(t), g(t) \in C[t] \setminus \{0\} \), let 
\( P(t) \in C[t] \) be a monic irreducible polynomial of non-zero degree, and assume 
\( h(t) = g(t)P(t)^m, (P(t), g(t)) = 1 \). Then define \( v_{P(t)}(h(t)) = m \). Further, 
define \( v_\infty(h(t)) = -\deg(h(t)) \). If \( f(t) = \frac{h_1(t)}{h_2(t)} \), where \( h_1(t), h_2(t) \in C[t] \setminus \{0\} \) 
and are relatively prime to each other, then set \( v_{P(t)}(f(t)) = v_{P(t)}(h_1(t)) - v_{P(t)}(h_2(t)) \) and similarly set \( v_\infty(f(t)) = v_\infty(h_1(t)) - v_\infty(f(t)) \). Then \( v_{P(t)} \) 
and \( v_\infty \) are valuations of \( C(t) \). Further, any valuation of \( C(t) \), trivial on \( C \), 
is equivalent to \( v_{P(t)} \) for some monic irreducible polynomial \( P(t) \) or \( v_\infty \). (See 
Chapter 1, Section 3 of [3] for the proof of this proposition.)

Note that from Proposition B.1.10 we know that any non-archimedean 
valuation of a global field must be an extension of a valuation on a rational 
field. Thus, knowing all the non-archimedean valuations of rational fields 
provides us with a lot of information about all the valuations of a generic 
global field. Among other things the reader can now easily prove the following 
results.
B.1.17 Proposition.
The residue field of any non-archimedean valuation of a global field is finite. In the case of the global function fields it is a finite extension of the field of constants.

B.1.18 Proposition.
Let \( x \) be an element of a global field \( K \). Then for all but finitely many non-archimedean primes \( p \) of \( K \) we have that \( \text{ord}_p x = 0 \).

Proposition B.1.17 gives rise to the following definition.

B.1.19 Definition.
Let \( p \) be a prime of a global function field \( K \) over a field of constants \( C \). Let \( R_p \) be the residue field of \( p \). Then \([R_p : C]\) is called the degree of \( p \). (This degree should not be confused with the relative degree defined earlier.)

The valuations of global fields form the rings which are the subject of the discussion in this book.

B.1.20 Definition.
Let \( K \) be a global field and let \( \mathcal{W} \) be a subset of its non-archimedean valuations. Then set
\[
O_{K,\mathcal{W}} = \{ x \in K | \text{ord}_p x \geq 0, \forall p \notin \mathcal{W} \}
\]

If \( K \) is a number field, then \( \mathcal{W} \) can be empty and in this case \( O_{K,\mathcal{W}} = O_K \) is the ring of algebraic integers of \( K \). In the case of function fields, we will never consider empty \( \mathcal{W} \) because the resulting ring would contain constants only. If \( \mathcal{W} \) contains all non-archimedean valuations of \( K \), then the ring \( O_{K,\mathcal{W}} = K \). In general we will consider \( \mathcal{W} \) which are finite and infinite. In the case of finite \( \mathcal{W} \) the ring \( O_{K,\mathcal{W}} \) is called a “ring of \( \mathcal{W} \)-integers”. If \( \mathcal{W} \) is infinite or finite and \( K \) is a function field, then \( O_{K,\mathcal{W}} \) is called a holomorphy ring, but unfortunately there is no corresponding accepted term for the situation with infinite \( \mathcal{W} \) in the case of number fields. Therefore we will extend the use of the term “\( \mathcal{W} \)-integers” to the rings with infinite \( \mathcal{W} \).

The following propositions describe important properties of the rings of \( \mathcal{W} \)-integers.
B.1.21 Proposition.

Let $K$ be a global field. Let $\mathcal{W}_K$ be a subset of primes of $K$. Then $O_{K,\mathcal{W}_K}$ is integrally closed. (See [37], Chapter I, Section 2 for definition of an integrally closed ring.)

Proof.

Suppose $x \in K \setminus O_{K,\mathcal{W}_K}$, and is integral over $O_{K,\mathcal{W}_K}$. Then for some $p \not\in \mathcal{W}_K$, we have that $\text{ord}_p x < 0$. Since $x$ is integral over $O_{K,\mathcal{W}_K}$, for some $a_0, \ldots, a_{n-1} \in O_{K,\mathcal{W}_K} \subset R(p)$ with $\text{ord}_p a_i \geq 0$, we have that $x^n + a_{n-1}x^{n-1} + \ldots + a_0 = 0$. Next observe that

$$\text{ord}_p x^n = n\text{ord}_p x < \min_{i=0,\ldots,n-1} \text{ord}_p (a_i x^i) \leq \text{ord}_p (a_{n-1}x^{n-1} + \ldots + a_0)$$

and therefore, by Corollary B.1.7, $\text{ord}_p (x^n + a_{n-1}x^{n-1} + \ldots + a_0) < 0$, which is impossible. Thus our assumption on existence of $x$ as described above is incorrect.

Then next proposition shows us that the integral closure of a ring of $\mathcal{W}$-integers in a finite extension is a ring of the same type.

B.1.22 Proposition.

Let $M/K$ be an extension of global fields. Let $\mathcal{W}_K$ be a subset of primes of $K$. Let $\mathcal{W}_M$ be the set of all primes of $M$ lying above $K$-primes in $\mathcal{W}_K$. Then the integral closure of $O_{K,\mathcal{W}_K}$ in $M$ is $O_{M,\mathcal{W}_M}$.

Proof.

In view of Proposition B.1.11, it is enough to show that being integral over $O_{K,\mathcal{W}_K}$ is equivalent to being integral over the valuation rings of every prime $p \in \mathcal{W}_K$. Indeed, let $x$ be integral over $O_{K,\mathcal{W}_K}$. Then for some $a_0, \ldots, a_{n-1} \in O_{K,\mathcal{W}_K}$,

$$x^n + a_{n-1}x^{n-1} + \ldots + a_0 = 0. \quad (B.1.1)$$

But for any prime $p \in \mathcal{W}_K$, the valuation ring $R(p)$ contains $O_{K,\mathcal{W}_K}$. Thus, $x$ is integral over $R(p)$.

Conversely, if $x$ is integral over every $R(p)$ with $p \in \mathcal{W}_K$, then any conjugate of $x$ over $K$ also has this property. Since the integral closure of a ring in a bigger ring (in this case the bigger ring is the Galois closure of $M$ over $K$) is also a ring (see Corollary to Proposition 2.2 in Section 2, Chapter I of [37]), the coefficients of the monic irreducible polynomial of $x$ over
K are also integral over \( O_{K,W} \) and are elements of \( K \). Thus, \( x \) satisfies a polynomial equation of the form (B.1.1) with \( a_0, \ldots, a_{n-1} \in O_{K,W} \) and therefore is integral over \( O_{K,W} \). Consequently, the integral closure of \( O_{K,W} \) is
\[
\bigcap_{p \in \mathcal{P}(M)} \bigcap_{\mathfrak{p} \mid p, R(\mathfrak{p}) = O_{M,W}} \mathfrak{p} \ |
\]
(Here \( \mathcal{P}(M) \) denote the set of all (non-archimedean) primes of \( M \).)

Our next goal is to describe a notion of the divisor for an element of a global field.

**B.1.23 Definition.**

Let \( K \) be a global field. Let \( x \in K \). Let \( \mathcal{P}(K) \) denote the set of all the non-archimedean primes of \( K \). Then let \( \mathcal{D}_K(x) = \prod_{p \in \mathcal{P}(K)} p^{\text{ord}_p x} \) denote the \( K \)-divisor of \( x \). (Note that by Proposition B.1.18, this product is effectively finite.) In general, a formal product \( \mathcal{D} = \prod_{i=1}^k p_i^{a_i} \), where \( p_i \) is a prime of \( K \) and \( a_i \in \mathbb{Z} \) will be called a divisor of \( K \). If all \( a_i \) are actually positive, then the divisor will be called integral. It is not hard to see that all algebraic integers of \( K \) have integral divisors.

For the case of \( K \) being a function field, this is a traditional definition of divisors. (See for example [33], Section 3.1.) In the case of a number field, the usual terminology would refer to a fractional ideal of the field and to the factorization of that fractional ideal into the product of prime ideals. (See [37], Chapter 1, Section 4.) However, in our case there are advantages to using the uniform terminology for both cases as in [80], Definition 1 in Section 10.1, Chapter 10).

When \( \mathcal{D} \) is an integral divisor and \( \mathcal{W} \) is a set of primes of the field not containing the factors of \( \mathcal{D} \), we can identify \( \mathcal{D} \) with a unique ideal of \( O_{K,W} \), i.e. the ideal of \( O_{K,W} \) which is the intersection \( \bigcap_{i=1}^k p_i^{a_i} \mathcal{O}_{K,W} \).

In the case of function fields we can also define the degree of integral divisors.

**B.1.24 Definition.**

Let \( \mathcal{D} \) be an integral divisor of a function field \( K \). Then define the degree of \( \mathcal{D} \), denoted by \( \deg_K(\mathcal{D}) \), to be \( \sum_{p \in \mathcal{P}(K), \text{ord}_p \mathcal{D} > 0} \text{deg}(p) \). (The degree of a function field prime was defined in B.1.19.)
Using the notion of divisor and its degree, we can define the notion of height for elements of function fields.

**B.1.25 Definition.**

Let $K$ be a global function field. Let $x \in K$. Let

$$\mathcal{D} = \prod_{p \in \mathcal{P}(K), \text{ord}_p x > 0} p^{\text{ord}_p x}.$$  

Then define the height of $x$ to be the degree of $\mathcal{D}$. We will refer to $\mathcal{D}$ as the zero divisor of $x$.

**B.1.26 Remark.**

The Product Formula (see Chapter 12 of [1]) implies that the height can also be measured using the pole divisor of the element, i.e. we can define the height of $x$ to be $\deg_K(\prod_{p \in \mathcal{P}(K), \text{ord}_p x < 0} p^{-\text{ord}_p x})$.

The rings of $\mathcal{W}$-integers are the only integrally closed subrings of global fields. This follows from the following proposition.

**B.1.27 Proposition.**

Let $K$ be a global field. Let $R$ be an integrally closed subring of $K$ such that the fraction field of $R$ is $K$. Then for some $\mathcal{W} \subseteq \mathcal{P}(K)$, we have that $R = O_{K,\mathcal{W}}$.

**Proof.**

Let $\mathcal{W} = \{p \in \mathcal{P}(K) : \exists x \in R, \text{ord}_p x < 0\}$. We will show that $R = O_{K,\mathcal{W}}$. We will treat the cases of number fields and function fields separately.

First let $K$ be a number field and observe that $O_K \subseteq R$ because $\mathbb{Z} \subseteq R$ and $O_K$ is the integral closure of $\mathbb{Z}$ in $K$. Next note that if $p \in \mathcal{P}(K)$ and there exists $x \in R$ with $\text{ord}_p x < 0$, then there exists $y \in R$ such that $y$ has a pole at $p$ only and no zeros. Indeed, first of all, by the Strong Approximation Theorem (see Theorem B.2.1), there exists $z \in O_K$ such that for all $q \neq p$ with $\text{ord}_q x < 0$, we have that $\text{ord}_q z > -\text{ord}_q x$, while $\text{ord}_p z = 0$. Note that $xz \in R$, $\text{ord}_p xz < 0$ and $xz$ has no other poles. Next consider $(xz)^h$, where $h$ is the class number of $K$, and observe that $(xz)^h = \alpha/\beta$, where $\alpha, \beta$ are integers which are relatively prime to each other and $\beta$ has a zero at $p$ only.
(See [37], Chapter I, Section 5 for definition the class number.) By the Strong Approximation Theorem again, there exist \(a, b \in \mathcal{O}_K\) such that \(a\alpha + b\beta = 1\). Now consider

\[
a(zx)^h + b = \frac{a\alpha + b\beta}{\beta} = 1 \in R.
\]

If \(\mathcal{W} = \emptyset\), then \(R = \mathcal{O}_K\) and we are done. If \(\mathcal{W}\) is not empty, then \(R \subseteq \mathcal{O}_K, \mathcal{W}\). Next for each \(p\) that can occur in the denominator of the divisor of an element of \(R\), let \(\beta\) constructed as above, be called \(\beta(p)\). Now let \(w \in \mathcal{O}_K, \mathcal{W}\). Note that for some positive natural number \(b\), we have that \(w^{bh} = \gamma/\delta, \delta = \prod \beta(p)^{a(p)}\), where \(\gamma \in \mathcal{O}_K, a(p) \in \mathbb{N}\) and \(\frac{1}{\beta(p)} \in R\). Thus, \(w^{bh} \in R\), and since \(R\) is integrally closed, \(w \in R\). Therefore, \(\mathcal{O}_K, \mathcal{W} \subseteq R\) and consequently, \(R = \mathcal{O}_K, \mathcal{W}\).

We now consider the case of \(K\) being a function field. First of all we observe that, given our assumptions on \(R\), we cannot have an empty \(\mathcal{W}\). Indeed, since the fraction field of \(R\) is \(K\), it must contain a non-constant element \(t\). A non-constant element must have at least one pole (and at least one zero) (see Corollary 3 in Chapter I, Section 4 of [3]). Next let \(C\) be the constant field of \(K\) and consider \(C[t] \subseteq C(t) \subseteq K\). Let \(q_{C(t)}\) be the degree valuation of \(C(t)\) as described in Proposition B.1.16. Then observe that \(C[t] = \mathcal{O}_{C(t), q_{C(t)}}\). Indeed, any polynomial has a pole at the degree valuation only. Next note that any rational function which is not a polynomial will have a pole at some other valuation, namely a valuation corresponding to an irreducible polynomial dividing the reduced denominator of the rational function. Thus, \(C[t]\) is integrally closed by Proposition B.1.21 and its integral closure in \(R\) is a ring of \(\mathcal{S}\)-integers where \(\mathcal{S}\) contains all the factors of \(q_{C(t)}\) in \(K\) by Proposition B.1.22. In this context \(\mathcal{O}_{K, \mathcal{S}}\) is often called a ring of integral functions by analogy with the rings of integers of number fields. From this point on the proof proceeds exactly as in the number field case with \(\mathcal{O}_{K, \mathcal{S}}\) playing the role of \(\mathcal{O}_K\) in the number field case. We will leave the remaining details to the reader and note only that the proof will require the function field version of the Strong Approximation Theorem.

Using Proposition B.1.11 and the Strong Approximation Theorem, one can also show that the following proposition is true. We leave the details to the reader.

**B.1.28 Proposition.**

Let \(K\) be a number field, let \(\mathcal{W}\) be a set of its primes. Let \(\mathcal{S}\) be an integral divisor of \(K\) (that is \(\mathcal{S}\) has a trivial denominator), and assume that no factor of \(\mathcal{S}\) is in \(\mathcal{W}\). Then \(\mathcal{O}_{K, \mathcal{W}}/\mathcal{S}\) is a finite ring. (We remind the reader that we can consider integral divisors as ideals of \(\mathcal{O}_K\) and \(\mathcal{O}_{K, \mathcal{W}}\) as long as \(\mathcal{W}\) does not
contain any factors of \( \mathcal{O} \).)

We will next discuss an important notion – the notion of an “integral basis”.

**B.1.29 Definition.**

Let \( M/K \) be a number field extension. Let \( \Omega = \{\omega_1, \ldots, \omega_n\} \subset O_M \) be a basis of \( M \) over \( K \). Then \( \Omega \) is called an integral basis of \( M \) over \( K \) if for every \( x \in O_M \), it is the case that \( x = \sum_{i=1}^{n} a_i \omega_i \), where \( a_i \in O_K \).

The most important for us fact concerning integral bases is stated below.

**B.1.30 Proposition.**

Every number field \( K \) has an integral basis over \( \mathbb{Q} \).

**Proof.**

This follows from Theorem 1 in Appendix B of [37].

We finish this section with two more technical observations concerning extensions of global fields.

**B.1.31 Lemma.**

Let \( E/F \) be a Galois extension of fields. Let \( M/F \) be any other extension of \( F \). Then \( ME/M \) is also a Galois extension.

**Proof.**

Let \( \alpha \) be a generator of \( E \) over \( F \). Then all the conjugates of \( \alpha \) over \( F \) are distinct and are in \( E \). \( \alpha \) will also be a generator of \( ME \) over \( M \). Further a conjugate of \( \alpha \) over \( M \) is also a conjugate of \( \alpha \) over \( F \) and therefore all the conjugate of \( \alpha \) over \( M \) are distinct and contained in \( ME \). Hence \( ME/M \) is a Galois extension.
B.1.32 Lemma.

Let $H$ be an algebraic function field over a perfect field of constants $C$ and let $t$ be a non-constant element of $H$. Then the following conditions are equivalent.

1. $t$ is not a $p$-th power in $H$.
2. The extension $H/C(t)$ is finite and separable.

(See [51][Chapter VI].)

B.2 Existence Through Approximation Theorems.

In this section we will list various propositions that are consequences of the Strong Approximation Theorem. Before we proceed, we need to say a few words about archimedean valuations. Non-archimedean or discrete valuations give rise to non-archimedean absolute values over number fields. If $K$ is a number field and $p$ is its prime, then for $x \in K$ we can define

$$|x|_p = \left( \frac{1}{N_p} \right)^{\text{ord}_p x},$$

where $N_p$ is the size of the residue field of $p$. It is not hard to verify that $|\cdot|_p$ is in fact an absolute value. Not all absolute values of number fields are generated by its primes. Some absolute values are extensions of the usual absolute value on $\mathbb{Q}$. These are the “archimedean” valuations. Each number field has a finite number of archimedean valuations equal to the number of distinct non-conjugate embeddings of the field into $\mathbb{C}$. For more information on archimedean valuations see, for example, [37], Chapter II, Section 4. Finally, we note that function fields do not have archimedean valuations.

We are now ready to state the Strong Approximation Theorem.

B.2.1 Theorem.

Let $K$ be a global field. Let $\mathcal{M}_K$ be the set of all the absolute values of $K$. Let $F_K \subset \mathcal{M}_K$ be a non-empty finite subset. Let $F_K = \{|_1, \ldots, |_l\}$. Let $a_1, \ldots, a_{l-1} \in K$. Then for any $\varepsilon > 0$ there exists $x \in K$ such that the following conditions are satisfied.

1. For $i = 1, \ldots, l-1$ we have that $|x - a_i| < \varepsilon$.
2. For any $| \notin F_K$ we have that $|x| \leq 1$. 

280
Proof.

A proof of this theorem can be found in the following books: [64], Theorem 33:11, Part I, Chapter III, Section 33G; [33], Chapter 3, Section 3.3, Proposition 3.3.1; [45], Chapter 3, Section 3.6, Proposition 3.6.4.

In the following two propositions we will use the Strong Approximation Theorem to show existence of elements in a global field necessary for the proofs in the chapter on definability of integrality at finitely many primes.

B.2.2 Proposition.

Let $K$ be a number field. Then there exists $g \in O_K$, satisfying conditions of Notation 4.2.1.

Proof.

Let the divisor of $aq^3$ be of the form $\prod \mathfrak{p}_j^{m_j}$, where each $\mathfrak{p}_j$ is a prime of $K$, and each $m_j$ is a positive integer. For each $i$, let $\alpha_i \in K$ be such $\text{ord}_{\mathfrak{p}_i} \alpha_i = 1$ and let $\gamma \in K$ be such that $\text{ord}_\mathfrak{c} \gamma = 1$. (Existence of these elements follows from the fact that valuation rings are local PID's.) Then by the Strong Approximation Theorem, there exists $g_0 \in K$, such that

- $\text{ord}_{\mathfrak{p}_i} (g_0 - \alpha_i^{-1}) > 1$,
- $\text{ord}_\mathfrak{c} (g_0 - \gamma) > 1$
- $\text{ord}_{\mathfrak{p}_j} (g_0 - 1) > 3m_j$
- $g_0$ is integral at all the other primes.

Note that

$$\text{ord}_{\mathfrak{p}_i} g_0 = \text{ord}_{\mathfrak{p}_i} ((g_0 - \alpha_i^{-1}) + \alpha_i^{-1}) = \min(\text{ord}_{\mathfrak{p}_i} (g_0 - \alpha_i^{-1}), \text{ord}_{\mathfrak{p}_i} \alpha_i^{-1}) = \text{ord}_{\mathfrak{p}_i} \alpha_i^{-1} = -1,$$

and similarly,

$$\text{ord}_\mathfrak{c} g_0 = \text{ord}_\mathfrak{c} (g - \gamma + \gamma) = \min(\text{ord}_\mathfrak{c} (g_0 - \gamma), \text{ord}_\mathfrak{c} \gamma) = \text{ord}_\mathfrak{c} \gamma = 1.$$

Finally we note that for all $i$ we have that $\text{ord}_{\mathfrak{p}_i} g_0 = 0$. Now let $g = g_0^{-1}$. Then we need to check only one condition:

$$\text{ord}_{\mathfrak{p}_i} (g - 1) = \text{ord}_{\mathfrak{p}_i} \frac{1 - g_0}{g_0} = \text{ord}_{\mathfrak{p}_i} (1 - g_0) > 3m_i.$$
B.2.3 Lemma.

Let $K$ be a global function field. Let $\mathcal{B}$ be an integral divisor of $K$ and let $a$ be a prime divisor of $K$ not dividing $\mathcal{B}$. Then for any sufficiently large $s$, there exists $u \in K$ with a pole of order $s$ at $a$, $u \equiv 1 \bmod \mathcal{B}$ and $u$ is integral at all the other primes of $K$.

Proof.

By the Strong Approximation Theorem, there exists $u_1 \in K$ such that $u \equiv 1 \bmod \mathcal{B}$ and $u$ is integral at all the primes of $K$ except for $a$. Next by a consequence of the Riemann-Roch Theorem ([113], Chapter II, Section 5, Corollary 5.5), we can show that for any natural number $s$ with $s > 2g - 2 + \deg(\mathcal{B})$, where $g$ is the genus of $K$, there exists $u_2 \in K$ such that $\text{ord}_a u_2 = -s$, $u_2 \equiv 0 \bmod \mathcal{B}$, $u_2$ is integral at all the other primes of $K$. Indeed, for any $s > 2g - 1 + \deg(\mathcal{B})$, the dimension of the space of functions with a pole order at most $s$ and zero modulo $\mathcal{B}$ is equal to $s \deg(a) - \deg(\mathcal{B}) - g + 1$ as a vector space over the field $C_K$ of constants of $K$. Similarly, the dimension of the space of functions with a pole of order at most $s - 1$ and zero modulo $\mathcal{B}$ is equal to $(s - 1) \deg(a) - \deg(\mathcal{B}) - g + 1$ as a vector space over the field $C_K$. Thus, the number of functions with a pole of order $s$ at $a$ and 0 modulo $\mathcal{B}$ is equal to

$$|C_K|^{(s-1)\deg(a) - \deg(\mathcal{B}) - g + 1} (|C_K|^{\deg(a)} - 1) \neq 0.$$ 

Now assume that the order of the pole of $u_1$ is less than $s$ and let $u = u_1 + u_2$. Observe now that $u$ satisfies all the requirements.

The next lemma plays a role in our construction of recursive presentations of number fields.

B.2.4 Proposition.

Let $K$ be a number field. Let $\Omega = \{\omega_1, \ldots, \omega_n\}$ be an integral basis of $K$ over $\mathbb{Q}$. Let $p$ be a rational prime and let $p$ be a factor of $p$ in $K$. Then there exists $\alpha \in K$ satisfying the following requirements.

1. $\alpha = \sum_{i=1}^n a_i \alpha_i$, $a_i \in \mathbb{Z}$, $|a_i| < p^2$
2. $\text{ord}_p \alpha = 1$
3. For all conjugates $q \neq p$ of $p$ over $\mathbb{Q}$, $\text{ord}_q \alpha = 0$. 

282
Proof.

By the Strong Approximation Theorem, there exists $\gamma \in O_K$ such that $\text{ord}_p \gamma = 1$ and for all conjugates $q \neq p$ of $p$ over $\mathbb{Q}$, $\text{ord}_q \gamma = 0$. Let $\gamma = \sum_{i=1}^n b_i \omega_i$, $b_i \in \mathbb{Z}$. For each $b_i$ there exists $a_i \in \mathbb{Z}$ such that $|a_i| < p^2$ and $a_i \equiv b_i \mod p^2$. Let $\alpha = \sum_{i=1}^n a_i \omega_i$. Then $p^2 | (\alpha - \gamma)$ and $\text{ord}_q \alpha = \text{ord}_q \gamma$ for every factor $q$ of $p$ in $K$.

B.3 Linearly Disjoint Fields.

In this section we explore some properties of linearly disjoint fields. Galois groups of products of linearly disjoint Galois extensions can be decomposed into the products of constituent Galois groups, allowing for a relatively easy analysis of prime splitting. This property makes products of linearly disjoint fields very attractive to us, and we use these fields extensively throughout the book.

A general discussion of linearly disjoint fields together with the definition of linear disjointness can be found in Section 2.5 of [33].

B.3.1 Lemma.

Suppose $M/F$ and $L/F$ are finite field extensions. Then $M$ and $L$ are linearly disjoint over $F$ if and only if $[LM : M] = [L : F]$. Further, $[LM : M] = [L : F]$ if and only if $[LM : L] = [M : F]$. (See Lemma 2.5.1 and Corollary 2.5.2, Chapter II, Section 5 of [33].)

The following corollary is obvious but useful.

B.3.2 Corollary.

Let $M$ and $L$ be two fields linearly disjoint over a common subfield $F$. Let $L_1, M_1$ be fields such that $F \subset M_1 \subset M$ and $F \subset L_1 \subset L$. Then $M_1$ and $L_1$ are also linearly disjoint over $F$.

B.3.3 Lemma.

Suppose $M/F$ and $L/F$ are finite field extensions, with $L/F$ being a Galois extension. Then $M$ and $L$ are linearly disjoint over $F$ if and only if $M \cap L = F$. 

283
First of all, it is clear that if $M \cap L \neq F$, then $M$ and $L$ are not linearly disjoint. Suppose now that $M$ and $L$ are not linearly disjoint. Let $\alpha$ be a generator of $L$ over $F$. Then by Lemma B.3.1, the monic irreducible polynomial $H(T)$ of $\alpha$ over $F$ will factor over $M$. Let $H_1(T)$ be a factor of $H(T)$ in $M$. Then the coefficients of $H_1(T)$ are, one hand, elements of $M$, and on the other hand, are symmetric functions of some conjugates of $\alpha$ over $F$, and thus contained in $L$ - the splitting field of $H(T)$. Hence, the coefficients of $H_1(T)$ are contained in $M \cap L$. However, since $H(T)$ does not factor in $F$, at least one of the coefficients of $H_1(T)$ is not in $F$. Thus, $M \cap L \neq F$.

B.3.4 Lemma.

Let $L$ be a function field over a finite field of constants $C$. Let $U$ be a finite extension of $L$ such that the constant fields of $U$ and $L$ are the same. Let $C'/C$ be a finite extension. Then $C'L$ and $U$ are linearly disjoint over $L$.

Proof.

By Lemma B.3.1 it is enough to show that $[C'U : U] = [C'L : L]$. Let $\alpha \in C'$ generate $C'$ over $C$. Then it is enough to note that by Theorem 11, Chapter XV, Section 3 of [1] we have that $[C(\alpha) : C] = [L(\alpha) : L] = [U(\alpha) : U]$.

B.3.5 Lemma.

Let $M, L, F$ be as in Lemma B.3.3. Then $\text{Gal}(ML/M) \cong \text{Gal}(L/F)$ and this isomorphism is realized by restriction.

Proof.

Let $\alpha$ be a generator of $L$ over $F$. Then $\alpha$ will generate $ML$ over $M$. Further, since $M$ and $L$ are linearly disjoint over $F$, $\alpha$ will have the same number of conjugates over $M$ as over $F$. Let $\alpha = \alpha_1, \ldots, \alpha_l$ be all the conjugates of $\alpha$ over $M$ and $F$, where $l = [L : F]$. Since $\{\alpha_i, i = 1, \ldots, l\} \subset L$, we can conclude that $\{\alpha_i, i = 1, \ldots, l\} \subset ML$. Thus, $ML/M$ is Galois and of the same degree as $L/F$. Next consider a map from $\text{Gal}(ML/M)$ to $\text{Gal}(L/F)$ implemented by restriction. Let $\sigma, \tau \in \text{Gal}(LM/M)$ restrict to the same map over $F$. Then $\sigma$ and $\tau$ send $\alpha$ to the same conjugate. Thus, $\sigma = \tau$, since each element of $\text{Gal}(ML/M)$ is determined by its action on the generator of the extension. Hence the restriction sends different maps to different maps.
Since both groups are of the same size, the image of the restriction contains all of \( \text{Gal}(L/F) \). Finally restriction is certainly a group homomorphism. Thus the groups are isomorphic.

The next two lemmas will generalize Lemma B.3.5 to the situations where we consider products of linearly disjoint fields.

### B.3.6 Lemma

Let \( N_1/F, N_2/F \) be two, linearly disjoint over \( F \), Galois extensions. Then

\[
\text{Gal}(N_1N_2/N_1) \cong \text{Gal}(N_2/F)
\]

\[
\text{Gal}(N_1N_2/N_2) = \text{Gal}(N_1/F)
\]

and

\[
\text{Gal}(N_1N_2/F) = \text{Gal}(N_1N_2/N_1) \times \text{Gal}(N_2N_1/N_2).
\]

**Proof.**

For \( i = 1, 2 \), let \( \alpha_i \) be a generator of \( N_i \) over \( F \). Let \( n_i = [N_i : F] \). Then by definition of linear disjointness, \( \alpha_i \) has \( n_i \) conjugates over \( N_j \) for \( j \neq i \) and \( i, j \in \{1, 2\} \). Let \( \alpha_{i,1} = \alpha_i, \ldots, \alpha_{i,n_i} \) be all the conjugates of \( \alpha_i \) over \( F \) and \( N_j \), for \( j \neq i \) and \( i, j \in \{1, 2\} \). Let \( \sigma_{i, j} : N_1N_2 \rightarrow N_1N_2 \) be defined by \( \sigma_{i, j}(\alpha_i) = \alpha_{i,j} \), \( \sigma_{i, j}(\alpha_k) = \alpha_k \) for \( k \neq i \), \( j \in \{1, \ldots, n_i\} \), and \( i, k \in \{1, 2\} \). Then \( \sigma_{i, j} \in \text{Gal}(N_1N_2/N_k) \subset \text{Gal}(N_1N_2/F) \). Further, \( \sigma_{1, k}\sigma_{2, j} = \sigma_{1, k}\sigma_{2, j} \) since both mappings send \( \alpha_1 \) to \( \alpha_{1,k} \) and \( \alpha_2 \) to \( \alpha_{2,j} \). Consider now the set of all products \( \{\sigma_{1, k}\sigma_{2, j}, i = 1, \ldots, n_1, j = 1, \ldots, n_2\} \subseteq \text{Gal}(N_1N_2/F) \). This set contains \( n_1n_2 \) distinct elements of \( \text{Gal}(N_1N_2/F) \) since each automorphism of \( N_1N_2 \) over \( F \) is determined by its action on \( \alpha_1 \) and \( \alpha_2 \). But \( |\text{Gal}(N_1N_2/F)| = n_1n_2 \) and therefore \( \{\sigma_{1, k}\sigma_{2, j}, i = 1, \ldots, n_1, j = 1, \ldots, n_2\} = \text{Gal}(N_1N_2/F) \). Finally consider

\[
\text{Gal}(N_1N_2/N_i) \rightarrow \text{Gal}(N_j/F),
\]

where \( i \neq j \) and \( i, j \in \{1, 2\} \) and the mapping between the groups is realized by restriction. This is an isomorphism by Lemma B.3.5.

### B.3.7 Lemma

Let \( N_1/F, \ldots, N_m/F \) be Galois field extensions. Assume further that

\[
G_i = \prod_{j=1, j \neq i}^{m} N_j
\]
is linearly disjoint from $N_i$ over $F$ for all $i = 1, \ldots, n$. Then

$$\Gal(N_1 \cdots N_m/F) \cong \Gal(N_1/F) \oplus \ldots \oplus \Gal(N_m/F),$$

$$\Gal(\prod_{j=1}^m N_j/G_i) \cong \Gal(N_i/F).$$

**Proof.**

To prove the first assertion of the lemma, we proceed by induction on $m$. For $m = 2$ the result follows from Lemma B.3.6. Assume the statement holds for $m = k$. Then, also by Lemma B.3.6, since $N_{k+1}$ and $\prod_{j=1}^k N_j$ are linearly disjoint over $F$ as subfields of linearly disjoint fields (see Corollary B.3.2), we have that

$$\Gal(N_{k+1} \prod_{j=1}^k N_j/F) \cong \Gal(N_{k+1}/F) \oplus (\Gal(N_1/F) \oplus \ldots \oplus \Gal(N_k/F))$$

$$\cong \Gal(N_{k+1}/F) \oplus \Gal(N_1/F) \oplus \ldots \oplus \Gal(N_k/F),$$

with $\Gal(\prod_{j=1}^{k+1} N_j/\prod_{i=1}^k N_i) \cong \Gal(N_{k+1}/F)$.

By renumbering the fields $N_i$ if necessary and setting $k = m - 1$, we also conclude that in general for $i = 1, \ldots, m$ we have that

$$\Gal(\prod_{j=1}^m N_j/G_i) \cong \Gal(N_i/F).$$

**B.3.8 Lemma.**

Let $G/F$, $H/F$ be Galois extensions of number fields, where $G, F$ are totally real and $H$ is a totally complex number field such that $[H : F] = 2$. Then $G$ and $H$ are linearly disjoint from each other over $F$.

**Proof.**

By Lemma B.3.3 it is enough to show that $G \cap H = F$. Since $[H : F]$ is a prime number, $G \cap H = F$ or $G \cap H = H$. Since $H$ is totally complex, $H \not\subseteq G$. Thus the first alternative holds.
**B.3.9 Proposition.**

Let $K$ be any number field. Let $q$ be a prime number. Let $n$ be an positive integer. Then in the algebraic closure of $K$, there exist $\beta_1, \ldots, \beta_n$ such that for all $i = 1, \ldots, n$, we have that $K(\beta_i)/K$ is a cyclic extension of degree $q$, $K(\beta_i)$ is linearly disjoint from $\prod_{j \neq i} K(\beta_j)$, and $\beta_1, \ldots, \beta_n$ are totally real, i.e. all their conjugates over $\mathbb{Q}$ are real.

**Proof.**

Let $p$ be a prime equivalent to 1 mod $q$ if $q$ is odd and let $p \equiv 1 \mod 4$ otherwise. (Such a prime exists by a theorem on primes in arithmetic progressions. See [90], Chapter 9, Section 4, Theorem 9.4.1.) Let $\xi_p$ be a primitive $p$-th root of unity. Then by Theorem 9.1 and Exercise 7, Chapter I, Section 9 of [37], we have that $\mathbb{Q}(\xi_p)/\mathbb{Q}$ is a cyclic extension of degree $p - 1$, where $p$ is ramified completely. Further, $\mathbb{Q}(\cos(2\pi/p))/\mathbb{Q}$ is a totally real subextension of degree 2. Let $H \triangleleft \text{Gal}(\mathbb{Q}(\cos(2\pi/p))/\mathbb{Q})$ be a normal subgroup of order $p - 1/2q$. Let $F_H$ be the fixed field of $H$. We claim that $F_H/\mathbb{Q}$ is a cyclic extension of degree $q$. Indeed, since $\text{Gal}(\mathbb{Q}(\cos(2\pi/p))/\mathbb{Q})$ is cyclic, every quotient group of $\text{Gal}(\mathbb{Q}(\cos(2\pi/p))/\mathbb{Q})$ is cyclic and $[F_H : \mathbb{Q}] = \frac{(p-1/2)}{(p-1/2q)} = q$.

Using the fact that there are infinitely many primes in arithmetic progression we can find a sequence $p_1, \ldots, p_n$ of prime numbers such that for all $i = 1, \ldots, n$, it is the case that $p_i$ is not ramified in the extension $K/\mathbb{Q}$, and $q \mid (p_i - 1)$ if $q$ is odd and $4\mid (p_i - 1)$ otherwise. Let $F_i$ be a totally real subfield of $\mathbb{Q}(\xi_{p_i})$ of degree $q$. Observe that in the extension $(K \prod_{j \neq i} F_j)/\mathbb{Q}$ we know that $p_i$ is not ramified, and in the extension $(K \prod_{j=1}^q F_j)/\mathbb{Q}$ we have that $p_i$ is ramified with ramification degree $q$. Thus,

$$[K \prod_{j=1}^n F_j : K \prod_{j \neq i} F_j] = q.$$

By Lemma B.3.1, $K \prod_{j \neq i} F_j$ and $F_i$ are linearly disjoint over $\mathbb{Q}$.

**B.3.10 Lemma.**

Let $p, q$ be distinct prime numbers. Let $\xi_p$ and $\xi_q$ be a $q$-th and a $p$-th primitive roots of unity respectively. Then $\mathbb{Q}(\xi_q)$ and $\mathbb{Q}(\xi_p)$ are linearly disjoint over $\mathbb{Q}$.

**Proof.**

The proof follows immediately from Lemma B.3.3 if we take into account the fact that $p$ and only $p$ is ramified completely in the first extension and $q$ and only $q$ is ramified completely in the second.
B.3.11 Corollary.

Let $K$ be a number field. Then for all but finitely many $p$, we have that $K$ and $\mathbb{Q}(\xi_p)$ are linearly disjoint over $\mathbb{Q}$.

**Proof.**

Let $p$ be a prime not ramified in $K$ and consider $\mathbb{Q}(\xi_p)$. Now, by Lemma B.3.3, we have that $\mathbb{Q}(\xi_p) \cap K$ are linearly disjoint if and only if $K \cap \mathbb{Q}(\xi_p) = \mathbb{Q}$. But since $p$ is ramified completely in $\mathbb{Q}(\xi_p)$ and not at all in $K$, the intersection of these fields must be $\mathbb{Q}$. Since only finitely many primes can ramify in a number field (see Theorem 7.3 of [37]), the conclusion of the corollary follows.

B.4 Divisors, Prime and Composite, under Extensions.

In this section we will examine how prime and composite divisors behave under finite extensions of global fields. We start with basic results.

B.4.1 Lemma.

Let $M/L$ be a Galois extension of global fields. Let $\mathfrak{p}$ be a prime of $L$ and let $\mathfrak{P}$ be a prime of $M$ above it. Let $R(\mathfrak{p}), R(\mathfrak{P})$ be the residue fields of $\mathfrak{p}$, and $\mathfrak{P}$ respectively. Let

$$G(\mathfrak{p}) = \{\sigma \in \text{Gal}(M/L) : \sigma(\mathfrak{p}) = \mathfrak{P}\}.$$ 

Then $G(\mathfrak{p})$ is called the *decomposition group of* $\mathfrak{p}$. Let

$$T(\mathfrak{p}) = \{\sigma \in \text{Gal}(M/L) : \sigma(x) = x + \mathfrak{p} \text{ for all } x \in M\}.$$ 

(In other words $T(\mathfrak{p})$ fixes all the classes modulo $\mathfrak{p}$.) Then $T(\mathfrak{p})$ is called the *inertia group of* $\mathfrak{p}$. The following statements are true.

- $|T(\mathfrak{p})| = e(\mathfrak{p}/\mathfrak{p}).$
- $|G(\mathfrak{p})| = e(\mathfrak{p}/\mathfrak{p})f(\mathfrak{p}/\mathfrak{p}).$
- The number of factors of $\mathfrak{p}$ in $M$ is equal to $[M : L]/|G(\mathfrak{p})|$ so that $\mathfrak{p}$ splits completely if and only if $|G(\mathfrak{p})|$ is trivial.
- $G(\mathfrak{p}) \cong \text{Gal}(M_{\mathfrak{p}}/L_\mathfrak{p})$. (Here $M_{\mathfrak{p}}$ and $L_\mathfrak{p}$ are completions of $M$ and $L$ under $\mathfrak{p}$ and $\mathfrak{p}$ respectively.)
• There exists a natural surjective homomorphism from $G(\mathfrak{p})$ to $\text{Gal}(R(\mathfrak{p})/R(p))$. The kernel of this homomorphism is $T(\mathfrak{p})$. $T(\mathfrak{p})$ is normal in $G(\mathfrak{p})$ and

$$G(\mathfrak{p})/T(\mathfrak{p}) \cong \text{Gal}(R(\mathfrak{p})/R(p))$$

is cyclic as a Galois group of a finite field extension.

• $\mathfrak{p}$ is totally ramified in the extension $M/M^{T(\mathfrak{p})}$, where $M^{T(\mathfrak{p})}$ is the fixed field of $T(\mathfrak{p})$, and $M^{T(\mathfrak{p})}/L$ is unramified with respect to $p$.

If $p$ is unramified in the extension $M/L$, then the generator of $G(\mathfrak{p})$ which is the inverse image of the Frobenius automorphism of $R(\mathfrak{p})/R(p)$ is called the Frobenius automorphism of $\mathfrak{p}$.

See Section 6.2 of [33] for more details.

The next result relates the divisor of a norm under a finite extension and the norm of the divisor.

**B.4.2 Proposition.**

Let $M/K$ be a global field extension of degree $n$. Let $y \in M$. Then $D_K(N_{M/K}y) = N_{M/K}(D_M(y))$. (Here $D_K(\ )$ denotes the $K$-divisor of an element of $K$, while $D_M(\ )$ denotes the $M$-divisor of an element of $M$.)

**Proof.**

This follows from Proposition 8.1, Section 8, Chapter I of [37].

The lemma below addresses the issue of the order of a norm at a prime not splitting in an extension. This proposition plays an important role in the definition of integrality at finitely many primes.

**B.4.3 Lemma.**

Let $M/K$ be an extension of degree $n$ of global fields. Let $q_K$ be a prime of $K$. Suppose $q_k$ does not split in the extension $M/K$. Let $x \in K$ be such that $x$ is a $K$-norm of some element $y \in M$. Then $\text{ord}_{q_k} x \equiv 0 \mod n$.

**Proof.**

Let $y \in M$ be such that $N_{M/K}(y) = x$. Let $D_M(y)$ be the divisor of $y$ in $M$. Then by Proposition B.4.2 and Corollary 8.5, Section 8, Chapter I of [37], we
deduce the following.

\[
N_{M/K}(D_M(y)) = \prod_{p_M \in \mathcal{M}} N_{M/K}(p_M^{\text{ord}_{p_M} y}) = \prod_{p_K \in \mathcal{M}_K} r(p_M/p_K)^{\text{ord}_{p_M} y} = D_K(x),
\]

where \( p_K \) is the \( K \)-prime below \( p_M \) in \( K \), and \( f(p_M/p_K) \) is the relative degree of \( p_M \) over \( K \). If a prime \( p_K \) does not split in the extension \( M/K \), it means there is only one factor \( p_M \) above it in \( M \). Therefore, by Theorem 1, Section 1, Chapter IV of [3] for the function field case and by Corollary 6.7, Section 6, Chapter I of [37] for the number field case, \( f(p_M/p_K) = n \). Thus for this prime \( p_K \) we have that \( \text{ord}_{p_K} x = \text{ord}_{p_K} D_K(x) = n \text{ord}_{p_M} y \).

The sequence of five lemmas below takes a close look at primes splitting and not splitting in products of linearly disjoint fields.

**B.4.4 Lemma.**

Let \( F \) be a global field. Let \( N_1 \) be a cyclic extensions of \( F \), let \( N_2 \) a Galois extension of \( F \), linearly disjoint from \( N_1 \) over \( F \). Then there are infinitely many primes \( p \) of \( F \) such that \( p \) does not split in \( N_1 \) and splits completely in \( N_2 \).

**Proof.**

Consider the extension \( N_1 N_2/F \). This extension is Galois. Further, linear disjointness guarantees by Lemma B.3.6 that

\[
\text{Gal}(N_1 N_2/F) \cong \text{Gal}(N_1/F) \times \text{Gal}(N_2/F),
\]

\[
\text{Gal}(N_1 N_2/N_1) \cong \text{Gal}(N_2/F),
\]

\[
\text{Gal}(N_1 N_2/N_2) \cong \text{Gal}(N_1/F),
\]

where the last two isomorphisms are realized by restriction. Let \( \sigma \) be a generator of \( \text{Gal}(N_1/F) \) and consider a \( N_1 N_2 \)-prime \( \wp \) whose Frobenius automorphism is \( (\sigma, \text{id}_{N_2}) \), where \( \text{id}_{N_2} \) is the identity element of \( \text{Gal}(N_2/F) \). Then \( \sigma \) is an element of the decomposition group of \( \wp_1 = \wp \cap N_1 \) over \( F \). Hence this decomposition group is all of \( \text{Gal}(N_1/F) \). Thus, \( p = \wp \cap F \) does not split in the extension \( N_1/F \). On the other hand, the decomposition group of \( \wp \) over \( N_2 \) is \( < (\sigma, \text{id}_{N_2}) > \cap \text{Gal}(N_1 N_2/N_2) = \text{Gal}(N_1 N_2/N_2) \). Then by looking at the
quotient of the decomposition group of $\mathfrak{p}$ over $F$ and over $N_2$, we conclude that the decomposition group of $\mathfrak{p}_2 = \mathfrak{p} \cap N_2$ over $F$ is trivial and therefore, $p = \mathfrak{p} \cap F$ splits completely in the extension $N_2/F$. Now the result follows by Chebotarev Density Theorem (see [37], Chapter V, Section 10, Theorem 10.4).

**B.4.5 Lemma.**

Let $K \subset L \subset M$ be a finite extension of global fields with $M/K, L/K$ being Galois extensions. Let $\mathfrak{p}_K$ be a prime of $K$. Let $\mathfrak{p}_{L,1}, \mathfrak{p}_{L,2}$ be any two factors of $\mathfrak{p}_K$ in $L$. Then in $M$, it is the case that $\mathfrak{p}_{L,1}, \mathfrak{p}_{L,2}$ have the same number of factors.

**Proof.**

By Proposition 11, Section 5, Chapter 1 of [46], there exists a $\bar{\sigma} \in \text{Gal}(L/K)$ such that $\bar{\sigma}(\mathfrak{p}_{L,1}) = \mathfrak{p}_{L,2}$. Let $\sigma \in \text{Gal}(M/K)$ be an extension of $\bar{\sigma}$ to $M$. Then every factor of $\mathfrak{p}_{L,1}$ has to be mapped to a factor of $\mathfrak{p}_{L,2}$ by $\sigma$. Thus $\mathfrak{p}_{L,1}, \mathfrak{p}_{L,2}$ must have the same number of factors in $M$.

The next four lemmas consider when splitting “below” implies splitting “above” and vice versa.

**B.4.6 Lemma.**

Let $K/E$ be a separable extension of global fields. Let $K_G$ be the Galois closure of $K$ over $E$. Then an $E$-prime $\mathfrak{p}_E$ splits completely in $K$ if and only if it splits completely in $K_G$. (See [45], Chapter 6, Section 3, Proposition 6.3.2.)

**B.4.7 Lemma.**

Let $N_1/F, N_2/F$ be two separable global field extensions, with $N_1, N_2$ linearly disjoint over $F$ and $N_1/F$ Galois. Let $p$ be a prime of $F$ splitting completely into distinct factors in the extension $N_1/F$. Let $\mathfrak{p}_2$ be a prime above $p$ in $N_2$. Then $\mathfrak{p}_2$ splits completely into distinct factors in the extension $N_1N_2/N_2$.

**Proof.**

First of all we observe that as in Lemma B.3.5 we have that $\text{Gal}(N_1N_2/N_2) \cong \text{Gal}(N_1/F)$ with the isomorphism realized by restriction. Let $\mathfrak{p}_{1,2}$ lie above $\mathfrak{p}_2$ and let $\sigma$ be any element of its decomposition group over $F$. Then $\sigma|_{N_1}$ is an
element of the decomposition group of \( \varphi_1 = \varphi_{1,2} \cap N_1 \). However, since \( p \) splits completely in \( N_1 \) into distinct factors, the decomposition group of \( \varphi_1 \) is trivial and therefore \( \sigma_{|N_1} = \text{id}_{N_1} \). Let \( \alpha \in N_1 \) generate \( N_1 \) over \( F \) and \( N_1N_2 \) over \( N_2 \). Therefore, \( \alpha = \sigma_{|N_1}(\alpha) = \sigma(\alpha) \). Thus the decomposition group of \( \varphi_{1,2} \) over \( N_2 \) is trivial and therefore \( \varphi_2 \) splits completely in the extension \( N_1N_2/N_1 \).

**B.4.8 Lemma.**

Let \( N_1/F, N_2/F \) be two separable global field extensions, with \( N_1, N_2 \) Galois over \( F \) and \( [N_1 : F] \) relatively prime to \( [N_2 : F] \). Let \( p \) be a prime of \( F \) not splitting in \( N_1 \). Let \( \varphi_2 \) be above \( p \) in \( N_2 \). Then \( \varphi_2 \) does not split in the extension \( N_1N_2/N_2 \).

**Proof.**

First, consider the diagram below.

Now note that the extension \( F \subset N_1 \subset N_1N_2 \) is a Galois extension by Lemma B.3.6. The number of factors \( p \) in \( N_1N_2 \) must be a divisor of \( [N_1N_2 : N_1] = [N_2 : F] \). Suppose \( \varphi_2 \) does not remain prime in the extension \( N_2 \subset N_2N_1 \). Then the number of factors of \( \varphi_2 \) in \( N_1N_2 \) is a non-trivial divisor of \( [N_1N_2 : N_1] \). Since \( N_1N_2/F \) is Galois, every factor of \( p \) in \( N_2 \) has the same number of factors in \( N_1N_2 \) by Lemma B.4.5, and therefore the number of factors of \( p \) in \( N_1N_2 \) must have a non-trivial common factor with \( [N_1 : F] \). But this contradicts the fact this number must be a divisor of \( [N_2 : F] \). Thus, \( \varphi_2 \) does not split in the extension \( N_1N_2/N_2 \).

**B.4.9 Lemma.**

Let \( F/E \) and \( H/E \) be Galois extensions of global fields with \( F \) and \( H \) linearly disjoint over \( E \). Let \( p_F \) be a prime of \( F \) not splitting in the extension \( HF/F \).
Let $p_E$ be the prime below it in $E$. Then there is only one prime above $p_E$ in $H$.

**Proof.**

Consider the following picture.

By Lemma B.3.5, $\text{Gal}(FH/F) \cong \text{Gal}(H/E)$ and the isomorphism is realized by restriction. Let $p_{FH}$ be the single factor of $p_F$ in $FH$. Then its Frobenius automorphism $\sigma$ is a generator of $\text{Gal}(FH/F)$ and restriction of $\sigma$ to $H$ will generate $\text{Gal}(H/E)$. But $\sigma|_H$ will fix $p_H = p_{FH} \cap H$ – a prime of $H$ lying above $p_E$. Thus, $p_E$ has only one prime above it in $H$.

The next lemma considers a slightly more complicated situation where one of the extensions under consideration is not necessarily Galois.

**B.4.10 Lemma.**

Let $K/E$ be a separable extension of global fields. Let $K_G$ be the Galois closure of $K$ over $E$. Let $M/E$ be a cyclic extension of $E$ such that

$$([M : E], [K_G : E]) = 1$$

and $[M : E]$ is a prime number. Let $p_1, \ldots, p_{[K:E]}$ be all the factors in $K$ of an $E$-prime $p_E$, splitting completely in the extension $K/E$. Then

- the following statements are equivalent:
  - for some $i$ we have that $p_i$ splits completely in the extension $MK/K$,
  - $p_E$ splits completely in the extension $EM/M$,
  - some factor of $p_E$ in $K_G$ splits completely in the extension $EK_G/K_G$,

- either all $p_1, \ldots, p_{[K:E]}$ split completely in $MK_G/K$ or none does.
Proof.

By Lemma B.4.6, $p_E$ splits completely in $K_G/E$ if and only if $p_E$ splits completely in $K/E$. Thus, we can conclude that for all $i$ we have that $p_i$ splits completely in the extension $K_G/K$. Therefore, $p_i$ splits completely in $MK_G/K$ if and only if every factor $p_{K_G}$ of $p_i$ in $K_G$ splits completely in the extension $MK_G/K_G$. By Lemma B.3.3, $([M:E],[K_G:E]) = 1$ implies that $M$ and $K_G$ are linearly disjoint over $E$ and consequently $[MK_G : K_G] = [M:E]$ is a prime number. Thus, either $p_{K_G}$ splits completely or it is inert in the extension $MK_G/K_G$. Therefore $([M:E],[K_G:E]) = 1$ also implies by Lemmas B.4.8 and B.4.7 that $p_{K_G}$ splits completely in $MK_G/K_G$ if and only if $p_E$ splits completely in the extension $MK_G/K_G$.

Applying an analogous argument to the Galois extension $K_GM/K$ we conclude that $p_{K_G}$ splits completely in $MK_G/K_G$ if and only if $p_i$ splits completely in $MK/K$.

Thus $p_i$ splits completely in the extension $MK/K$ if and only if $p_E$ splits completely in the extension $M/E$. So the splitting behavior is uniform across $p_E$-factors in $K$.

The next lemma deals with cyclic extensions of prime degree. They play an important role in implementation of the norm method for defining integrality at finitely many primes.

**B.4.11 Lemma.**

Let $q$ be a rational prime. Let $G$ be any field of characteristic different from $q$. Let $a \in G$, and let $\alpha$ be a root of the polynomial $T^q - a$. Then the following statements are true.

1. If $a \in G$ is not a $q$-th power, then the polynomial $X^q - a$ is irreducible over $G$.

2. Assume that $G$ has all the $q$-th roots of unity. Then $[G(\alpha) : G] = q$ or $[G(\alpha) : G] = 1$. Further, in the first case, the extension is cyclic.

3. If $G$ is a global field and $\mathfrak{p}$ is a prime of $G$ such that $\text{ord}_\mathfrak{p} q = 0$ and $\text{ord}_\mathfrak{p} a = 0$, then $\mathfrak{p}$ is not ramified in the extension $G(\alpha)/G$, and $\mathfrak{p}$ has a relative degree one factor in this extension if and only if $a$ is equivalent to a $q$-th power modulo $\mathfrak{p}$. If $G$ has primitive $q$-th root of unity, then we can substitute “will split completely” for “will have a relative degree one factor”.

294
4. If $G$ is a global field, $\text{ord}_p a \not\equiv 0 \mod q$ and the extension $G(\alpha)/G$ is not trivial, then $\mathfrak{p}$ is ramified completely in this extension.

**Proof.**

Part of the Lemma follows from Theorem 16, p. 221 of [47]. The rest is left as an exercise for the reader.

The next proposition describes a generalization of sorts for the notion of integral basis. This result allows us to make sure that the norm equations widely used in this book have the solutions we require.

**B.4.12 Lemma.**

Let $K/F$ be a finite separable global field extension. Let $K_G$ be the Galois closure of $K$ over $F$. Let $\Omega = \{\omega_1, \ldots, \omega_m\} \subset K$ be a basis of $K$ over $F$. Let $\mathcal{D}$ be the determinant of the matrix $(\omega_{i,j})$, where $\omega_{i,1} = \omega_1, \ldots, \omega_{i,m}$ are all the conjugates of $\omega_i$ over $F$. (Note that $\mathcal{D}^2$ is the discriminant of $\Omega$.) Let $p$ be a prime of $F$ such that all the elements of $\Omega$ are integral with respect to $p$. Let $p = \prod_{i=1}^s p_i^{e_i}$ be the factorization of $p$ in $K_G$. Let $h \in K$ be integral at $p$ and let $h = \sum_{i=1}^m a_i \omega_i$, where $a_i \in F$. Then for $i = 1, \ldots, m$ we have that $\text{ord}_p a_i \geq e^{-1} \text{ord}_p \mathcal{D}^{-1}$, for all $j = 1, \ldots, s$. In particular, if for all $j = 1, \ldots, s$, we have that $\text{ord}_p \mathcal{D} = 0$, then for all $i = 1, \ldots, m$, we also have that $a_i$'s are integral at $p$, and $\Omega$ is an integral basis with respect to $p$. Finally, in all cases $\mathcal{D}^2 a_i$ is integral at $p$.

**Proof.**

Consider the following linear system.

$$\sum_{i=1}^m a_i \omega_{i,r} = h_r,$$

where $r = 1, \ldots, m$ and $h_1 = h, \ldots, h_m$ are all the conjugates of $h$ over $F$. The determinant of this system is $\mathcal{D}$. Solving this system by Cramer's rule, we conclude that

$$a_i = \frac{\mathcal{D}_i}{\mathcal{D}},$$

where $\mathcal{D}_i \in K_G$ is integral with respect to $p$.

The following proposition explains how to determine whether a particular prime splits in a finite extension.
B.4.13 Lemma.

Let $K$ be a global field. Let $p$ be a prime of $K$. Let $E/K$ be a finite separable extension of $K$ generated by an element $\gamma \in E$, integral at $p$. Let $g(t)$ be the monic irreducible polynomial of $\gamma$ over $K$. Assume further that the discriminant of $\gamma$ is a unit at $p$ and $g(t) = \prod_{i=1}^{k} g_i(t) \mod p$, where $g_i(t)$ is a monic polynomial irreducible in the residue field of $p$ of degree $f_i$. Then in $E$ we have that $p = \prod_{i=1}^{k} p_i$, where $p_i$ is a prime of $E$ of relative degree $f_i$ over $p$.

Proof.

See Proposition 25, Chapter I, Section 8 of [46] and Lemma B.4.12.

The lemma below tells us that for each prime we can find an extension where it splits. This issue comes up in the discussion of definability of the set of non-zero elements of local subrings of number fields.

B.4.14 Lemma.

Let $K$ be a global field. Let $p$ be any prime of $K$. Then there exists an extension $M$ of $K$ where $p$ has two or more distinct factors.

Proof.

Let $q \neq p$ be any other prime of $K$. By the Strong Approximation Theorem there exists $a \in O_K$ such that $\text{ord}_q a = 1$ and $a \equiv 1 \mod p$. Let $\alpha$ be a root of $T^p - a$, where $p$ is a rational prime distinct from the characteristic of the field and relatively prime to $p$ in the case of a number field. Then $M = K(\alpha)$ is an extension of degree $p$, $p$ does not divide the discriminant of $\alpha$, and $T^p - a$ factors modulo $p$. Thus, by Lemma B.4.13 and Lemma B.4.12, $p$ splits in the extension $M/K$ into distinct factors.

When dealing with function fields, it is often useful to assume that primes under consideration are of degree 1. The next lemma tells us what needs to be done to achieve this.

B.4.15 Lemma.

Let $M$ be a function field over a finite field of constants. Let $p$ be a prime of $M$. Let $C_p$ be the residue field of $p$. Then in the extension $C_p M/M$, we have that $p$ will split completely into factors of degree 1.
Proof.

Let $\gamma \in C_p$ be a generator of $C_p$ over $C_M$ – the constant field of $M$. Then $\gamma$ will also generate the extension $C_p M/M$. Let $f(t)$ be the monic irreducible polynomial of $\gamma$ over $C_M$ and $M$ (it must be the same by Theorem 11, Section 3, Chapter XV of [1]). Then it splits completely mod $p$, since all finite extensions of finite fields are Galois. Further, since $\alpha$ is a constant its discriminant over $M$ is not divisible by $p$. Thus, by Lemma B.4.13, $p$ will split into $[C_p M : M]$ factors of relative degree 1 over $p$. Hence the residue field of every factor of $p$ will be $C_p$. But by Theorem 13, Section 3, Chapter XV of [1], the constant field of $C_p M$ is $C_p$ and therefore every factor of $p$ will be of degree 1.

The result below describes a useful property of degree one primes.

B.4.16 Lemma.

Let $M$ be a function field over a finite field of constants. Let $p$ be a prime of $M$ of degree 1. Let $E/M$ be a constant field extension. Then $p$ will not split in the extension $E/M$ and retain degree 1.

Proof.

Let $\gamma \in C_E$, the constant field of $E$, generate the extension. Let $f(t)$ be the monic irreducible polynomial of $\gamma$ over $M$. Then $f(t)$ must also be the monic irreducible polynomial of $\gamma$ over $C_M$ by Theorem 11, Section 3, Chapter XV of [1]. Thus, $f(t)$ will remain prime modulo $p$. Therefore, by Lemma B.4.13, $p$ will remain prime in $E$. The single factor of $p$ in $E$ will therefore have a relative degree $[E : M]$ over $p$ and thus the residue field of the factor must be of degree $[E : M]$ over the residue field of $p$ equal to $C_M$. But by Theorem 13, Section 3, Chapter XV of [1], the constant field of $E$ is equal to $C_M(\gamma)$ and therefore is also of degree $[E : M]$ over $C_M$. Since the residue field of the factor must be an extension of the constant field of $E$, these fields must be equal.

The following proposition explains why constant field extensions are intrinsically simpler than non-constant ones.

B.4.17 Lemma.

Let $M$ be a function field over a finite field of constants. Let $E/M$ be a constant field extension. Then no prime of $M$ ramifies in this extension.
Proof.

Since $E/M$ is a constant field extension, it is generated by a constant element of $E$. The discriminant of the power basis of this constant element is not divisible by any prime. Therefore, by Proposition 8, Section 2, Chapter III of [46], no prime ramifies in this extension.

The next two lemmas tell us how to generate large sets of elements without zeros at any prime belonging to a fixed infinite set of primes.

B.4.18 Lemma.

Let $M/K$ be a separable global field extension generated by an element $\alpha$ of $M$. Let $G(T)$ be the monic irreducible polynomial of $\alpha$ over $K$. Let $\mathfrak{p}_K$ be a prime of $K$ such that $\mathfrak{p}_K$ does not have a relative degree one factor in $M$, does not divide the discriminant of $G(T)$ and is not a pole of any coefficient of $G(T)$. Then for all $x \in K$, we have that $\text{ord}_{\mathfrak{p}_K} G(x) \leq 0$.

Proof.

By Lemma B.4.12, the power basis of $\alpha$ is an integral basis with respect to $\mathfrak{p}_K$. Therefore, by Proposition 25, Section 7, Chapter I of [46], $G(T)$ has no roots modulo $\mathfrak{p}_K$ if and only if $\mathfrak{p}_K$ has no relative degree one factors in $M$. Thus if $\text{ord}_{\mathfrak{p}_K} x \geq 0$ we conclude that $\text{ord}_{\mathfrak{p}_K} G(x) = 0$. On the other hand, if $\text{ord}_{\mathfrak{p}_K} x < 0$, then $\text{ord}_{\mathfrak{p}_K} G(x) < 0$, since $G(T)$ is monic and all the coefficients are integral at $\mathfrak{p}_K$.

B.4.19 Lemma.

Let $K$ be a global field. Let $\mathcal{W}$ be a set of non-archimedean primes of $K$ such that in some finite extension $M$ of $K$ only finitely many primes of $\mathcal{W}$ have a factor of relative degree one. Then there exists a polynomial $F(X) \in K[X]$, such that for all $x \in K$ and for all $p \in \mathcal{W}$ we have that $\text{ord}_p F(x) \leq 0$.

Proof.

From Lemma B.4.18 we know that there exists a monic $G(X) \in K[X]$ such the for all but finitely $p \in \mathcal{W}$, for all $x \in K$ we have that $\text{ord}_p G(x) \leq 0$. Let $p_1, \ldots, p_l$ be all the “exceptions”. Let $G(X) = \sum_{i=0}^k A_i X^i$. Let $m = \max\{|\text{ord}_{p_i} A_j| : i = 1, \ldots, l, j = 1, \ldots, k\}$. Let $a \in K$ be such that for all $i = 1, \ldots, l$ we have that $\text{ord}_{p_i} a = -2m$ (such an $a$ exists by the Strong
Approximation Theorem) and consider \( F(X) = G(X^{3m} + a) \). Observe that by assumptions on \( G(X) \), for all \( p \in \mathcal{W} \setminus \{p_1, \ldots, p_l\} \), for all \( x \in K \), it is the case that \( \text{ord}_p F(x) \leq 0 \). Next let \( x \in K \) and consider \( \text{ord}_p F(x) \). Suppose, \( \text{ord}_p x \geq 0 \). Then \( \text{ord}_p (x^{3m} + a) = \text{ord}_p a = -2m \). Thus,

\[
\text{ord}_p F(x) = \text{ord}_p \left( \sum_{j=0}^{k} A_j (x^{3m} + a)^j \right)
\]

\[
= \min \{ \text{ord}_p A_i + \text{ord}_p (a + x^{3m})^i, i = 0, \ldots, k \} = \\
\min \{ \text{ord}_p A_i - 2im, i = 0, \ldots, k \} = -2km < 0,
\]

since for \( i = 0, \ldots, k - 1 \) we have that

\[
\text{ord}_p A_i - 2im \geq -2im - m \geq -2(k - 1)m - m = \\
-2km + m > -2km = \text{ord}_p (a + x^{3m})^k.
\]

Suppose now that \( \text{ord}_p x < 0 \). In this case \( \text{ord}_p (x^{3m} + a) = 3m \text{ord}_p x < -3m \). Further, as above, we have

\[
\text{ord}_p F(x) = \text{ord}_p \left( \sum_{j=0}^{l} A_j (x^{3m} + a)^j \right) = \\
\min \{ \text{ord}_p A_i + \text{ord}_p (a + x^{3m})^i, i = 0, \ldots, k \} \leq -3km < 0,
\]

since for \( i = 0, \ldots, k - 1 \) we have that

\[
\text{ord}_p A_i + \text{ord}_p (a + x^{3m})^i \geq 3im \text{ord}_p x - m \geq 3(k - 1)m \text{ord}_p x - m \\
= 3km \text{ord}_p x - (3m \text{ord}_p x + m) > 3km \text{ord}_p x = \text{ord}_p (a + x^{3m})^k.
\]

Thus for all \( p \in \mathcal{W} \), for all \( x \in K \), we have that \( \text{ord}_p F(x) \leq 0 \).

The next lemma explains how to determine the intersection of a ring of \( \mathcal{W} \)-integers with a subextension, knowing the pattern of the prime splitting for primes below primes in \( \mathcal{W} \).

**B.4.20 Lemma.**

Let \( K/L \) be a finite extension of global fields. Let \( \mathcal{W}_K \) be a set of \( K \)-primes. Let \( \mathcal{W}_L \) be the set of all the primes \( p_L \) of \( L \) such that every \( K \)-factor of \( p_L \) is in \( \mathcal{W}_K \). Then \( \mathcal{O}_{K, \mathcal{W}_K} \cap L = \mathcal{O}_{L, \mathcal{W}_L} \).
Proof.

Suppose \( x \in \mathcal{O}_{K,\mathcal{U}_K} \cap L \). Then for all \( q \notin \mathcal{U}_K \) we have that \( \text{ord}_{q} x \geq 0 \). Let \( t_L \) be a prime of \( L \) not in \( \mathcal{U}_L \). Then there exists at least one \( K \)-factor \( \mathcal{T}_K \) of \( t_L \) such that \( \mathcal{T}_K \notin \mathcal{U}_K \). Therefore, \( \text{ord}_{\mathcal{T}_K} x \geq 0 \). Next consider the divisor of \( x \) in \( L \):

\[
 t_L^2 \prod t_{L,i}^{a_i}.
\]

where \( a_i \in \mathbb{Z} \), only finitely many \( a_i \) are not zero, for all \( i \), we have that \( t_{L,i} \neq t_L \), and all \( t_{L,i} \) are distinct. Hence the divisor of \( x \) in \( K \) has the form

\[
 \prod_{j} \mathcal{T}_K^{e_j} \prod_{j} \prod_{k,j} t_{K,i,j}^{a_i e_j}.
\]

where \( t_L = \prod_j \mathcal{T}_K^{e_j} \), \( t_{L,i} = \prod_j \mathcal{T}_K^{e_j} \). Thus, in \( K \) we have that

\[
 \text{ord}_{\mathcal{T}_K} x = ae_j.
\]

But for some \( j \), this order must be non-negative. Since ramification degree is always positive, we must conclude that \( a \geq 0 \). Thus, \( \text{ord}_K x \geq 0 \) for all \( t_L \notin \mathcal{U}_L \) and consequently \( x \in \mathcal{O}_{K,\mathcal{U}_K} \).

Conversely, suppose \( x \in \mathcal{O}_{L,\mathcal{U}_L} \). Let \( \mathcal{T}_K \notin \mathcal{U}_K \). Let \( t_L \) be the prime below \( \mathcal{T}_K \) in \( L \). Then by definition of \( \mathcal{U}_L \), we have that \( t_L \notin \mathcal{U}_L \) and \( \text{ord}_L x \geq 0 \). Next as before, let \((B.4.1)\) be the \( L \)-divisor of \( x \) and let \((B.4.2)\) be the \( K \)-divisor of \( x \). Then \( a \geq 0 \) and for some \( j \), we have that \( \text{ord}_{\mathcal{T}_K} x = ae_j \geq 0 \) for all \( \mathcal{T}_K \notin \mathcal{U}_K \). Hence, \( x \in \mathcal{O}_{K,\mathcal{U}_K} \). Since by assumption \( x \in L \), we can conclude that \( x \in \mathcal{O}_{K,\mathcal{U}_K} \cap L \).

The following proposition tells us that only non-constant extensions change the degree of divisors.

**B.4.21 Lemma.**

Let \( H/L \) be a finite separable extension of function fields and let \( C_H \) be the constant field of \( H \). Let \( u \) be an integral divisor of \( L \). Then \( \text{degd}_{H}(u) = [H : C_H L] \text{degd}_{L}(u) \). (See [1, Theorem 9 and Theorem 14, Section 3, Chapter XV])

The next lemma describes behavior of some primes under constant field extensions.
**B.4.22 Lemma.**

Let $H$ be a function field over a finite field of constants $C$. Let $p$ be a prime of $H$. Let $\hat{C}$ be a finite extension of $C$ such that $[\hat{C} : C]$ is prime to the degree of $p$. Then $p$ remains prime in $\hat{C}H$.

**Proof.**

Since $\hat{C} / C$ is a separable extension, by Theorem 14, Section 3, Chapter XV of [1], we have that $\hat{C}$ is the constant field of $\hat{C}H$. Let $\wp$ be a $\hat{C}H$-prime above $p$, let $R_p$ and $R_{\wp}$ be the residue fields of $p$ and $\wp$ respectively, and consider the following diagram:

```
\begin{aligned}
\hat{C} & \longrightarrow & R_{\wp} \\
C & \aleq & R_p
\end{aligned}
```

From the diagram we can conclude that

$$[R_{\wp} : C] = [R_{\wp} : R_p][R_p : C] = [R_{\wp} : \hat{C}][\hat{C} : C].$$

or, in other words,

$$f(\wp/p)\deg(p) = \deg(\wp)[\hat{C} : C].$$

Thus, since $([\hat{C} : C], \deg(p)) = 1$, we must conclude that $\deg(p)$ divides $\deg(\wp)$. Hence, $\deg(\wp)$ is at least as big as the degree of the divisor $p$ in $\hat{C}H$ because by Lemma B.4.21, the degree of a divisor stays the same under a separable constant field extension. On the other hand, since $\wp \mid p$, $\deg(\wp)$ is less or equal to the degree of $p$ as a divisor of $\hat{C}H$. Thus, we must conclude that $\deg(p)$ as a divisor of $\hat{C}H$ is equal to the degree(\wp) and $\wp$ is the only prime of $\hat{C}H$ above $p$.

The following two propositions are necessary ingredients of the proof of the fact that if under a separable extension of function fields there is one prime which does not split, then there are infinitely many such primes. This assertion plays an important role in the proof of Diophantine undecidability of global function fields.
B.4.23 Lemma.

Let $M$ be a Galois extension of an algebraic function field $L$ over a finite field of constants, and assume $U$ is an algebraic function field such that $L \subset U \subset M$, and $U$ is not necessarily Galois over $L$. Further, let $p_L$ be a prime of $L$ which does not split in $U$. Let $p_U$ be the prime above $p_L$ in $U$, let $p_M$ be a prime of $M$ above $p_U$, let $G(p_M)$ be the decomposition group of $p_M$ over $L$, and let $\sigma \in G(p_M)$ be such that its coset modulo the inertia group of $p_M$ induces the Frobenius automorphism $\phi_{p_M}$ on the residue field of $p_M$ over the residue field of $p_L$. (In other word, $\phi_{p_M}(c) = c^{p_L}$ for all $c$ in the residue field of $p_M$.) The picture below corresponds to the data in the lemma with $T(p_M)$ being the inertia group of $p_M$ and $M^{T(p_M)}$ the fixed field of $T(p_M)$.

Then $\sigma^{f(p_U/p_L)} \in \text{Gal}(M/U)$, and $f(p_U/p_L) = [U : L]$ is the smallest positive exponent such that the corresponding power of $\sigma$ is in $\text{Gal}(M/U)$

Proof.

First of all observe that since $p_L$ does not split in $U$, $p_U$ is not ramified over $L$ and therefore indeed $U \subset M^{T(p_M)}$ by Lemma B.4.1. Further, $T(p_M) \subset \text{Gal}(M/U)$. Next observe that since the equivalence class of $\sigma$ generates $G(p_M)/T(p_M)$, every element $\phi \in G(p_M)$ can be written as $\sigma^i \psi$, $\psi \in T(p_M)$, $i = 0, \ldots, f(p_M/p_L) - 1$. Let $H(p_M)$ be the decomposition group of $p_M$ with respect to $U$ and note that $T(p_M) \subset H(p_M)$. Next we observe that

$$f(p_U/p_L) = \frac{f(p_M/p_L)}{f(p_M/p_U)} = \frac{|G(p_M)/T(p_M)|}{|H(p_M)/T(p_M)|} = \frac{|G(p_M)|}{|H(p_M)|}$$

Further observe that

$$H(p_M) = G(p_M) \cap \text{Gal}(M/U)$$

$$= \{\sigma^i \psi, \psi \in T(p_M), i = 0, \ldots, f(p_M/p_L) - 1\} \cap \text{Gal}(M/U).$$

On the other hand for $\psi \in T(p_M)$, we have that $\sigma^i \psi \in H(p_M)$ if and only if $\sigma^i \in H(p_M)$ since $T(p_M) \subset H(p_M)$. Let $r$ the smallest positive exponent.
such that $\sigma^r \in H(p_M)$. Then every element of $H(p_M)$ can be written as $\sigma^m \psi$, where $\psi \in T(p_M)$ and $m \in \mathbb{N}$. Thus,

$$f(p_U/p_L) = \frac{|G(p_M)|}{|H(p_M)|} = r.$$

**B.4.24 Corollary.**

Let $M, L, U, \sigma$ as in Lemma B.4.23. Let $q_M$ be a prime of $M$ whose Frobenius automorphism over $L$ is $\sigma$. Let $q_L = q_M \cap L$. Then $q_L$ does not split in the extension $U/L$.

**Proof.**

By assumption $q_L$ is not ramified in the extension $U/L$ and $G(q_M)$ – the decomposition group of $q_M$ over $L$ is a cyclic group generated by $\sigma$. Similarly, $H(q_M)$ – the decomposition group of $q_M$ over $U$ is also a cyclic group generated by $\sigma$. Further the size of the quotient group

$$|G(q_M)/H(q_M)| = r,$$

since $r$ is the smallest positive integer such that $\sigma^r \in \text{Gal}(M/U) \cap G(q_M) = H(q_M)$. Therefore, by Lemma B.4.23,

$$f(q_U/q_L) = \frac{f(q_M/q_L)}{f(q_M/q_U)} = \frac{|G(q_M)|}{|H(p_M)|} = r = [U : L],$$

where $q_U = q_M \cap U$. Therefore the assertion of the corollary is true.

The next nine lemmas play an important role in the proofs of results concerning Diophantine definability over holomorphy rings of function fields. Their main role is to assure existence of “sufficiently” many degree one primes not splitting in the given cyclic extensions. (See Section 10.2 for more details.)

**B.4.25 Lemma.**

Let $L$ be a function field over a finite field of constants $C$. Let $q$ be a prime of $L$. Let $F(T) \in L[T]$ be monic and irreducible with coefficients integral with respect to $q$. Assume $F(T)$ remains irreducible modulo $q$. Let $R(q)$ be the residue field of $q$. Let $E = R(q)L$ and let $\tau$ be a prime above $q$ in $E$. Then $F(T)$ is irreducible modulo $\tau$. 
Proof.

It is enough to show that the residue fields of \( q \) and \( t \) are the same. By Lemma B.4.14, we know that \( q \) will split into factors of degree 1 in \( E \). Thus, the residue field of \( t \) is the constant field of \( E \). Since constant field extensions of global fields are separable, by Theorem 13, Section 3, Chapter XV of [1], the constant field of \( E \) is actually \( R(q) \).

B.4.26 Lemma.

Let \( U/L \) be a finite separable extension of function fields over finite field of constants. Assume the constant fields of \( U \) and \( L \) are the same and denote this finite field by \( C \). Let \( q_L \) be a prime of \( L \) not splitting in \( U \). Let \( C'/C \) be a finite extension where \([C' : C] = \deg(q_L)\). Let \( q'_L \) lie above \( q_L \) in \( L' = C'L \). Then \( q'_L \) does not split in the extension \( U'/L' \), where \( U' = C'U \).

Proof.

By Lemma B.3.4, \([U' : L'] = [U : L]\). Let \( \alpha \in U \) be an element integral at \( q_L \) and such that its residue class modulo \( q_U \) generate the residue field of \( q_U \) over the residue field of \( q_L \). (Here \( q_U \) is the \( U \)-prime above \( q_L \).) Then \( \alpha \) also generates \( U \) over \( L \), the discriminant of the monic irreducible polynomial of \( \alpha \) over \( L \) is a unit at \( q_L \), and by Lemma B.4.13, this polynomial does not factor modulo \( q \). Since a finite field has only one extension of every degree, by Lemma B.4.15, \( q \) will split completely into degree 1 factors in the extension \( U'/U \). Thus \( q' \) is of degree 1 and its residue field is \( C' \), which is also the residue field of \( q \). Since \([U' : L'] = [U : L]\), the monic irreducible polynomial of \( \alpha \) over \( L \) is the same as over \( L' \), and by Lemma B.4.25, the monic irreducible polynomial of \( \alpha \) over \( L' \) will be irreducible modulo \( q' \). Therefore, again by Lemma B.4.13, \( q' \) will not split in the extension \( U'/L' \).

B.4.27 Proposition.

Let \( M \) be a Galois extension of an algebraic function field \( L \) over a finite field of constants, let \( C_L \) be the constant field of \( L \), let \( C_M \) be the constant field of \( M \), let \( t \) be a non-constant element of \( L \). Let \( \sigma \in \text{Gal}(M/L) \), and let

\[ \mathscr{C} = \{ \tau \sigma \tau^{-1} | \tau \in \text{Gal}(M/L) \} \]

Let \( \mathcal{P}(L) \), as before, be the set of all primes of \( L \). Then for a positive integer \( k \), let

\[ \mathcal{P}_k(L) = \{ p_L | p_L \in \mathcal{P}(L) \land \deg(p_L) = k \land p_L \text{ is unramified over } C_L(t) \} \]
Further, let \( p^r \) be the size of \( C_L \), let \( \phi = \phi_{C_L} \) be the generator of \( \text{Gal}(C_M/C_L) \) sending each element \( c \in C_M \) to \( c^{p^r} \), and assume that for every \( \psi \in \mathcal{C} \), we have that \( \psi|_{C_M} = \phi^a \) for some natural integer \( a \) different from zero. Then if \( k \) is a positive integer such that \( k \equiv a \) modulo \( [C_M : C_L] \), \( d = [L : C_L(t)] \), and

\[
C_k(M/L, \mathcal{C}) = \{ p_L | p_L \in \mathcal{P}_k(L) \wedge \exists \mathcal{P}_M \in \mathcal{P}(M) : p_L \wedge \left( \frac{M/L}{\mathcal{P}_M} \right) \in \mathcal{C} \},
\]

then

\[
\left| C_k(M/L, \mathcal{C}) - \frac{|\mathcal{C}|}{km} p^{rk} \right| < \frac{|\mathcal{C}|}{km} \left( (m+2g_M)p^{rk/2} + m(3g_L+1)p^{3kr/4} + 2(g_M+dm) \right).
\]

(B.4.3)

where \( g_M, g_L \) are genus of \( M \) and \( L \) respectively. (The proof of this proposition can be found in [34][Proposition 13.4].)

**B.4.28 Corollary.**

Let \( M/L \) be a Galois extension of function fields over the same finite field of constants \( C \). Let \( t, d, m, r, g_L, g_M \) be as in Proposition B.4.27. Let \( \sigma \in \text{Gal}(M/L) \). Then for any sufficiently large positive integer \( k \), there exists an \( L \)-prime \( p_L \) of degree \( k \) such that \( \sigma \) is the Frobenius automorphism of a factor of \( p_L \) in \( M \).

**Proof.**

Since we have assumed that \( M \) and \( L \) have the same field of constants, the Inequality (B.4.3) holds for any \( k \) and implies

\[
\left| C_k(M/L, \mathcal{C}) \right| > \frac{|\mathcal{C}|}{km} p^{rk/2} \left( 1 - \frac{(m+2g_M)}{p^{rk/2}} - \frac{m(3g_L+1)}{p^{3kr/4}} - \frac{2(g_M+dm)}{p^{rk/2}} \right).
\]

(B.4.4)

Thus for all sufficiently large \( k \), we have that \( |C_k(M/L, \mathcal{C})| > 1 \).

**B.4.29 Corollary.**

Let \( M/L \) be a Galois extension of function fields over the same finite field of constants \( C \). Let \( t, d, m, r, g_L, g_M \) be as in Proposition B.4.27. Let \( \sigma \in \text{Gal}(M/L) \), let \( \mathcal{C} \) be the conjugacy class of \( \sigma \), and assume that

\[
\frac{1}{4} |\mathcal{C}| > (m + 4g_M + 3mg_L + 2dm)^2.
\]

Then \( |C_1(M/L, \mathcal{C})| > \frac{|\mathcal{C}|}{2m}. \)
Proof.

As in Corollary B.4.28 we start with Inequality (B.4.4). Substituting 1 for $k$, and keeping in mind that $|C| = p^r$, we obtain

$$|C_1(M/L, \mathcal{C})| > \frac{|C|}{m} p^r \left(1 - \frac{(m + 2gM)}{p^{r/2}} - \frac{m(3gL + 1)}{p^{3r/4}} - \frac{2(gM + dm)}{p^r}\right),$$

(B.4.5)

$$|C_1(M/L, \mathcal{C})| > \frac{|C|}{m} \left(1 - \frac{(m + 3gLm + 4gM + 2dm)}{\sqrt{|C|}}\right) > \frac{|C|}{2m}$$

(B.4.6)

B.4.30 Corollary.

Let $G/F$ be a cyclic extension of function fields over the same finite field of constants $|C| = p^r$. Let $d = [F : C(t)]$. Let $m = [G : F]$. Let $g_G, g_F$ be the genus’ of $G$ and $F$ respectively. Let $l > 2 \log_p 2(m + 4g_G + 3mg_F + 1 + 2dm)$, $l \equiv 0 \mod r$. Let $C_i$ be the splitting field of the polynomial $X^p - X$ over the field of characteristic $p$. Then there are more than $p{l/2m}$ primes of $C_iF$ of degree 1 not splitting in the extension $C_iG/C_iF$.

Proof.

By Lemma B.3.5, $C_iG/C_iF$ is also a cyclic extension. Let $\sigma$ be a generator of the Galois group and let $\mathcal{C} = \{\sigma\}$. We want to estimate the lower bound on $|C_1(C_iG/C_iF, \mathcal{C})|$. First of all, we note that the constant field of $C_iF$ and $C_iG$ is indeed $C_i$ and $|C_i| > (2(m + 4g_G + 3mg_F + 1 + 2dm))^2$. Thus we can apply Corollary B.4.29 to conclude that

$$|C_1(C_iG/C_iF, \mathcal{C})| > |C_i|/2m > p{l/2m}$$

On the other hand, all the primes in $C_1(C_iG/C_iF, \mathcal{C})$ do not split in the extension $C_iG/C_iF$.

B.4.31 Proposition.

Let $G/F$ be a cyclic extension of function fields over the same field of constants $C$ of size $p^r$ for some positive $r \in \mathbb{N}$. Let $m, l, d, t, g_G, g_F, C_i$ be as in Corollary B.4.30. Let $C_{qG}, C_{qI}$ be finite extensions of $C_i$ and $C_i$ respectively of degree $q$, where $(l, q) = 1$ and $(m, q) = 1$. Then there are at least $p{l/2m}$ primes of $C_iF$ of degree 1 not splitting in the extension $C_{qG}/C_iF$. Further, if $p_{C_{qG}}$ is a degree 1 prime of $C_{qG}$ not splitting in the extension $C_{qG}/C_iF$ and a $p_{C_iG}$ is a prime above it in $C_iG$, then $p_{C_iG}$ – the prime below $p_{C_{qG}}$ in $G$, does not split in the extension $C_{qG}/G$. 

Proof.

Consider the following picture.

First of all we observe that \(C_l\) and \(C_{qr}\) are linearly disjoint over \(C_r\) since

\[
[C_l : C_r] = l, \quad \quad [C_{qr} : C_r] = q,
\]

\((q, l) = 1\), and therefore

\(C_l \cap C_{qr} = C_r\).

Consequently, \(C_lC_q = C_{lq}\) and \([C_{lq} : C_l] = q\). Further,

\([GC_{lq} : GC_l] = [C_{lq} : C_q] = q\).

Next directly from Corollary B.4.30, we conclude that \(C_lF\) has the requisite number of degree 1 primes not splitting in the extension \(C_lG/C_lF\). We show that these degree 1 primes of \(C_lF\) actually continue to be inert in the extension \(C_{lq}G/C_lF\). So let \(p_{C_lF}\) be a degree 1 prime of \(C_lF\) inert in the extension \(C_lG/C_lF\). Let \(p_{C_lG}\) lie above \(p_{C_lF}\) in \(C_lG\). Then, since the constant fields of \(C_lF\) and \(C_lG\) are the same,

\[
\deg(p_{C_lG}) = m = [G : F] = [C_lG : C_lF]
\]

by Lemma B.4.21. Thus, by Lemma B.4.22, \(p_{C_lG}\) will not split in the extension \(C_{lq}G/C_lG\) because the degree of the extension \(q\) is relatively prime to the degree of this prime \(m\). This proves the first assertion of the lemma.

Next we note that \(C_lG\) and \(C_{qr}G\) are linearly disjoint Galois extensions of \(G\), by Lemma B.3.3, since \(C_lG \cap C_{qr}G = (C_l \cap C_{qr})G = C_rG = G\). Now we can conclude that that \(p_G\) does not split in the extension \(C_{qr}G/G\) by Lemma B.4.9, since the prime \(p_{C_lG}\) above it does not split in the extension \(C_{lq}G/C_lG\).
**B.4.32 Lemma.**

Let $C$ be a finite field of positive characteristic $p$ of size $p^r$. Let $t$ be transcendental over $C$, let $q 
eq p$ be a rational prime. Let $\beta$ be an element of the algebraic closure of $C$ of degree $q$ over $C$. Let $l \in \mathbb{N}$ be such that $(l, qr) = 1$. Let $P(t)$ be a polynomial in $t$ over $C$ such that $P(t)$ is a prime factor of

$$t^{p^l} - t,$$  \hspace{1cm} (B.4.7)

in $C[t]$ and $C(t)$-prime $\mathfrak{P}$ correspond to the polynomial $P(t)$. Then neither $\mathfrak{P}$, nor $P(t)$ split in the extension $C(t, \beta)/C(t)$.

**Proof.**

Let $\alpha$ be a root of $P(t)$ in the algebraic closure of $C$. Then $P(t)$ is the monic irreducible polynomial of $\alpha$ over $C$ and $\alpha^{p^l} - \alpha = 0$. Therefore $\alpha \in C_l - \text{a finite field of } p^l \text{ elements with } [C_l : \mathbb{F}_p] = l$. Let $n_\alpha = [\mathbb{F}_p(\alpha) : \mathbb{F}_p]$. Then $n_\alpha | l$ and therefore $(n_\alpha, qr) = 1$. Consequently, $\mathbb{F}_p(\alpha)$ and $C$ are linearly disjoint over $\mathbb{F}_p$ and therefore, the monic irreducible polynomial $P(t)$ of $\alpha$ over $C$ is also of degree $n_\alpha$. Further $P(t) \in \mathbb{F}_p[t]$ and will not factor under the extension of degree $q$. Finally, the prime corresponding to $P(t)$ is also of degree $n(\alpha)$ and thus it will not factor in the extension $C(t, \beta)/C$ by Lemma B.4.22.

The next proposition bounds the number of ramified primes in a series of extensions of global function fields.

**B.4.33 Proposition.**

Let $M/K$ be a finite separable extension of function fields. Let $\mathcal{E}_{M/K}$ be the set of all the primes of $M$ ramified in the extension $M/K$. Let

$$\mathcal{E}_{M/K} = \prod_{\mathfrak{e} \in \mathcal{E}_{M/K}} \mathfrak{e}.$$  

Let $C_K$ be the constant field of $K$ and let $C/C_K$ be a finite separable extension. Then the number of $CM$ primes ramified in the extension $CM/C_K$ is bounded by the degree of the divisor $\mathcal{E}_{M/K}$ in $M$.

**Proof.**

Consider the following diagram.
Observe the following. By Lemma B.4.17, no prime ramifies in the extensions $CM/M$ and $CK/K$. Let $\mathfrak{p}_{CM}$ be a prime of $CM$. Let $\mathfrak{p}_M, \mathfrak{p}_{CK},$ and $\mathfrak{p}_K$ be the primes below $\mathfrak{p}_{CM}$ in $M, CK$, and $K$ respectively. Then,

$$e(\mathfrak{p}_{CM}/\mathfrak{p}_K) = e(\mathfrak{p}_{CM}/\mathfrak{p}_{CK}) e(\mathfrak{p}_{CK}/\mathfrak{p}_K) = e(\mathfrak{p}_{CM}/\mathfrak{p}_M) e(\mathfrak{p}_M/\mathfrak{p}_K).$$

Thus, since $e(\mathfrak{p}_{CM}/\mathfrak{p}_M) = e(\mathfrak{p}_{CK}/\mathfrak{p}_K) = 1$, we conclude that $e(\mathfrak{p}_{CM}/\mathfrak{p}_{CK}) = e(\mathfrak{p}_M/\mathfrak{p}_K)$. Therefore, a prime of $CM$ is ramified in the extension $CM/CK$ if and only if the prime below it in $M$ is ramified in the extension $M/K$. Let $\mathcal{E}'$ be the set of all the primes of $CM$ ramified in the extension $CM/CK$. Let $\mathcal{E}' = \prod_{\mathfrak{p} \in \mathcal{E}'} \mathfrak{p}$. Then if we consider $\mathfrak{e}_{M/K}$ as a divisor of $CM$, we conclude that $\mathfrak{e}_{M/K} = \mathcal{E}'$. Further by Lemma B.4.21,

$$\deg_M(\mathfrak{e}_{M/K}) = \deg_{CM}(\mathfrak{e}_{M/K}) = \deg_{CM}(\mathcal{E}').$$

Therefore, the number of primes in $\mathcal{E}'$ cannot exceed $\deg_M(\mathfrak{e})$.

The lemma below bounds a number of “inconvenient” primes that can occur in a series of finite extensions of global function fields.

**B.4.34 Proposition.**

Let $M/K$ be a finite separable extension of function fields of degree $k$ over the same field of constants. Let $\alpha \in M$ be a generator of $M$ over $K$. Let $A = \{1, \ldots, \alpha^{k-1}\}$ be the power basis of $\alpha$. Let $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_{k-1}$ be all the conjugates of $\alpha$ over $K$. Let

$$\mathcal{D}(\alpha) = \prod_{i < j} (\alpha_i - \alpha_j)^2,$$

let

$$n(\alpha) = \prod_{q \in \mathcal{D}(K), \ord_q \mathcal{D}(\alpha) > 0} q,$$
let
\[ \varphi(\alpha) = \prod_{q \in \varphi(K), \alpha \text{ is not integral at } q} q. \]

Let \( C_K \) be the constant field of \( K \) and let \( C/C_K \) be a finite separable extension. Then the number of \( CK \) primes \( q_{CK} \) such that \( A \) is not an integral basis with respect to \( q_{CK} \) is bounded by the \( \deg(n(\alpha)\varphi(\alpha)) = n(\alpha) \) in \( K \).

Proof.

First of all, we point out that by Lemma B.3.4, \( A \) is also a power basis of \( CM \) over \( CK \). Next by Lemma B.4.12, if \( q_{CK} \) is a prime of \( CK \) such that \( A \) is not an integral basis with respect to \( q_{CK} \), then either \( \alpha \) is not integral at \( q_{CK} \) or \( \text{ord}_{q_{CK}} \varphi(\alpha) > 0 \). Let \( q_K \) be a \( K \)-prime below \( q_{CK} \). Then \( \alpha \) is not integral at \( q_K \) or \( q_K \) is a zero of \( \varphi(\alpha) \). Therefore, \( \text{ord}_{q_K}(n(\alpha)\varphi(\alpha)) > 0 \) and consequently
\[ \text{ord}_{q_{CK}}(n(\alpha)\varphi(\alpha)) > 0 \quad (B.4.8) \]
in \( CK \). The number of primes in \( CK \) satisfying (B.4.8) is bounded by \( CK \) degree of \( n(\alpha)\varphi(\alpha) \). On the other hand, by Lemma B.4.21, \( \deg_{CK}(n(\alpha)\varphi(\alpha)) = \deg_K(n(\alpha)\varphi(\alpha)) \) and the assertion of the lemma holds.

B.4.35 Lemma.

Let \( H/K \) be a separable extension of global fields. Let \( p \) be a prime of \( K \) remaining prime in \( H \). Then there exists an element \( \delta \in H \), generating \( H \) over \( K \), such that the power basis of \( \delta \) is an integral basis with respect to \( p \) and the monic irreducible polynomial of \( \delta \) over \( K \) remains irreducible modulo \( p \).

Proof.

Let \( \wp \) be the single factor of \( p \) in \( K \). Let \( \delta \in H \) be an element integral at \( p \) and such that its residue class generates the residue field of \( \wp \) over the residue field of \( p \). Let \( f(T) \) be the monic irreducible polynomial of \( \delta \) over \( K \). Let \( \tilde{f}(T) \) be the polynomial obtained from \( f(T) \) by reducing its coefficients modulo \( p \). Then \( \tilde{f} \) is irreducible over the residue field of \( p \) and therefore cannot have multiple roots. Thus, \( p \) does not divide the discriminant of \( f(T) \) and thus by Lemma B.4.12, the power basis of \( \delta \) is integral with respect to \( p \).

B.4.36 Lemma.

Let \( G/F \) be a finite extension of function fields over the same field of constants \( C \). Let \( p \) be a degree one prime of \( G \). Then it lies above a degree one
prime of $F$.

**Proof.**

Let $\mathfrak{p}$ be a prime below $p$ in $F$. Then the residue field of $\mathfrak{p}$ is a finite extension of $C$ which must be contained in the residue field of $p$, which is $C$. Thus, the residue field of $\mathfrak{p}$ is $C$.

## B.5 Density of Prime Sets.

In this section we will discuss density of prime sets in global fields. One could think of the density of an infinite prime set as a way to describe its size. There are two commonly used kinds of density: Dirichlet and natural. We start with defining Dirichlet density.

### B.5.1 Definition.

Let $K$ be a global field. Let $\mathcal{P}$ be the set of all the non-archimedean primes of $K$. Let $\mathcal{A} \subseteq \mathcal{P}$. Then the Dirichlet density of $\mathcal{A}$ (denoted by $\delta(\mathcal{A})$) is the following limit assuming it exists:

$$
\lim_{\Re(s) > 1} \sum_{\mathfrak{p} \in \mathcal{A}} \frac{1}{N_{\mathfrak{p}}} = \lim_{\Re(s) > 1} \frac{1}{\sum_{\mathfrak{p} \in \mathcal{P}} \frac{1}{N_{\mathfrak{p}}}},
$$

where $N_{\mathfrak{p}}$ is the norm of the prime $\mathfrak{p}$, i.e. the number of elements in the residue field of $\mathfrak{p}$.

In the case of number fields there is an alternative (but equivalent) definition of Dirichlet density which can be found in Section 6.5 of [33].

$$
\delta(\mathcal{A}) = \lim_{\Re(s) > 1} \frac{\sum_{\mathfrak{p} \in \mathcal{A}} \frac{1}{N_{\mathfrak{p}}} = \frac{1}{\sum_{\mathfrak{p} \in \mathcal{P}} \frac{1}{N_{\mathfrak{p}}}} - \log(1 - q^{1-s}).
$$

The advantage of this form is the fact that the denominator does not depend on the field. This simplifies comparisons of densities of prime sets of different fields. In the function field case there is a similar formula but it depends on the size of the constant field and so should be used for interfield comparisons only when the constant fields are the same.
where $q$ is the size of the constant field of $K$. (See Lemma 6.4.10 of [33].)

One of the main tools for determining the density of a set is Chebotarev Density Theorem. It can be found for the number field case in [37], Chapter V, Theorem 10.4 and for the function field case in [33], Chapter 6. An immediate consequence of this theorem is the following lemma.

**B.5.2 Lemma.**

Let $E/K$ be a Galois extension of global fields. Let $\mathcal{W}_K$ be the set of all the primes of $K$ unramified and splitting completely in $E/K$. Then the Dirichlet density of $\mathcal{W}_K$ is equal to $\frac{1}{[E:K]}$.

**Proof.**

A prime $p_K$ splits completely into distinct factors if and only if one of its factors has identity as its Frobenius automorphism. The conjugacy class of identity contains just one element. Thus, the density of unramified $K$ primes splitting completely in $E$ is $\frac{1}{[K:E]}$ by Chebotarev Density Theorem.

The next two lemma describes important properties of Dirichlet density.

**B.5.3 Lemma.**

Let $K$ be a global field. Let $\mathcal{P}(K)$ denote the set of all the primes of $K$. For $p \in \mathcal{P}(K)$, let $N_p$ denote the norm of $p$, that is the size of the residue field. Then for any $s$ such that $\Re s > 1$, we have that $\sum_{p \in \mathcal{P}(K)} N_p^{-s} < \infty$, i.e. $\left| \sum_{p \in \mathcal{P}(K)} N_p^{-s} \right|$ is bounded, and $\lim_{s \to 1^+} \sum_{p \in \mathcal{P}(K)} N_p^{-s} = \infty$.

**Proof.**

For the function field case the lemma follows from the fact that as $s \to 1^+$, we have that $\sum_{p \in \mathcal{P}(K)} N_p^{-s} = -\log(1 - q^{1-s}) + O(1)$, where $q$ is the size of the constant field of $K$. (See Lemma 6.4.10 of [33].)

For the number field case the lemma follows from the fact that

$$\sum_{p \in \mathcal{P}(K)} N_p^{-s} = -\log(s - 1) + O(1).$$

(See Section 6.5 of [33].)
B.5.4 Lemma.

Let \( K/E \) be a finite separable extension of global fields (not necessarily Galois). Let \( \mathcal{U}_K \) be a set of primes of \( K \) containing all primes of \( K \) of relative degree 1 over \( E \). Then the Dirichlet density of \( \mathcal{U}_K \) is 1.

Proof.

Enough to show that the density of the complement of \( \mathcal{U}_K \) is 0. Let \( \mathcal{H}_K \) be the complement of \( \mathcal{U}_K \). Then, by Lemma B.5.3,

\[
0 \leq \lim_{s \to 1^+} \frac{\sum_{p \in \mathcal{H}_K} N_p^{-s}}{\sum_{p \in \mathcal{P}(K)} N_p^{-s}} \leq \lim_{s \to 1^+} [K : E] \frac{\sum_{p \in \mathcal{P}(E)} |N_p^{-2s}|}{\sum_{p \in \mathcal{P}(K)} N_p^{-s}}
\]

\[
\leq \lim_{s \to 1^+} [K : E] \frac{\sum_{p \in \mathcal{P}(E)} |N_p^{-2}|}{\sum_{p \in \mathcal{P}(K)} N_p^{-s}} = 0.
\]

Thus, \( \delta(\mathcal{H}_K) = 0 \).

The next two lemmas contain the details of the density calculations for the sets we used for our definability results over number and function fields. We treat the number field case first.

B.5.5 Lemma.

Let \( F \subset K \subset K_G \) be a finite extension of number fields with \( K_G \) being the Galois closure of \( K \) over \( F \). Let \( M \) be a cyclic extensions of \( F \) of prime degree \( q \) not dividing \( [K_G : F] \). Let \( \mathcal{U}_K \) be a set of primes of \( K \) formed in the following fashion from the set \( \mathcal{P}(K) \) of all primes of \( K \). From each set of primes of \( K \) lying above the same prime of \( F \), remove the prime of the highest relative degree over \( F \). Next remove all the primes splitting in the extension \( MK/K \). The remaining primes will form the set \( \mathcal{U}_K \). Then the Dirichlet density of \( \mathcal{U}_K \) exists and is greater than 1 \(- [K : F]^{-1} - \frac{1}{q} \).

Proof.

Let \( \mathcal{V}_K = \mathcal{P}(K) \setminus \mathcal{U}_K \). We would like to estimate the density of \( \mathcal{V}_K \). Let \( \mathcal{V}_1 \) be the set of all primes of \( \mathcal{V}_K \) which were removed in the first step. Let \( \mathcal{H} \) be all the primes of \( K \) which split in the extension \( MK/K \). Let \( \mathcal{H}_1 = \mathcal{V}_1 \cap \mathcal{H} \). We want to estimate the Dirichlet density of \( \mathcal{H}_1 \). By Lemma B.5.4, we can
disregard all the primes of $\mathcal{K}_1$ of relative degree higher than 1 over $F$. Let $\mathcal{K}_1 = \mathcal{K}_1 \cap \{ \text{primes of relative degree 1 over } F \}$. Let

$$\mathcal{K}_F = \{ \mathfrak{p}_F \in \mathcal{P}(F) : \mathfrak{p}_F \text{ splits completely in the extension } MK_G/F \}$$

Let $\mathcal{K}_K$ be the set of all primes of $K$ above $\mathcal{K}_F$. We claim that $\tilde{\mathcal{K}}_1$ contains exactly one prime per each set of $F$-conjugates in $\mathcal{K}_K$ and no other primes. Indeed, suppose $p \in \tilde{\mathcal{K}}_1$. Then it is a prime of relative degree 1 over $F$ and also is of the highest relative degree among its conjugates over $F$. Thus, all the conjugates of $p$ are of relative degree 1 over $F$ and $p$ lies above a prime $p_F$ of $F$ splitting completely in the extension $K/F$, and therefore, by Proposition 6.3.2, Section 3, Chapter 6 of [45], splitting completely in the extension $K_G/F$. Further we have that $p$ splits completely in the extension $KM/K$. By Lemma B.4.10 this can happen if and only if all the $F$-conjugates of $p$ split completely in the extension $MK/K$ and all the conjugates of $p_F$ in $K_G$ split completely in the extension $MK_G/K_G$. Thus $p_F$ splits completely in the extension $MK_G/F$. Conversely, let $p$ be a prime lying above a prime of $p_F$ splitting completely in the extension $MK_G/F$. Then all of the $F$-conjugates of $p$ are of relative degree one over $F$ and by Lemma B.4.10 again, $p$ and all of its $F$-conjugates split completely in the extension $MK/K$.

Now using the alternative formula for Dirichlet density (Definition B.5.1) and the fact that all the $F$-conjugates of elements in $\tilde{\mathcal{K}}_1$ are of relative degree 1 we can conclude that

$$\delta(\tilde{\mathcal{K}}_1) = \delta(\mathcal{K}_F) = \frac{1}{[K_G : F]q},$$

where the last equality follows from Lemma B.5.2 and Lemma B.3.6.

Next consider the density of $\mathcal{V}_1$. As above, we need to consider the primes of relative degree 1 only. Thus it is enough to look at the set of primes of $K$ containing exactly one representative for every set of conjugates lying above a prime of $F$ splitting completely in the extension $K/F$, which is the same set as the set of $F$-primes splitting completely in the extension $K_G/F$ by Proposition 6.3.2, Section 3, Chapter 6 of [45] again. Thus $\delta(\mathcal{V}_1) = \frac{1}{[K_G : F]}$. Further by similar arguments, the Dirichlet density of $\mathcal{K}$ exists and is equal to $\frac{1}{q}$.

Since $\mathcal{V}_1$, $\mathcal{K}$, and $\mathcal{V}_1 \cap \mathcal{K}$ have Dirichlet density, we conclude that $\mathcal{V}_1 \cup \mathcal{K}$ also has density, and by Proposition 4.6, Chapter IV of [37], this density is less or equal to the density of $\mathcal{V}_1$ plus the density of $\mathcal{K}$. Thus, the density of $\mathcal{V}$ is less or equal to the density of $\mathcal{V}_1$ plus the density of $\mathcal{K}$, and consequently the density of $\mathcal{V}$ is less or equal to $\frac{1}{[K: F]} + \frac{1}{q}$. Thus, the Dirichlet density of $\mathcal{V}$ is greater than $1 - \frac{1}{[K_G:F]} - \frac{1}{q}$.

We now prove the analogous result for the function field case.
B.5.6 Proposition.

Let $K/E$ be a separable extension of function fields over the same finite field of constants $C$. Let $K_G$ be the Galois closure of $K$ over $E$. Let $M/E$ be a constant field extension of $E$ of prime degree such that $([M : E], [K_G : E]) = 1$. Then the following statements are true.

1. Let $\mathcal{V}_{K,1}$ be the set of primes of $K$ splitting completely in the extension $MK_G/K$. Then $\delta(\mathcal{V}_{K,1}) = \frac{1}{[K_G : K][MK : K]}$, where $\delta$ denotes the Dirichlet density.

2. Let $\mathcal{U}_{K,1}$ be the set of all the $K$-primes lying above $E$-primes splitting completely in the extension $K/E$. Let $\mathcal{Z}_{K,1} = \mathcal{U}_{K,1} \setminus \mathcal{V}_{K,1}$. Then $\delta(\mathcal{Z}_{K,1}) = \frac{[MK : K]^{-1}}{[MK_G : K]}$.

3. Let $\mathcal{Z}_{E,1}$ be the set of $E$-primes below the primes $\mathcal{Z}_{K,1}$. Then all the primes in $\mathcal{Z}_{E,1}$ split completely in $K_G/E$. No prime above $\mathcal{Z}_{E,1}$ is in $\mathcal{V}_{K,1}$.

4. Let $\mathcal{G}_{K,1}$ be a set of $K$-primes such that it contains exactly one prime above each prime in $\mathcal{Z}_{E,1}$. Then $\mathcal{G}_{K,1} \subset \mathcal{Z}_{K,1}$ and $\delta(\mathcal{G}_{K,1}) = \frac{\delta(\mathcal{Z}_{K,1})}{[K : E]} = \frac{[MK : K]^{-1}}{[MK_G : E]}$.

5. Let $\mathcal{V}_{K,2}$ be the set of all the primes of $K$ of relative degrees greater than or equal to 2 over $E$. Let $\mathcal{V}_K = \mathcal{V}_{K,1} \cup \mathcal{G}_{K,1} \cup \mathcal{V}_{K,2}$. Let $\mathcal{U}_K = \mathcal{P}(K) \setminus \mathcal{V}_K$. Then $\delta(\mathcal{U}_K) = 1 - \frac{[MK : K]^{-1}}{[MK_G : E]}. \frac{1}{[K_G : K][MK : K]} > 1 - \frac{1}{[K : E]} - \frac{1}{[MK : K]}$, no prime of $\mathcal{U}_K$ has a relative degree 1 factor in the extension $MK_G/K$ and no prime of $E$ has all of its $K$-conjugates in $\mathcal{U}_K$.

The picture below illustrates the extensions under discussion.
Proof.

1. First of all we note that given that \([M : E], [K_G : E]) = 1\), it is the case that \(M \cap K = E\), \(MK \cap K_G = K\) and thus \([MK_G : K] = [K_G : K][MK : K]\), by Lemma B.3.3. Further, the extension \(MK_G/K\) is Galois. Thus the first assertion follows by Lemma B.5.2.

2. Let \(p \in \mathcal{Z}_{K,1}\) and assume \(p\) lies above an \(E\)-prime without \(MK_G\)-factors ramified in the extension \(MK_G/E\). Then \(p\) lies above a prime \(\mathfrak{p}_E\) of \(E\) splitting completely in the extensions \(K/E\). Therefore by Lemma B.4.6, \(p\) splits completely in the extension \(K_G/K\), and thus the number of factors of \(p\) in \(MK_G\) is divisible by \([K_G : K]\) by Proposition B.1.11.

On the other hand, since \(p\) is not splitting completely in \(MK_G\), the number of factors of \(p\) in \(MK_G\) is not equal to \([MK_G : K] = [MK : K][K_G : K]\), but must be a divisor of this number by Proposition B.1.11 again. Since \([MK : K]\) is a prime number, we must conclude that \(p\) has exactly \([K_G : K]\) factors in \(MK_G\). Thus, the Frobenius automorphism of any factor of \(p\) in the extension \(MK_G/K\) must be of order \([MK : K]\). Similarly, the Frobenius automorphism of any factor of \(\mathfrak{p}_E\) in \(\text{Gal}(MK_G/E)\) must also be of order \([MK : K] = [M : E]\).

Conversely, if a \(K\)-prime \(p\) with no factors ramified in the extension \(MK_G/K\) lies above an \(E\)-prime \(\mathfrak{p}_E\) not ramified in the extension \(MK_G/E\) and whose factors in \(MK_G\) have Frobenius automorphisms of order \([MK : K]\), then \(p\) lies above an \(E\)-prime splitting completely in \(K\) and \(p\) will have \([K_G : K]\) factors in \(MK_G\), thus not splitting completely. Therefore, a \(K\)-prime \(p\) with no ramified factors in the extension \(MK_G/E\) is in \(\mathcal{Z}_{K,1}\) if and only if it lies above an \(E\)-prime not ramified in the extension \(MK_G/E\) and whose factors in \(MK_G\) have Frobenius automorphisms over \(E\) of order \([MK : K] = [M : E]\).

Further, \(\text{Gal}(MK_G/E) = \text{Gal}(K_G/E) \times \text{Gal}(M/E)\), by Lemmas B.3.3 and B.3.6, and for \(\sigma \in \text{Gal}(M/E), \tau \in \text{Gal}(K_G/E)\) we have that \(\sigma \tau = \tau \sigma\). Thus, the only elements of order \([M : E]\) in \(\text{Gal}(MK_G/E)\) are non-trivial elements of \(\text{Gal}(M/E)\). Since there are \([M : E] - 1 = [MK : K] - 1\) such elements, by Chebotarev Density Theorem, the density of the set of \(E\)-primes whose factors have Frobenius automorphisms of order \([M : E]\) is \([MK; K]^{-1} \frac{[MK; K]^{-1}}{[MK_G; E]}\). On the other hand, for each such \(E\)-prime, there are \([K : E]\) primes in \(\mathcal{Z}_{K,1}\) and the norms of primes in \(\mathcal{Z}_{K,1}\) are the same as the norms of the corresponding \(E\)-primes below. Therefore using the alternative definition of Dirichlet density for function fields (see Definition B.5.1) and the fact that \(E\) and \(K\) have the same field of constants, we can conclude that the density of primes in \(\mathcal{Z}_{K,1}\) is \([K : E]^{-1} \frac{[MK; K]^{-1}}{[MK_G; E]}\).

3. For each prime of \(\mathcal{Z}_{E,1}\), there exists at least one factor \(p\) in \(K\) not splitting
completely in the extension $MK_G/K$. Thus, by Lemma B.4.10, no conjugate of $p$ over $E$ splits completely in the extension $MK_G/K$, and thus no conjugate of $p$ is in $V_{K,1}$.

4. From the discussion above it follows that $\mathcal{Z}_{K,1}$ is closed under conjugation over $E$ and each set of conjugates contains exactly $[K : E]$ primes. Hence, $G_{K,1}$ will contain one prime per each $\mathcal{Z}_{K,1}$-set of conjugates over $E$. Thus, $\delta(G_{K,1}) = \frac{\delta(\mathcal{Z}_{K,1})}{[K : E]} = \frac{[MK_G : K] - 1}{[MK_G : E]}$.

5. First of all we observe that by Lemma B.5.3 it is the case that $\delta(V_{K,2}) = 0$. Note also that the density of the set $\mathcal{Z}_{K,2} = V_{K,2} \setminus (V_{K,1} \cup G_{K,1})$ is zero by the same lemma. Now the sets $\mathcal{Z}_{K,2}, G_{K,1}, V_{K,1}$ are all disjoint and have Dirichlet densities. Thus the density of their union is just the sum of the densities of the three sets. Therefore the density calculation for $W_K$ follows from the density calculations for $\mathcal{Z}_{K,2}, V_{K,1}$ and $G_{K,1}$.

Next we consider a prime $p$ in $W_K$. By construction, $p \notin V_{K,1}$ and thus does not split completely in the extension $MK_G/K$. Therefore, $p$ has no factors of relative degree 1 in the extension $MK_G/K$. Finally, let $\wp_E$ be a prime of $E$. If $\wp_E$ splits completely in the extension $MK_G/E$, then none of its factors is in $W_K$. If $\wp$ does not split completely in the extension $MK_G/E$ but splits completely in the extension $K/E$ (and therefore by Lemma B.4.6 in the extension $KG/E$), then $\wp_E \in \mathcal{Z}_{E,1}$ and by construction $\wp_E$ will be missing a factor in $W_K$. Finally, if $\wp_E$ does not split completely in $K$, then it has a factor of relative degree at least 2 in $K$ and all such primes were removed from $W_K$.

B.5.7 Lemma.

Let $K$ be a global field. Let $F_1/K, \ldots, F_n/K$ be cyclic extensions of prime degree $q$ linearly disjoint over $K$. Then the Dirichlet density of the set of $K$ primes splitting in every extension $F_i/K$ is $\frac{1}{q^n}$.

Proof.

Let $F = \prod_{i=1}^{n} F_i$ and let $\wp$ be a prime in the product field. Then

$$\text{Gal}(F/K) = \text{Gal}(F_1/K) \oplus \ldots \oplus \text{Gal}(F_n/K)$$

by Lemma B.3.7. Let $\wp_i$ be the prime below $\wp$ in $F_i$. Let $(\sigma_1, \ldots, \sigma_n), \sigma_i \in \text{Gal}(F_i/K)$ be the Frobenius of $\wp$ over $K$. Then $\sigma_i$ is an element of the decomposition group of $\wp_i$ over $K$. Since the $[F_i : K] = q$, a prime number,
unless \( \sigma_i \) is equal to the identity element, it will generate \( \text{Gal}(F_i/K) \). Let \( \mathfrak{p}_K \) be the prime below \( \mathfrak{p} \) in \( K \). Then \( \mathfrak{p}_K \) splits in every \( F_i \) if and only if \( \sigma_i = \text{id}_i \) for all \( i \). (Here \( \text{id}_i \) is the identity element of \( \text{Gal}(F_i/K) \).) Thus by Chebotarev Density Theorem, the Dirichlet density of the set of \( K \)-primes splitting in every \( F_i \) is equal to \( \frac{1}{q^n} \).

B.5.8 Lemma.

Let \( K \) be a function field over a finite field of constants. Let \( K_0 = K \subset K_1 \subset \ldots \subset K_n \) be a tower of constant field extensions with \( [K_{i+1} : K_i] = q \), where \( q \) is a prime number. Let \( \mathcal{W} \) be the set of all the primes \( p \) of \( K \) such that for some \( i \), all the factors of \( p \) in \( K_i \) do not split in the extension \( K_{i+1}/K_i \). Then the Dirichlet density of \( \mathcal{W} \) is \( \frac{\phi(q^n-1)}{q^n} \).

Proof.

First of all we note the following. Let \( p \) be a \( K \)-prime. Let \( p_{i,1} \) and \( p_{i,2} \) be two factors of \( p \) in \( K_i \). Then either both of this factors split in \( K_{i+1} \) or neither does. (This follows from the fact that \( K_{i+1}/K_i \) is Galois extension and by Lemma B.4.5.) Suppose now that \( p \notin \mathcal{W} \). Let \( p_n \) be a factor of \( p \) in \( K_n \) and let \( p_i = p_n \cap K_i \). Then since all the extensions in the tower are of prime degree and \( p \notin \mathcal{W} \) we have that \( f(p_{i+1}/p_i) = 1 \). (Otherwise some factor of \( p \) in \( K_i \) does not split in \( K_{i+1} \) implying that all the factors of \( p \) in \( K_i \) do not split in \( K_{i+1} \) and \( p \in \mathcal{W} \).) Thus, \( f(p_n/p) = 1 \) and \( p \) splits completely in this extension. By Chebotarev Density Theorem, the Dirichlet density of this set is \( \frac{1}{q^n} \) and the assertion of the lemma follows.

We now proceed to a brief discussion of natural density.

B.5.9 Definition.

Let \( K \) be a number field. Let \( \mathcal{P}(K) \) be the set of all primes of \( K \). Let \( \mathcal{I}(K) \subset \mathcal{P}(K) \). Then the natural density of \( \mathcal{I}(K) \) is defined to be the following limit if it exists.

\[
\lim_{X \to \infty} \frac{\# \mathfrak{p} \in \mathcal{I}(K) : N\mathfrak{p} \leq X}{\# \mathfrak{p} \in \mathcal{P}(K) : N\mathfrak{p} \leq X}
\]

If the limit above does not exist, we can consider \( \lim \sup \) or \( \lim \inf \) in place of \( \lim \). If \( \lim \sup \) replaces the limit, then the resulting number is called the upper natural density. Similarly, if we use \( \lim \inf \), we will obtain the lower natural density.
B.5.10  Proposition.

Let $K, \mathcal{T}(K), \mathcal{P}(K)$ be as in Definition B.5.9. Assume the natural density of $\mathcal{T}(K)$ exists and denote it by $d$. Then $\delta(\mathcal{T}(K))$ – the Dirichlet density of $\mathcal{T}(K)$ also exists and is equal to natural density of $\mathcal{T}(K)$.

Proof.

Unfortunately, a detailed proof of this proposition would be rather lengthy and somewhat tedious. Since this proposition has no direct bearing on any other proposition in the book and is included here for the sake of completeness only, we will restrict ourselves to outlining the main ideas of a proof suggested to us by Bjorn Poonen.

The starting point for the proof is the following estimates. The first one is a version of the Prime Number Theorem:

$$\# \{p \in \mathcal{P}(K), N_p \leq x\} = \frac{x}{\log x} + \varepsilon_1(x) \frac{x}{\log x},$$

where $\varepsilon_1(x) \to 0$ as $x \to \infty$. (See Theorem 4, Section 5, Chapter XV of [46].) The second one is really the alternative definition of Dirichlet density introduced at the beginning of this section.

$$\lim_{s \to 1^+} \log(s - 1) \sum_{p \in \mathcal{P}(K)} N_p^{-s} = -1. \quad (B.5.1)$$

The third and fourth inequalities are of elementary nature. Let $s = \sigma + it$, where $\sigma, t \in \mathbb{R}$. Then there exists a positive real constant $C$ such that for all $s$ sufficiently close to 1 while $\sigma > 1$ we have that

$$\left| \frac{s - 1}{\sigma - 1} \right| < C. \quad (B.5.2)$$

(See Chapter IV, Section 2 of [37].) Further there exists a positive real constant $\varepsilon$ such that for any real $h$ with $|h - 1| < \varepsilon$ and any complex $s$ with $\Re s > 1$ and $|s - 1| < \varepsilon$, we have that

$$\Re h^s > 0. \quad (B.5.3)$$

Finally we need the following familiar expansion for $0 < x < 1$:

$$-\log(1 - x) = \sum_{i=1}^{\infty} \frac{x^i}{i}. \tag{B.5.4}$$

Now we are ready to proceed. Throughout our discussion below we will assume that $r$ and $s = \sigma + it, \sigma, t \in \mathbb{R}$ are close enough to 1 so that (B.5.2) and
(B.5.3) with \( h = r \) hold. From the definition of natural density we can conclude that

\[
\#\{p \in \mathcal{D}(K), N_p \leq x\} = d \frac{x}{\log x} + \varepsilon_2(x) \frac{x}{\log x},
\]

where \( \varepsilon_2(x) \to 0 \) as \( x \to \infty \).

Next let \( r > 1 \) be a real transcendental number and note that

\[
\mu(n) = \#\{p \in \mathcal{D}(K), r^n < N_p < r^{n+1}\} = \frac{r - 1}{\log r} \frac{r^n}{n} + \varepsilon_3(r^n) \frac{r^n}{n \log r},
\]

where \( \varepsilon_3 \to 0 \) as \( r^n \to \infty \). Similarly,

\[
\mu_T(n) = \#\{p \in \mathcal{D}(K), r^n < N_p < r^{n+1}\} = \frac{d}{\log r} \frac{r^n}{n} + \varepsilon_4(r^n) \frac{r^n}{n \log r},
\]

where we have that \( \varepsilon_4(r^n) \to 0 \) as \( r^n \to \infty \). Next let \( s \in \mathbb{C} \) with \( \Re s > 1 \) and write

\[
\sum_{p \in \mathcal{D}(K)} N_p^{-s} = 
\sum_{n=1}^{\infty} \sum_{p \in \mathcal{D}(K), r^n < N_p < r^{n+1}} r^{-(n+1)s} + \infty \sum_{n=1}^{\infty} \sum_{p \in \mathcal{D}(K), r^n < N_p < r^{n+1}} r^{-(n+1)s} \delta(s, r, n, p),
\]

where \( \delta(s, r, n, p) = (r^{(n+1)s} - 1) \) while \( r^n < N_p < r^{n+1} \). Thus,

\[
\sum_{p \in \mathcal{D}(K)} N_p^{-s} = 
\sum_{n=1}^{\infty} \mu_T(n) r^{-(n+1)s} + \infty \sum_{n=1}^{\infty} \sum_{p \in \mathcal{D}(K), r^n < N_p < r^{n+1}} r^{-(n+1)s} \delta(s, r, n, p) \leq 
\sum_{n=1}^{\infty} \left| \sum_{p \in \mathcal{D}(K), r^n < N_p < r^{n+1}} d \frac{r - 1}{\log r} \frac{r^n}{n} r^{-(n+1)s} \right| + \sum_{n=1}^{\infty} \left| \sum_{p \in \mathcal{D}(K), r^n < N_p < r^{n+1}} \varepsilon_4(r^n) \frac{r^n}{n \log r} r^{-(n+1)s} \right| + 
\sum_{n=1}^{\infty} \left| \sum_{p \in \mathcal{D}(K), r^n < N_p < r^{n+1}} \frac{d}{\log r} \frac{r^n}{n} r^{-(n+1)s} \delta(s, r, n, p) \right| + \sum_{n=1}^{\infty} \left| \sum_{p \in \mathcal{D}(K), r^n < N_p < r^{n+1}} \varepsilon_4(r^n) \frac{r^n}{n \log r} r^{-(n+1)s} \delta(s, r, n, p) \right|,
\]

where \( \varepsilon_4(r^n) \to 0 \), as \( r^n \to \infty \), and \( \delta(s, r, n) = \max_{r^n < N_p < r^{n+1}} |\delta(s, r, n, p)| \). The analogous formula holds for \( \mathcal{D}(K) \) too of course but with \( d = 1 \).

Now noting that \( |N_p^{-s}| = N_p^{-\sigma} \), we proceed to get an upper bound for \( \delta(s, r, n) \). In order to do this we observe that if \( r^n < N_p < r^{n+1} \), then

\[
1 < \left| \frac{r^{n+1}}{N_p} \right| < r,
\]

320
and therefore (B.5.3) will hold with \( h = \frac{r^{n+1}}{N^p} \). Thus, for \( s \) sufficiently close to 1 (given a fixed value of \( r \)),

\[
\delta(s, r, n) = \max |(r^{(n+1)s}N^p - 1) - r^s| \leq r^\sigma - 1 + r^\sigma |\sin(t \ln r)| = \delta(r, s).
\]  

(B.5.4)

Observe that we have a bound on \( \delta(s, r, n) \) independent of \( n \). Observe also that for any \( \varepsilon > 0 \) we can find an \( r > 1 \) and arbitrarily close to 1 such that for all \( s \) sufficiently close to 1 we have that \( \delta(s, r) < \varepsilon \). Now to finish the proof, it is enough to show that for any \( \delta > 0 \) for some \( r \) and all \( s \) sufficiently close to 1, we have that

\[
\sum_{n=1}^{\infty} \left| r - \frac{r^n}{\log r} n^{-1} \right| \delta(s, r, n) < \delta \log |s - 1|,  
\]  

(B.5.5)

and

\[
\left| \sum_{n=1}^{\infty} \varepsilon(r^n) \frac{n^{-1} - r^{-(n+1)s}}{\log r} \right| < \delta \log |s - 1|,  
\]  

(B.5.6)

Indeed if we show that (B.5.5) and (B.5.6) hold, then in view of (B.5.1) we will be able to conclude that the Dirichlet density of \( \mathcal{F}(K) \) and \( \mathcal{P}(K) \) "resides" for the most part in the sums

\[
\sum_{n=1}^{\infty} r - \frac{r^n}{\log r} n^{-1} \]  

and

\[
\sum_{n=1}^{\infty} \frac{r - r^n}{\log r} n^{-1} \]  

respectively. From that point on it will not be hard to obtain the desired ratio. Further, if we let \( s = \sigma + it, \sigma > 1 \) as above, then using (B.5.2) we can also replace \( |s - 1| \) by \( |\sigma - 1| \) in our estimates and simplify our calculations.

Now we will show that (B.5.5) holds. First we observe that

\[
\lim_{r \to 1} \frac{r - 1}{\log r} = C_1,  
\]

where \( C_1 \) does not depend on \( r \). Further observe that

\[
\lim_{\sigma \to 1} \frac{1 - r^{1-\sigma}}{\sigma - 1} = C(r),  
\]

where \( C(r) \) depends on \( r \) only.
Next consider the following inequalities for some fixed $r, s$ sufficiently close to 1 so that (B.5.4) holds.

\[
\sum_{n=1}^{\infty} \left| r^{-(n+1)s} r^n r - \frac{1}{n \log r} \right| \delta(s, r, n) < -r^{-\sigma} \delta(s, r) \frac{r - 1}{\log r} \sum_{n=1}^{\infty} \frac{r^{n(1-\sigma)}}{n} \\
< -r^{-\sigma} \delta(s, r) \frac{r - 1}{\log r} \log(1 - r^{1-\sigma}) = \\
-r^{-\sigma} \delta(s, r) \frac{r - 1}{\log r} \left( \log(\sigma - 1) - \log \left( \frac{1 - r^{1-\sigma}}{\sigma - 1} \right) \right) = \\
-r^{-\sigma} \delta(s, r) \frac{r - 1}{\log r} \left( \log(\sigma - 1) \right) - r^{-\sigma} \delta(s, r) \frac{r - 1}{\log r} \log \left( \frac{1 - r^{1-\sigma}}{\sigma - 1} \right) \\
< -\delta(s, r) \frac{r - 1}{\log r} \log(\sigma - 1) + \tilde{C}(r),
\]

where $\tilde{C}(r)$ depends on $r$ only. By moving $r$ closer to 1 if necessary and then letting $s \to 1$ we can make sure that (B.5.5) holds.

We now show that (B.5.6) holds. Fix $1 < r < 2$ and let $M$ be a positive integer such that for all $n > M$ we have that $|\varepsilon(r^n)| < \log(r)\varepsilon$, where $\varepsilon$ is an arbitrary positive real number. Finally consider the following inequalities

\[
\left| \sum_{n=1}^{\infty} \varepsilon(r^n) \frac{r^{-(n+1)s+n}}{n \log r} \right| \leq \sum_{n=1}^{M} |\varepsilon(r^n)| \frac{1}{n \log r} + \sum_{n=M+1}^{\infty} |\varepsilon(r^n)| \frac{r^{-(n+1)s+n}}{n \log r} \\
\leq \tilde{C}(r) - \varepsilon \sum_{n=M}^{\infty} \log(1 - r^{1-\sigma}) < \tilde{C}(r) - \varepsilon \log(\sigma - 1) - \varepsilon \log \left( \frac{1 - r^{1-\sigma}}{\sigma - 1} \right) \\
< \tilde{C}(r) - \varepsilon \log(\sigma - 1)
\]

where $\tilde{C}(r), \tilde{C}(r)$ are constants depending on $r$ only. We leave the rest of the proof to the reader.

We leave the following easy proposition as another exercise for the reader.

**B.5.11 Proposition.**

Let $\mathcal{A}, \mathcal{B}$ be sets of primes of a number field $K$ such that both sets have natural density. Assume further that the natural density of $\mathcal{A}$ is 1. Then the natural density of $\mathcal{B} \cap \mathcal{A}$ exists and is equal to the natural density of $\mathcal{B}$.
B.6 Elliptic Curves.

In this section we discuss some general properties of elliptic curves which played a role in the proof of Poonen’s results. We will use the following notation.

B.6.1 Notation.

- $K$ will denote a global field.
- $\bar{K}$ will denote the algebraic closure of $K$.
- $M$ will denote a finite extension of $K$.
- $E/K$ will denote an elliptic curve defined over $K$ for which we will fix an (affine) Weierstrass equation:

$$y^2 = x^3 + a_2x^2 + a_4x + a_6,$$

where for $i = 2, 4, 6$ we have that $a_i \in K$.

- $E(M)$ will be the set of all points of $E/K$ in $M$, or the set of all solutions to ($B.6.1$) in $M$ together with the point at infinity $O$ – the unit element of the group.

- $E[m](M) \subset E(M)$ will be the set of all points of $E(M)$ of order dividing $m$.

- $\mathcal{P}(K)$ will denote the set of all non-archimedean primes of $K$.

- $p$ will denote a non-archimedean prime of $K$ such that
  - For $i = 2, 4, 6$ we have that $\text{ord}_p a_i \geq 0$.
  - $p$ does not divide the discriminant of the chosen Weierstrass equation and therefore $E$ has a good reduction mod $p$. (See Chapter VII, Section 2 of [113] for the definition of a reduction of an elliptic curve.)
  - $p$ is not ramified over $\mathbb{Q}$.

- Let $\mathcal{S}_0(K)$ denote the set of all primes $q$ of $K$ such that $q$ does not satisfy the requirements for $p$, listed above. (Note that $\mathcal{S}_0(K)$ is finite.)

- $\mathcal{M}_K$ will denote the set of all normalized absolute values of $K$. (See Definition of normalized valuations in Section 5, Chapter VIII of [113].)
• $\mathcal{M}_{K,\infty} \subset \mathcal{M}_K$ will denote the set of all archimedean absolute values of $K$.

• $\mathcal{M}_{K,0} \subset \mathcal{M}_K$ will denote the set of all normalized non-archimedean absolute values of $K$.

• $\mathcal{M}_{K,\mathcal{S}_0(K)} \subset \mathcal{M}_{K,0}$ will denote the set of all non-archimedean absolute values of $K$ corresponding to primes of $\mathcal{S}_0$.

• $k$ will denote the residue field of $p$.

• $K_p$ will denote the completion of $K$ under the corresponding $p$-adic absolute value.

• $E(K_p)$ will be the set of all points of $E$ in $K_p$, or the set of all solutions to (B.6.1) in $K_p$ together with the point at infinity $O$ — the unit element of the group.

• $R_p$ will denote the ring of integers of $K_p$, i.e. elements of $K_p$ with non-negative order at $p$.

• $\mathcal{M}$ will denote the maximum ideal of $R_p$.

• $\hat{E}$ will denote the formal group over $R_p$ associated to $E$. (See the definition of a formal group in Section 2, Chapter IV of [113] and a description of $\hat{E}$ in Example 2.2.3, Section 3, Chapter IV of [113].)

• $\hat{E}(\mathcal{M})$ will denote the group associated to $\hat{E}$.

• Let $E_0(K_p) = E(K_p)$.

• For $n \geq 1$ let $E_n(K_p)$ be the set of $K_p$-points of $E$ whose affine coordinates $(x, y)$ derived from the fixed Weierstrass equation of $E$, have a pole of order at least $2n$ and $3n$ at $p$ respectively.

• Let $\pi : E(K) \rightarrow E(k)$ be the reduction modulo $p$.

• Let $\Pi : E(K_p) \rightarrow E(k)$ be the reduction modulo $p$.

• Given a point $P \in E(K) \setminus \{O\}$ of infinite order and an integer $n \neq 0$, define $x_n(P), y_n(P)$ to be the affine coordinates of $[n]P$ derived from the fixed Weierstrass equation of $E$.

• For an integer $n \neq 0$ write the divisor of $x_n(P)$ in the form $\frac{a_n}{a_n s_n}$, where
  
  - For $n \geq 1$ let $a_n(P) = \prod a^a(q)$, where the product is taken over all the primes $q \in \mathcal{P}(K) \setminus \mathcal{S}_0(K)$ such that $a(q) = \text{ord}_q x_n > 0$.
\[ d_n(P) = \prod_{q \in \mathcal{P}(K) \setminus \mathcal{S}_0(K)} q^{a(q)}, \]
where the product is taken over all the primes \( q \in \mathcal{P}(K) \setminus \mathcal{S}_0(K) \) such that \( a(q) = \text{ord}_q x_n < 0 \).

\[ s_n(P) = \prod_{q \in \mathcal{S}_0(K)} q^{a(q)}, \]
where the product is taken over all the primes \( q \in \mathcal{S}_0(K) \) such that \( a(q) = \text{ord}_q x_n \).

- For an integer \( n \neq 0 \) let \( d_n \in O_K \) be an element whose divisor is \( d_n^{h_K} \), where \( h_K \) is the class number of \( K \).
- For an integer \( n \neq 0 \) let \( \mathcal{S}_n(P) = \{ q \in \mathcal{P}(K) | \text{ord}_q \mathcal{S}_n(P) > 0 \} \).
- For any \( P \in K \), let \( \hat{h}(P) \) be the canonical height of \( P \). (See Definition in Section 9, Chapter VIII of [113].)

The first proposition asserts existence of an elliptic curve necessary for carrying out the proof of Poonen’s results.

### B.6.2 Proposition.

Consider the curve \( E \) defined by the equation \( y^2 = x^3 - 6x^2 + 17x \). Then the following statements are true.

1. This equation defines an elliptic curve.
2. \( E(\mathbb{Q}) \cong \mathbb{Z}/2 \oplus \mathbb{Z} \).
3. \( E(\mathbb{R}) \cong \mathbb{R}/\mathbb{Z} \) as topological groups.
4. \( E \) does not have complex multiplication.
Proof.

1. This statement follows by Proposition 3.1, Section 3, Chapter III of [113]. (The discriminant of this equation $\Delta = -2^917^2$. See Section 1, Chapter III of [113] for the definition of the discriminant.)

2. The proof of this statement is in the Example 4.10, Section 4, Chapter X of [113].

3. First of all, observe that the discriminant of this curve is negative. Secondly by Corollary 2.3.1, Section 2, Chapter V of [114], an elliptic curve defined over $\mathbb{R}$ having negative discriminant is isomorphic as a topological group to $\mathbb{R}/\mathbb{Z}$.

4. By Theorem 6.1, Section 6, Chapter II of [114], if $E$ has complex multiplication, then its $j$-invariant is an integer. The $j$-invariant of this curve is $(\frac{36-24(17/2)}{-2^917^2}) \not\in \mathbb{Z}$. (See Section 1, Chapter III of [113] for the definition of the $j$-invariant).

The following sequence of propositions (B.6.3 – B.6.8) describes the behavior of primes in the denominators of multiples of a point of infinite order.

B.6.3 Proposition.

The map $\phi : \hat{E}(M) \rightarrow E_1(K_p)$ defined by $z \mapsto \left(\frac{z}{w(z)}, -\frac{1}{w(z)}\right) = (x, y)$, where $w(z) \in \mathbb{R}_p[[z]]$ is defined in Proposition 1.1, Section 1, Chapter IV of [113], is a group isomorphism. (See Proposition 2.2, Section 2, Chapter VII of [113] for a proof.)

B.6.4 Proposition.

Let $P \neq O$ be a point of infinite order on $E$. Let $n \in \mathbb{Z}_{\geq 0}$. Then

$$\{l \in \mathbb{Z} \setminus \{0\} : p^l|b_l\} \cup \{0\}$$

is a subgroup of $\mathbb{Z}$ under addition.

Proof.

Let $\phi : \hat{E}(M) \rightarrow E_1(K_p)$ be the map defined in Proposition B.6.3. Then from the definition of $w(z)$ it follows that for all $n \in \mathbb{Z}_{\geq 0}$ we have that

$$\text{ord}_p z = n \iff \text{ord}_p x = -2n \land \text{ord}_p y = -3n.$$
In other words, \( \phi : \hat{E}(\mathcal{M}^n) \to E_n(K_p) \) is also an isomorphism. Therefore \( E_n(K_p) \) is a group for all \( n \in \mathbb{Z}_{>0} \). Finally, we observe that \( E_n(K) = E(K) \cap E_n(K_p) \) and the assertion of the proposition holds.

From this proposition we derive the following corollary.

**B.6.5 Corollary.**

Let \( \mathfrak{b} \) be any integral divisor of \( K \). Then \( \{ l \in \mathbb{Z} \setminus \{0\} : \mathfrak{b} | l \} \cup \{0\} \) is a subgroup of \( \mathbb{Z} \) under addition.

**B.6.6 Proposition.**

Let \( P \in E_1(K_p) \) (so that \( \text{ord}_p x(P) < 0 \)). Then

1. if \( n \in \mathbb{R}_p \setminus \mathcal{M} \), \( \text{ord}_p x_n(P) = \text{ord}_p x_1(P) \) and \( \text{ord}_p y_n(P) = \text{ord}_p y_1(P) \).

2. if \( p \) is a rational prime below \( p \), then \( \text{ord}_p x_p(P) = \text{ord}_p x_1(P) + 2 \) and \( \text{ord}_p y_p(P) = \text{ord}_p y_1(P) + 3 \).

**Proof.**

By assumption and Proposition 2.2, Section 3, Chapter VII of [113], for some \( z \in \mathcal{M} \),

\[
(x_1(P), y_1(P)) = \left( \frac{z}{w(z)}, -\frac{1}{w(z)} \right).
\]

Further, \( [p]z = pf(z) + g(z^n) \), by Proposition 2.3, Section 3, Chapter IV, and Corollary 4.4, Section 4, Chapter IV of [113], where \( [p] \) is the multiplication by \( p \) in the formal group and \( f(T), g(T) \) are power series in \( T \) with \( g(0) = 0 \) and \( f(z) = z + \) higher order terms. Thus, since \( p | p \), we have \( x_1([p]P) \) will have a pole of order exactly 2 greater than \( x_1(P) \) and similarly \( y_1([p]P) \) will have a pole of order exactly 3 greater than \( y_1(P) \). On the other hand, if we replace \( p \) with a rational prime \( q \neq p \) with \( p \nmid q \), then \( x_1([q]P) \) and \( y_1([q]P) \) will have the same order at \( p \) as \( x_1(P) \) and \( y_1(P) \) respectively.

From this lemma and the definition of \( \delta_i(P) \) for a point \( P \in E(K) \) of infinite order, we derive the following corollary.

**B.6.7 Corollary.**

Let \( m, k \in \mathbb{Z}_{>0}, m | k \). Then \( \delta_m(P) | \delta_k(P) \).
B.6.8 Lemma.

There exists $c \in \mathbb{R}$, such that $h_0(d_n(P)) = (c - o(1))n^2$ as $n \rightarrow \infty$.

Proof.

By Theorem 9.3, Section 9, Chapter VIII of [113], we have that

$$h(x_n(P)) + O(1) = \hat{h}(nP) = n^2 \hat{h}(P).$$

Thus, for some positive constant $\hat{c}$ it is the case that $h(x_n(P)) = \hat{c}n^2 + O(1)$ and $h_K h(x_n(P)) = h_K n^2 \hat{c} + O(1)$. Next for $i \in \mathbb{N}$, we can write

$$x_i^{h_K}(P) = \frac{a_i(P)}{d_i(P)} s_i(P),$$

where $a_i(P)$ has the divisor $a_i^{h_K}(P)$, $d_i(P)$ has the divisor $d_i^{h_K}(P)$, and only primes of $\mathcal{O}_0(K)$ occur in the divisor of $s_i(P)$. By definition of $h(x_n(P))$ (see Definitions of regular and logarithmic height and height notation in Section 5, Chapter VIII of [113]), and the Product Formula

$$h(x_n(P)) = [K : \mathbb{Q}]^{-1} \sum_{v \in \mathbb{M}_K} n_v \log \max(|x_n(P)|_v, 1),$$

$$= [K : \mathbb{Q}]^{-1} \left( \sum_{v \in \mathbb{M}_{K,0}} n_v \log \max(|x_n(P)|_v, 1) + \sum_{v \in \mathbb{M}_{K,\infty}} n_v \log \max(|x_n(P)|_v, 1) \right),$$

$$= [K : \mathbb{Q}]^{-1} \left( - \sum_{v \in \mathbb{M}_{K,0}} h_K^{-1} n_v \log |d_n(P)|_v + \sum_{v \in \mathbb{M}_{K,\infty} \cup \mathcal{O}_0} n_v \log \max(|x_n(P)|_v, 1) \right),$$

$$= h_K^{-1} h_0(d_n(P)) + [K : \mathbb{Q}]^{-1} \left( \sum_{v \in \mathbb{M}_{K,\infty} \cup \mathcal{O}_0} n_v \log \max(|x_n(P)|_v, 1) \right).$$

Thus, by Theorem on page 101 of [89],

$$h_0(d_n(P)) = h_K h(x_n(P)) + o(h(x_n(P)))$$

$$= h_K n^2 \hat{c} + O(1) + o(h(x_n(P))) = (c - o(1))n^2.$$

From the definition of $h_0$ it is clear that the following lemma is true.
B.6.9 Lemma.
Let \( u, v \in O_K \setminus \{0\} \). Then

1. \( h_0(uv) = h_0(u) + h_0(v) \).
2. \( u | v \implies h_0(u) \leq h_0(v) \).

The next sequence of results (B.6.10–B.6.14) deals with automorphisms of torsion elements of elliptic curves.

B.6.10 Proposition.
Let \( \overline{F} \) be any algebraically closed field. Let \( m \in \mathbb{N} \). If \( \text{char}(\overline{F}) = 0 \) or if \( m \) is prime to \( \text{char}(\overline{F}) \), then \( E(\overline{F})[m] = (\mathbb{Z}/m) \times (\mathbb{Z}/m) \). (See Corollary 6.4, Section 6, Chapter III of [113].)

B.6.11 Proposition.
Let \( m \geq 1 \) be prime to \( p \). Then \( \pi \) restricted to \( E(K)[m] \) is injective.

Proof.
By Proposition 3.1(b), Section 3, Chapter VII of [113], \( \Pi \) is injective when restricted to \( E(K_p)[m] \). Since \( \pi \) is the restriction of \( \Pi \) to \( K \), the assertion follows.

B.6.12 Corollary.
Let \( m \in \mathbb{N}, m \geq 1 \) be prime to \( p \). Suppose \( E(K)[m] \cong \mathbb{Z}/m \times \mathbb{Z}/m \). Then \( E(K)[m] \cong E(\overline{k})[m] \) as groups and reduction modulo \( p \) induces an isomorphism. (Here \( \overline{k} \) is the algebraic closure of \( k \).)

Proof.
\( \pi(E(K)[m]) \subseteq E(k)[m] = \mathbb{Z}/m \times \mathbb{Z}/m \), since \( m \) is prime to \( p \). But \( \pi \) injective on \( E(K)[m] \). Thus, \( |\pi(E(K)[m])| = |E(\overline{k})[m]| \), and the assertion follows.
B.6.13 Proposition.

Let \( l \) be a rational prime number. Then the group \( \text{Aut}(E(\bar{K})[l]) \) of automorphisms of \( E(\bar{K})[l] \) is isomorphic to \( GL_2(\mathbb{Z}/l) \). Further, let

\[
n_l = \frac{\#\{\sigma \in \text{Aut}(E(\bar{K})[l]) : \exists P \in E(\bar{K})[l] \setminus \{O\}, \sigma(P) = P\}}{\#\{\sigma \in \text{Aut}(E(\bar{K})[l])\}}.
\] (B.6.2)

Then as \( l \to \infty \), we have that \( n_l = 1/l + O(1/l^2) \).

Proof.

Since \( E(\bar{K})[l] = \mathbb{Z}/l \times \mathbb{Z}/l \) is a two dimensional vector space over \( \mathbb{Z}/l \), \( \text{Aut}(E(\bar{K})[l]) \) is isomorphic to the space of \( 2 \times 2 \) invertible matrices, otherwise known \( GL_2(\mathbb{Z}/l) \). Thus, we need to determine the size of \( GL_2(\mathbb{Z}/l) \), as well as the number of matrices with a fixed non-zero vector. Let

\[
\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{Z}/l).
\] (B.6.3)

We need to determine the number of distinct \( 4 \)-tuples \( (a, b, c, d) \in (\mathbb{Z}/l)^4 \) such that \( ac - bd = 0 \) in \( \mathbb{Z}/l \). If \( a \neq 0 \), then \( c \) is uniquely determined for any value of \( b \) and \( d \). Thus, we get \( (l-1)l^2 \) singular matrices for this case. If \( a = 0 \), then for any values of \( c \) we can have any of the \( 2l-1 \) values of the pair \( (b, d) \), where one entry is 0. Thus, for this case we have \( l(2l-1) \) singular matrices. So altogether there are \( (l-1)^2 + l(2l-1) = l^3 - l^2 + 2l^2 - l = l^3 + l^2 - l \) singular \( 2 \times 2 \) matrices over \( \mathbb{Z}/l \). Hence there are \( l^4 - l^3 - l^2 + l = (l^2 - 1)(l^2 - 1) \) matrices in \( GL_2(\mathbb{Z}/l) \).

Next we calculate the number of non-singular matrices with a fixed non-zero vector. To this effect we first determine the number of matrices of the form (B.6.3) satisfying

\[
\begin{align*}
(a - 1)(d - 1) - bc &= 0 \\
ad - bc &= 0.
\end{align*}
\] (B.6.4)

This system of equations implies that \( (a - 1)(d - 1) = ad \) or \( 1 - a = d \). Thus we have that \( a(1 - a) = bc \). Using the same strategy as above, we conclude that if \( b \neq 0 \), it is the case that \( c \) is determined by the value of \( a \), and therefore we have \( l(l-1) \) solutions in this case. If \( b = 0 \), then \( a = 1, 0 \) and \( c \) can take any value. Therefore for this case we have \( 2l \) solutions. So the total number of matrices satisfying (B.6.4) is \( l(l-1) + 2l = l^2 + l \). Consequently the number of non-singular matrices satisfying \( (a - 1)(d - 1) - bc = 0 \) is \( l^3 + l^2 - l - l^2 - l = l^3 - 2l \). Hence,

\[
n_l = \frac{l^3 - 2l}{l^4 - l^3 - l^2 + l} = \frac{1}{l} + o\left(\frac{1}{l^2}\right).
\]
as \( l \to \infty \).

**B.6.14 Proposition.**

Let \( l \) be a rational prime number. Then the following statements are true.

1. \( \text{Gal}(\bar{K}/K) \) acts on \( E(\bar{K})[l] \) for all \( l \), or, in other words, there is a homomorphism
   \[
   \Lambda_l : \text{Gal}(\bar{K}/K) \longrightarrow \text{Aut}(E(\bar{K})[l]) \cong GL_2(\mathbb{Z}/l).
   \]
   (See Section 7, Chapter 3 of [113].)

2. There exists a finite set of rational primes \( \mathcal{S}(K) \) such that for all rational primes \( l \not\in \mathcal{S}(K) \) we have that \( \Lambda_l \) is onto. (See (7) on page 260 of [87].)

**B.7 Coordinate Polynomials.**

In this section we introduce coordinate polynomials – a computational device designed to simplify translation from the polynomials with variables ranging in a finite extension of a field to polynomials with variables ranging in the field below. This definition of coordinate polynomials has been suggested to the author by Laurent Moret-Bailly. We start with a definition of a map.

**B.7.1 Definition.**

Let \( F \) be a field, let \( M \) be a finite extension of \( F \). Let \( \Omega = \{\omega_1, \ldots, \omega_k\} \) be a basis of \( M \) over \( K \). Then let \( \pi : F^k \longrightarrow M \) be defined by

\[
(b_1, \ldots, b_k) \mapsto \sum_{i=1}^{k} b_i \omega_i.
\]

Let

\[
\bar{\sigma} = (\sigma_1, \ldots, \sigma_k) : M \longrightarrow F^k
\]

be a linear \( F \)-section of \( \pi \) defined by \( \sigma_j(\sum_{i=1}^{k} b_i \omega_i) = b_j \). Next we extend \( \bar{\sigma} \) to polynomials over \( M \). Let \( Q(z_1, \ldots, z_m) \in M[z_1, \ldots, z_m] \) and suppose

\[
Q(z_1, \ldots, z_m) = \sum_{i_1, \ldots, i_m} A_{i_1, \ldots, i_m} z_1^{i_1} \cdots z_m^{i_m},
\]

where \( A_{i_1, \ldots, i_m} \in M \). Then define

\[
\sigma_j(Q(z_1, \ldots, z_m)) = \sum_{i_1, \ldots, i_m} \sigma_j(A_{i_1, \ldots, i_m}) z_1^{i_1} \cdots z_m^{i_m}
\]

331
so that
\[ \bar{\sigma}(Q(z_1, \ldots, z_m)) = (\sigma_1(Q(z_1, \ldots, z_m)), \ldots, \sigma_k(Q(z_1, \ldots, z_m))). \]

We are now ready to define the coordinate polynomials.

**B.7.2 Definition.**

Let \( M, F, \Omega \) be as above. Let
\[ P(X_1, \ldots, X_m, w_1, \ldots, w_u) \in M[X_1, \ldots, X_m, w_1, \ldots, w_u]. \]
Then define the \( k \)-tuple of polynomials
\[
\bar{\sigma}(P(\sum_{i=1}^{k} x_{1,i} \omega_i, \ldots, \sum_{i=1}^{k} x_{m,i} \omega_i), w_1, \ldots, w_u) =
\]
\[ (P_1^\Omega(x_{1,1}, \ldots, x_{k,m}, w_1, \ldots, w_u), \ldots, P_k^\Omega(x_{1,1}, \ldots, x_{k,m}, w_1, \ldots, w_u)) \]

\( \) to be the coordinate polynomials of \( P(X_1, \ldots, X_m, w_1, \ldots, w_u) \) with respect to \( \Omega \) and \( \bar{X} = (X_1, \ldots, X_m) \).

The most important properties of the coordinate polynomials are described in the following lemma whose proof we leave to the reader.

**B.7.3 Lemma.**

In the above notations, the following statements are true.

1. For \( j = 1, \ldots, k \), we have that
\[ P_j^\Omega(x_{1,1}, \ldots, x_{k,m}, w_1, \ldots, w_u) \in F[x_{1,1}, \ldots, x_{k,m}, w_1, \ldots, w_u]. \]

2. \[ P(\sum_{j=1}^{k} x_{1,j} \omega_j, \ldots, \sum_{j=1}^{k} x_{m,j} \omega_j, w_1, \ldots, w_u) = \]
\[ \sum_{j=1}^{m} P_j^\Omega(x_{1,1}, \ldots, x_{m,k}, w_1, \ldots, w_u) \omega_j. \]
3. \[ \exists X_1, \ldots, X_m \in M, \ w_1, \ldots, w_u \in F : P(X_1, \ldots, X_m, w_1, \ldots, w_u) = 0 \]

\[ \begin{align*}
\exists x_1, \ldots, x_m, k, \ w_1, \ldots, w_u \in F & : \ \bigwedge_{i=1}^k P_i^\Omega(x_1, \ldots, x_m, k, \ w_1, \ldots, w_u) = 0 \\
\end{align*} \]

4. Let \( A_{ijr} = \sigma_r(\omega_i \omega_j) \). Then the coefficients of coordinate polynomials are themselves polynomials in \( \{A_{ijr}, i, j, r \in \{1, \ldots, k\}\} \). Furthermore, these polynomials depend on \( P(X_1, \ldots, X_m, w_1, \ldots, w_u) \) only and can be computed effectively and uniformly in \( P(X_1, \ldots, X_m, w_1, \ldots, w_u) \) from coefficients of \( P(X_1, \ldots, X_m, w_1, \ldots, w_u) \). (Here by a “uniform in \( P \)” procedure we mean an effective procedure which takes the coefficients of \( P \) as inputs and produces the coefficients of \( P_i^\Omega \).)

**B.7.4 Remark.**

If \( P[X_1, \ldots, X_m, w_1, \ldots, w_u] \in F[X_1, \ldots, X_m, w_1, \ldots, w_u] \), then the procedure described in Part 4 of Lemma B.7.3, can be carried out even if the given set \( \{\omega_1, \ldots, \omega_k\} \) is not a basis of some finite extension \( M \) over \( F \) but simply is a set of elements in the algebraic closure of \( F \) subject to the condition \( \omega_i \omega_j = \sum_{r=1}^k A_{i,j,r} \omega_r \) for all pairs \( (i, j) \in \{1, \ldots, k\}^2 \) for some set \( A = \{A_{i,j,r}, i, j, r \in \{1, \ldots, k\}\} \subset F \).

Note that once we have a set \( A \) as above, then inductively we can rewrite any finite product of elements of \( \Omega \) as a linear combination of elements of \( \Omega \) with coefficients in \( F \).

If \( \Omega \) is not a basis of some finite extension \( M \) of \( F \) (or we are not sure if \( \Omega \) is a basis, as will happen below), we will call the polynomials generated by this procedure “pseudo-coordinate” polynomials. We will use the notation \( P_{\Omega,A}^\Omega \) for these polynomials. Note that Parts 1 and 2 of Lemma B.7.3 remain true for pseudo-coordinate polynomials also, while Part 3 fails if \( \Omega \) is not basis.

A situation which occurs frequently can be described as follows. Let \( F \) be a field as above, let \( a_0, \ldots, a_m \) represent variables ranging over \( F \), and let \( t \) be a variable ranging over the algebraic closure of \( F \). Assume the variables satisfy the following equation:

\[ t^m + a_{m-1}t^{m-1} + \ldots + a_0 = 0. \quad \text{(B.7.1)} \]
Let \( \Omega = \{1, t, \ldots, t^{m-1}\} \). So for this \( \Omega \) we have that \( \omega_i = t^{i-1} \). Then from (B.7.1) we conclude that for \( i + j < m \) we have that \( A_{i,j,i+j} = a_{i+j} \) and \( A_{i,j,r} = 0 \) for \( r \neq i + j \). Next we consider the case of \( i + j = m \). Here we have \( A_{i,j,r} = a_r \). For the case of \( i + j > m \) we proceed inductively. Assume, that for \( m < i + j < k \) we have that \( A_{i,j,r} = Q_{i+j,r}(a_0, \ldots, a_{m-1}) \in F[a_0, \ldots, a_{m-1}] \). Then observe that

\[
t^k = -a_{m-1} t^{k-1} - \ldots - a_0 t^{k-m} =
\]

\[
- a_{m-1} \sum_{r=0}^{m-1} Q_{k-1,r}(\bar{a}) t^r - \ldots - a_0 \sum_{r=0}^{m-1} Q_{k-m,r}(\bar{a}) t^r = \sum_{r=0}^{m-1} Q_{k,r}(\bar{a}) t^r,
\]

where \( \bar{a} = (a_0, \ldots, a_{m-1}) \). Thus, we conclude that assuming \( \bar{a} = (a_{m-1}, \ldots, a_0) \) takes values in \( F^m \), we have that \( A_{i,j,r} = Q_{i+j,r}(\bar{a}) \in F[\bar{a}] \) for all \( i, j, r \in \{0, \ldots, m-1\} \) and we can construct pseudo-coordinate polynomials \( P_{\Omega,\bar{A}} \) whose coefficients will be polynomials in \( a_0, \ldots, a_{m-1} \). Note further that these polynomial coefficients depend on \( m \) only and can be constructed effectively given an \( m \).

For those values of \( \bar{a} \) for which the polynomial \( T^m + a_{m-1} T^{m-1} + \ldots + a_0 \) is irreducible over \( F \), the pseudo-coordinate polynomials will actually be the real thing. But it is important to note that pseudo-coordinate polynomials are defined unconditionally.

With the discussion above in mind we prove the following lemma.

**B.7.5 Lemma.**

Let \( L \) be a field. Let \( G(T, Z_1, \ldots, Z_l) \in F[T, Z_1, \ldots, Z_l] \) be a monic polynomial in \( T \) of degree \( d \) in \( T \). Let

\[
P(X_1, \ldots, X_m, w_1, \ldots, w_u) \in F[X_1, \ldots, X_m, w_1, \ldots, w_u].
\]

For \( k = 1, \ldots, d - 1 \), let \( \Omega_k = \{1, t, \ldots, t^{k-1}\} \), where \( t \) is a root of the equation \( G(T, z_1, \ldots, z_l) = 0 \) for some \( z_1, \ldots, z_l \in F \). Further, let \( A^{(k)} = \{A_{i,j,t}^{(k)}\} \) be generated formally as above from the equation \( t^k + a_{k-1,1} t^{k-1} + \ldots + a_{k,0} = 0 \). Let \( P_{i,\Omega_k,\bar{A}^{(k)}}^d, k < d \), as above be the \( i \)-th pseudo-coordinate polynomial corresponding to \( \Omega_k \) and \( A^{(k)} \). The set \( A^{(d)} \) should be generated using coefficients of \( G(T, z_1, \ldots, z_l) \). Then for any \( z_1, \ldots, z_l \in F \), for any \( t \) in the algebraic closure of \( F \) satisfying \( G(t, z_1, \ldots, z_l) = 0 \),

\[
\exists X_1, \ldots, X_m \in F(t), w_1, \ldots, w_u \in F : P(X_1, \ldots, X_m, w_1, \ldots, w_u) = 0
\]

(B.7.2)
Lemma B.7.3 and Remark B.7.4

\[ \exists a_{1,0}, \ldots, a_{d-1,d-2}, b_{1,0}, \ldots, b_{d-1,d-2}, x_{1,0}, \ldots, x_{m,d-1}, w_1, \ldots, w_u \in F : \]
\[ \bigvee_{k=1}^{d-1} \left\{ \begin{equation} \begin{aligned} t^k + a_{k,k-1}t^{k-1} + a_{k,0} &= 0 \\ \bigwedge_{j=1}^{k} P_j^{\Omega_k, A^{(k)}}(x_{1,0}, \ldots, x_{m,k-1}, w_1, \ldots, w_u) &= 0 \end{aligned} \right. \]
\[ \bigwedge_{j=0}^{d-1} P_j^{\Omega_d, A^{(d)}}(x_{1,0}, \ldots, x_{m,d-1}, w_1, \ldots, w_u) = 0. \] (B.7.3)

Here the equality
\[ (T^i + a_{i,i-1}T^{i-1} + a_{i,0})(T^{d-i} + b_{i,d-i-1}T^{d-i-1} + \ldots + b_{i,0}) = G(T, z_1, \ldots, z_r) \]
should be read as an equality of polynomials in \( T \) which can be rewritten as a system of polynomial equations in variable \( a_{i,j}, b_{k,l} \) and \( z_s \). Also for \( 1 \leq k < d \) and \( 1 \leq j \leq k \) we have that
\[ P_j^{\Omega_k, A^{(k)}}(x_{1,0}, \ldots, x_{m,k-1}, w_1, \ldots, w_u) = R_{j,k}(a_{0,0}, \ldots, a_{k,k-1}, x_{1,0}, \ldots, x_{m,k-1}, w_1, \ldots, w_u), \]
where \( R_{j,k}(a_{0,0}, \ldots, a_{k,k-1}, x_{1,0}, \ldots, x_{m,k-1}, w_1, \ldots, w_u) \) is a polynomial over \( F \) whose coefficients depend on \( P, j \) and \( k \) only and can be constructed effectively from these data. While,
\[ P_j^{\Omega_d, A^{(d)}}(x_{1,0}, \ldots, x_{m,d-1}, w_1, \ldots, w_u) = R_{j,d}(x_{1,0}, \ldots, x_{m,d-1}, w_1, \ldots, w_u), \]
where \( R_{j,d}(x_{1,0}, \ldots, x_{m,d-1}, w_1, \ldots, w_u) \) is a polynomial over \( F \) whose coefficients depend on \( G, P \) and \( j \) only and can be constructed effectively from these data.

**Proof.**

Let \( t, z_1, \ldots, z_r \) be given. Let \( 1 \leq k \leq d \) be the degree of \( t \) over \( F \). Let \( T^k + c_{k-1}T^{k-1} + \ldots + c_0 \) be the monic irreducible polynomial of \( t \) over \( F \). Then either \( k = d \) and \( G(T, z_1, \ldots, z_r) \) is irreducible, or \( k < d \) and for \( a_{k,i} = c_i \) and some \( F \)-values of \( b_{k,i} \)'s the polynomial-in-\( T \) equation in (B.7.3) holds. Further, for this value of \( k \), we also have that \( P_i^{\Omega_k, A^{(k)}} = P_i^{\Omega_k, A^{(k)}}, i = 1, \ldots, k \) are coordinate polynomials. Now the conclusion of the lemma follows from Lemma B.7.3 and Remark B.7.4.
B.8 Basic Facts about Local Fields.

In this section we define local fields and list their properties important for our purposes. We start with defining notation.

B.8.1 Notation.

Let \( K \) be a global field and let \( p \) be a non-archimedean prime of \( K \). Let \( K_p \) denote the completion of \( K \) under the non-archimedean absolute value corresponding to \( p \).

B.8.2 Hensel's Lemma.

Let \( f(X) \in K_p[X] \) be such that all the coefficients of \( f \) are integral. Suppose there exists an integral \( K_p \)-element \( \alpha_0 \) such that \( \text{ord}_p f(\alpha_0) > 2\text{ord}_p f'(\alpha_0) \). Then \( f(x) \) has a root \( \alpha \) in \( K_p \). (See [46], Proposition 2, Section 2, Chapter II.)

B.8.3 Lemma.

Let \( q \) be a rational prime relatively prime to the characteristic \( p > 0 \) of the residue field of \( K_p \). Let \( a \in K_p \) be a unit such that \( a \) is a \( q \)-th power modulo \( p \). Then \( a \) is a \( q \)-th power in \( K_p \).

Proof.

First of all observe the following. If \( K \) is a function field then \( q \) is automatically prime to \( p \). If \( K \) is a number field, then \( p \) is a factor of \( p \). Thus, if \( p \) is prime to \( q \), \( p \) is prime to \( q \). Next consider the polynomial \( f(X) = X^q - a \) with \( f'(X) = qX^{p-1} \). Let \( b^q \equiv a \mod p \). Note that

\[
2\text{ord}_p f'(b) = 2\text{ord}_p q + 2(q - 1)\text{ord}_p b = 0 < \text{ord}_p f(b),
\]

by assumption. Therefore, by Hensel's lemma (see Lemma B.8.2), \( f(X) \) has a root \( \alpha \) in \( K_p \) or in other words for some \( \alpha \in K_p \), we have that \( \alpha^p - a = 0 \).

B.8.4 Lemma.

Let \( K \) be a number field. Let \( p > 0 \) be the characteristic of the residue field of \( p \). Let \( a \) be a unit of \( K_p \) such that for some \( \varepsilon \in K \), we have that \( \varepsilon^p \equiv a \mod p^{2e(p/p)+1} \). Then \( a \) is a \( p \)-th power in \( K_p \).
Proof.

We apply Hensel’s lemma again. Let $f(X) = X^p - a$ as before and note that

$$2\text{ord}_p f'(\epsilon) = 2\text{ord}_p p + 2(p - 1)\text{ord}_p \epsilon = 2e(p/p) < 2e(p/p) + 1 = \text{ord}_p f(\epsilon).$$

Thus $f$ has a root in $K_p$ and $a$ is a $p$-th power.

B.8.5 Lemma.

Let $M$ be a finite separable extension of $K$. Let $P$ be a factor of $p$ in $M$. Finally, let $M_P$ be the completion of $M$ under $P$. Then if $P/p$ is unramified, every $K_p$ unit is a norm of some element of $M_P$. (See [1], Theorem 2, Section 2, Chapter 7 or [119] (Corollary to Proposition 6, Section 2, Chapter XII ).)

B.9 Derivations.

In this section we discuss derivations over function fields. They are used to insure that zeros and poles of certain functions are simple. To introduce the notions of global and local derivations we will need a proposition stated below.

B.9.1 Proposition.

Let $K$ be a function field over a finite field of constants $C$. Let

$$K_0 = \{w^p, w \in K\}$$

and let $t \in K$ be such that $K/C(t)$ is a separable extension. Then $K = K_0(t)$ and $[K : K_0] = p$.

(See [21], Chapter III, Section 2 for proof.)

B.9.2 Definition.

Let $t, K, K_0$ be as in Proposition B.9.1. Let $x \in K, x = \sum_{i=0}^{p-1} u_i t^i, u_i \in K_0$. Then define $dx/dt = \sum_{i=0}^{p-2} i u_i t^{i-1}$.

Proposition B.9.1 assures us that we have defined $dx/dt$ for all $x$.

We leave the proof of the next proposition to the reader.
B.9.3 Proposition.

The global derivation in Definition B.9.2 satisfies the usual differentiation rules concerning the derivative of the sum and the product of functions as well as the Chain Rule.

Next we state the main proposition of this section.

B.9.4 Proposition.

Let $K$ be a function field over a finite field of constants $C_K$. Let $p$ be a prime of $K$ and let $t \in K$ be such that $K/C_K(t)$ is separable and $\text{ord}_p t = 1$. Then for any $x \in K$, if $\text{ord}_p x \geq 0$, then $\text{ord}_p \frac{dx}{dt} \geq \text{ord}_p x - 1$.

Proof.

We present a proof of this proposition suggested to the author by Laurent Moret-Bailly. First of all we observe that by Proposition B.9.1, the derivation with respect to $t$ is well defined. Next write $x = \sum_{i=0}^{p-1} u_i t^i$, where $u_i \in K_0$ as in Definition B.9.2. Observe that $\text{ord}_p u_i t^i \equiv i \mod p$ and therefore for $i \neq j$ we have that $\text{ord}_p u_i t^i \neq \text{ord}_p u_j t^j$. Thus,

$$0 \leq \text{ord}_p x = \min_{i=0, \ldots, p-1} \text{ord}_p u_i t^i$$

and $\text{ord}_p u_i \geq 0$. Now using the definition of derivation we consider two cases. In the first case $\text{ord}_p x \equiv 0 \mod p$ and therefore

$$\text{ord}_p x = \text{ord}_p u_0 \leq \min_{1 \leq j \leq p-1} \{\text{ord}_p t^j u_j\} - 1.$$

Thus

$$\text{ord}_p \frac{dx}{dt} = \min\{\text{ord}_p u_1, \text{ord}_p 2 u_2 t, \ldots, \text{ord}_p (p-1) u_{p-1} t^{p-2}\}$$

$$\geq \min_{1 \leq j \leq p-1} \{\text{ord}_p t^j u_j\} - 1 \geq \text{ord}_p x.$$ 

In the second case we have that $\text{ord}_p x \not\equiv 0 \mod p$. Then

$$\min_{i=0, \ldots, p-1} \text{ord}_p (u_i t^i) = \text{ord}_p (u_j t^j),$$

where $1 \leq j \leq p - 1$. But in this case,

$$\text{ord}_p u_j t^j = \min\{\text{ord}_p u_1, \text{ord}_p 2 u_2 t, \ldots, \text{ord}_p (p-1) u_{p-1} t^{p-2}\},$$

so that $\text{ord}_p \frac{dx}{dt} = \text{ord}_p x - 1$.

We can strengthen the result of the lemma in the following fashion.
B.9.5 Corollary.

Let $q$ be a prime of a global function field $K$ of characteristic $p$, let $w \in K$ be such that $\text{ord}_q w = 1$. Let $t \in K$ be as before such that $K/C(t)$ is separable. Assume further $\text{ord}_q \frac{dw}{dt} \geq 0$. Then for any $x \in K$ integral at $q$, we have that $\text{ord}_q \frac{dx}{dt} \geq \text{ord}_q x - 1$.

Proof.

Since $w$ has order 1 at a prime, it is not a $p$-th power and therefore derivation with respect to $w$ is defined. Now we use the Chain Rule:

$$\text{ord}_q \frac{dx}{dt} = \text{ord}_q \frac{dx}{dw} + \text{ord}_q \frac{dw}{dt} \geq \text{ord}_q \frac{dx}{dw} \geq \text{ord}_q x - 1,$$

where the last inequality holds by Proposition B.9.4.

B.9.6 Remark.

Using the product rule, it is not hard to show that the corollary above holds even if $x$ is not integral at $p$. We leave the details to the reader.

B.9.7 Corollary.

Let $K$ be a function field over a finite field of constants $C$. Let $t \in K$ be such that $t$ is not a $p$-th power in $K$. Let $p$ be a prime of $K$ such that it is not ramified in the extension $K/C(t)$ and is not a pole of $t$. Then for any $x \in K$, if $\text{ord}_p x > 1$, then $\text{ord}_p \frac{dx}{dt} > 0$.

Proof.

Let $P(t)$ be a monic irreducible polynomial corresponding to the prime of $C(t)$ lying below $p$. (We know such a polynomial exists because $p$ is not a pole of $t$.) Now, since $p$ is not ramified over $C(t)$ we must have $\text{ord}_p P(t) = 1$. Further, $\frac{dP(t)}{dt}$ is a polynomial and therefore $\text{ord}_p \frac{dP(t)}{dt} \geq 0$. Thus, by Corollary B.9.5, for any $x \in K$ integral at $p$ we have that $\text{ord}_p \frac{dx}{dt} \geq \text{ord}_p x - 1$. Hence the conclusion of the corollary follows.

B.10 Some Calculations.

In this section we carry out some calculations necessary for various proofs in the book but not of any independent interest.
B.10.1 Lemma.

Let $X_i$ be a sequence of positive real numbers such that
\[ \limsup_{l \to \infty} \frac{X_i}{l^2 \log X_i} \leq c \in \mathbb{R}^+. \]

Then for some constant $\bar{c} \in \mathbb{R}^+$ we have that $\limsup_{l \to \infty} \frac{X_i}{l^2 \log l} \leq \bar{c}$.

Proof.

First of all, we observe that our assumptions imply that for some $C \in \mathbb{R}$, for all $l \in \mathbb{N} \setminus \{0\}$, it is the case that $X_i \leq Cl^2$. Thus for some constant $\bar{C} \in \mathbb{R}$, we have that $X_i \leq \bar{C}l^2 \sqrt{X_i}$. Therefore, for all $l \in \mathbb{N} \setminus \{0\}$ and some constant $\tilde{C} \in \mathbb{R}$, we have that $X_i < \tilde{C}l^4$. Now observe that as $l \to \infty$ we have that
\[ \frac{X_i}{l^2 \log l} \leq \frac{\bar{C}l^2 \log X_i}{l^2 \log l} \leq \frac{\bar{C} \log(\bar{C}l^2 \sqrt{X_i})}{\log l} \leq D + \frac{\tilde{C} \log \log X_i}{\log l} \]
for some positive constants $D$ and $\tilde{C}$. Since $X_i < \tilde{C}l^4$, we also have as $l \to \infty$ that
\[ \frac{\tilde{C} \log \log X_i}{\log l} \leq \frac{\tilde{C} \log \log \tilde{C}l^4}{\log l} \to 0. \]

Thus, the assertion of the lemma is true.

B.10.2 Proposition.

Let $\{\alpha_i, i \in \mathbb{N}\} \subset \mathbb{R}$ be such that
1. $\sum_{i=1}^{\infty} \alpha_i = \infty$,
2. $\sum_{i=1}^{\infty} \alpha_i^2 < \infty$,
3. $0 < \alpha_i < 1$,
4. For all $i \in \mathbb{N}$ we have that $\alpha_i > \alpha_{i+1}$ and $\lim_{i \to \infty} \alpha_i = 0$.

Let $S(n) = \sum_{i=1}^{n} \alpha_i$. Let $\mathcal{A}(n) = \{\alpha_1, \ldots, \alpha_n\}$. Then the following statements are true.

1. $G(n) = \prod_{i=1}^{n} (1 - \alpha_i) = O(1) e^{-S(n)}$.
2. For all $k$ we have that
\[ S_k(n) = G(n) \sum_{\text{all } k\text{-element subsets of } \mathcal{A}(n) \frac{\alpha_i \ldots \alpha_k}{(1 - \alpha_i) \ldots (1 - \alpha_k)} \to 0 \text{ as } n \to \infty. \]
Proof.

1. Observe that \( \log G(n) = \sum_{i=1}^{n} \log(1 - \alpha_i) = -\sum_{i=1}^{n} \alpha_i + O(1) = -S(n) + O(1) \). Therefore, \( G(n) = O(1)e^{-S(n)} \).

2. We show that \( S_k(n) < O(1)S^k(n)G(n) \). Indeed, using the fact that all the terms in the sum are positive, we see the following.

\[
S_k(n) = G(n) \sum_{\text{all } k\text{-element subsets of } \mathcal{S}(n)} \frac{\alpha_{i_1} \ldots \alpha_{i_k}}{(1 - \alpha_{i_1}) \ldots (1 - \alpha_{i_k})} < (1 - \alpha_1)^{-k}(S(n))^kG(n) \rightarrow 0
\]

as \( n \to \infty \).

B.10.3 Lemma.

Let \( F/G \) be a finite field extension. Let \( \Omega = \{\omega_1, \ldots, \omega_n\} \) be a basis of \( F \) over \( G \). Then for \( l = 1, \ldots, n \) there exist

\[
P_l(X_1, \ldots, X_n, Y_1, \ldots, Y_n) \in G[X_1, \ldots, X_n, Y_1, \ldots, Y_n]
\]

depending on \( \Omega \) only such that for all \( a_1, \ldots, a_n, b_1, \ldots, b_n \in G \) we have that

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

Proof.

Let \( A_{i,j,l} \in G \) be such that \( \omega_i\omega_j = \sum_{l=1}^{n} A_{i,j,l}\omega_l \). Then

\[
\sum_{i=1}^{n} a_i\omega_i \sum_{j=1}^{n} b_j\omega_j = \sum_{i,j} a_i b_j A_{i,j,l}\omega_l = \sum_{l=1}^{n} \sum_{i,j} A_{i,j,l} a_i b_j \omega_l.
\]

Thus, we can set \( P_l(X_1, \ldots, X_n, Y_1, \ldots, Y_n) = \sum_{i,j} A_{i,j,l} X_i Y_j \).

B.10.4 Lemma.

Let \( R \) be an integral domain with a quotient field \( F \). Let \( A_1, \ldots, A_k \in F, a, a_1, \ldots, a_k \in R \), and assume that for \( i = 1, \ldots, k \) we have that \( aA_i = a_i \). Let

\[
P(X_1, \ldots, X_k) = \sum_{i_1 + \ldots + i_k \leq d} a_{i_1} \ldots a_{i_k} X_1^{i_1} \ldots X_k^{i_k}
\]
be a polynomial over $F$ of degree $d$. Let $b$ be a common denominator of all the coefficients of $P$ with respect to $R$. Let

$$P_R(Y_1, \ldots, Y_k, Z) = \sum_{i_1 + \ldots + i_k \leq d} b a_{i_1, \ldots, i_k} Y_1^{i_1} \cdots Y_k^{i_k} Z^{d-(i_1+\ldots+i_k)}$$

be a polynomial over $R$. Then

$$a^d b P(A_1, \ldots, A_k) = P_R(a_1, \ldots, a_k, a) \in R,$$

and $P(X_1, \ldots, X_k) = 0$ has solutions in $F$ if and only if $P_R(Y_1, \ldots, Y_k, Z) = 0$ has solutions in $R$ with $Z \neq 0$.

**Proof.**

Since the second assertion of the lemma is obvious, we will verify the first one only.

$$a^d b P(A_1, \ldots, A_k) = a^d b \sum_{i_1 + \ldots + i_k \leq d} a_{i_1, \ldots, i_k} A_1^{i_1} \cdots A_k^{i_k} =$$

$$\sum_{i_1 + \ldots + i_k \leq d} (b a_{i_1, \ldots, i_k})(a_1^{i_1}A_1^{i_1}) \cdots (a_k^{i_k}A_k^{i_k}) a^{d-i_1-\ldots-i_k} \in R,$$

since every term in the product is now in $R$.

**B.10.5 Lemma.**

Let $F \subseteq G \subseteq L$ be finite extensions of fields. Let $\Omega = \{\omega_1, \ldots, \omega_k\}$ be a basis of $L$ over $F$. Let $\Lambda = \{\lambda_1, \ldots, \lambda_m\}$ be a basis of $G$ over $F$. (Given our assumptions, $m \leq k$.) Assume $\Omega$ is ordered in such a way that the matrix $(c_{i,j})$, $i, j = 1, \ldots, m$, where $c_{i,j} \in F$ and $\lambda_i = \sum_{j=1}^m c_{i,j}\omega_j$, is nonsingular. Then there exist $P_1, \ldots, P_m, T_1, \ldots, T_{k-m} \in F[x_1, \ldots, x_m]$, depending on $G, L, \Omega$ and $\Lambda$ only, such that for any $a_1, \ldots, a_k, b_1, \ldots, b_m \in F$, the following two statements are equivalent.

$$\sum_{i=j}^k a_i \omega_j = \sum_{i=1}^m b_i \lambda_i,$$  \hspace{1cm} (B.10.1)

and

$$\begin{cases}
  b_i = P_i(a_1, \ldots, a_m), i = 1, \ldots, m, \\
  a_{m+j} = T_j(a_1, \ldots, a_m), j = 1, \ldots, k - m.
\end{cases}$$  \hspace{1cm} (B.10.2)
Proof.

The matrix \((c_{i,j})\) has rank \(m \leq k\). By assumption, the first \(m\) columns are linearly independent. We can rewrite (B.10.1) as

\[
\sum_{i=j}^{k} a_j \omega_j = \sum_{i=1}^{m} b_i \sum_{j=1}^{k} c_{i,j} \omega_j = \sum_{j=1}^{k} \sum_{i=1}^{m} b_i c_{i,j} \omega_j.
\]

This equality leads to a system

\[
\begin{cases}
\sum_{i=1}^{m} b_i c_{i,1} = a_1 \\
\ldots \\
\sum_{i=1}^{m} b_i c_{i,m} = a_m \\
\sum_{i=1}^{m} b_i c_{i,k} = a_k
\end{cases}
\]  

(B.10.3)

where we consider \(b_1, \ldots, b_m\) as variables. Given our assumptions, we have the following information about the system (B.10.3).

1. This system has a solution.
2. The first \(m\) equations of the system have a unique solution.

Thus, if we solve the first \(m\) equations, the rest of the system will be satisfied automatically. Using Cramer’s rule to solve the \(m \times m\) system we deduce that \(b_i = P_i(a_1, \ldots, a_m)\), where for each \(i\) we have that \(P_i\) is a fixed polynomial over \(F\) depending on \(G, L, \Omega\) and \(\Lambda\) only. Further, if we consider the remaining \(k - m\) equations, we will conclude that

\[
a_{m+j} = \sum_{i=1}^{m} b_i c_{i,m+j} = \sum_{i=1}^{m} P_i(a_1, \ldots, a_m) c_{i,m+j}, j = 1, \ldots, k - m.
\]

This proves that (B.10.1) implies (B.10.2). On the other hand all the steps in the proof above are reversible. Thus, (B.10.2) implies (B.10.1) also.

B.10.6 Lemma.

Let \(G/F\) be a finite field extension and let

\[
\Omega = \{\omega_1, \ldots, \omega_k\}
\]

be a basis of \(G\) over \(F\). Let \(a_1, \ldots, a_k \in F\). Then there exist

\[
P_1, \ldots, P_k, Q \in F[x_1, \ldots, x_k]
\]
depending on \( F, G \) and \( \Omega \) only such that \( \sum_{i=1}^{k} a_i \omega_i \neq 0 \) if and only if
\[
Q(a_1, \ldots, a_k) \neq 0
\]
and
\[
\sum_{i=1}^{k} P_i(a_1, \ldots, a_k) \omega_i \left( \sum_{i=1}^{k} a_i \omega_i \right) = 1.
\]

**Proof.**

Let \( A_1, \ldots, A_k \in F \) be such that \( \sum_{i=1}^{k} A_i \omega_i = 1 \). For all \( i, j = 1, \ldots, k \), let \( B_{i,j,1}, \ldots, B_{i,j,k} \in F \) be such that
\[
\omega_i \omega_j = \sum_{r=1}^{k} B_{i,j,r} \omega_r.
\]

Note that
\[
A_1, \ldots, A_k, B_{1,1,1}, \ldots, B_{k,k,k}
\]
depend on \( \Omega \) only. Next note that \( \sum_{i=1}^{k} a_i \omega_i \neq 0 \) if and only if there exist \( c_1, \ldots, c_k \in F \) such that
\[
\sum_{i=1}^{k} a_i \omega_i \left( \sum_{i=1}^{k} c_i \omega_i \right) = 1.
\]
The last equation holds if and only if
\[
\sum_{i=1}^{k} A_i \omega_i = 1 = \sum_{i=1}^{k} a_i \omega_i \sum_{i=1}^{k} c_i \omega_i = \sum_{i,j=1}^{k} a_i c_j \omega_i \omega_j = \sum_{i,j,r=1}^{k} a_i c_j B_{i,j,r} \omega_r.
\]
Thus, \( \sum_{i=1}^{k} a_i \omega_i \neq 0 \) if and only if there exist \( c_1, \ldots, c_k \) such that the following system is satisfied.
\[
\sum_{i,j=1}^{k} a_i c_j B_{i,j,r} = A_r, \ r = 1, \ldots, k,
\]
\[
\sum_{j=1}^{k} \sum_{i=1}^{k} a_i B_{i,j,r} c_j = A_r.
\]

By Cramer’s Rule, we can conclude that \( \sum_{i=1}^{k} a_i \omega_i \neq 0 \) if and only if \( c_1, \ldots, c_k \) have the required form. (The polynomial in the denominator is the determinant of the system which is not zero if and only if the system has a unique solution. The last condition is true if and only if \( \sum_{i=1}^{k} a_i \omega_i \neq 0 \).)
B.10.7 Lemma.
Let $\delta = \{\delta_1, \ldots, \delta_p\}$, $\bar{\tau} = \{\tau_1, \ldots, \tau_q\}$ be two sets of complex numbers such that $\bar{\delta} \cap \bar{\tau} = \emptyset$. Let

$$C_{\delta, \bar{\tau}} = \min_{i=1, \ldots, q, j=1, \ldots, p} (|\tau_i - \delta_j|).$$

Let $z \in \mathbb{C}$ and let $C_{\bar{\tau}, z} = \min_{i=1, \ldots, q} (|\tau_i - z|)$, $C_{\delta, z} = \min_{j=1, \ldots, p} (|z - \delta_j|)$. Then

$$\max(C_{\bar{\tau}, z}, C_{\delta, z}) \geq \frac{1}{2} C_{\delta, \bar{\tau}}.$$

Proof.
The proof of this lemma is a simple consequence of the triangular inequality. Indeed, suppose $C_{\bar{\tau}, z} < \frac{1}{2} C_{\delta, \bar{\tau}}$. Note that for all $i, j$ we have that

$$|\tau_i - \delta_j| \leq |z - \delta_j| + |z - \tau_i|.$$

Thus, for all $i, j$ it is the case that $|z - \delta_j| \geq |\tau_i - \delta_j| - |z - \tau_i| \geq C_{\delta, \bar{\tau}} - |z - \tau_i|$. Let $i_0$ be such that $\frac{1}{2} C_{\delta, \bar{\tau}} > C_{\bar{\tau}, z} = |z - \tau_{i_0}|$. Then for all $j$ we have that $|z - \delta_j| \geq \frac{1}{2} C_{\delta, \bar{\tau}}$. Hence, $C_{\delta, z} \geq \frac{1}{2} C_{\delta, \bar{\tau}}$.

B.10.8 Lemma.
Let $n \in \mathbb{Z}_{>0}$, let $\bar{\tau}_1 = \{\tau_{1,1}, \ldots, \tau_{1,q_1}\}, \ldots, \bar{\tau}_{n+1} = \{\tau_{n+1,1}, \ldots, \tau_{n+1,q_{n+1}}\}$ be a collection of $n + 1$ pairwise disjoint sets of complex numbers. Let

$$C = \min_{u \neq j, l = 1, \ldots, q_u, j = 1, \ldots, q_j} (|\tau_{u,l} - \tau_{j,j}|).$$

Let $\{z_1, \ldots, z_n\}$ be a set of complex numbers. Let

$$C_u = \min_{j=1, \ldots, q_u, l=1, \ldots, n} (|z_l - \tau_{u,l}|).$$

Then for some $u$, we have that $C_u \geq \frac{1}{2} C$.

Proof.
For $l = 1, \ldots, n$ and $u = 1, \ldots, n+1$ call $z_l$ close to $\bar{\tau}_u$ if

$$C_{u,l} = \min_{j=1, \ldots, q_u} (|z_l - \tau_{u,j}|) < \frac{1}{2} C.$$

By Lemma B.10.7, each $z_l$ can be close to at most one $\bar{\tau}_u$. Thus, there is at least one $\bar{\tau}_u$ such that there is no $z_l$ close to it.
B.10.9 Lemma.

Let $K$ be a field. Let $x$ be an element of the algebraic closure of $K$. Let 
$\{F_i(T) = a_{i,0} + a_{i,1}T + \ldots + a_{i,n}T^n, i = 0, \ldots, n\}$ be a finite collection of polynomials with $a_{i,j} \in K$ and such that the matrix $(a_{i,j})$ is non-singular. Suppose for all $i = 0, \ldots, n$, we have that $F_i(x) \in K$. Then $x \in K$.

Proof.

By assumption, for $i = 0, \ldots, n$ it is the case that $F_i(x) = c_i \in K$. Therefore, we have the following linear system.

$$
\begin{pmatrix}
1 \\
x \\
\vdots \\
x^n
\end{pmatrix}
\begin{pmatrix}
(a_{i,j})
\end{pmatrix}
\begin{pmatrix}
c_0 \\
c_1 \\
\vdots \\
c_n
\end{pmatrix} =
\begin{pmatrix}
c_i
\end{pmatrix}, c_i \in K.
$$

Let $C_j$ be the matrix obtained by replacing the $j$-th column of $A = (a_{i,j})$ by the column vector

$$
\begin{pmatrix}
c_0 \\
c_1 \\
\vdots \\
c_n
\end{pmatrix}.
$$

Since the system is non-singular, we can solve for $x$ using Cramer’s rule to obtain

$$
x = \frac{\det C_1}{\det A},
$$

where the numerator and the denominator of the fraction are clearly in $K$. Therefore $x \in K$.

B.10.10 Corollary.

Let $K$ be a field of characteristic 0. Let $x$ be an element of the algebraic closure of $K$. Let 
$\{F_i(T) = (T + i + 1)^n, i = 0, \ldots, n\}$. Assume $F_i(x) \in K$. Then $x \in K$.

Proof.

By assumption $F_i(T) = \sum_{j=0}^{n} \binom{n}{j} (i + 1)^j T^{n-j}$. Therefore, in the notation of Lemma B.10.9, $a_{i,j} = \binom{n}{j} (i + 1)^j$. Thus,

$$
\det(a_{i,j}) = \prod_{j=0}^{n} \binom{n}{j} \det((i + 1)^j),
$$

346
where $\det(i+1)^j$ is a Vandermonde determinant not equal to 0. Consequently, the corollary holds by Lemma B.10.9.
Bibliography


[72] Bjorn Poonen. Elliptic curves whose rank does not grow and Hilbert’s Tenth Problem over the rings of integers. Private Communication.


Index

$O_K,\mathcal{O}_K$, 273
$\mathcal{O}_K$, 143
$\mathcal{P}$-integers, 2, 73, 122, 209, 261, 277
$\mathcal{W}$-integers, 24, 27, 48, 81, 99, 105, 113, 115, 125, 126, 136, 138, 139, 267, 273, 274, 276, 298
$\mathcal{W}$-units, 81, 82, 103, 110, 111
$\equiv_T$, 247, 249, 250, 254, 263
$\equiv_e$, 40, 247, 249, 250, 254, 263
$\equiv_{Dioph}$, 26, 40, 110, 112, 138, 139
$\leq_T$, 246, 248
$\leq_e$, 36–39, 248
$\leq_{Dioph}$, 13–16, 19–27, 37, 39, 43–45, 105, 114, 120–126, 131–136, 138, 139, 141, 184, 188, 190–193, 195, 197, 198, 205, 227
$p$-th power equations, 148, 176, 231
ord, 271
algebraic integers, 2, 25, 73, 107, 206, 233, 275
algebraic set, 5, 199–203, 205, 207, 208
c.e., 244
Cantor, David, 233
Chebotarev Density Theorem, 103, 137, 192, 215, 218, 289, 311, 315, 317
Church’s thesis, 237
Colliot-Thélène, Jean-Louis, 199
computable
field, 33
function, 32, 46, 236, 237, 239, 240, 243–245, 254, 259
presentation, 33
set, 138, 207, 236, 239, 240
computably enumerable sets, 36, 46, 140, 236, 244
decomposition group, 66, 103, 287, 289, 290, 300–302, 316
defining
field, 13–17, 20, 45
polynomial, 13, 22, 25
sets, 14, 15
degree of a divisor, 152, 275, 299, 300, 307, 309
degree of a prime, 151, 273, 275, 299, 306
Denef, Jan, 25, 72, 105, 108, 110, 142, 232, 234, 235
density
Dirichlet, 69, 71, 113, 133–135, 137, 139, 192, 193, 204, 206, 211, 310–318, 320
natural, 137, 209, 211, 214–219, 221–225, 310, 317–
 derivation, 159, 167, 336–338
dioph-gen, 13, 14, 19, 21
dioph-reg, 25, 26, 121, 123, 198, 227
dioph-regular, 24, 26, 27, 122, 138, 198
diophantine
  basis, 13–17, 19, 20, 22, 45
classes, 3, 8, 9, 13, 26, 27, 39, 40, 48, 175, 179, 183, 195
decidability, 31, 33, 36, 183
definability, 2, 3, 8, 31, 33, 36, 39, 40, 139, 183, 184, 204, 231, 234, 300, 302
equations, 1
equivalence, 8, 31
family, 26–30, 140, 195, 196
generation, 4, 8, 9, 13, 14, 16, 21, 24, 26, 31, 37, 40, 42, 44, 123, 126, 132, 138, 139, 192, 195, 197, 198, 258
model, 4, 42, 43, 46, 47, 141, 142, 148, 176, 177, 206, 207, 210, 211, 227, 229, 234
problem, 3, 5, 7, 8, 48, 229, 231, 234
regularity, 138
undecidability, 31, 40, 125, 142, 176, 231, 232, 234, 258
unsolvability, 234
Dirichlet unit theorem, 81, 84, 86, 93, 204
Eisenträger, Kirsten, 48, 142, 231, 235
equivalent, 247, 254, 264, 265
field
  compositum, 3
  function, 2–4, 9, 29, 48, 50, 57, 58, 60, 62, 63, 70, 71, 142, 148, 149, 154, 155,
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Field-Diophantine</td>
<td>13–15, 19</td>
</tr>
<tr>
<td>Definition</td>
<td>10–14, 16, 18, 19, 21</td>
</tr>
<tr>
<td>Fried, Michael</td>
<td>3, 233</td>
</tr>
<tr>
<td>Frobenius</td>
<td>103, 134, 215, 216, 218, 288, 289, 292, 300, 301, 304, 311, 315, 316</td>
</tr>
<tr>
<td>Green, Barry</td>
<td>233</td>
</tr>
<tr>
<td>Haran, Dan</td>
<td>233</td>
</tr>
<tr>
<td>Hasse Norm Principle</td>
<td>48, 50, 54, 60, 63, 231</td>
</tr>
<tr>
<td>Hasse-Minkowskii Theorem</td>
<td>73</td>
</tr>
<tr>
<td>Height</td>
<td>72, 73, 154, 155, 179–181, 275, 276, 324, 327</td>
</tr>
<tr>
<td>Logarithmic</td>
<td>327</td>
</tr>
<tr>
<td>Hensel’s Lemma</td>
<td>335</td>
</tr>
<tr>
<td>Hilbert, 1</td>
<td></td>
</tr>
<tr>
<td>Hilbert Class Field</td>
<td>231</td>
</tr>
<tr>
<td>Hilbert’s Tenth Problem</td>
<td>1, 2, 4, 5, 7, 40, 87, 135, 142, 210, 230, 233, 245</td>
</tr>
<tr>
<td>Horizontal problems</td>
<td>27</td>
</tr>
<tr>
<td>Jarden, Moshe</td>
<td>3, 233</td>
</tr>
<tr>
<td>Kim, H.</td>
<td>48, 230, 231, 234, 235</td>
</tr>
<tr>
<td>Least operator</td>
<td>236</td>
</tr>
<tr>
<td>Linearly disjoint fields</td>
<td>282</td>
</tr>
<tr>
<td>Lipshitz, Leonard</td>
<td>105, 110, 142</td>
</tr>
<tr>
<td>Local</td>
<td>degree, 56, 61, 67, 68</td>
</tr>
<tr>
<td>Derivation</td>
<td>167</td>
</tr>
<tr>
<td>Extension</td>
<td>50</td>
</tr>
<tr>
<td>Field</td>
<td>73, 335</td>
</tr>
<tr>
<td>Integral basis</td>
<td>184</td>
</tr>
<tr>
<td>Norm</td>
<td>50, 55, 56, 60, 61, 67, 68</td>
</tr>
<tr>
<td>Ring</td>
<td>235, 269, 295</td>
</tr>
<tr>
<td>Uniformizing parameter</td>
<td>54, 56</td>
</tr>
<tr>
<td>Local-global principle</td>
<td>233</td>
</tr>
<tr>
<td>Macintyre, Angus</td>
<td>233</td>
</tr>
<tr>
<td>Matiyasevich, Yuri</td>
<td>1, 4, 5, 27, 38, 39, 41, 139, 208, 209</td>
</tr>
<tr>
<td>Mazur, Barry</td>
<td>2–5, 139, 199, 200, 203, 206, 209, 210, 227</td>
</tr>
<tr>
<td>Moret-Bailly, Laurent</td>
<td>233, 235, 330, 337</td>
</tr>
</tbody>
</table>
partial degrees, 246
Pell Equation, 87, 88, 110
Penzin, Yuri, 48
Pheidas, Thanases, 105, 108, 141, 142, 199, 229, 231
point of infinite order on an elliptic curve, 210
Poonen, Bjorn, 2–5, 8, 113, 139, 141, 199, 203, 209, 227, 229, 318, 322, 324
Pop, Florian, 233
Prestel, Alexander, 233
Product Formula, 276, 324, 327
Prunescu, Mihai, 231
pseudo-coordinate polynomials, 57, 332, 333
Putnam, Hilary, 1, 208
r.e., 244, 264

Razon, Aharon, 233
Recursion Theory, 3, 5, 236
recursive
  presentation, 38, 41–43, 45, 46, 249, 252, 254–260, 281
  ring, 1, 7, 8, 256, 258
  sets, 4, 5, 31, 138, 209, 236, 240, 244, 245, 249, 250, 255
  recursively enumerable sets, 1, 4, 5, 39, 48, 208, 236, 244
Robinson, Julia, 1, 48, 208, 229, 233
Roquette, Peter, 233
Roush, Fred, 48, 230, 231, 234, 235
Rumely, Robert, 48, 231, 233
Schmid, J., 233
Skorobogatov, Alexei, 199
Strong Approximation Theorem, 279
Strong Vertical Method, 105, 107, 108
Swinnerton-Dyer, Peter, 199

362
Turing
  degrees, 38, 246, 254
  equivalent, 247, 252, 254, 264, 265
  machine, 237
  reducibility, 246, 247

valuation
  archimedean, 2, 72, 141, 279
  non-archimedean, 56, 268–274, 279, 297, 310, 322, 323, 335

van den Dries, Lou, 233
vertical problems, 27
Videla, Carlos, 142
Völklein, Helmut, 233

weak presentation, 8, 31–40, 259
Weak Vertical Method, 82, 105, 107, 110, 111, 115, 118, 119, 126, 129, 141, 183–185, 188

Zahidi, Karim, 141, 142, 176, 199, 207, 229, 235