# 1
# Introduction

## 1.1 In the beginning

The subject of this book dates back to the beginning of the twentieth 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 the construction of an algorithm which could determine whether an arbitrary polynomial equation in several variables had solutions in the 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 a "yes" or "no" answer to the question "Are there integer solutions?" This problem became known as Hilbert's Tenth Problem (HTP).

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, that Hilbert's Tenth Problem was unsolvable. The original proof and its immediate implications have been described in detail. The reader is referred to, for example, a book by Matiyasevich (see [52] – the original Russian edition – or [53], an English translation), an article by Davis (see [12]) or an article by Davis, Matiyasevich, and Robinson (see [14]). 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 the Diophantine definability of $\mathbb{Z}$. As we will see in this book, the 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 the 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 for 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 global function fields of positive characteristic over finite fields of constants. The main unanswered questions here have to do with Diophantine definability. In particular, we still do not know whether $\mathcal{S}$-integers have a Diophantine definition over a function field though in some senses we have come "arbitrarily close" to such a definition.

I would also like to address the main motivation in writing this book. What was wanted was a single coherent account of various methods employed so far in generalizing Hilbert's Tenth Problem to domains other than $\mathbb{Z}$ that are contained in global fields. In particular, I 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 my opinion the relative comparison of these two cases brings to light the nature of the difficulty encountered over the number fields: the 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 (computability) theory. The required background information is collected 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, *Introduction to Theory of Algebraic Functions of One Variable* by C. Chevalley, Mathematical Surveys, volume 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 the 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 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, a few words about the structure of this book 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 the algebraic and logical concepts presented in this book. Chapters 4–12 are the technical core of the book: Chapter 4 discusses the definability of order at a prime over 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). The chapters on the definition of order at a prime in number fields and function fields and on 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 the material on Diophantine models in Section 3.4.

Parts of the book could be used as a text for an undergraduate course. For an algebra course, one could cover the following chapters and sections: Chapters 1–3 and Sections 6.3 and 7.1–7.3. Such a course would thus include some general ideas on Diophantine definability and would 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 would be to cover the Diophantine classes of number fields; using Chapters 1–3, Sections 4.1 and 4.2, and Chapters 5–7. Another option would be to cover the analogous material for function fields, using Chapters 1–3, Sections 4.1 and 4.3, and Chapters 8–10. A third possibility would be to cover Mazur's conjectures and Poonen's results, using Chapters 1–3, Sections 11.2 and 11.4, and Chapter 12. Such a course would also require a background in elliptic curves. The 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 sets, which we describe and discuss in the next section.

## 1.2 Diophantine definitions and Diophantine sets

**Definition 1.2.1.** 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

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

such that for all $(t_1, \dots, t_n) \in R^n$,

$$(t_1, \dots, t_n) \in \mathcal{A} \Leftrightarrow \exists x_1, \dots, x_m,\ f(t_1, \dots, t_n, x_1, \dots, x_m) = 0.$$

The set $\mathcal{A}$ is called *Diophantine over* $R$.

We can now state the precise result obtained by Matiyasevich.

**Theorem 1.2.2.** *The Diophantine sets over $\mathbb{Z}$ coincide with the recursively (computably) enumerable sets.*

The negative answer to Hilbert's problem is an immediate corollary of this theorem since not all the recursively enumerable (r.e.) sets are recursive. (For the definitions of recursive (computable) and recursively enumerable sets and their relationship to each other, see Definitions A.1.2, A.1.3, and A.2.1, Lemma A.2.2, and Proposition A.2.3 in Appendix A.)

Indeed, suppose that 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 would exist 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 could 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 would also determine whether $t \in A$. 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 implies 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 used above naturally identifies these sets as number-theoretic objects. Matiyasevich's theorem tells us that these sets also belong in recursion theory. However, as we will see from the lemma below, one could also consider Diophantine sets as 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 one views Diophantine sets. In this book we display a pronounced bias towards the number-theoretic view 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 the unsolvability of the Diophantine problem for other rings. Before we can explain in more detail how this is done, we have to make the following observation.

**Lemma 1.2.3.** *Let $R$ be a ring whose quotient field $K$ is not algebraically closed.* (Here we remind the reader that by 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*

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

*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 that $h(x) = a_0 + a_1 x + \cdots + a_n x^n$, where $a_0, \ldots, a_n \in R$ and $a_n \neq 0$. Further, note that

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

is also a polynomial without roots in $K$. Indeed, if for some $b \neq 0$, we have that $g(b) = 0$, then $b^n h(1/b) = 0$ and consequently $h(1/b) = 0$. 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 $(b_1, \ldots, b_r) \in R^r$ we have that $H(b_1, \ldots, b_r) = 0$ and $f_1(b_1, \ldots, b_r) \neq 0$. Then

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

However, 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 defense we offer two arguments. As demonstrated by the lemma above, this distinction makes no difference for the 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 establish the following.

**Proposition 1.2.4.** *Let $R_1 \subset R_2$ be two recursive (i.e. computable) rings. Suppose that the fraction field of $R_2$ is not algebraically closed. Assume that the Diophantine problem of $R_1$ is undecidable and that $R_1$ has a Diophantine definition over $R_2$. Then the Diophantine problem of $R_2$ is also undecidable.*

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

$$\begin{cases} g(t_1, \dots, t_k) = 0; \\ f(t_1, x_1, \dots, x_r) = 0; \\ \vdots \\ f(t_k, x_1, \dots, x_r) = 0. \end{cases} \tag{1.2.1}$$

Clearly the equation $g(t_1, \dots, t_k) = 0$ will have solutions in $R_1$ if and only if the 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 $T(g)(t_1, \dots, t_k, x_1, \dots, x_r) \in R_2[t_1, \dots, t_k, x_1, \dots, x_r]$ such that the corresponding polynomial equation $T(g)(t_1, \dots, t_k, x_1, \dots, x_r) = 0$ has solutions over $R_2$ if and only if (1.2.1) has solutions in $R_2$.

Suppose now that the Diophantine problem of $R_2$ is decidable. Then for each polynomial $g$ over $R_1$ we can effectively decide whether $g(t_1, \dots, t_r) = 0$ 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. □

**Remark 1.2.5.** 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 the 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 for possible investigation of more general questions of Diophantine definability.

# 2

# Diophantine classes: definitions 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 [94].

## 2.1 Diophantine generation

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

**Definition 2.1.1.** 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 that there exists a polynomial

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

with coefficients in $R$ such that

$$\begin{aligned} &\forall\, a_1, \dots, a_k, b, x_1, \dots, x_m \in R, \\ &f(a_1, \dots, a_k, b, x_1, \dots, x_m) = 0 \quad \Rightarrow \quad b \neq 0 \end{aligned} \tag{2.1.1}$$

and

$$\begin{aligned} A = \{(t_1, \dots, t_k) \in F^k | \exists a_1, \dots, a_k, b, x_1, \dots, x_m \in R, \\ bt_1 = a_1, \dots, bt_k = a_k,\ f(a_1, \dots, a_k, b, x_1, \dots, x_m) = 0\}. \end{aligned} \tag{2.1.2}$$

Then we will say that $A$ is *field-Diophantine* over $R$ and will call $f$ a 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.

**Lemma 2.1.2.** *Suppose that $R$, $A$, $F$, $k$, $m$ are as in Definition 2.1.1. Assume further that $A \subset R^k$ and that $F$ is not algebraically closed. Then $A$ has a Diophantine definition over $R$ if and only if it has a field-Diophantine definition over $R$.*

*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

$$g = (a_1, \dots, a_k, b, x_1, \dots, x_m)$$

be a field-Diophantine definition of $A$ over $R$. Then

$$f(t_1, \dots, t_k, b, x_1, \dots, x_m) = g(t_1 b, \dots, t_k b, b, x_1, \dots, x_m)$$

is a Diophantine definition of $A$ over $R$ in the sense that, for all $t_1, \dots, t_k \in R$,

$$\exists b, x_1, \dots, x_m \in R,\ f(t_1, \dots, t_k, b, x_1, \dots, x_m) = 0 \quad \Leftrightarrow \quad (t_1, \dots, t_k) \in A.$$

Indeed, suppose that, for some $t_1, \dots, t_k, b, x_1, \dots, x_m \in R$,

$$f(t_1, \dots, t_k, b, x_1, \dots, x_m) = 0.$$

Then

$$g(t_1 b, \dots, t_k b, b, x_1, \dots, x_m) = 0$$

and consequently

$$b \neq 0,$$

while

$$(t_1 b/b, \dots, t_k b/b) = (t_1, \dots, t_k) \in A.$$

Conversely, suppose that $(t_1, \dots, t_k) \in A$. Then by our assumption on $g$,

$$\exists x_1, \dots, x_m, b \in R, \quad g(bt_1, \dots, bt_k, b, x_1, \dots, x_m) = 0.$$

Thus, there exist $x_1, \dots, x_m, b \in R$ such that

$$f(t_1, \dots, t_k, b, x_1, \dots, x_m) = 0.$$

Suppose now that $f(t_1, \dots, t_k, x_1, \dots, x_m)$ is a Diophantine definition of $A$ over $R$. Then consider the following system of equations:

$$\begin{cases} f(a_1, \dots, a_k, x_1, \dots, x_m) = 0; \\ b = 1. \end{cases} \tag{2.1.3}$$