universität wien

MASTERARBEIT / MASTER'S THESIS

Titel der Masterarbeit / Title of the Master's Thesis

On Hilbert's Tenth Problem over Rings of Algebraic Integers

verfasst von / submitted by

Tim Benedikt Herbstrith BSc

angestrebter akademischer Grad /
in partial fulfilment of the requirements for the degree of

Master of Science (MSc)

Wien, 2019 / Vienna 2019

Studienkennzahl lt. Studienblatt / degree programme code as it appears on the student record sheet:	UA 066 821
Studienrichtung lt. Studienblatt / degree programme as it appears on the student record sheet:	Masterstudium Mathematik
Betreut von / Supervisor:	ao. Univ.-Prof. Mag. Dr. Christoph Baxa

Contents

1 Prerequisites and central notions

In the year 1900 David Hilbert posed 23 mathematical problems to be solved in the twentieth century. The tenth of these problems and its variants are the subject of this thesis. In the classical setting it asks to find an algorithm that can decide upon receiving a multivariate polynomial p with integral coefficients, whether p has integral roots. One immediately obtains variants of the problem by letting the coefficients and solutions range over different commutative rings with unity.

To tackle Hilbert's tenth problem over rings of algebraic integers we need to define three central notions. Firstly, we will formalize what we mean by an algorithm; secondly, it will be defined what it means to decide a problem; and thirdly, we will define the rings we are interested in.

The first section of the preliminaries will settle our first task and give a definition of computability. The second section will provide the techniques required to encode polynomials with roots and helps us derive further variants of Hilbert's tenth problem. The third section of the preliminaries is devoted to defining algebraic integers and will remind the reader of some of their important properties.

Throughout this thesis the symbol $\mathbb{N}$ shall denote the set of non-negative integers $\{0, 1, 2, \ldots\}$.

1.1 Prerequisites from computability theory

Fuelled by the task of deciding another problem stated by Hilbert—the so-called *Entscheidungsproblem*—Austrian mathematician Gödel [15], American mathematician Church [2, 3], and British mathematician Turing [48] developed very different formalizations of the intuitive notion of *computation*.

Gödel's approach can be seen as an algebraic one. He defines '[primitive] recursive functions' as the smallest class of functions containing initial functions closed under composition and recursion. Based on a suggestion of Herbrand in a letter of April 1931, Gödel [14] later extended this class to 'general recursive functions' by closing them under minimization (cf. Lem. 1.1.7) as well. Church introduced 'λ-definable functions' to capture the notion of 'effective calculability'. His *λ-calculus* is still used as the formal basis of functional programming languages like *Haskell*. Turing took a 'purely mechanical' approach. His 'computability machines' are the very foundation of the principles today's computers are based on. Being aware of each others work Church [3], Kleene [21], and Turing [48] proved the equivalence of the three models of computability.

Maybe a bit ironically for an Austrian student writing on a topic of algebra, I will make use of Turing's definition of computability. The three main goals for this section are formalizing and defining the notions of *Turing machines* and *decidability*, as well as providing a more or less natural example of an undecidable problem. To this end, I will loosely follow the lecture notes on the subject by Müller [28] and present some results of the textbook [4].

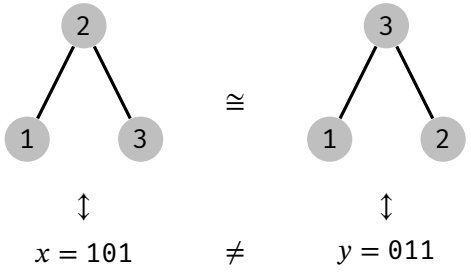


Figure 1.1: Two strings encoding two isomorphic graphs

1.1.1 Turing machines, problems, and decidability

DEFINITION. We consider the set of finite 0-1-strings $\omega = \{0,1\}^*$, where we include the empty string $\lambda \in \omega$, and define a *(decision) problem* to be a subset of ω. The set $\{0,1\}$ is called *alphabet* and its elements 0 and 1 are called *bits*.

One immediate objection against this definition is that not all problems arise as subsets of these strings. However, such problems Q are captured up to an encoding.

DEFINITION. Let $\mathcal{Q}$ be a set. An *encoding* of $\mathcal{Q}$ is an injective function

$$\ulcorner . \urcorner : \mathcal{Q} \to \omega.$$

Remark. Since the set of finite strings ω is countable, each and every subset Q of ω is either finite or countable. Thus, problems are by definition at most countable. Note however, that there are uncountably many—$2^{\aleph_0}$ to be precise—many subsets of ω and therefore uncountably many problems.

One usually does not concern oneself with the details of this encoding. However, the encoding should capture the structure of the problem—a notion that will be made precise in Section 1.2.3.

EXAMPLE 1.1.1. Consider the set $Q \subseteq \omega$ of strings of the form

$$x := \begin{array}{ccccc} b_{1,2} & b_{1,3} & \dots & b_{1,n} \\ & b_{2,3} & \dots & b_{2,n} \\ & & \ddots & \vdots \\ & & & b_{n-1,n}, \end{array}$$

of length $n(n-1)/2$. We can consider each $x \in Q$ as the encoding of an undirected graph without multiedges or loops on n vertices, where vertex i and vertex j are adjacent if and only if $b_{i,j} = 1$ (for $1 \leq i < j \leq n$). In other words, x encodes the right-upper triangle of the adjacency matrix.

Note however that two different strings $x, y \in Q$ can encode two isomorphic graphs. For example $x := 101$ and $y := 011$ encode two isomorphic graphs (cf. Fig. 1.1).

As a next step, we want to formalize the intuitive notion of 'computation'. As was remarked above we will use a variant of the machine model of Turing [48]. Specifically, our machines will consist of a *read-write head* and a *storage tape*. This storage tape consists of discrete cells stretching infinitely in one direction.The head will read at every step of the computation one symbol written on the tape and change the state of the machine, write a new symbol to the tape, and move to the left, right, or stay on the current cell. An end of tape symbol § will tell the head not to move too far to the left and all but finitely many cells will contain the blank symbol _. More formally a Turing machine can be described as follows.

DEFINITION. A *Turing machine* $\mathbb{A}$ on the *alphabet* $A = \{\S, \_, 0, 1\}$ is a tuple (S, δ), where S is a finite set, called *set of states*, that contains at least the states s_{start}, s_{halt} and a function

$$\delta : S \times A \to S \times A \times \{-1, 0, 1\},$$

called *transition function*. If $\delta(s, a) = (s', b, m)$, one demands that the following axioms are satisfied

(i) $a = \S$ if and only if $b = \S$,
(ii) if $a = \S$ then $m \neq -1$, and
(iii) if $s = s_{\text{halt}}$ then $s' = s_{\text{halt}}$, $a = b$ and $m = 0$.

The transition function should be understood as the logic behind the actions of the machine. It is applied at every step of the computation. Its arguments are the current state of the machine and the symbol currently read by the head. The image of the transition function determines the new state, the symbol written to the tape, and the movement of the head. From this intuitive view the axioms of a Turing machine state

(i) that the end of tape symbol § may never be written to nor deleted from the tape,
(ii) that the end of tape symbol marks the left-most cell of the tape, and
(iii) that once the halting state s_{halt} is reached, the machine remains in this state and does not move anymore.

Let us look at the example of the Turing machine in Fig. 1.2. During the run of the machine the head reads the symbol 0 at the current position and the machine evaluates the transition function δ at 0 and the current state s_{overflow}. Now assume that

$$\delta(s_{\text{overflow}}, 0) = (s_{\text{return}}, 1, -1).$$

One interprets this in the following way: The Turing machine changes its state to s_{return}, the head writes 1 in the current cell and moves one cell to the left. The movement is determined by the last item of the triple $\delta(s_{\text{overflow}}, 0)$, where -1 indicates moving to the left, 1 indicates moving to the right, and 0 indicates not moving at all. This notion of step-wise computation is formalized in the subsequent definitions.

DEFINITION. Let $\mathbb{A} = (S, \delta)$ be a Turing machine. A *configuration* of $\mathbb{A}$ is a triple $(s, j, c) \in S \times \mathbb{N} \times A^{\mathbb{N}}$. It reflects the current state s of $\mathbb{A}$, the current position j of its head, and the content c of its work-tape.

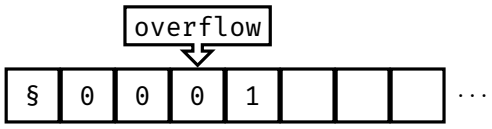


Figure 1.2: A Turing machine

A configuration of the form $(s_{\text{halt}}, 0, c)$ is called *halting*. A *start configuration* is of the form $(s_{\text{start}}, 0, c)$ such that $c(0) = \S$ and there exists an $n \in \mathbb{N}$ such that $c(i) = \_$ if and only if $i > n$. This means that in a start configuration the work-tape reads

$$\S c(1)c(2)...c(n)\_\_...$$

It will be very convenient to identify the finite string $c(1)c(2)...c(n) \in \omega$ with this tape content. Note however, that albeit every string can be associated with a tape content, the converse is not true, for instance

$$\texttt{§001\_0\_\_...}$$

is a valid tape content but we cannot interpret it as a finite string in the alphabet $\{\texttt{0}, \texttt{1}\}$. Nevertheless, if reference is clear, the symbols $b_1 b_2 ... b_n \in \omega$ shall denote both the string and the tape content

$$c(i) := \begin{cases} \S & \text{if } i = 0 \\ b_i & \text{if } 1 \leq i \leq n \\ \_ & \text{otherwise} \end{cases}$$

DEFINITION. Let (s, j, c) and (s', j', c') be configurations of a Turing machine $\mathbb{A} = (S, \delta)$. One writes $(s, j, c) \vdash_1 (s', j', c')$ and calls (s', j', c') a *successor configuration* of (s, j, c) if there exists an $m \in \{-1, 0, 1\}$ such that

- $\delta(s, c(j)) = (s', c'(j), m)$,
- $j' = j + m$, and
- $c'(\ell) = c(\ell)$ for all $\ell \neq j$.

This relation makes the set of all configurations of $\mathbb{A}$ into a directed graph, called *computation graph*. A *run* or *computation* of $\mathbb{A}$ on $x \in \omega$ is a path in this directed graph starting at the start configuration $(s_{\text{start}}, 0, x)$. A run of $\mathbb{A}$ on x is *halting* or *complete* if it reaches a halting configuration $(s_{\text{halt}}, 0, y)$ with $y \in \omega$. In this case I write $\mathbb{A}(x) = y$. If $\mathbb{A}$ does not halt on input x, the symbol $\mathbb{A}(x)$ shall be undefined.

I will describe Turing machines using listings, where the fact that $\delta_{\text{delta}}(s_{\text{state}}, b) = (s_{\text{state'}}, b', m)$ is encoded by

```
delta "state" b = ("state'", b', m)
```

Variables match all possible states or characters in the alphabet respectively. However, I follow the convention that if an assignment of variables matches more than one pattern, the first matching pattern is chosen. This means that

Listing 1.1: A Turing machine adding one to the input string

```
-- start by entering the "overflow" state ...
add1 "start"    '§'    = ("overflow", '§', 1 )
-- ... and stay in this state, as long as you read only '1'-s
add1 "overflow" '1'    = ("overflow", '0', 1 )
-- if you read the first '0' or an empty cell replace it by '1'
-- and enter the "return" state to move the head to the first cell
add1 "overflow" '0'    = ("return",   '1', -1)
add1 "overflow" '_'    = ("return",   '1', -1)
-- we finish if we read '§' again or ...
add1 "return"   '§'    = ("halt",     '§', 0 )
-- ... continue to move to the left and don't change the cell
-- content. Here `b` matches '0' or '1'
add1 "return"   b      = ("return",   b  , -1)
add1 _state     _char  = ("error",    '_', 0 )
```

```
delta "state" 1 = ("state'",   b', m )
delta "state" b = ("state''", b'', m')
```

should be interpreted as

$$\delta(s,b) = \begin{cases} (s_{\text{state'}}, b', m) & \text{if } s = s_{\text{state}} \wedge b = 1 \\ (s_{\text{state''}}, b'', m') & \text{if } s = s_{\text{state}} \wedge b \neq 1 \end{cases}.$$

This kind of pattern matching may seem unconventional at first glance but yields mutually exclusive definitions of the cases and is standardized in the specifications of the *Haskell 2010* programming language[1]. See Appendix A.1 on how to simulate Turing machines using these listings.

EXAMPLE 1.1.2. Consider the Turing machine $\mathbb{A}_{\text{add1}} = (\{s_{\text{start}}, s_{\text{halt}}, s_{\text{overflow}}, s_{\text{return}}, s_{\text{error}}\}, \delta_{\text{add1}})$ that adds 1 to a (possibly zero-patched) binary representation of a natural number n. Its transition function is described in Listing 1.1. The last line of the program ensures, that δ is a total function, as it matches all remaining pairs of states and characters and lets the machine enter the state s_{error}.

The complete run of $\mathbb{A}_{\text{add1}}$ on `1101`can be seen in Fig. 1.3. To ease readability the binary representation of natural numbers is reversed. Thus, the string `1101` does in fact encode $11 = 2^3 + 2^1 + 2^0$.

DEFINITION. Let $\mathbb{A}$ be a Turing machine.

(i) $\mathbb{A}$ *computes* the partial function that maps each $x \in \omega$ with a complete run to the output $\mathbb{A}(x)$ and is undefined for all other strings in ω.
(ii) $\mathbb{A}$ *accepts* all $x \in \omega$ such that $\mathbb{A}(x) = 1$ and *rejects* them if $\mathbb{A}(x) = 0$.
(iii) A partial function on $\{0,1\}^*$ is *computable* if there exists a Turing machine computing it. Sometimes computable functions are referred to as *recursive* or *efficient* functions.

[1] see `https://www.haskell.org/onlinereport/haskell2010`

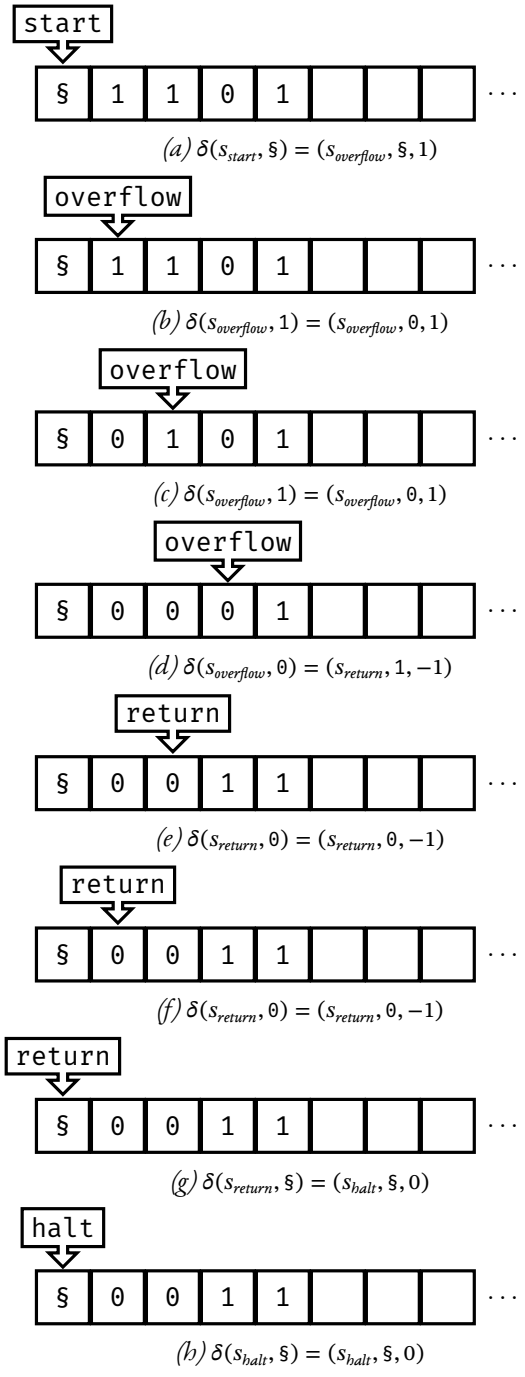


Figure 1.3: The complete run of $\mathbb{A}_{add1}$ *on* `1101`

(iv) A subset of $\omega = \{0, 1\}^*$, i.e. a problem, is *decidable* if there exists a Turing machine computing its characteristic function.
(v) A problem is called *semi-decidable* or *computably enumerable* if there exists a Turing machine accepting precisely the elements of the problem.

The last item of the definition above means that a problem is semi-decidable if there is a Turing machine affirming membership of the corresponding set but the machine might not be able to refute membership.

EXAMPLE 1.1.3. Let Q be a finite problem then Q is decidable. To see this let n be the maximal length of a string in Q and construct a Turing machine $\mathbb{A}$ with the states

$$S = \left\{s_{\text{start}}, s_{\text{halt}}, s_{\text{accept}}, s_{\text{reject}}\right\} \sqcup \left\{s_{b_1 \dots b_k} \,:\, b_1 \dots b_k \in \omega \text{ for } 0 \leq k \leq n\right\},$$

where $\sqcup$ denotes the disjoint union. As for the transition function δ, we define

$$\begin{aligned}
\delta(s_{\text{start}}, §) &:= (s_\lambda, §, 1) && (\lambda \text{ denotes the empty string as above})\\
\delta(s_{b_1 \dots b_k}, 1) &:= \begin{cases} (s_{b_1 \dots b_k 1}, 1, 1) & \text{if } k < n \\ (s_{\text{reject}}, _, -1) & \text{otherwise} \end{cases}\\
\delta(s_{b_1 \dots b_k}, 0) &:= \begin{cases} (s_{b_1 \dots b_k 0}, 0, 1) & \text{if } k < n \\ (s_{\text{reject}}, _, -1) & \text{otherwise} \end{cases}\\
\delta(s_{b_1 \dots b_k}, _) &:= \begin{cases} (s_{\text{accept}}, _, -1) & \text{if } b_1 \dots b_k \in Q \\ (s_{\text{reject}}, _, -1) & \text{if } b_1 \dots b_k \notin Q \end{cases},
\end{aligned}$$

where the schemes in the last three lines should be understood as one instruction per string $b_1 \dots b_k \in \omega$ for $1 \leq k \leq n$. This way we obtain

$$1 + 3 \sum_{i=0}^{n} 2^i = 1 + 3\left(2^{n+1} - 1\right)$$

equations for δ. The idea of this machine is that it enters the state that corresponds to the string on the tape that the machine has read so far. Now one of three things can happen:

- either the input string continues and we have read less than n symbols so far, then the machine continues reading (first case of lines 2 and 3); or
- the machine reads a blank symbol _, then we must check if the string is in Q and accept or reject accordingly (line 4); or
- we have already read n symbols, then we can reject for sure as Q contains no string with more than n symbols (second case of lines 2 and 3).

It is now easy to extend δ into a total function $S \times A \to S \times A \times \{-1, 0, 1\}$ such that once $\mathbb{A}$ reaches s_{accept}, the machine clears the tape except for a single 1, and if $\mathbb{A}$ reaches s_{reject}, it clears the tape except for a single 0, and halts.

Note that the construction above fails if Q is infinite because in this case the set of states S is infinite. However, if Q is co-finite we can exchange s_{accept} and s_{reject} in the construction above to obtain a Turing machine deciding Q. In Prop. 1.1.9 we will see that the complements of decidable sets are decidable in general.

Before we can prove that further sets are decidable we need a bit more theory of computable functions.

LEMMA 1.1.4. *Let $\mathbb{A}_1 = (S_1, \delta_1)$ and $\mathbb{A}_2 = (S_2, \delta_2)$ be Turing machines computing the functions $f_1 : D_1 \to \omega$ and $f_2 : D_2 \to \omega$ respectively, where D_1, D_2 are subsets of ω. Then there exists a Turing machine $\mathbb{A}_{f_2 \circ f_1}$ computing the partial function $f_2 \circ f_1 : D_1 \cap f_1^{-1}(D_2) \to \omega$ obtained by composing f_1 and f_2.*

Proof. If $s_{\text{start}} = s_{\text{halt}}$ then machine $\mathbb{A}_1$ and machine $\mathbb{A}_2$ compute the identity function on ω and the claim is trivial. Similarly, if $\delta_1(s_{\text{start}}, \S) = (s_{\text{halt}}, \S, 0)$, then $\mathbb{A}_1$ computes the identity and the claim is proven by setting $\mathbb{A}_{f_2 \circ f_1} = \mathbb{A}_2$.

We can therefore assume that we are not in these trivial cases and construct $\mathbb{A}_{f_2 \circ f_1}$ from $\mathbb{A}_1$ and $\mathbb{A}_2$ as follows: Let $S_1' := S_1 \setminus \{s_{\text{start}}, s_{\text{halt}}\}$ and $S_2' := S_2 \setminus \{s_{\text{start}}, s_{\text{halt}}\}$, then set $S = \{s_{\text{start}}, s_{\text{halt}}\} \sqcup S_1' \sqcup S_2' \sqcup \{s_{\text{compose}}\}$, where $\sqcup$ denotes the disjoint union. Now for a state $s \in S$ and a symbol $b \in A$ we define

$$\delta(s, b) := \begin{cases} \delta_1(s, b) & \text{if } s \in S_1' \cup \{s_{\text{start}}\} \\ (s_{\text{compose}}, b, m) & \text{if } s \in S_1 \text{ and } \delta_1(s, b) = (s_{\text{halt}}, b', m) \\ \delta_2(s, b) & \text{if } s \in S_2' \cup \{s_{\text{halt}}\} \\ \delta_2(s_{\text{start}}, b) & \text{if } s = s_{\text{compose}} \end{cases}$$

Then $\mathbb{A}_{f_2 \circ f_1} = (S, \delta)$ computes $f_2 \circ f_1$ because δ is defined to first run the program of $\mathbb{A}_1$ and if this machine reaches a halting state run $\mathbb{A}_2$. □

EXAMPLE 1.1.5. One can encode a natural number n

(1) in tally notation

$$n \mapsto \underbrace{1 \ldots 1}_{n\text{-times}}, \quad \text{if } n > 0,$$
$$0 \mapsto \lambda;$$

(2) by its (reversed) binary representation

$$n = 2^k + \sum_{i=0}^{k-1} b_i 2^i \mapsto b_0 \ldots b_{k-1} 1, \quad \text{if } n > 0$$
$$0 \mapsto \mathtt{0}; \text{ or}$$

Listing 1.2: A Turing machine checking whether the input is tally-encoded

```
-- start by entering the "check" state and ...
tally "start"    '§'    = ("check",    '§', 1 )
-- ... stay in this state while reading only '1'-s
tally "check"    '1'    = ("check",    '1', 1 )
-- on reading '_' accept the input and clear the tape ...
tally "check"    '_'    = ("accept",   '_', -1)
tally "accept"   '1'    = ("accept",   '_', -1)
-- ...except for cell c(1), where you write a '1'
tally "accept"   '§'    = ("accept",   '§', 1 )
tally "accept"   '_'    = ("halt",     '1', -1)
-- however, if you read a '0' first, reject the input
-- by moving to the end of the input string ...
tally "check"    '0'    = ("rejectMR", '0', 1 )
tally "rejectMR" '_'    = ("reject",   '_', -1)
tally "rejectMR" b      = ("rejectMR",   b, 1 ) -- `b` matches '0' or '1'
-- ... and clear the tape except for cell c(1) where you
-- write a '0'
tally "reject"   '§'    = ("reject",   '§', 1 )
tally "reject"   '_'    = ("halt",     '0', -1)
tally "reject"   b      = ("reject",   '_', -1) -- `b` matches '0' or '1'
tally _state     _char  = ("error",    '_', 0 )
```

(3) by a shifted and truncated form of its binary representation

$$n = 1 + \sum_{i=0}^{k} b_i 2^i \mapsto b_0 ... b_k, \quad \text{if } n > 0,$$
$$0 \mapsto \lambda.$$

In other words, n is mapped to the n-th string if one orders $\{0,1\}^*$ lexicographically. I will write $<_{lex}$ for the lexicographical ordering of $\omega = \{0,1\}^*$. As ω traditionally denotes the non-negative integers in the fields of logic and especially set theory, this last encoding is the reason why I am using the symbol ω to denote the set of finite strings $\{0,1\}^*$.

In either case the set obtained by encoding $\mathbb{N}$ is easily seen to be decidable. In the case of the tally notation (1), check that the string contains only copies of the bit 1. Indeed, this can be achieved by the Turing machine

$$\mathbb{A}_{\text{tally}} = (\{s_{\text{start}}, s_{\text{halt}}, s_{\text{check}}, s_{\text{accept}}, s_{\text{reject}}, s_{\text{rejectMR}}, s_{\text{error}}\}, \delta),$$

whose transition function is displayed in Listing 1.2. As for the binary representation (2), it suffices to check that the string has length 1 or ends in a 1, and in the third encoding (3) every string is accepted.

Remark. Let Q_0 be a decidable problem and $Q \subseteq Q_0$ a subset. If there exists a Turing machine $\mathbb{A}$ that upon receiving $x \in Q_0$ as input decides whether $x \in Q$, then Q is decidable. To obtain a Turing machine deciding Q we first run the Turing machine deciding Q_0 and reject x if $Q_0(x) = \mathtt{0}$ otherwise we run $\mathbb{A}$ on x.

To see the usefulness of this technique consider the set of even non-negative integers Q encoded in binary encoding. Taking $Q_0 \supseteq Q$ to be the set of all non-negative integers $\mathbb{N}$ encoded in binary encoding, Q is easily seen to be decidable by checking whether the first bit of a given string $x \in Q_0$ is $\mathtt{0}$.

Taking another look at the definition of computability, one sees that only functions in one argument defined on subsets of ω mapping to subsets of ω can be computable. However, one can easily extend this to functions on multiple arguments. To do this, one uses an injective function $\langle \cdot, \cdot \rangle : D^2 \to \omega$, where $D \subseteq \omega$ is decidable and encodes tuples by elements of ω in such a way, that the image

$$\{\langle x_1, x_2 \rangle : x_1, x_2 \in D\}$$

is decidable and the projections $p_i(\langle x_1, x_2 \rangle) \mapsto x_i$ for $i \in \{0, 1\}$ are computable. This means, there are Turing machines $\mathbb{P}_1, \mathbb{P}_2$ computing p_1 or p_2 respectively.

EXAMPLE 1.1.6 (PAIRING FUNCTIONS). (1) Using tally notation (cf. Example 1.1.5.(1)) one can encode $(n, m) \in \mathbb{N}^2$ by

$$\langle \ulcorner n \urcorner, \ulcorner m \urcorner \rangle = \underbrace{\mathtt{1}\ldots\mathtt{1}}_{n\text{-times}}\ \mathtt{0}\ \underbrace{\mathtt{1}\ldots\mathtt{1}}_{m\text{-times}}\ .$$

To test, whether a given string $x \in \omega$ encodes a pair of non-negative integer, one only needs to check whether x contains a single $\mathtt{0}$ and all other symbols are $\mathtt{1}$-s. As for the projections, machine $\mathbb{P}_1$ clears everything after the first $\mathtt{0}$ on the tape and $\mathbb{P}_2$ deletes everything up to the first zero and then moves the second block of $\mathtt{1}$-s cell by cell from left to right.

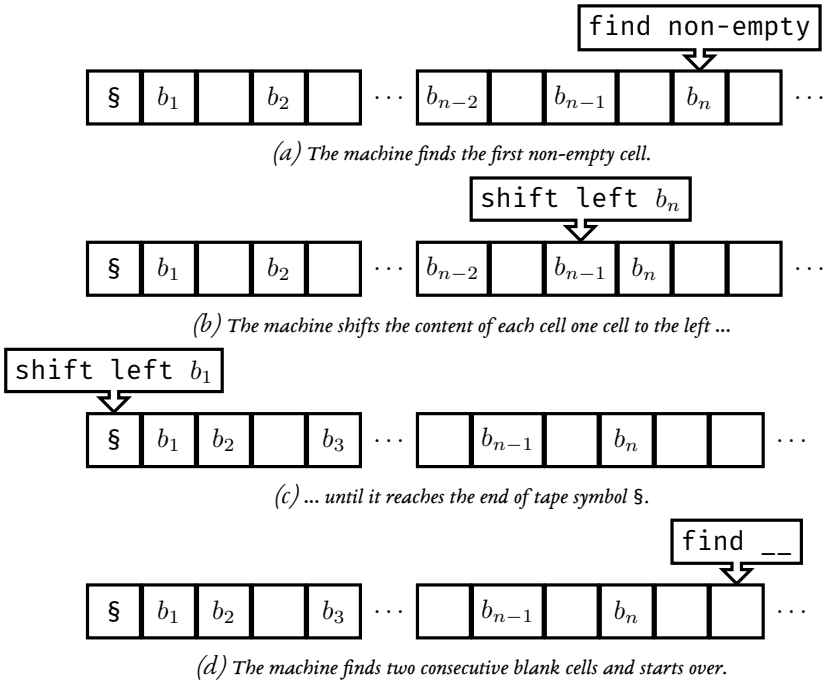
(2) A simple pairing function encodes the pair $(b_1 b_2 \ldots b_n, c_1 c_2 \ldots c_m) \in \omega^2$ by

$$\langle b_1 b_2 \ldots b_n, c_1 c_2 \ldots c_m \rangle = b_1 b_1 b_2 b_2 \ldots b_n b_n\ \mathtt{01}\ c_1 c_2 \ldots c_m.$$

Again it is easy to check whether a given string encodes a tuple. The second projection in this encoding is obtained completely analogously as in the previous example. As for the first projection, the machine $\mathbb{P}_1$ first moves to the right, deleting every second symbol until it reaches the substring $\mathtt{01}$ indicating the end of the first component. At this point, the machine deletes all symbols to its right until it reaches the first blank symbol and returns to the left until it reads b_n in cell $2n - 1$. The tape will now look like the one in Fig. 1.4a.

Next it starts shifting the content of all cells one cell to the left until it reaches the end of tape symbol $\S$ (cf. Fig. 1.4b and c). The machine can find the end of the string by moving to the right until it finds two consecutive blank cells (cf. Fig. 1.4d). At this point the whole process starts over, except when shifting left, the machine must check, if the cell it wants to write to is empty. If it is not empty, it starts moving right again to find two consecutive blank cells. The process stops if it reads two consecutive blank cells before reading a single blank cell.

By applying a pairing function iteratively one obtains an n-ary pairing function. The projections



(a) The machine finds the first non-empty cell.

(b) The machine shifts the content of each cell one cell to the left ...

(c) ... until it reaches the end of tape symbol §.

(d) The machine finds two consecutive blank cells and starts over.

Figure 1.4: A schematic run of the first projection associated to the pairing function in Example 1.1.6.(2)

need to be composed accordingly. For example

$$(x_1, x_2, x_3) \mapsto \langle x_1, \langle x_2, x_3 \rangle \rangle$$

yields a ternary pairing function and $\pi_1 \circ \pi_2$ is the projection onto x_2. Using any of the pairing functions above, one can consider n-ary computable functions by providing the encoded pair $\langle x_1, x_2, ..., x_n \rangle$ as the single argument of a Turing machine $\mathbb{A}$. If the context is clear, I will write $\mathbb{A}(x_1, \dots, x_n)$ in this situation. Furthermore, these pairing functions allow us to define decidable relations on ω^n.

DEFINITION. Let $R \subseteq \omega^n$ be an n-ary relation on ω. Then R is called (*semi-*)*decidable* if the set

$$\{\langle x_1, \dots, x_n \rangle : x_1, \dots, x_n \in \omega, R(x_1, \dots, x_n)\}$$

is a (semi-)decidable subset of ω.

When trying to find solution of equations or witnesses for relations the concept of *efficient search* is very important. In the theory of computability it is modelled by a minimization operator.

DEFINITION. Let $R \subset \omega^2$ be a semi-decidable relation. We say $f : D_R \to \omega$ is obtained from R via *minimization* and write

$$f(x) = \mu y : R(x, y)$$

if

$$D_R = \{x \in \omega : \exists y \in \omega \text{ with } R(x, y)\},$$

there exists a Turing machine $\mathbb{A}$ semi-deciding R, such that for all $x \in D_R$ the machine $\mathbb{A}$ can refute $R(x, y)$, i.e. $\mathbb{A}(x, y) = 0$, for all $y <_{lex} f(x)$, and $R(x, f(x))$ holds.

LEMMA 1.1.7. *If $f : D_R \to \omega$ is obtained from a semi-decidable relation $R \subset \omega^2$ via minimization, then f is computable.*

Proof. Let $x \in D_R$. We will start by trying whether the empty string λ satisfies $R(x, \lambda)$. If this is the case, then $f(x) = \lambda$ and we are done. Otherwise, the Turing machine semi-deciding R can refute $R(x, \lambda)$ and we move on to try the next string in lexicographical order. By definition of D, there exists a string $y \in \omega$ such that $R(x, y)$ holds and this string will appear in our listing of ω after finitely many steps. Thus, f is computable.

More formally, such a Turing machine computing f can be obtained as follows. First apply a Turing machine that transforms a string $b_1 b_2 ... b_n \in \omega$ into the tape content

$$\S\ b_1 \_\_\ b_2 \_\_ ... b_n$$

Starting to count at index 0, the cells whose index is congruent 2 modulo 3 encode the empty string λ. We apply a Turing machine that computes the pairing $\langle b_1 b_2 ... b_n, \lambda \rangle$ as in Example 1.1.6.(2) from the cells whose index is congruent 1 or 2 modulo 3 and writes only to the cells whose index is congruent 0 modulo 3. Then the tape will read something like

$$\S\ b_1 \_ b_1\ b_2 \_ b_1\ b_3 \_ b_2 ....$$

Now transform the Turing machine $\mathbb{A}_R$ used in the definition of minimization into one that only uses cells congruent 0 modulo 3 and apply it to the tape content. If $\mathbb{A}_R$ accepts we have found $f(x)$.

Otherwise, we use a slight modification of the Turing machine of Example 1.1.2, to obtain a Turing machine that upon receiving x as input, outputs the next string in lexicographical order and uses only cells whose index is congruent 2 modulo 3. At this point, we start the next iteration. □

We are now able to state equivalent definitions of decidable and semi-decidable sets.

PROPOSITION 1.1.8. *Let Q be a problem. The following properties are equivalent.*

(i) Q is semi-decidable.
(ii) Q is the domain of a (partial) computable function.
(iii) Q is the image of a (partial) computable function.
(iv) There exists a decidable relation $R \subseteq \omega^2$ such that

$$x \in Q \quad \Leftrightarrow \quad \exists y \in \omega : R(x, y).$$

Proof. (i)⇒ (ii): Let $\mathbb{A}$ be a Turing machine witnessing that Q is semi-decidable. Then $\mathbb{A}$ halts on all $x \in Q$ and returns 1. If on the other hand $x \notin Q$ then $\mathbb{A}$ outputs an arbitrary string $y \neq 1$, or does not halt on x.

Consider the Turing machine $\mathbb{A}_{check1}$ defined in Listing 1.3. It outputs 1 on input 1 and does not halt on any other input. The machine obtained by composing $\mathbb{A}$ and $\mathbb{A}_{check1}$ does halt on x if and only if $x \in Q$.

(ii)⇒ (iii): Let $\mathbb{A}$ be a Turing machine, that halts on $x \in \omega$ if and only if $x \in Q$. We construct a Turing machine $\mathbb{B}$ that outputs x whenever $\mathbb{A}$ halts on x. Then Q is the range of the computable function computed by $\mathbb{B}$. Machine $\mathbb{B}$ will perform the following three operations.

Firstly, it transforms the string $x = b_1...b_n \in \omega$ into the tape content

$$\S b_1 b_1 ... b_n b_n \_ ....$$

In a second step, the machine checks by a modification of Turing machine $\mathbb{A}$ that only uses cells with an even index, whether cells with even index correspond to an element in Q. If x was indeed contained in Q, then the machine will stop after finitely many steps and can transform the tape content back to

$$\S b_1 ... b_n \_.$$

This can be achieved by a slight modification of the machine computing the first projection in Example 1.1.6.(2).

If on the other hand x is not contained in Q, then in the second step of the computation the machine will not stop. Thus x is not in the image of the function computed by $\mathbb{B}$.

(iii)⇒ (iv): Let f be a computable function with image Q and let $\mathbb{A}$ be a Turing machine computing f. For each non-negative integer $n \in \mathbb{N}$ and all strings $x := b_1...b_i, y := c_1...c_j$ in ω, I consider the relation $R \subseteq \omega^3$ defined by

$$R(n, x, y) \quad :\Leftrightarrow \quad \mathbb{A} \text{ halts on } x \text{ in at most } n \text{ steps; } i, j \leq n; \text{ and } f(x) = y.$$

Note that for a fixed integer n the relation can contain at most 2^{2n} triples. Thus, R is decidable for fixed n. However, using induction on n one sees easily that R is decidable as a ternary relation. (If $R(n, x, y)$ holds, so does $R(m, x, y)$ for all $m \geq n$. If $R(n, x, y)$ does not hold, then either x or y contains more than n bits; or $\mathbb{A}$ did not halt on x in n steps; or $\mathbb{A}(x)$ is not y. In the last two cases, we perform one more step of the computation and can check whether $\mathbb{A}$ outputs y.) Finally, we obtain

$$y \in Q \quad \Leftrightarrow \quad \exists z \in \omega : R(\pi_1(z), \pi_2(z), y),$$

as claimed.

(iv)⇒ (i): By Lem. 1.1.7 the function $f(x) = \mu y : R(x, y)$ is computable. Compose f with a function that returns 1 on all inputs to obtain a computable function that outputs 1 for all $x \in Q$ and is undefined otherwise. □

Remark. The third equivalent property (iii) in the proposition above is the reason why semi-decidable sets are also called *listable* or *computably enummerable* sets.

The following proposition—which is sometimes referred to as *Post's theorem*—is intuitively clear. It states that if we have an algorithm that can affirm membership of a problem Q and if there is an algorithm that can refute membership, then we can decide Q. However, a formal proof is technically quite intricate.

PROPOSITION 1.1.9. *Let Q be a problem. Then Q is decidable if and only if Q and $\omega \setminus Q$ are semi-decidable.*

Listing 1.3: A Turing machine that halts and accepts only on input `1`

```
-- start by entering the "check" state
check1 "start"       '§'    = ("check",       '§', 1 )
-- if you read a 1, check that the next cell is blank, and accept
check1 "check"       '1'    = ("check_blank", '1', 1 )
check1 "check_blank" '_'    = ("accept",      '_', -1)
-- if either of these conditions is not the case, reject
check1 "check"       b      = ("reject",       b,  1 )
check1 "check_blank" b      = ("reject",       b,  1 )
-- accepting and rejecting actions
check1 "accept"      1      = ("halt",         1,  -1)
check1 "reject"      b      = ("error",        b,  1 )
check1 _state        _char  = ("error",      '_',  0 )
```

Proof. Assume Q to be decidable by the Turing machine $\mathbb{A}$, then Q is in particular semi-decidable. Now compose $\mathbb{A}$ with a Turing machine $\mathbb{B}$ with the property $\mathbb{B}(\mathtt{1}) = \mathtt{0}$ and $\mathbb{B}(\mathtt{0}) = \mathtt{1}$. One obtains a Turing machine deciding the complement of Q and $\omega \setminus Q$ is thus semi-decidable, as claimed.

If on the other hand, Q and $\omega \setminus Q$ are semi-decidable, then there are Turing machines $\mathbb{A}$ and $\mathbb{A}^c$ semi-deciding Q and $\omega \setminus Q$ respectively. By Prop. 1.1.8 we may assume that these machines only halt on strings contained in Q or $\omega \setminus Q$ respectively, and that their only output is $\mathtt{1}$.

We want to run these Turing machines in parallel. As each string $x \in \omega$ is either contained in Q or not, one of these machines will halt and output $\mathtt{1}$, indicating whether x belongs to Q or not.

To this end, construct a Turing machine $\mathbb{A}_{copy4}$ that transforms an input string $x_1x_2...x_n \in \omega$ to

$$\mathtt{10100}x_1\mathtt{0}x_1\mathtt{0}x_2\mathtt{0}x_2...\mathtt{0}x_n\mathtt{0}x_n.$$

Starting to count at 1, cells with an index $i \equiv 1 \mod 4$ indicate if the head of machine $\mathbb{A}$ is currently reading the cell with index $i + 1$, in this case a $\mathtt{1}$ is placed inside this cell, $\mathtt{0}$ otherwise; cells with an index $i \equiv 2 \mod 4$ represent the tape of machine $\mathbb{A}$; and cells with indices congruent 3 or 0 modulo 4 represent the corresponding information for machine $\mathbb{A}^c$. The first block of 4 bits represents the ends of the tapes of machine $\mathbb{A}$ and $\mathbb{A}^c$ respectively.

Now construct a Turing machine $\mathbb{D}$ whose states $S = S_1 \times S_2 \times S_{aux}$ are triples of states of machine $\mathbb{A}$, states of machine $\mathbb{A}^c$, and some auxiliary states S_{aux}.

Say machine $\mathbb{D}$ is in state (s_1, s_2, s_a). At odd stages of the computation of $\mathbb{D}$ the head rests at the end of tape symbol § and starts moving to the right until it finds the first $\mathtt{1}$ in a cell with an index $i \equiv 1 \mod 4$. All computation steps necessary for this will only effect s_a and preserve s_1 and s_2. Next the machine will mark cell i with $\mathtt{0}$ and will then carry out one step of the computation of $\mathbb{A}$, reading the cell with index $i + 1$ and writing in one of the cells with indices $i - 3, i + 1$, or $i + 5$. Thereby the state s_1 will be changed to the state dictated by the transition function of machine $\mathbb{A}$. Finally, the head moves one cell to the left, marks by writing a $\mathtt{1}$ the last position of its head, and moves back to the end of the tape.

At even stages the head moves to the right until it finds the first $\mathtt{1}$ in a cell with an index $i \equiv 3 \mod 4$ and carry out the analogous steps for machine $\mathbb{A}^c$ as in the even case.

At some point either the computation of $\mathbb{A}$ or the computation of $\mathbb{A}^c$ will halt. Then $\mathbb{D}$ has reached a state where either the first or the second component of $(s_1, s_2, s_a) \in S$ is a halting state. Then $\mathbb{D}$ can clear the tape and write $\mathtt{1}$ or $\mathtt{0}$ to the cell with index $\mathtt{1}$ to indicate whether s_1 equals s_{halt} or s_2 does. □

1.1.2 Church-Turing thesis and the halting problem

In the remainder of this thesis I will make use of the following meta-mathematical thesis, which cannot be mathematically proven but has been heuristically justified for all of the generally accepted[2] formalizations of computation. It allows one to state properties of computability without referring to a specific model.

> CHURCH-TURING THESIS. The class of intuitively computable functions coincides with the class of all Turing computable functions.

In his foundational paper [48] Turing proved a crucial result for the whole field of computability theory and its practical applications. He noted

> It is possible to invent a single machine which can be used to compute any computable sequence.

This may seem not surprising to the reader of the twenty-first century, who is used to being surrounded by machines that can carry out nearly all tasks imaginable, but the insight, that it is possible to build a single machine that can carry out all computations, can hardly be overestimated.

THEOREM 1.1.10. *There exists a Turing machine $\mathbb{U}$ that computes upon receiving the tuple $\langle \ulcorner \mathbb{A} \urcorner, x \rangle$ as input the output of Turing machine $\mathbb{A}$ on x, i.e.*

$$\mathbb{U}(\ulcorner \mathbb{A} \urcorner, x) = y \quad \Leftrightarrow \quad \mathbb{A}(x) = y$$

As a final task of this section we want to find a set $\mathcal{K} \subseteq \omega$ that is semi-decidable but not decidable. This set will be the key ingredient in the task of settling Hilbert's tenth problem. Note that it is not hard to see that an undecidable problem exists, as there are only countably many Turing machines[3] but uncountably many problems. However, to find such a set within the semi-decidable ones we turn our attention to a problem that quite naturally arises in computability theory.

> HALTING PROBLEM. Given a machine $\mathbb{A}$ and a string x. Does $\mathbb{A}$ halt on x?

The contradiction to the existence of a Turing machine deciding this problem is obtained by a diagonalization technique that is also present in Cantor's proof that the power set of the integers is uncountable or Russel's paradox. However, the idea is best encapsulated by the self-referential nature of the Pinocchio paradox, whose illustration by Carlo Chiostri is displayed in Fig. 1.5.

THEOREM 1.1.11. *The halting problem is undecidable.*

Proof. Assume there exists a Turing machine $\mathbb{B}$ that decides the halting problem, i.e. for all Turing machines $\mathbb{A}$ and all strings x

$$\mathbb{B}(\ulcorner \mathbb{A} \urcorner, x) = \begin{cases} \mathtt{1} & \text{if } \mathbb{A} \text{ halts on } x \\ \mathtt{0} & \text{if } \mathbb{A} \text{ does not halt on } x \end{cases}$$

[2] The interested reader should find the comment [6] on hyper-computation by Davis quite revealing.

[3] To be precise, there are countably many non-isomorphic computation graphs.

Figure 1.5: Pinocchio says a lie and stretches his nose. What happens if he says 'My nose grows now'? Does it grow, or does it shrink?[4]

holds. Now using $\mathbb{B}$ construct a Turing machine $\mathbb{B}'$ that simulates $\mathbb{B}(\ulcorner\mathbb{A}\urcorner, \ulcorner\mathbb{A}\urcorner)$ on its input $\ulcorner\mathbb{A}\urcorner$ and enters an infinite loop if $\mathbb{B}(\ulcorner\mathbb{A}\urcorner, \ulcorner\mathbb{A}\urcorner) = 1$. Expressed more formally this means

$$\mathbb{B}' \text{ halts on } \ulcorner\mathbb{A}\urcorner \quad \Leftrightarrow \quad \mathbb{A} \text{ does not halt on } \ulcorner\mathbb{A}\urcorner.$$

Setting $\mathbb{A} = \mathbb{B}'$ yields the desired contradiction. □

For a more detailed proof of this theorem and a lot more information on computability see [4]. As the halting problem is undecidable the *halting set* defined by

$$\mathcal{K} = \{\langle \ulcorner\mathbb{A}\urcorner, x\rangle \,:\, \mathbb{A} \text{ halts on } x\}$$

is undecidable. However, using the universal Turing machine it is seen to be semi-decidable.

COROLLARY 1.1.12. *The halting set is semi-decidable but not decidable.*

Remark. Note that the halting set contains the information of *all* semi-decidable sets in the following sense: Given a semi-decidable set Q, there is a total computable function $f : \omega \to \omega$ such that

$$x \in Q \quad \Leftrightarrow \quad f(x) \in \mathcal{K}. \tag{1.1.1}$$

Indeed, since Q is semi-decidable, by Prop. 1.1.8 there exists a Turing machine $\mathbb{A}$ that halts on x if and only if $x \in Q$. This means that

$$x \in Q \quad \Leftrightarrow \quad \langle \ulcorner\mathbb{A}\urcorner, x\rangle \in \mathcal{K}.$$

Setting $f(x) := \langle \ulcorner\mathbb{A}\urcorner, x\rangle$ yields the claim.

We say a problem Q is *many-one reducible* to a second problem Q' if there exists a total computable function $f : \omega \to \omega$ as in (1.1.1), i.e.

$$x \in Q \quad \Leftrightarrow \quad f(x) \in Q'.$$

[4] Own SVG-tracing, derived of an illustration by Carlo Chiostri published in Collodi, Carlo. *Le avventure di Pinocchio : Storia di un burattino.* Firenze Bemporad & Figlio, 1901.

One writes $Q \leq_m Q'$ in this situation. In the previous remark we have seen that all semi-decidable sets are many-one reducible to $\mathcal{K}$. The key step in settling Hilbert's tenth problem is proving that $\mathcal{K}$ is many-one reducible to a collection of sets which are definable by polynomial equations. This suffices to prove the undecidability of Hilbert's tenth problem, since we have the following properties of many-one reducibility.

PROPOSITION 1.1.13. *(i) Let $Q, Q' \subseteq \omega$ be problems such that $Q \leq_m Q'$. Then if Q' is (semi-)decidable, so is Q.*

(ii) If problem Q is many-one reducible to problem Q', and Q' is many-one reducible to Q'', then Q is many-one reducible to Q''. In other words the relation of many-one reducibility is transitive.

Proof. (i) Let $f : \omega \to \omega$ be the computable function witnessing many-one reducibility of Q to Q' and assume that Q' is the domain of the computable function g. Then Q is the domain of the computable function $g \circ f$. Indeed, assume that $x \in Q$, then $f(x) \in Q'$ and thus $g(f(x))$ is defined. Otherwise, $f(x) \notin Q'$ and thus $g(f(x))$ is undefined.

To see the claim for the case of Q' being decidable, note that f witnesses many-one reducibility of $\omega \setminus Q$ to $\omega \setminus Q'$ as well. By Prop. 1.1.9 both Q' and $\omega \setminus Q'$ are semi-decidable and thus Q and $\omega \setminus Q$ are semi-decidable by the case that was just proven. Now Prop. 1.1.9 implies that Q is decidable.

(ii) By assumption there exist computable functions $f : \omega \to \omega$ and $g : \omega \to \omega$ such that x is in Q precisely if its image $f(x)$ is contained in Q' and x is in Q' precisely if $g(x)$ is in Q''. Consider the composition $g \circ f$. It is a total computable function by Lem. 1.1.4, and has the property that x is in Q if and only if $(g \circ f)(x)$ is contained in Q''. Thus, Q is many-one reducible to Q'' as claimed. □

1.2 Prerequisites from model theory

The idea of model theory is to differentiate between the statements we can make about mathematical objects and the implementation of these mathematical objects. We will define *languages* and their syntax and will describe what it means for a mathematical object to *model a theory*. In this section I will closely follow Chapter 1 of the textbook [25].

1.2.1 Formulae and models

Informally, a first-order formula is just a string of symbols that signify distinguished constants, functions, and relations. We demand that a formula is well-behaved according to the interpretability of constants, functions, and relations. We do however not make any assumptions on the implementation of these symbols. So a formula captures the *syntax* of a collection of mathematical objects. A model, on the other hand, describes the *semantics* of an object. It gives concrete interpretations of the symbols of a language and tells us, how the formulae are to be understood.

DEFINITION. A *language* $\mathcal{L}$ is a quadruple $(\mathcal{F}, \mathcal{R}, \mathcal{C}, ar : \mathcal{F} \cup \mathcal{R} \to \mathbb{N} \setminus \{0\})$, where $\mathcal{F}$ is a set of function symbols, $\mathcal{R}$ is a set of relation symbols, and $\mathcal{C}$ is a set of constant symbols, such that all of these sets are pair-wise disjoint. The function $ar : \mathcal{F} \cup \mathcal{R} \to \mathbb{N}$ assigns to every function symbol $f \in \mathcal{F}$ and every relation symbol $R \in \mathcal{R}$ the *arity* n_f or n_R respectively.

By the the arity n_f of a function symbol f we describe that f should eventually be interpreted as a function on n_f variables. Analogously, the arity n_R of a relation symbol R describes that R will denote an n_R-ary relation.

It is customary to denote the language $\mathcal{L} = (\mathcal{F}, \mathcal{R}, \mathcal{C}, ar : \mathcal{F} \cup \mathcal{R} \to \mathbb{N} \setminus \{0\})$ by

$$\mathcal{L} = \{f \in \mathcal{F}; R \in \mathcal{R}; c \in \mathcal{C}\}$$

and thereby drop the arity function from the notation.

EXAMPLE 1.2.1. Examples of languages include

(1) the language of pure sets $\mathcal{L} = \varnothing$;
(2) the language of (reflexive) orderings $\mathcal{L}_{\leq} = \{\leq\}$, where $\leq$ is a binary relation symbol;
(3) the language of groups $\mathcal{L}_{group} = \{\cdot, ^{-1}; \mathtt{e}\}$, where $\cdot$ is a binary function symbol, $^{-1}$ is an unary function symbol, and $\mathtt{e}$ is a constant; and
(4) the language of rings with unity $\mathcal{L}_{ring} = \{+, -, \cdot; \mathtt{0}, \mathtt{1}\}$, where $+, -$, and $\cdot$ are binary function symbols and $\mathtt{0}, \mathtt{1}$ are constants.

These languages allow for various interpretations—not all of them might be the intended ones—and each of these interpretations is called a model. More formally, we have the following definition.

DEFINITION. Let $\mathcal{L} = \{f \in \mathcal{F}; R \in \mathcal{R}; c \in \mathcal{C}\}$ be a language. A *model* $\mathfrak{A}$ of $\mathcal{L}$ is a non-empty set A, called the *universe* or *carrier set* of $\mathfrak{A}$, together with

(i) a function $f^{\mathfrak{A}} : A^{n_f} \to A$ for every function symbol $f \in \mathcal{F}$,
(ii) a relation $R^{\mathfrak{A}} \subseteq A^{n_R}$ for every relation symbol $R \in \mathcal{R}$, and
(iii) a constant $c^{\mathfrak{A}} \in A$ for every constant symbol $c \in \mathcal{C}$.

We will use the notation

$$\mathfrak{A} = \langle A; f^{\mathfrak{A}} \in \mathcal{F}; R^{\mathfrak{A}} \in \mathcal{R}; c^{\mathfrak{A}} \in \mathcal{C}\rangle$$

to denote this model.

A model in a language without relation symbols is called *algebraic structure*.

EXAMPLE 1.2.2. We list some examples of models for the languages defined above.

(1) In the language of pure sets $\mathcal{L} = \varnothing$, every non-empty set S gives rise to a model $\mathfrak{S} = \langle S\rangle$.
(2) An example of a model in the language of (reflexive) orderings $\mathcal{L}_{\leq} = \{\leq\}$ is $\mathfrak{N}_{\leq} := \langle \mathbb{N}, \leq\rangle$, where $\leq$ denotes the usual ordering of the non-negative integers.
(3) As for $\mathcal{L}_{group} = \{\cdot, ^{-1}; \mathtt{e}\}$, any group G induces a model. Indeed, consider the algebraic structure $\mathfrak{G} := \langle G; \cdot^{\mathfrak{G}}, {}^{-1^{\mathfrak{G}}}; \mathtt{e}^{\mathfrak{G}}\rangle$, where $\cdot^{\mathfrak{G}}$ denotes the binary group-operation, ${}^{-1^{\mathfrak{G}}}$ denotes inversion, and $\mathtt{e}^{\mathfrak{G}} \in G$ is the neutral element of G. However, $\mathfrak{N}_{sg} = \langle \mathbb{N}; +, \mathbf{0}; 0\rangle$, where $\mathbf{0} : \mathbb{N} \to \mathbb{N}$ is defined by $n \mapsto 0$ for all $n \in \mathbb{N}$, is an $\mathcal{L}_{group}$-structure as well.
(4) Let R be a ring with unity, then $\mathfrak{R} := \langle R; +^{\mathfrak{R}}, -^{\mathfrak{R}}, .^{\mathfrak{R}}; \mathtt{0}^{\mathfrak{R}}, \mathtt{1}^{\mathfrak{R}}\rangle$, where $+^{\mathfrak{R}}, -^{\mathfrak{R}}, .^{\mathfrak{R}}$ are the respective binary ring-operations and $\mathtt{0}^{\mathfrak{R}}, \mathtt{1}^{\mathfrak{R}}$ are the neutral elements with respect to addition and multiplication, is a model in $\mathcal{L}_{ring}$. Of special interest to us will be the $\mathcal{L}_{ring}$-structures $\mathfrak{Z} := \langle \mathbb{Z}; +, -, \cdot; 0, 1\rangle$ denoting the structure of rational integers and $\mathfrak{O}_K := \langle \mathcal{O}_K; +, -, \cdot; 0, 1\rangle$ denoting the structure of algebraic integers (cf. Section 1.3). However, we will also consider the $\mathcal{L}_{ring}$-structure

$\mathfrak{N} := \langle \mathbb{N}; +, \dot{-}, \cdot; 0, 1\rangle$ of the non-negative integers, where $\dot{-} : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ is defined by $n \dot{-} m = \max(0, n - m)$.

As a next step we want to define the syntax of formulae but at first we consider terms.

DEFINITION. Let $\mathcal{L} = \{f \in \mathcal{F}; R \in \mathcal{R}; c \in \mathcal{C}\}$ be a language. The set of *$\mathcal{L}$-terms* is the smallest set $T(\mathcal{L})$, such that

(i) every constant symbol $c \in \mathcal{C}$ is a term,
(ii) every variable symbol $\mathtt{x}_1, \mathtt{x}_2, \mathtt{x}_3, \ldots$ is a term, and
(iii) if $t_1, \ldots, t_{n_f} \in T(\mathcal{L})$ are terms then $f(t_1, \ldots, t_{n_f})$ is a term for all function symbols $f \in \mathcal{F}$.

For example $+(+(\cdot(\mathtt{x}_1, \mathtt{x}_1), \cdot(\mathtt{x}_2, \mathtt{x}_2)), \mathtt{1})$ is an $\mathcal{L}_{ring}$ term. It is more conventional—and more legible—to write this term in infix-notation to obtain the 'polynomial'

$$\mathtt{x}_1 \cdot \mathtt{x}_1 + \mathtt{x}_2 \cdot \mathtt{x}_2 + \mathtt{1},$$

Using the very important technique of *structural induction*, we can show that every term in an $\mathcal{L}_{ring}$-structure is a polynomial (see Lem. 1.2.3). In order to do this we need to consider terms as functions. There is just a little technicality in our way, that can be avoided by defining $S^0 := \{\emptyset\}$ for every set S and interpreting a constant c as a 0-ary function $c : S^0 \to S$.

DEFINITION. Let $\mathcal{L} := \{f \in \mathcal{F}; R \in \mathcal{R}; c \in \mathcal{C}\}$ be a language and let $\mathfrak{A}$ be a model of $\mathcal{L}$ with universe A. For a term $t(\mathtt{x}_1, \ldots, \mathtt{x}_n) \in T(\mathcal{L})$ that contains at most the variables $\mathtt{x}_1, \ldots, \mathtt{x}_n$ we define the *term function* $t^{\mathfrak{A}} : A^n \to A$ associated to $t(\mathtt{x}_1, \ldots, \mathtt{x}_n)$ recursively as follows:

(i) If $t(\mathtt{x}_1, \ldots, \mathtt{x}_n) = c \in \mathcal{C}$, then $t^{\mathfrak{A}}(\alpha_1, \ldots, \alpha_n) = c^{\mathfrak{A}}$ for all $\alpha_1, \ldots, \alpha_n \in A$.
(ii) If $t(\mathtt{x}_1, \ldots, \mathtt{x}_n) = \mathtt{x}_i$ for $1 \leq i \leq n$, then $t^{\mathfrak{A}} := \pi_i^n$ is the projection onto the i-th coordinate.
(iii) If $t(\mathtt{x}_1, \ldots, \mathtt{x}_n)$ is of the form

$$t(\mathtt{x}_1, \ldots, \mathtt{x}_n) = f(t_1(\mathtt{x}_1, \ldots, \mathtt{x}_n), \ldots, t_{n_f}(\mathtt{x}_1, \ldots, \mathtt{x}_n))$$

for some basic function $f \in \mathcal{F}$ and some terms $t_1(\mathtt{x}_1, \ldots, \mathtt{x}_n), \ldots, t_{n_f}(\mathtt{x}_1, \ldots, \mathtt{x}_n)$, then

$$t^{\mathfrak{A}}(\alpha_1, \ldots, \alpha_n) := f^{\mathfrak{A}}(t_1^{\mathfrak{A}}(\alpha_1, \ldots, \alpha_n), \ldots, t_{n_f}^{\mathfrak{A}}(\alpha_1, \ldots, \alpha_n)).$$

In other words, the set of term functions of a given model $\mathfrak{A}$ is the smallest set of functions, that contains all projections, all constants, as well as all basic functions of $\mathfrak{A}$, and is closed under composition. If $\mathfrak{A}$ is an algebraic structure, the set of term functions of $\mathfrak{A}$ is sometimes called the *function clone* of $\mathfrak{A}$.

LEMMA 1.2.3. *Let R be a ring with unity and $\mathfrak{R}$ its associated $\mathcal{L}_{ring}$-structure. The set of term functions of $\mathfrak{R}$ is the set of polynomial functions with integral coefficients $\mathbb{Z}[X_1, X_2, \ldots]$.*

Proof. Let $t \in T(\mathcal{L}_{ring})$ be a term. We argue by structural induction, that is induction on the number of symbols appearing in t.

(i) If $t = c$ is a constant, then $t = \mathtt{0}$ or $\mathtt{1}$. Both are constant polynomials with integral coefficients.

(ii) If $t = \mathtt{x_i}$ for some $i \in \mathbb{N} \setminus \{0\}$, then $t^{\mathfrak{R}} = X_i$ is a monomial.

(iii) Finally, if $t = f(t_1, t_2)$, where $f \in \{+, -, \cdot\}$ and t_1, t_2 are terms, then we can assume that $t_1^{\mathfrak{R}}$ and $t_2^{\mathfrak{R}}$ are polynomials with integral coefficients and as $\mathbb{Z}[X_1, X_2, ...]$ is closed under sums, differences and products of polynomials, the term functions are indeed contained in $\mathbb{Z}[X_1, X_2, ...]$

To see the converse inclusion note that every positive integer n can be expressed as the $\mathcal{L}_{ring}$-term

$$\underbrace{\mathtt{1 + 1 + ... + 1}}_{n\text{-times}}$$

and every non-positive integer n can be expressed as

$$\mathtt{0} - \underbrace{\mathtt{1 - 1 - ... - 1}}_{|n|\text{-times}}.$$

Then a monomial $aX_{i_1}...X_{i_d} \in \mathbb{Z}[X_1, X_2, ...]$, with $i_1, ..., i_d \in \mathbb{N} \setminus \{0\}$ not necessarily distinct, can be expressed as the term

$$\mathtt{a} \cdot x_{i_1} \cdot ... \cdot x_{i_d},$$

where $\mathtt{a}$ is the term representing the integer a. Finally, since every polynomial p is a finite sum of monomials $p = m_1 + ... + m_k$ we can find a term

$$t = \mathtt{m_1} + ... + \mathtt{m_k},$$

where $\mathtt{m_i}$ is the term representing m_i $(1 \leq i \leq k)$, such that $t^{\mathfrak{R}} = p$. □

In the lemma above I have considered the polynomial functions

$$p_1 : R \to R,\ p_1(X_1) := X_1^2 + 1 \quad \text{and} \quad p_2 : R^2 \to R,\ p_2(X_1, X_2) := X_1^2 + 1$$

as the same polynomial function. This can be justified by identifying all polynomials in the ring $\mathbb{Z}[X_1, X_2, ...]$ with functions $p : R^{\mathbb{N}} \to R$ depending only on finitely many arguments.

Finally, we have all tools at hand to formally define formulae in a language.

DEFINITION. Let $\mathcal{L} := \{f \in \mathcal{F}; R \in \mathcal{R}; c \in \mathcal{C}\}$ be a language. We call a string ϕ *atomic $\mathcal{L}$-formula* if

(i) there exist $\mathcal{L}$-terms t_1, t_2 such that $\phi = t_1 \doteq t_2$, or[5]
(ii) there exist $\mathcal{L}$-terms $t_1, ..., t_{n_R}$ and a relation symbol $R \in \mathcal{R}$ such that $\phi = R(t_1, ..., t_{n_R})$.

The set of *formulae* in $\mathcal{L}$ is the smallest set $\Phi(\mathcal{L})$ containing all atomic $\mathcal{L}$-formulae that is closed under the following constructions:

(iii) If $\phi \in \Phi(\mathcal{L})$ is a formula, so is its *negation* $\neg\phi \in \Phi(\mathcal{L})$.
(iv) If $\phi_1, \phi_2 \in \Phi(\mathcal{L})$ are formulae, then their *conjunction* $(\phi_1 \wedge \phi_2) \in \Phi(\mathcal{L})$ is a formula.

[5] Note the difference between the two symbols $=$ and $\doteq$ in this equation. While $=$ denotes an equality on the meta-level, i.e. it denotes that both strings contain the same symbols in the same order, $\doteq$ is just a symbol contained in the strings.

(v) If $\phi(x) \in \Phi(\mathcal{L})$ is a formula containing at least the variable x in one of its terms, then $\exists x : \phi(x) \in \Phi(\mathcal{L})$ is a formula.

Just for convenience we define the following abbreviations:

(vi) If $\phi_1, \phi_2 \in \Phi(\mathcal{L})$ are formulae, we define their *disjunction* $(\phi_1 \vee \phi_2)$ by $\neg(\neg\phi_1 \wedge \neg\phi_2)$.
(vii) If $\phi_1, \phi_2 \in \Phi(\mathcal{L})$ are formulae, then $\phi_1 \to \phi_2$ is short for $\neg(\phi_1 \wedge \neg\phi_2)$.
(viii) If $\phi(x) \in \Phi(\mathcal{L})$ is a formula containing at least the variable x, then we abbreviate $\neg\exists x : \neg\phi(x)$ by $\forall x : \phi(x)$.

Note that formulae as defined above are just strings and do not inherit any meaning or truthfulness.[6] However, once we interpret a formula in a model, we can say whether the formula is true or false. Let us consider some examples in the language $\mathcal{L}_{ring}$ of rings with one.

EXAMPLE 1.2.4. The following are $\mathcal{L}_{ring}$-formulae:

(1) $\mathsf{x}_1 \cdot \mathsf{x}_2 \doteq \mathsf{x}_3$
(2) $\exists \mathsf{x}_2 : \mathsf{x}_1 \cdot \mathsf{x}_2 \doteq 1$
(3) $\forall \mathsf{x}_1 : \forall \mathsf{x}_2 : \forall \mathsf{x}_3 : (\mathsf{x}_1 + \mathsf{x}_2) \cdot \mathsf{x}_3 \doteq \mathsf{x}_1 \cdot \mathsf{x}_3 + \mathsf{x}_2 \cdot \mathsf{x}_3$

Intuitively, the formulae above can be interpreted as

(1) x_1 times x_2 equals x_3,
(2) x_1 is invertible with inverse x_2, and
(3) the ring operations satisfy the distributivity condition.

In the formulae of the previous example one technical obstacle becomes apparent. While the formula of Example 1.2.4.(3) is either true or false in a given $\mathcal{L}_{ring}$-structure, the formulae in (1) and (2) depend on the choice of elements for x_1, x_2 and x_3. For this reason we must distinguish between two kinds of appearances of variables.

DEFINITION. Let x be a variable and let ϕ be a formula containing x. If ϕ contains $\exists x : \psi(x)$ as a sub-formula for some formula ψ, we call this appearance of x *bound appearance*. All appearances of x that are not of this shape are called *free appearances*.

In Example 1.2.4.(3) all appearances of x_1, x_2 and x_3 are bound. In (2) variable x_2 appears bounded while x_1 is free and in (1) all variables appear freely. For a formula ϕ we will write $\phi(\mathsf{x}_1, \dots, \mathsf{x}_n)$ to emphasize that at most the variables $\mathsf{x}_1, \dots, \mathsf{x}_n$ appear freely in ϕ.

DEFINITION. Let $\mathcal{L}$ be a language and let $\mathfrak{A}$ be model of $\mathcal{L}$ with universe A. For a formula $\phi = \phi(\mathsf{x}_1, \dots, \mathsf{x}_n)$ and elements $\alpha_1, \dots, \alpha_n \in A$ we say that $\phi(\alpha_1, \dots, \alpha_n)$ is *true* in $\mathfrak{A}$ or $\mathfrak{A}$ *models* $\phi(\alpha_1, \dots, \alpha_n)$ and write

$$\mathfrak{A} \vDash \phi(\alpha_1, \dots, \alpha_n)$$

if the following recursively defined conditions are met:

(i) If $\phi = t_1 \doteq t_2$ for two terms t_1, t_2, then $\mathfrak{A} \vDash \phi(\alpha_1, \dots, \alpha_n)$ if

$$t_1^{\mathfrak{A}}(\alpha_1, \dots, \alpha_n) = t_2^{\mathfrak{A}}(\alpha_1, \dots, \alpha_n).$$

[6] Note however, that there are formulae that are true in all models, for instance $\forall \mathsf{x}_1 : \mathsf{x}_1 \doteq \mathsf{x}_1$ is easily seen to hold in all models.

(ii) If $\phi = R(t_1, ..., t_{n_R})$ for a relation symbol R and terms $t_1, ..., t_{n_R}$, then $\mathfrak{A} \vDash \phi(\alpha_1, \dots, \alpha_n)$ if

$$R^{\mathfrak{A}}(t_1^{\mathfrak{A}}(\alpha_1, \dots, \alpha_n), ..., t_{n_R}^{\mathfrak{A}}(\alpha_1, \dots, \alpha_n)).$$

(iii) If $\phi = \neg\psi$ for a formula ψ, then $\mathfrak{A} \vDash \phi(\alpha_1, \dots, \alpha_n)$ if $\mathfrak{A} \vDash \psi(\alpha_1, \dots, \alpha_n)$ does not hold.
(iv) If $\phi = (\psi_1 \wedge \psi_2)$ for two formulae ψ_1, ψ_2, then $\mathfrak{A} \vDash \phi(\alpha_1, \dots, \alpha_n)$ if both $\mathfrak{A} \vDash \psi_1(\alpha_1, \dots, \alpha_n)$ and $\mathfrak{A} \vDash \psi_2(\alpha_1, \dots, \alpha_n)$ hold.
(v) If $\phi(\mathsf{x}_1, \dots, \mathsf{x}_n) = \exists x : \psi(x, \mathsf{x}_1, \dots, \mathsf{x}_n)$, then $\mathfrak{A} \vDash \phi(\alpha_1, \dots, \alpha_n)$ if there exists an $\alpha \in A$ such that $\mathfrak{A} \vDash \psi(\alpha, \alpha_1, \dots, \alpha_n)$.

Remark. (1) I leave it as an exercise to check that our abbreviations $\vee$, $\rightarrow$ and $\forall$ have their intended interpretation of *disjunction*, *implication* and *universal quantification*.

(2) Note that variables can have both free *and* bound appearances in the same formula, for example x_2 in

$$(\exists \mathsf{x}_2 : \mathsf{x}_1 \cdot \mathsf{x}_2 \doteq \mathsf{x}_2) \wedge (\mathsf{x}_2 + \mathsf{x}_3 \doteq \mathsf{x}_1).$$

By the definition of what it means that a formula is true in a model, we can restrict our attention to formulae, such that all variables appear *either* freely *or* bounded but not both, and if a variable appears bound, then it is bound by a single quantifier. For instance, it is easy to check that the formula above is true in a model if and only if the following formula is true

$$(\exists \mathsf{x}_2 : \mathsf{x}_1 \cdot \mathsf{x}_2 \doteq \mathsf{x}_2) \wedge (\mathsf{x}_4 + \mathsf{x}_3 \doteq \mathsf{x}_1).$$

Variables that appear freely in a formula are also called *free variables.*

A formula without free variables is called a *sentence*. In a fixed model a sentence is either true or false. This follows easily form the definition of truth in a model.

1.2.2 Morphisms, theories, and decidability

In this section I introduce some very important notions from model theory and universal algebra. I start with the concept of *morphism*. The reader should already have encountered morphisms in basic lectures on abstract algebra. They are just mappings that respect the basic operations of structures. More formally, one defines a morphism as follows.

DEFINITION. Let $\mathcal{L} := \{f \in \mathcal{F}; R \in \mathcal{R}; c \in \mathcal{C}\}$ be a language and $\mathfrak{A}, \mathfrak{B}$ two models in $\mathcal{L}$ with universes A and B respectively. A function $\varphi : A \rightarrow B$ is called *$\mathcal{L}$-morphism* if

(i) $\varphi(f^{\mathfrak{A}}(\alpha_1, \dots, \alpha_{n_f})) = f^{\mathfrak{B}}(\varphi(\alpha_1), ..., \varphi(\alpha_{n_f}))$ holds for all $f \in \mathcal{F}$ and all $\alpha_1, \dots, \alpha_{n_f} \in A$;
(ii) $R^{\mathfrak{A}}(\alpha_1, \dots, \alpha_{n_R})$ implies $R^{\mathfrak{B}}(\varphi(\alpha_1), ..., \varphi(\alpha_{n_r}))$ for all $R \in \mathcal{R}$ and all $\alpha_1, \dots, \alpha_{n_R} \in A$; and
(iii) $\varphi(c^{\mathfrak{A}}) = c^{\mathfrak{B}}$ for all $c \in \mathcal{C}$.

Remark. (1) Despite the similarity of the definition of $\mathcal{L}_{ring}$-morphisms to ring-morphisms in the sense of abstract algebra, not every $\mathcal{L}_{ring}$-morphism is a ring-morphism and vice versa. Consider for example the identity $\mathrm{id}_{\mathbb{N}}$ on the $\mathcal{L}_{ring}$-structure $\mathfrak{N}$. As $\mathbb{N}$ is not a ring in the sense of abstract algebra, $\mathrm{id}_{\mathbb{N}}$ is not a ring-morphism, but it is clearly an $\mathcal{L}_{ring}$-morphism.

On the other hand, the mapping $\varphi : \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ defined by

$$\varphi(\alpha) = (0, \alpha)$$

is a ring-morphism that is not an $\mathcal{L}_{ring}$-morphism, as 1 is not mapped to the neutral element $(1, 1)$ in $\mathbb{Z} \times \mathbb{Z}$.

(2) As in abstract algebra, an injective morphism is called *monomorphism*, a surjective one *epimorphism*, and a bijective morphism is called *isomorphism*.

DEFINITION. Let $\mathcal{L}$ be a language.

(i) A set of $\mathcal{L}$-sentences is called an *$\mathcal{L}$-theory*.
(ii) Let $\mathfrak{A}$ be a model in $\mathcal{L}$. We say $\mathfrak{A}$ satisfies a theory T and write $\mathfrak{A} \vDash T$ if $\mathfrak{A}$ models all sentences in T.
(iii) A class of models $\mathcal{M}$ in $\mathcal{L}$ is called *elementary class* if there exists an $\mathcal{L}$-theory T such that for all models $\mathfrak{A}$ the following equivalence holds

$$\mathfrak{A} \in \mathcal{M} \quad \Leftrightarrow \quad \mathfrak{A} \vDash T.$$

(iv) An elementary class $\mathcal{V}$ of algebraic structures is called *universal variety* if the defining theory T does only include universally quantified atomic formulae.

EXAMPLE 1.2.5. The class of groups forms a universal variety with respect to $\mathcal{L}_{group}$. This is the case since the group axioms

$$\begin{aligned}
&\forall x_1 \colon x_1 \cdot e \doteq x_1,\\
&\forall x_1 \colon e \cdot x_1 \doteq x_1,\\
&\forall x_1 \colon \forall x_2 : \forall x_3 : (x_1 \cdot x_2) \cdot x_3 \doteq x_1 \cdot (x_2 \cdot x_3),\\
&\forall x_1 \colon x_1 \cdot x_1^{-1} \doteq e, \text{ and}\\
&\forall x_1 \colon x_1^{-1} \cdot x_1 \doteq e
\end{aligned}$$

characterize groups completely. Another example of a universal variety are rings with unity. Note however, that fields do not form a universal variety with respect to $\mathcal{L}_{ring}$, as we demand that elements unequal to 0 are invertible which can be expressed by the sentence

$$\forall x_1 : (\neg x_1 \doteq 0) \to (\exists x_2 : x_1 \cdot x_2 \doteq 1)$$

containing both universal and existential quantifiers.

Universal varieties are useful, as substructures can be characterized by embeddings, e.g. we have that a subset S of a ring with unity R is a sub-ring if and only if S carries an $\mathcal{L}_{ring}$-structure $\mathfrak{S}$ such that the embedding

$$\iota : S \to R, \quad \iota(\alpha) = \alpha$$

is an $\mathcal{L}_{ring}$-morphism between $\mathfrak{S}$ and the $\mathcal{L}_{ring}$-structure of R. Moreover, we have the following important result.

THEOREM 1.2.6. *Let $\mathfrak{A}$ and $\mathfrak{B}$ be two $\mathcal{L}$-structures, with universe A and B respectively, and let $\varphi : A \to B$ be a bijective $\mathcal{L}$-morphism. Then $\mathfrak{A}$ and $\mathfrak{B}$ are* elementary equivalent, *i.e. for all $\mathcal{L}$-sentences ϕ, $\mathfrak{A}$ models ϕ if and only if $\mathfrak{B}$ models ϕ.*

A proof of the theorem using induction on the structure of formulae can be found in the textbook [25, Thm 1.1.10]. For the reader who wants to learn more about universal algebra the textbook [1] is an excellent reference.

To conclude this section we describe theories of special importance to our task of settling Hilbert's tenth problem and define what it means to decide a theory.

DEFINITION. Let $\mathcal{L}$ be a language and let $\mathfrak{A}$ be a model with universe A in $\mathcal{L}$.

(i) The *full theory of* $\mathfrak{A}$ is the set

$$\mathtt{Th}(\mathfrak{A}) := \{\phi \in \Phi(\mathcal{L}) : \phi \text{ is a sentence and } \mathfrak{A} \vDash \phi\}$$

of all sentences true in $\mathfrak{A}$.

(ii) The *purely Diophantine theory of* $\mathfrak{A}$ is the set

$$\mathtt{H10}^*(\mathfrak{A}) := \{\phi \in \Phi(\mathcal{L}) \mid \phi = \exists \mathtt{x}_{i_1} : \ldots \exists \mathtt{x}_{i_k} : \psi(\mathtt{x}_{i_1}, \ldots, \mathtt{x}_{i_k}), \psi \text{ is atomic, and } \mathfrak{A} \vDash \phi\}$$

of all fully existentially quantified atomic formulae that are satisfied by $\mathfrak{A}$.

(iii) The *primitive positive theory of* $\mathfrak{A}$ is the set

$$\mathtt{Th}_{\exists+}(\mathfrak{A}) := \left\{\phi \in \Phi(\mathcal{L}) \;\middle|\; \begin{array}{l}\phi = \exists \mathtt{x}_{i_1} : \ldots \exists \mathtt{x}_{i_k} : \bigwedge_{j=1}^{m} \psi_j(\mathtt{x}_{i_1}, \ldots, \mathtt{x}_{i_k}), \\ \psi_j \text{ is atomic for } 1 \leq j \leq m, \text{ and } \mathfrak{A} \vDash \phi\end{array}\right\}$$

of all fully existentially quantified conjunctions of atomic formulae that are satisfied by $\mathfrak{A}$.

Let us take a look at some examples to get a better understanding of these abstract definitions.

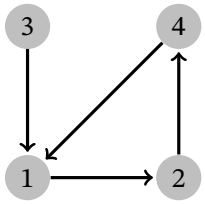
EXAMPLE 1.2.7. (1) Let $\mathfrak{Q} := \langle \mathbb{Q}; +, -, \cdot; 0, 1\rangle$ be the $\mathcal{L}_{ring}$-structure of the rationals. Then

$$\mathfrak{Q} \vDash \forall \mathtt{x}_1 : (\neg \mathtt{x}_1 \doteq \mathtt{0}) \to (\exists \mathtt{x}_2 : \mathtt{x}_1 \cdot \mathtt{x}_2 \doteq \mathtt{1})$$

and therefore this sentence is contained in $\mathtt{Th}(\mathfrak{Q})$. However, $2 \in \mathbb{Z} \setminus \{0\}$ is not invertible in $\mathbb{Z}$. Thus, the sentence is not in $\mathtt{Th}(\mathfrak{Z})$.

(2) Consider $\phi := \exists \mathtt{x}_1 : \mathtt{x}_1^2 + \mathtt{1} \doteq \mathtt{0}$. Then ϕ can be satisfied by the witness $i \in \mathbb{C}$ in $\mathfrak{C} := \langle \mathbb{C}; +, -, \cdot; 0, 1\rangle$ as $i^2 + 1 = 0$ holds in $\mathfrak{C}$. Thus, ϕ is contained in $\mathtt{H10}^*(\mathfrak{C})$, but the sentence is not contained in $\mathtt{H10}^*(\mathfrak{Z})$.

(3) Consider the directed graph $\mathfrak{G} := \langle \{1, 2, 3, 4\}; E\rangle$ below.



Here E denotes the binary adjacency relation, where for instance $E(1,2)$ holds but $E(2,1)$ does not. The following sentence intuitively says that a graph contains a cycle of length 3.

$$\phi := \exists x_1 : \exists x_2 : \exists x_3 : (E(x_1, x_2) \wedge E(x_2, x_3) \wedge E(x_3, x_1))$$

Using 1 as witness for x_1 and 2, 4 as witnesses for x_2, x_3, we obtain that ϕ is contained in $\mathrm{Th}_{\exists+}(\mathfrak{G})$, and it is not difficult to find a directed graph that does not model ϕ.

While we can already state a lot of properties in the languages we have considered so far, we can for instance not formulate a sentence in the language $\mathcal{L}_{ring}$ that says a specific polynomial has a root. Take for instance the $\mathcal{L}_{ring}$-structure $\mathfrak{C}$ of $\mathbb{C}$, we cannot formulate a sentence that says the polynomial $X^2 - i \in \mathbb{C}[X]$ has a root in $\mathbb{C}$. To get around this limitation we define *diagrams*.

DEFINITION. Let $\mathcal{L}$ be a language and $\mathfrak{A}$ a model in $\mathcal{L}$ with universe A. We define the A-language as

$$\mathcal{L}_A := \mathcal{L} \cup \{c_a \mid a \in A\}$$

the union of $\mathcal{L}$ and a constant symbol for each element of A.

Clearly, $\mathfrak{A}$ is also a model in $\mathcal{L}_A$ by additionally interpreting $c_a^{\mathfrak{A}} := a$ for all $a \in A$.

DEFINITION. Let $\mathcal{L}$ be a language and let $\mathfrak{A}$ be a model with universe A in $\mathcal{L}$. We define the following $\mathcal{L}_A$-theories.

(i) The *complete diagram* of $\mathfrak{A}$ is the set

$$D^c(\mathfrak{A}) := \{\phi \in \Phi(\mathcal{L}_A) \mid \phi \text{ is a sentence and } \mathfrak{A} \vDash \phi\}$$

of all $\mathcal{L}_A$-sentences true in $\mathfrak{A}$.

(ii) The *Diophantine theory* of $\mathfrak{A}$ is the set

$$\mathrm{H10}(\mathfrak{A}) := \{\phi \in \Phi(\mathcal{L}_A) \mid \phi = \exists x_{i_1} : ...\exists x_{i_k} : \psi(x_{i_1}, ..., x_{i_k}), \psi \text{ is atomic, and } \mathfrak{A} \vDash \phi\}$$

of all fully existentially quantified atomic $\mathcal{L}_A$-formulae that are satisfied by $\mathfrak{A}$.

(iii) The *primitive positive diagram* of $\mathfrak{A}$ is the set

$$D_{\exists+}(\mathfrak{A}) := \left\{\phi \in \Phi(\mathcal{L}) \;\middle|\; \begin{array}{c}\phi = \exists x_{i_1} : ...\exists x_{i_k} : \bigwedge_{j=1}^{m} \psi_j(x_{i_1}, ..., x_{i_k}), \\ \psi_j \text{ is atomic for } 1 \leq j \leq m, \text{ and } \mathfrak{A} \vDash \phi\end{array}\right\}$$

of all full existentially quantified conjunctions of atomic $\mathcal{L}_A$-formulae that are satisfied by $\mathfrak{A}$.

(iv) The *atomic diagram* of $\mathfrak{A}$ is the set

$$D(\mathfrak{A}) := \left\{\phi \in \Phi(\mathcal{L}_A) \;\middle|\; \begin{array}{c}\text{there exists an atomic formula } \psi \text{ with} \\ \phi = \psi, \text{ or } \phi = \neg\psi \text{ and } \mathfrak{A} \vDash \phi\end{array}\right\}$$

of all atomic $\mathcal{L}_A$-sentences and negations of atomic $\mathcal{L}_A$-sentences that are satisfied by $\mathfrak{A}$.

Of special interest to us is the Diophantine theory of rings with unity. The name can be justified by the following lemma.

THEOREM 1.2.8. *Let R be a ring with unity and let $\mathfrak{R}$ be its $\mathcal{L}_{ring}$-structure.*

(i) *The set of term functions associated to $\mathcal{L}_R$-terms is the set of polynomial functions $R[X_1, X_2, ...]$.*
(ii) *Let $\mathsf{P} \subseteq \Phi(\mathcal{L}_R)$ be the set of all existentially quantified atomic $\mathcal{L}_R$-formulae. There exists a surjection*

$$\pi : \mathsf{P} \to R[X_1, X_2, ...]$$

such that for all sentences $\phi \in \mathsf{P}$ we have

$$\phi \in \mathtt{H10}(\mathfrak{R}) \quad \Leftrightarrow \quad \pi(\phi) \text{ has roots in } R.$$

Proof. (i) Let t be an $\mathcal{L}_R$-term. One proves completely analogously to the proof of Lem. 1.2.3, that $t^{\mathfrak{R}} \in R[X_1, X_2, ...]$ is a polynomial function. The only difference is that constants now range over all of R instead of $\{0, 1\}$ thus yielding the different coefficients.

To see the converse inclusion we note that monomials $\alpha X_{i_1} ... X_{i_d} \in R[X_1, X_2, ...]$, with indices $i_1, ..., i_d \in \mathbb{N} \setminus \{0\}$ not necessarily distinct, correspond to terms

$$\mathsf{c}_\alpha \cdot \mathsf{x}_{\mathsf{i}_1} \cdot ... \cdot \mathsf{x}_{\mathsf{i}_d}.$$

Since every polynomial p is a finite sum of monomials we obtain a term representing p by joining the terms representing the monomials using the symbol $+$.

(ii) Let $\phi \in \mathsf{P}$ be a sentence. By definition of P there exists an atomic $\mathcal{L}_R$-formula ψ such that

$$\phi = \exists \mathsf{x}_{\mathsf{i}_1} : ... \exists \mathsf{x}_{\mathsf{i}_k} : \psi(\mathsf{x}_{\mathsf{i}_1}, ..., \mathsf{x}_{\mathsf{i}_k}).$$

Since $\mathcal{L}_R$ contains no relation symbols, all atomic $\mathcal{L}_R$-formulae are identities of terms. Thus, there exist terms t_1, t_2 such that

$$\psi = t_1 \doteq t_2.$$

By part (i) of the theorem, the term functions $t_1^{\mathfrak{R}}$ and $t_2^{\mathfrak{R}}$ are polynomial functions in $R[X_1, X_2, ...]$. We set $\pi(\phi) := t_1^{\mathfrak{R}} - t_2^{\mathfrak{R}}$.

To see that π is surjective let $p \in R[X_1, X_2, ...]$ be a polynomial. Then by (i) there exists a term t such that $t^{\mathfrak{R}} = p$. Now set

$$\phi := \exists \mathsf{x}_{\mathsf{i}_1} : ... \exists \mathsf{x}_{\mathsf{i}_k} : t(\mathsf{x}_{\mathsf{i}_1}, ..., \mathsf{x}_{\mathsf{i}_k}) \doteq \mathtt{0},$$

where $\mathsf{x}_{\mathsf{i}_1}, ..., \mathsf{x}_{\mathsf{i}_k}$ are all variable symbols appearing in t. Then $\pi(\phi) = p$ as claimed.

Let now $\phi \in \mathtt{H10}(\mathfrak{R})$ be a sentence that is true in $\mathfrak{R}$. By the discussion above we find that

$$\phi := \exists \mathsf{x}_{\mathsf{i}_1} : ... \exists \mathsf{x}_{\mathsf{i}_k} : t_1(\mathsf{x}_{\mathsf{i}_1}, ..., \mathsf{x}_{\mathsf{i}_k}) \doteq t_2(\mathsf{x}_{\mathsf{i}_1}, ..., \mathsf{x}_{\mathsf{i}_k}),$$

for some $\mathcal{L}_R$-terms t_1, t_2. Using the definition of truth in a model this is the case if and only if there exist elements $\alpha_{i_1}, ..., \alpha_{i_k} \in R$ such that

$$t_1^{\mathfrak{R}}(\alpha_{i_1}, ..., \alpha_{i_k}) = t_2^{\mathfrak{R}}(\alpha_{i_1}, ..., \alpha_{i_k}).$$

But this identity holds if and only if $\pi(\phi) = t_1 - t_2$ has roots in R.

□

To finish our last task of this section we have to overcome once more a technical difficulty: If we want to define what it means to *decide* a theory, we must identify the theory with subsets of ω. To this end, Gödel [15] introduced a method that is today commonly known as *Gödelization*.

DEFINITION. Let $\mathcal{L}$ be an at most countable language and let

$$i : \mathcal{L} \cup \{\doteq, \neg, \wedge, \exists, :, (,), \mathsf{x}, '\} \to \mathbb{N} \setminus \{0\}$$

be an injective function such that $i(s) > 9$ for all $s \in \mathcal{L}$ and the image of i is an initial segment of the usual order of $\mathbb{N} \setminus \{0\}$.

The *Gödel number* $\mathrm{gn}(\phi)$ of a formula $\phi \in \Phi(\mathcal{L})$ is obtained by first replacing every variable symbol x_j in ϕ by the string

$$\mathsf{x}\overbrace{'\ldots'}^{j\text{-times}}.$$

Say the resulting string is

$$\mathbf{s} = s_1 s_2 \ldots s_n,$$

where s_i is a symbol contained in $\mathcal{L} \cup \{\doteq, \neg, \wedge, \exists, (,), \mathsf{x}, '\}$ then

$$\mathrm{gn}(\phi) := p_1^{i(s_1)} p_2^{i(s_2)} \ldots p_n^{i(s_n)},$$

where $p_i \in \mathbb{N}$ is the i-th prime.

By the uniqueness of the prime factorization in $\mathbb{N}$, two different formulae cannot have the same Gödel number. Finally, one obtains an encoding $\ulcorner . \urcorner : \Phi(\mathcal{L}) \to \omega$ by composing gn with an encoding of the natural numbers (see Example 1.1.5.(3)).

EXAMPLE 1.2.9. To get a feeling for how fast the Gödel numbers grow let us consider the Gödelization of the following $\mathcal{L}_{ring}$-formula

$$\exists \mathsf{x}_1 : \mathsf{x}_1 \doteq \mathsf{0}.$$

We choose the function i as described in the table below.

s	$\doteq$	$\neg$	$\wedge$	$\exists$	$:$	$($	$)$	x	$'$	$+$	$-$	$\cdot$	$\mathsf{0}$	$\mathsf{1}$
$i(s)$	1	2	3	4	5	6	7	8	9	10	11	12	13	14

Using the notation from the definition we obtain

$$\mathbf{s} = \exists x' : x' \doteq 0$$

yielding the Gödel number

$$\mathrm{gn}(\phi) = 2^4 3^8 5^9 7^5 11^8 13^9 17^1 19^{13},$$

which already has 52 decimal digits.

DEFINITION. Let $\mathcal{L}$ be an at most countable language. An $\mathcal{L}$-theory T is *decidable* (*semi-decidable*)

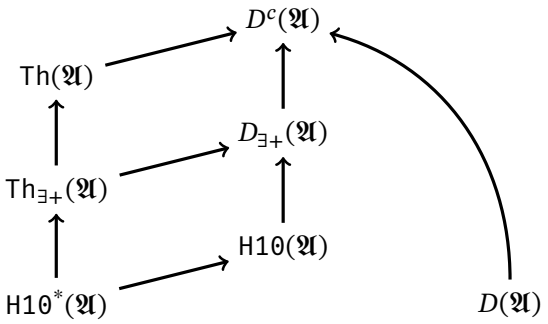


Figure 1.6: The theories defined in Section 1.2.2 may be ordered by set-inclusion (arrows pointing from sub- to super-sets) and many-one reducibility

if the set

$$\{\ulcorner\phi\urcorner : \phi \in T\}$$

is decidable (semi-decidable).

Remark. Let $\mathfrak{A}$ be a model. If one orders the theories defined above with respect to set-inclusion, the interrelations depicted in Fig. 1.6 hold.

If the language and the universe of $\mathfrak{A}$ are at most countable then we can Gödelize these theories and identify them with their set of Gödel numbers. In this setting it is not hard to see that the theories

- $S(\mathtt{Th}(\mathfrak{A})) := \{\phi \in \Phi(\mathcal{L}) \mid \phi \text{ is a sentence}\}$,
- $S(\mathtt{H10}^*(\mathfrak{A})) := \{\phi \in \Phi(\mathcal{L}) \mid \phi = \exists \mathtt{x}_{\mathtt{i}_1} : \ldots \exists \mathtt{x}_{\mathtt{i}_k} : \psi(\mathtt{x}_{\mathtt{i}_1}, \ldots, \mathtt{x}_{\mathtt{i}_k}), \psi \text{ is atomic}\}$
- $S(\mathtt{Th}_{\exists+}(\mathfrak{A})) := \left\{\phi \in \Phi(\mathcal{L}) \;\middle|\; \begin{smallmatrix}\phi = \exists \mathtt{x}_{\mathtt{i}_1} : \ldots \exists \mathtt{x}_{\mathtt{i}_k} : \bigwedge_{j=1}^{m} \psi_j(\mathtt{x}_{\mathtt{i}_1}, \ldots, \mathtt{x}_{\mathtt{i}_k}),\\ \psi_j \text{ is atomic for } 1 \leq j \leq m\end{smallmatrix}\right\}$
- $S(D^c(\mathfrak{A})) := \{\phi \in \Phi(\mathcal{L}_A) \mid \phi \text{ is a sentence}\}$,
- $S(\mathtt{H10}(\mathfrak{A})) := \{\phi \in \Phi(\mathcal{L}_A) \mid \phi = \exists \mathtt{x}_{\mathtt{i}_1} : \ldots \exists \mathtt{x}_{\mathtt{i}_k} : \psi(\mathtt{x}_{\mathtt{i}_1}, \ldots, \mathtt{x}_{\mathtt{i}_k}), \psi \text{ is atomic}\}$,
- $S(D_{\exists+}(\mathfrak{A})) := \left\{\phi \in \Phi(\mathcal{L}) \;\middle|\; \begin{smallmatrix}\phi = \exists \mathtt{x}_{\mathtt{i}_1} : \ldots \exists \mathtt{x}_{\mathtt{i}_k} : \bigwedge_{j=1}^{m} \psi_j(\mathtt{x}_{\mathtt{i}_1}, \ldots, \mathtt{x}_{\mathtt{i}_k}),\\ \psi_j \text{ is atomic for } 1 \leq j \leq m\end{smallmatrix}\right\}$, and
- $S(D(\mathfrak{A})) := \left\{\phi \in \Phi(\mathcal{L}_A) \;\middle|\; \begin{smallmatrix}\text{there exists an atomic formula } \psi \text{ with}\\ \phi = \psi, \text{ or } \phi = \neg\psi\end{smallmatrix}\right\}$

are decidable. A Turing machine deciding these theories must only check whether a string encodes a syntactically valid sentence using the allowed symbols [cf. 4, Chap. 8.1].

Let now $T \in \{\mathtt{Th}(\mathfrak{A}), \mathtt{H10}^*(\mathfrak{A}), \mathtt{Th}_{\exists+}(\mathfrak{A}), D^c(\mathfrak{A}), \mathtt{H10}(\mathfrak{A}), D_{\exists+}(\mathfrak{A}), D(\mathfrak{A})\}$ be a theory and $U \subseteq T$ a subtheory contained in $\{\mathtt{Th}(\mathfrak{A}), \mathtt{H10}^*(\mathfrak{A}), \mathtt{Th}_{\exists+}(\mathfrak{A}), D^c(\mathfrak{A}), \mathtt{H10}(\mathfrak{A}), D_{\exists+}(\mathfrak{A}), D(\mathfrak{A})\}$. We prove that $U \leq_m T$ holds. For this purpose note that $U = T \cap S(U)$ holds and consider the sentence

$$\phi_\perp := \mathtt{0} \doteq \mathtt{1},$$

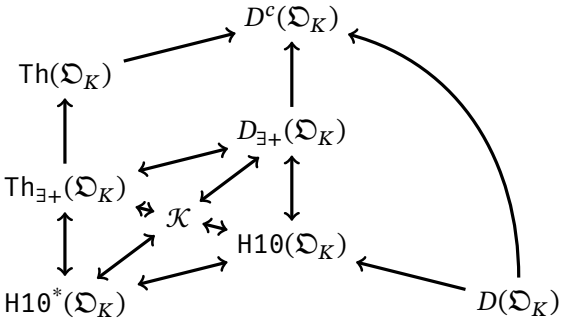


Figure 1.7: For models of algebraic integers $\mathfrak{O}_K$ the diagram collapses w.r.t. many-one reducibility if $\mathcal{K} <_m D_{\exists+}(\mathfrak{O}_K)$

which is contained in $S(T)$ but not in T. The function $f : \omega \to \omega$ defined by

$$f(x) := \begin{cases} x & \text{if } x \in \ulcorner S(U) \urcorner \\ \ulcorner \phi_\perp \urcorner & \text{otherwise} \end{cases}$$

is computable, as $S(U)$ is decidable. Additionally, it has the property that a string x is contained in $\ulcorner U \urcorner$ if and only if $f(x)$ is contained in T. Indeed if x encodes a sentence ϕ that is part of $S(U)$ then $f(x) = x$. In this case, x is in T if and only if x is in $S(U) \cap T = U$. If on the other hand x is not in $\ulcorner S(U) \urcorner$ then x is surely not contained in $\ulcorner U \urcorner$ and $f(x) = \ulcorner \phi_\perp \urcorner$ which is not turn contained in $\ulcorner T \urcorner$. Thus proving the claim.

Concerning rings of algebraic integers (incl. $\mathbb{Z}$) and their models $\mathfrak{O}_K$, we will see in Lem. 2.1.5 that $\mathtt{Th}_{\exists+}(\mathfrak{O}_K)$ is many-one reducible to $\mathtt{H10}^*(\mathfrak{O}_K)$ and that $D_{\exists+}(\mathfrak{O}_K)$ is many-one reducible to $\mathtt{H10}^*(\mathfrak{O}_K)$ In order to settle Hilbert's tenth problem we will show for some rings of algebraic integers that the halting set $\mathcal{K}$ is many-one reducible to $D_{\exists+}(\mathfrak{O}_K)$ and vice versa. However, even more is true as we will show that this is sufficient for the interrelations—with respect to many-one reducibility—depicted in Fig. 1.7 to hold between the theories.

1.2.3 Computable structures and decidable models

Up to this point the encoding of problems was treated as some kind of black-box. This subsection takes a categorical view on computability and ensures us, that—up to a sensible definition—encodings of the rings we concern ourselves with do not matter. The interested reader may whish to consult the excellent textbook by Stoltenberg-Hansen and Tucker [46] on this subject. However, I am using the notation of the paper [20] and the textbook [4, Chap. 16].

Throughout this section I will identify the set of non-negative integers $\mathbb{N}$ with the set of strings ω via the encoding described in Example 1.1.5.(3).

DEFINITION. Let $\mathcal{L}$ be an at most countable language. We say $\mathcal{L}$ is *computable* if we can Gödelize the set of $\mathcal{L}$-formulae $\Phi(\mathcal{L})$ in such a way, that $\mathsf{gn}(\Phi(\mathcal{L}))$ is decidable.

Note that we can only change the function i described in the definition of the Gödelization. Thus, we can rearrange the symbols of our language to simplify our computations. In this view, a language $\mathcal{L} = \{f \in \mathcal{F}; R \in \mathcal{R}; c \in \mathcal{C}\}$ is computable if we can encode its basic symbols in such a way that

1. the sets $i(\mathcal{F})$, $i(\mathcal{R})$, and $i(\mathcal{C})$ are decidable; and
2. the function $\mathtt{ar} : i(\mathcal{F}) \cup i(\mathcal{R}) \to \omega$ defined by $i(\ell) \mapsto \mathrm{ar}(\ell)$ is computable.

Indeed, if this is the case, we can use the properties of the Gödelization to obtain from an encoded formula $\mathrm{gn}(\phi)$ the sequence of symbols that ϕ contains and then check efficiently using structural induction, whether ϕ is a well-formed formula.

LEMMA 1.2.10. *Let $\mathcal{L}$ be a computable language. For a fixed Gödelization, the following numbers are computable for every $\mathcal{L}$-formula ϕ from the Gödel number* $\mathrm{gn}(\phi)$.

(i) The length $\mathrm{ln}(\phi)$ *of ϕ, which is the number of symbols appearing in ϕ.*
(ii) For every $\mathtt{i} \in \{1, ..., \mathrm{ln}(\phi)\}$*, the code* $\mathtt{i}(s)$ *of the symbol* s *appearing in the* $\mathtt{i}$*-th position of ϕ.*
(iii) The number of quantifiers appearing in ϕ and the number of free variables.
(iv) The Gödel number of the negation of ϕ.
(v) If a second formula ψ is given, one can efficiently obtain the Gödel number of the conjunction of ϕ and ψ.
(vi) If $\phi(x)$ contains the free variable x and the Gödel number of a term t is given, one can efficiently obtain the Gödel number of $\phi(t)$, i.e. the Gödel number of the formula, where each free appearance of x is replaced by t.

The lemma is easily proven using that the prime factorization of a positive integer is computable. All of the numbers above can then be computed by manipulating the factorizations.

Of course, all languages we will consider—and have considered so far—are computable. In fact, they are all either finite, or contain only finitely many non-constant symbols.

DEFINITION. Let $\mathcal{L}$ be a computable language and let $i : \mathcal{L} \to \mathbb{N}$ be the function used to Gödelize $\mathcal{L}$.

(i) A model $\mathfrak{A}$ in $\mathcal{L}$, with universe $A \subseteq \omega$, is called *computable* if A is decidable and there exist two computable functions F, C and a decidable relation R such that

$$\mathsf{F}(i(f), \langle \alpha_1, \dots, \alpha_{n_f} \rangle) = f^{\mathfrak{A}}(\alpha_1, \dots, \alpha_{n_f})$$

holds for all function symbols $f \in \mathcal{F}$ and all elements $\alpha_1, \dots, \alpha_{n_f} \in A$,

$$\mathsf{R}(i(R), \langle \alpha_1, \dots, \alpha_{n_R} \rangle) \quad \Leftrightarrow \quad R^{\mathfrak{A}}(\alpha_1, \dots, \alpha_{n_R})$$

holds for all relation symbols $R \in \mathcal{R}$ and all elements $\alpha_1, \dots, \alpha_{n_R} \in A$, and

$$\mathsf{C}(i(c)) = c^{\mathfrak{A}}$$

holds for all constant symbols $c \in \mathcal{C}$. As before angled brackets $\langle \cdot \rangle$ in the expressions above indicate pairings like in Example 1.1.6.(2).

(ii) A model $\mathfrak{A}$ with universe A is called *efficiently presentable* if $\mathfrak{A}$ is isomorphic to a computable model with universe $\Omega_A \subseteq \omega$ in the same language.

(iii) A morphism between computable models is called *computable morphism* if it is computable as a partial function.

Remark. (1) An efficient presentation of a ring R is a ring-homomorphism $\ulcorner\cdot\urcorner : R \to \Omega_R$ of R, where $\Omega_R \subseteq \omega$ is decidable and all operations of Ω_R are computable functions.

(2) Stoltenberg-Hansen and Tucker [46] use a slightly modified definition of computable rings. They consider *effective enumerations* $\alpha_R : \Omega_R \to R$, where $\Omega_R \subseteq \omega$ is a computable $\mathcal{L}_{ring}$-structure in the sense of the definition above and α_R is an $\mathcal{L}_{ring}$-epimorphism. Then the ring R is called computable if there exists an effective enumeration $\alpha_R : \Omega_R \to R$ such that the equivalence relation

$$x_1 \equiv_{\alpha_R} x_2 \quad \Leftrightarrow \quad \alpha_R(x_1) = \alpha_R(x_2)$$

is decidable on Ω_R.

This definition can have slight technical advantages. But note that in this case Ω_R need not be a ring in the sense of abstract algebra, an $\mathcal{L}_{ring}$-structure in the sense of universal algebra suffices. Let $\lfloor \alpha_R^{-1}(\{\eta\}) \rfloor \in \Omega_R$ denote the smallest element of $\alpha_R^{-1}(\{\eta\})$ in lexicographic order. By setting $\ulcorner\eta\urcorner = \lfloor \alpha_R^{-1}(\{\eta\}) \rfloor$ for each $\eta \in R$ one obtains a ring-isomorphism $R \to \Omega_R$ that gives rise to an efficient presentation of R. So R is computable in the sense of Stoltenberg-Hansen and Tucker [46] if and only if it is efficiently presentable in the sense of this thesis.

The following alternative characterization of efficiently presentable models can easily be proven via structural induction.

LEMMA 1.2.11. *Let $\mathcal{L}$ be an at most countable language and $\mathfrak{A}$ a model in $\mathcal{L}$ with universe A. Then the following are equivalent.*

(i) $\mathfrak{A}$ *is efficiently presentable as a model in* $\mathcal{L}$.
(ii) $\mathfrak{A}$ *is efficiently presentable as a model in* $\mathcal{L}_A$.
(iii) The atomic diagram of $\mathfrak{A}$ *is decidable.*

EXAMPLE 1.2.12. (1) Every finite structure $\langle S; f_1, ..., f_n \rangle$ with $S \subseteq \omega$ is computable. The set S is decidable as it is finite and the domain of each operation f_i for $1 \leq i \leq n$ is finite as well. A Turing machine computing f_i can store the images of all elements in the domain in memory.

(2) In Example 1.1.5.(1) the non-negative integer n was encoded by a string of n consecutive 1-s. I have also already presented the algorithm deciding $\ulcorner\mathbb{N}\urcorner \subseteq \omega$ with respect to this encoding. Considering $\mathbb{N}$ as an $\mathcal{L}_{ring}$-structure, one finds that the tally encoding gives rise to an efficient presentation of $\mathbb{N}$.

The constants 0 and 1 are trivially computable, by clearing the tape in the first case and writing a single 1 in the second case. Using the pairing function of Example 1.1.6.(1) the binary operations $+$, $\dot{-}$, and $\cdot$ are also easily seen to be computable. As for $+$ the algorithm takes the input

$$1...101...1$$

and replaces the 0-symbol by an 1 and deletes the rightmost 1.

(3) If R is a computable integral domain, then the polynomial algebras $R[X_1, ..., X_n]$ in arbitrary many indeterminates and $R[X_1, X_2, ...]$ in countably many indeterminates are efficiently presentable R-algebras.

A possible implementation starts by implementing the monoid $\langle M; \cdot; X_i \mid i \in \mathbb{N} \rangle$ and extends it to the R-algebra $R[X_1, X_2, ...]$. Within $R[X_1, X_2, ...]$ the domain of every subalgebra $R[X_1, ..., X_n]$

is decidable and therefore the structure is computable. See the textbook [46, Sec. 4.4] for a more detailed discussion and Appendix A.2 for a sample implementation based on this idea.

(4) In general $\mathbb{Z}$ and every finitely generated free $\mathbb{Z}$-algebra viewed as $\mathcal{L}_{ring}$-structure is efficiently presentable. As for integers, one extends the presentation of $\mathbb{N}$ by a sign-bit.

To present free $\mathbb{Z}$-algebras one uses a basis, say $\xi_1, ..., \xi_n$. Then any element η can be encoded as an n-tuple of integers. Addition and subtraction are defined coordinate-wise. To implement the multiplication one stores the finite multiplication table of the basis elements

	ξ_1	ξ_2	⋯	ξ_n
ξ_1	ξ_1^2	$\xi_1\xi_2$	⋯	$\xi_1\xi_n$
ξ_2	$\xi_2\xi_1$	ξ_2^2	⋯	$\xi_2\xi_n$
⋮	⋮	⋮	⋱	⋮
ξ_n	$\xi_n\xi_1$	$\xi_n\xi_2$	⋯	ξ_n^2

in memory and extends it to all of the $\mathbb{Z}$-algebra linearly.

(5) $\langle \mathbb{N}, \leq \rangle$ is efficiently presentable using the tally encoding and $n \leq m$ if and only if $n \dot{-} m = 0$. So deciding $n \leq m$ boils down to applying floor subtraction and checking whether the tape is empty. Both operations are clearly computable.

It is a natural question whether two efficient presentations of the same model are computably isomorphic, i.e. if there exists a computable isomorphism between them. We will see that the last example differs from the others in this regard. But before studying computable isomorphisms we need a lemma.

LEMMA 1.2.13. *Let $f : Q \to Q'$ be a computable bijection between the problems $Q, Q' \subseteq \omega$. Then the inverse mapping $f^{-1} : Q' \to Q$ is computable as well.*

Proof. Let $x \in Q'$ be given. To find $f^{-1}(x)$ one lists all elements of ω and checks for every $y \in \omega$ whether y is contained in Q. Since Q is decidable, this can be carried out efficiently. If y is not contained in Q, we try the next element in ω. Otherwise, we compute $f(y)$ and check whether $f(y) = x$ holds. In this case, we set $f^{-1}(x) := y$ and are finished. If $f(y)$ does not equal x we take the next element of ω and start over. The process will stop at some point as f is surjective. □

DEFINITION. Let $\mathcal{L}$ be a computable language. A model is called *computably categorical* if it is efficiently presentable and every pair of efficient presentations is computably isomorphic.

In the case of rings of algebraic integers (see Cor. 1.3.12) the following theorem applies and assures us that the decidability of HIO does in fact not depend on the encoding chosen.

THEOREM 1.2.14. *Let R be a finitely generated, efficiently representable ring. Then R is computably categorical.*

This theorem follows from a more general result of Mal'cev [24]. The idea of the proof is to let $\xi_1, ..., \xi_n \in R$ be a set of generators of R over R and let $\varphi_1 : R \to R_1, \varphi_2 : R \to R_2$ be the effi-

cient representations of R together with the respective ring isomorphisms. Then $\varphi_1(\xi_1), ..., \varphi_1(\xi_n)$ generate R_1 over R_1 and $\varphi_2(\xi_1), ..., \varphi_2(\xi_n)$ generate R_2 over R_2. Storing these finitely many values of the isomorphism $\varphi_2 \circ \varphi_1^{-1}$ in memory one can use the computability of R_1 and R_2 respectively to extend the partial mapping in a natural way.

As for the decidability of HIO over some ring of algebraic integers $\mathcal{O}_K$ this means, that if we have two encodings of $\mathcal{O}_K$ that allow to evaluate polynomial expressions, then we can efficiently transform a statement in one encoding into a statement in the other encoding and vice versa.

EXAMPLE 1.2.15. Another example of a computably categorical structure is $\mathfrak{N}$, the $\mathcal{L}_{ring}$-structure of $\mathbb{N}$. To see this let $\mathfrak{N}_1$ and $\mathfrak{N}_2$ be two computable representations of $\mathbb{N}$. A computable isomorphism f between the two structures can be obtained by defining $f(\mathtt{0}^{\mathfrak{N}_1}) := \mathtt{0}^{\mathfrak{N}_2}$ and then recursively

$$f(\mathtt{c}_{n+1}{}^{\mathfrak{N}_1}) := f(\mathtt{c}_n{}^{\mathfrak{N}_1}) + 1^{\mathfrak{N}_2},$$

where $\mathtt{c}_n$ is as before the constant representing the integer n.

Note however, that there are structures where the choice of presentation matters. In fact, $\langle \mathbb{N}, \leq \rangle$ is not computably categorical. A proof using the undecidability of the halting problem can be found in the paper [45, Prob. 1.6].

LEMMA 1.2.16. *Let R be a computable, commutative ring with unity and $\mathfrak{R}$ its $\mathcal{L}_{ring}$-structure. Then the Diophantine theory $\mathtt{H10}(\mathfrak{R})$ is semi-decidable.*

Proof. Since R is computable, $\mathcal{L}_R$ is computable and as a consequence the set of (Gödel numbers of) fully existentially quantified atomic $\mathcal{L}_R$-formulae is decidable.

Let now $\phi = \exists \mathtt{x}_1 : ... : \exists \mathtt{x}_n : \psi(\mathtt{x}_1, ..., \mathtt{x}_n)$ be a fully existentially quantified $\mathcal{L}_R$-formula. By Thm 1.2.8 there exists a polynomial $p \in R[X_1, ..., X_n]$ such that for all $\alpha_1, ..., \alpha_n \in R$ we have that

$$\mathfrak{R} \vDash \psi(\alpha_1, ..., \alpha_n) \quad \Leftrightarrow \quad p(\alpha_1, ..., \alpha_n) = 0.$$

In fact, the polynomial p can be obtained from the Gödel number $\mathrm{gn}(\phi)$ efficiently. Thus, the relation $H \subseteq \omega^2$ defined by

$$H(\mathrm{gn}(\phi), \langle \alpha_1, ..., \alpha_n \rangle) \quad :\Leftrightarrow \quad p(\alpha_1, ..., \alpha_n) = 0$$

is computable and the Diophantine theory $\mathtt{H10}(\mathfrak{R})$ is semi-decidable by Prop. 1.1.8. □

1.3 Prerequisites from number theory

1.3.1 Number fields and rings of algebraic integers

In this section I will closely follow Chapter 1 of the German textbook [29]. However, the content is also present in the English reference [27, Chap. 2], and sometimes the presentation of this reference will be recited. We start with a series of definitions and remind the reader of some important results from algebraic number theory and commutative algebra. But at first let us fix an important notation.

Let R and S be commutative rings with unity. Let $\varphi : R \to S$ be a ring-homomorphism mapping 1_R to 1_S, then S is called an *R-algebra* and we write $a\alpha$ as a short form for $\varphi(a) \cdot \alpha$ ($a \in R$ and

$\alpha \in S$). We are especially interested in the case where $R \subseteq S$ and φ is chosen to be the embedding of R into S. In this situation we denote by $R[\alpha_1, \dots, \alpha_n]$ the smallest ring inside S containing R and all $\alpha_1, \dots, \alpha_n \in S$. Then $R[\alpha_1, \dots, \alpha_n]$ contains all polynomial expressions in $\alpha_1, \dots, \alpha_n$ with coefficients in R, i.e. all elements of the form

$$\sum_{(i_1,\dots,i_n)\in\mathbb{N}^n} a_{i_1,\dots,i_n}\alpha^{i_1}\dots\alpha^{i_n},$$

where only finitely many $a_{i_1,\dots,i_n} \in R$ are non-zero.

DEFINITION. A finite field-extension K of the rationals $\mathbb{Q}$ is called *algebraic number field*. This means that K is a field and at the same time a $\mathbb{Q}$-algebra, that is finite-dimensional viewed as a $\mathbb{Q}$-vector space. The *degree* $[K : \mathbb{Q}]$ is the dimension of K viewed as a $\mathbb{Q}$-vector space.

For convenience we will always assume that K is a subset of the complex pane $\mathbb{C}$.

EXAMPLE 1.3.1. (1) $\mathbb{Q}$ is (up to isomorphism) the only algebraic number field of degree 1.

(2) $\mathbb{Q}[\sqrt{2}] = \left\{a + b\sqrt{2} : a, b \in \mathbb{Q}\right\}$ is an algebraic number field of degree 2. The inverse of $a + b\sqrt{2}$, where not both a and b are 0, is given by $\frac{a-b\sqrt{2}}{a^2-2b^2}$.

(3) $\mathbb{Q}[\sqrt[3]{2}] = \left\{a + b\sqrt[3]{2} + c\sqrt[3]{4} : a, b, c \in \mathbb{Q}\right\}$ is an algebraic number field of degree 3.

Let K/M be an extension of number fields, then K/M is in fact an *algebraic extension*. This means that every $x \in K$ is the root of some non-zero polynomial with coefficients in M. We denote by $\mu_{M,x} \in M[X]$ the monic polynomial with root x dividing (in $M[X]$) all other polynomials with root x. The polynomial $\mu_{M,x}$ is called *minimal polynomial* of x over M. By the minimality condition (w.r.t. divisibility in $M[X]$) on $\mu_{M,x}$ this polynomial must be irreducible.

In fact, every element x in K is algebraic over the rationals $\mathbb{Q}$. Note that the field of all algebraic elements $\overline{\mathbb{Q}}$—called *algebraic closure* of $\mathbb{Q}$—is however not a number field, as the extension $\overline{\mathbb{Q}}/\mathbb{Q}$ is (countably) infinite.

DEFINITION. Let $R \subseteq S$ be commutative rings with unity. Then $\alpha \in S$ is called *integral* over R if it is the root of a monic polynomial with coefficients in R, i.e. if α satisfies an equation of the form

$$\alpha^n + a_{n-1}\alpha^{n-1} + \dots + a_0 = 0$$

for some $n \geq 1$ and some $a_0, \dots, a_{n-1} \in R$. If all elements of S are integral over R then S is called *integral* over R. If R is an integral domain then R is *integrally closed* if for all elements $x \in \mathrm{Quot}(R)$ being integral over R implies $x \in R$.

Of course, if one wants to use tools from algebra some structure on the considered sets is needed. Thus, the following theorem, implying that if $\alpha, \beta \in S$ are algebraic over S, so are their sum and product, is very desirable.

THEOREM 1.3.2. *Let $R \subseteq S$ be commutative rings with unity. Then the elements of S that are integral over R form a subring of S.*

Richard Dedekind gave a proof of this theorem using the following proposition.

PROPOSITION 1.3.3. *Let $R \subseteq S$ be commutative rings with unity. Then $\alpha \in S$ is integral over R if and only if there exists a finitely generated non-zero R-module $M \subseteq S$ such that $\alpha M \subseteq M$, in fact $M = R[\alpha]$ can be chosen.*

Proof of Thm 1.3.2. Let $\alpha, \beta \in S$ be integral over R and let M and N be finitely generated R-modules contained in S such that $\alpha M \subseteq M$ and $\beta N \subseteq N$ hold. We define the product of the two modules as

$$MN := \left\{ \sum_{i=1}^{k} m_i n_i \,:\, k \in \mathbb{N}, m_1, \dots, m_k \in M, n_1, \dots, n_k \in N \right\}.$$

Clearly, MN contains 0 as M (and N) contains 0. Furthermore, it is closed under addition, and the inverse of an element in MN can be found by inverting all $m_i \in M$ (or $n_i \in N$) in the sum. Thus, MN forms a subgroup of S. Note that am_i is contained in M for all $a \in R$ and $m_i \in M$ since M is an R-module. As a consequence,

$$a \sum_{i=1}^{k} m_i n_i = \sum_{i=1}^{k} \underbrace{a m_i}_{\in M} n_i$$

is contained in MN for all $a \in R$ and all $m_1, \dots, m_k \in M$, $n_1, \dots, n_k \in N$, and we can deduce that MN is an R-module.

Let $\{e_1, \dots, e_m\} \subseteq M$ generate M and $\{f_1, \dots, f_n\} \subseteq N$ generate N. Then it is easily seen that the finite set

$$\{e_i f_j \,:\, 1 \leq i \leq m, 1 \leq j \leq n\} \subseteq MN$$

generates MN.

We finish the proof by showing that $\alpha\beta$ and $\alpha \pm \beta$ satisfy $\alpha\beta\, MN \subseteq MN$ and $(\alpha \pm \beta)MN \subseteq MN$ respectively. Then the proposition implies the claim. But this is the case since

$$\alpha\beta \sum_{i=1}^{k} m_i n_i = \sum_{i=1}^{k} \underbrace{\alpha m_i}_{\in M}\ \underbrace{\beta n_i}_{\in N} \in MN$$

holds for all $m_1, \dots, m_k \in M$ and all $n_1, \dots, n_k \in N$, and

$$(\alpha \pm \beta) \sum_{i=1}^{k} m_i n_i = \sum_{i=1}^{k} \underbrace{\alpha m_i}_{\in M}\ n_i \pm \sum_{i=1}^{k} m_i\ \underbrace{\beta n_i}_{\in N} \in MN$$

holds as well. □

Similarly, one can deduce from Prop. 1.3.3 that being integral is a transitive relation on rings. More formally, we have the following proposition.

PROPOSITION 1.3.4. *Let $R \subseteq S \subseteq T$ be commutative rings with unity. If S is integral over R and $\alpha \in T$ is integral over S, then α is integral over R.*

The set $\overline{R}^S$ of all elements of S that are integral over R is called *integral closure* of R in S. By the

theorem above $\overline{R}^S$ is a subring of S.

We will now return our attention from the general case to our specific situation and consider the elements of $\mathbb{C}$ that are integral over $\mathbb{Z}$. These elements are called *algebraic integers* and the integral closure of $\mathbb{Z}$ in $\mathbb{C}$ is denoted by $\mathcal{O}$. Given a number field K, we denote by $\mathcal{O}_K$ the intersection of $\mathcal{O}$ with K. In other words, $\mathcal{O}_K$ is the integral closure of $\mathbb{Z}$ in K. To emphasize that we are considering the ring $\mathbb{Z}$ and not any $\mathcal{O}_K$, we call $\mathbb{Z}$ the ring of *rational integers*.

We have that $\overline{\mathbb{Z}}^{\mathbb{Q}} = \mathcal{O} \cap \mathbb{Q} = \mathbb{Z}$. Thus, $\mathbb{Z}$ is integrally closed. This follows from a more general result stating that factorial rings are integrally closed. By Prop. 1.3.4 this property of $\mathbb{Z}$ extends to all rings of algebraic integers, formally we have $\overline{\mathcal{O}_K}^K = \mathcal{O}_K$. To make the analogue complete we prove that K is the fraction field of $\mathcal{O}_K$ (see Thm 1.3.6). However, even more is true, as one can choose the denominator in the quotient to be a rational integer. More precisely, the following holds.

PROPOSITION 1.3.5. *Let K be a number field and $\mathcal{O}_K$ its ring of algebraic integers. For all $x \in K$ there exists a non-zero rational integer $n \in \mathbb{Z} \setminus \{0\}$ such that their product nx is an algebraic integer.*

THEOREM 1.3.6. *The quotient field of $\mathcal{O}_K$ is (isomorphic to) K for all number fields K.*

Proof. By the proposition above every $x \in K$ can be written as $x = \alpha n^{-1}$, where $\alpha \in \mathcal{O}_K$ is an algebraic and $n \in \mathbb{Z} \setminus \{0\}$ is a rational integer. If $x = \beta m^{-1}$ is another representation of this form, then $\alpha m = \beta n$ must hold in $\mathcal{O}_K$ and thus we can embed K into the quotient field $\mathrm{Quot}(\mathcal{O}_K)$ by mapping $x = \alpha n^{-1}$ to the representative $[\alpha, n] \in \mathrm{Quot}(\mathcal{O}_K)$.

If on the other hand $[\alpha, \beta] \in \mathrm{Quot}(\mathcal{O}_K)$ with $\beta \neq 0$ is given, then $\alpha\beta^{-1}$ an element of K. Thus, there exist $\gamma \in \mathcal{O}_K$ and $n \in \mathbb{Z} \setminus \{0\}$ such that $\gamma n^{-1} = \alpha\beta^{-1}$—or put differently, such that $[\gamma, n] \in \mathrm{Quot}(\mathcal{O}_K)$ is in the same equivalence class as $[\alpha, \beta]$. As a consequence, the embedding defined above is surjective. □

We can now deduce that an element $x \in K$ is an algebraic integer if and only if its minimal polynomial $\mu_{\mathbb{Q},x}$ has rational integral coefficients. Indeed, if x is a root of the monic polynomial $p \in \mathbb{Z}[X]$ then $\mu_{\mathbb{Q},x}$ divides p and thus every root of $\mu_{\mathbb{Q},x}$ is an algebraic integer as well. Now decompose

$$\mu_{\mathbb{Q},x}(X) = \prod_{i=1}^{n}(X - \alpha_i),$$

for some $\alpha_1, \ldots, \alpha_n \in K$, then since $\mathcal{O}_K$ is a ring, the minimal polynomial must have coefficients in $\mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$ and the claim is proven. In fact, we can always find an algebraic integer $\alpha \in K$ that completely determines the number field K.

THEOREM 1.3.7 (PRIMITIVE ELEMENT THEOREM). *Let L/K be an extension of number fields then there exists a* primitive element $\alpha \in \mathcal{O}_L$ *such that $L = K[\alpha]$. Moreover, if $\mu_{K,\alpha} \in K[X]$ is the minimal polynomial of α over K then the degree of $\mu_{K,\alpha}$ and the degree of the field extension L/K coincide. A K-basis of L is given by $\{1, \alpha, \ldots, \alpha^{n-1}\}$, where $n = [L : K]$.*

Important tools for studying number fields and algebraic integers are given by the norm and trace, which are defined below.

DEFINITION. For an extension L/K of number fields and a fixed element $x \in L$ we consider the

linear transformation $\lambda_x : L \to L$ defined by $\lambda_x(z) = xz$ and define the *trace* of x as

$$Tr_{L/K}(x) := Tr(\lambda_x)$$

as well as the *norm* of x as

$$N_{L/K}(x) := \det(\lambda_x).$$

By basic facts from linear algebra, we find that the trace $Tr_{L/K} : L \to K$ is in fact a homomorphism between the additive groups of the number fields and the norm $N_{L/K} : L^* \to K^*$ is in fact a homomorphism between the groups of units.

From the view of Galois theory one can reinterpret the norm and trace as follows.

THEOREM 1.3.8. *Let L/K be an extension of number fields of degree n. Then there exist exactly n embeddings $\sigma_1, \dots, \sigma_n : L \to \mathbb{C}$ that fix K point-wise. Furthermore, for all $x \in L$ we have that*

(i) $Tr_{L/K}(x) = \sum_{i=1}^{n} \sigma_i(x)$, *and*
(ii) $N_{L_K}(x) = \prod_{i=1}^{n} \sigma_i(x)$.

One calls an extension L/K of number fields *normal extension* if the embeddings $\sigma_i : L \to \mathbb{C}$ that fix K point-wise are in fact automorphisms of L. We do however have the following equivalent characterizations as well.

PROPOSITION 1.3.9. *For an extension L/K of number fields the following properties are equivalent.*

(i) *L/K is a normal extension.*
(ii) *If an irreducible polynomial $p \in K[X]$ has one root in L, then p splits in linear factors over L.*
(iii) *L is the splitting field of some irreducible polynomial $p \in K[X]$.*

From the proposition above we see immediately that every extension $K/\mathbb{Q}$ of degree 2 is normal. Moving on to degree 3 this changes as for instance $\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q}$ is not normal. The irreducible polynomial $X^3 - 2 \in \mathbb{Q}[X]$ has the root $\sqrt[3]{2}$ in $\mathbb{Q}[\sqrt[3]{2}]$, but both of the other non-real roots are not contained in the number field. One can however enlarge $\mathbb{Q}[\sqrt[3]{2}]$ to obtain a normal extension. More generally, if L/K is an extension of number fields, then there exists (up to isomorphism) a unique number field $N \supseteq L$, such that the extension N/K is normal. We call N the *normal closure* of the extension. In fact, if $L = K[\alpha]$ then N is the splitting field of $\mu_{K,\alpha}$. Using the normal closure of L/K one can show that norm and trace behave well w.r.t. towers of field extensions.

COROLLARY 1.3.10. *Let $K \subseteq M \subseteq L$ be a tower of extensions of number fields. Then we have*

$$Tr_{L/K} = Tr_{M/K} \circ Tr_{L/M} \quad \text{and} \quad N_{L/K} = N_{M/K} \circ N_{L/M}.$$

We fix an extension L/K of number fields and take another look at Thm 1.3.8. Then we find for an algebraic integer $\alpha \in \mathcal{O}_L$ that its norm $N_{L/K}(\alpha)$ and trace $Tr_{L/K}(\alpha)$ are in fact products and sums of algebraic integers and thus algebraic integers themselves. Now since norm and trace are mappings from L to K we can deduce that both $N_{L/K}(\alpha)$ and $Tr_{L/K}(\alpha)$ are contained in $\mathcal{O}_K$. In particular, we find for all $\alpha \in \mathcal{O}_L$ that $N_{L/\mathbb{Q}}(\alpha)$ and $Tr_{L/\mathbb{Q}}(\alpha)$ are rational integers.

Furthermore, one finds that an algebraic integer $\alpha \in \mathcal{O}_L$ is a unit if and only if its norm $N_{L/K}(\alpha)$ is a unit in $\mathcal{O}_K$. Indeed, if $\beta N_{L/K}(\alpha) = 1$ holds for some algebraic integer $\beta \in \mathcal{O}_K$, we can rewrite

the norm to find that

$$1 = \alpha \underbrace{\beta \prod_{i=2}^{n} \sigma_i(\alpha)}_{\in \mathcal{O}_L}$$

holds, where $\mathrm{id} = \sigma_1, \dots, \sigma_n$ denote all the complex embeddings of L that fix K point-wise. In the special case that $K = \mathbb{Q}$ we find that $\alpha \in \mathcal{O}_L$ is a unit if and only if $N_{L/\mathbb{Q}}(\alpha)$ is ± 1.

As a next step we will further investigate the algebraic structure of $\mathcal{O}_K$.

THEOREM 1.3.11. *Let K be an algebraic number field. Then $\mathcal{O}_K$ is a finitely generated free $\mathbb{Z}$-module.*

We call a module-basis of $\mathcal{O}_L$ over $\mathcal{O}_K$ an *integral basis* of L over K. In particular, we can deduce that $\mathcal{O}_L$ is a finitely generated free $\mathbb{Z}$-module by setting $K = \mathbb{Q}$ in the theorem above. Every integral basis $\{\xi_1, \dots, \xi_n\} \subseteq \mathcal{O}_L$ is in fact a vector space basis of L over K as well, thus its cardinality must coincide with the degree of the extension. Note however, that not every K-basis of L containing only algebraic integers is an integral basis of L over K. In full generality it is hard to find an integral basis, but once the basis is known the structure of $\mathcal{O}_L$ behaves very nicely with respect to computability, which is the content of the following corollary.

COROLLARY 1.3.12. *Let K be a number field and $\mathcal{O}_K$ its ring of algebraic integers. Then $\mathcal{O}_K$ is an efficiently presentable and computably categorical $\mathcal{L}_{ring}$-structure.*

Proof. By the theorem above $\mathcal{O}_K$ is a finitely generated free $\mathbb{Z}$-module. In fact, it even carries a $\mathbb{Z}$-algebra structure. Thus, it is efficiently presentable by Example 1.2.12.(4). Since $\mathcal{O}_K$ is a ring with unity, it is finitely generated and as a consequence of Thm 1.2.14 $\mathcal{O}_K$ is computably categorical. □

1.3.2 Ideals of $\mathcal{O}_K$

We view algebraic integers as generalizations of rational integers. Given a fixed algebraic integer α one can show using induction on the absolute value of its norm $N_{K/\mathbb{Q}}(\alpha)$ that α decomposes into a product of irreducible elements. However, unlike in the case of rational integers this decomposition is not unique. Indeed, in $\mathbb{Q}[i\sqrt{5}]$ one can decompose

$$21 = 3 \cdot 7 = (1 + i2\sqrt{5}) \cdot (1 - i2\sqrt{5}),$$

where $3, 7, 1 + i2\sqrt{5}$ and $1 - i2\sqrt{5}$ are irreducible and pair-wise non-associated algebraic integers.[7]

It was the idea of German mathematician Ernst Eduard Kummer to generalize the prime decomposition to 'ideal numbers'. In his view, there should be ideal primes $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3$ and $\mathfrak{p}_4$ such that

$$3 = \mathfrak{p}_1\mathfrak{p}_2, \quad 7 = \mathfrak{p}_3\mathfrak{p}_4, \quad 1 + 2\sqrt{-5} = \mathfrak{p}_1\mathfrak{p}_3, \text{ and } 1 - 2\sqrt{-5} = \mathfrak{p}_2\mathfrak{p}_4$$

then

$$21 = (\mathfrak{p}_1\mathfrak{p}_2)(\mathfrak{p}_3\mathfrak{p}_4) = (\mathfrak{p}_1\mathfrak{p}_3)(\mathfrak{p}_2\mathfrak{p}_4)$$

and the decomposition is again unique.

[7] For full details see the first example in [29, Chap. 1, § 3].

Since divisibility by a fixed number $n \in \mathbb{Z}$ gives rise to a congruence relation $m_1 \equiv m_2 \mod n$ defined by $n \mid m_1 - m_2$, it is quite natural—and was indeed carried out by Richard Dedekind—to view these 'ideal numbers' as congruence relations on $\mathcal{O}_K$. Then the equivalence class containing 0 is an *ideal* in the sense of modern abstract algebra and 'divisibility' of ideals $\mathfrak{a}$ by $\mathfrak{b}$ can be replaced by the inclusion of sets $\mathfrak{a} \subseteq \mathfrak{b}$. On the other hand, for a given ideal $\mathfrak{a}$ we get back to the congruence if we define $\alpha \equiv \beta \mod \mathfrak{a}$ by $\alpha - \beta \in \mathfrak{a}$.

Compare this to the well known case of rational integers. Here every ideal is a principal ideal. Thus, there exist $\alpha, \beta \in \mathbb{Z}$ such that $\mathfrak{a} = (\alpha)$ and $\mathfrak{b} = (\beta)$ and α is divisible by β if and only if $\mathfrak{a} \subseteq \mathfrak{b}$.

As with rational integers, one can define addition and multiplication of ideals by

$$\mathfrak{a} + \mathfrak{b} := \{\alpha + \beta : \alpha \in \mathfrak{a}, \beta \in \mathfrak{b}\}, \text{ and}$$
$$\mathfrak{a}\mathfrak{b} := \left\{ \sum_{i=0}^{n} \alpha_i \beta_i : n \in \mathbb{N}, \alpha_0, \alpha_1, \dots, \alpha_n \in \mathfrak{a}, \beta_0, \beta_1, \dots, \beta_n \in \mathfrak{b} \right\}.$$

It is easy to prove that sums and products of ideals are again ideals. In fact, the set of all ideals of $\mathcal{O}_K$ is a monoid with respect to multiplication, where the neutral element is given by $\mathcal{O}_K = (1)$. However, unlike in the case of rational integers we have that

$$\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{a}, \mathfrak{b} \subseteq \mathfrak{a} + \mathfrak{b}$$

and thus that

$$\mathfrak{a}, \mathfrak{b} \mid \mathfrak{a}\mathfrak{b} \quad \text{and} \quad \mathfrak{a} + \mathfrak{b} \mid \mathfrak{a}, \mathfrak{b}.$$

Before we can further study divisibility of ideals, we need to investigate the algebraic properties of rings of algebraic integers $\mathcal{O}_K$.

DEFINITION. An integral domain D is called *Dedekind domain* if D is Noetherian—i.e. every ideal of D is finitely generated—integrally closed, and every non-zero prime ideal $\mathfrak{p} \subseteq D$ is a maximal ideal.

To study the ideals of algebraic integers the following theorem is essential.

THEOREM 1.3.13. *Let K be a number field. Then its ring of algebraic integers $\mathcal{O}_K$ is a Dedekind domain.*

Note that for two ideals $(0) \subsetneq \mathfrak{a}, \mathfrak{b} \subsetneq \mathcal{O}_K$, the sum $\mathfrak{a} + \mathfrak{b}$ is the smallest (w.r.t. set-inclusion) ideal containing both $\mathfrak{a}$ and $\mathfrak{b}$. Indeed, if $\mathfrak{c}$ contains $\mathfrak{a}$ and $\mathfrak{b}$ then it contains all sums of elements in $\mathfrak{a}$ and $\mathfrak{b}$. As a consequence, we call $\mathfrak{a} + \mathfrak{b}$ the *greatest common divisor* of $\mathfrak{a}$ and $\mathfrak{b}$.

Similarly, the intersection $\mathfrak{a} \cap \mathfrak{b}$ is the greatest ideal of $\mathcal{O}_K$ contained in both $\mathfrak{a}$ and $\mathfrak{b}$. Thus, we call $\mathfrak{a} \cap \mathfrak{b}$ the *least common multiple* of the ideals $\mathfrak{a}$ and $\mathfrak{b}$. Before we study the role of prime ideals with respect to this notion of divisibility, an example is in order.

EXAMPLE 1.3.14. Consider the ring of rational integers $\mathbb{Z}$ and fix two integers $n_1, n_2 \in \mathbb{Z}$. We denote by d their greatest common divisor and by m their least common multiple. As for their principal

ideals the following hold

$$(n_1) \cap (n_2) = n_1\mathbb{Z} \cap n_2\mathbb{Z} = \{n \in \mathbb{Z} : n_1 \mid n \text{ and } n_2 \mid n\} = \{n \in \mathbb{Z} : m \mid n\} = (m),$$
$$(n_1)(n_2) = \left\{\sum_{i=0}^{n} \alpha_i\beta_i : n \in \mathbb{N}, \alpha_0, \alpha_1, \dots, \alpha_n \in n_1\mathbb{Z}, \beta_0, \beta_1, \dots, \beta_n \in n_2\mathbb{Z}\right\} =$$
$$= \left\{\sum_{i=0}^{n} n_1k_in_2\ell_i : n \in \mathbb{N}, k_0, k_1, \dots, k_n, \ell_0, \ell_1, \dots, \ell_n \in \mathbb{Z}\right\} = (n_1n_2),$$

and using Bézout's identity

$$(n_1) + (n_2) = \{\alpha + \beta : \alpha \in (n_1), \beta \in (n_2)\} = \{n_1k + n_2\ell : k, \ell \in \mathbb{Z}\} = (d).$$

Thus, in the case of rational integers greatest common divisor and least common multiple have their intended meaning if one replaces integers n with their respective principal ideals (n).

THEOREM 1.3.15. *Let $\mathcal{O}_K$ be the ring of of algebraic integers in some number field K and let $\mathfrak{a} \subsetneq \mathcal{O}_K$ be a non-zero ideal. Then there exist up to reordering unique prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_n \subseteq \mathcal{O}_K$ such that*

$$\mathfrak{a} = \mathfrak{p}_1 \dots \mathfrak{p}_n.$$

Combining multiple occurrences of the same prime ideal in the decomposition described in the theorem, one writes

$$\mathfrak{a} = \prod_{\substack{\mathfrak{p} \subseteq \mathcal{O}_K \\ \mathfrak{p} \text{ prime ideal}}} \mathfrak{p}^{\nu_\mathfrak{p}},$$

where all $\nu_\mathfrak{p}$ are a non-negative integers and all but finitely many exponents are zero.[8] Using this product notation of the prime decomposition of ideals, one obtains for

$$\mathfrak{a} = \prod_{\substack{\mathfrak{p} \subseteq \mathcal{O}_K \\ \mathfrak{p} \text{ prime ideal}}} \mathfrak{p}^{\nu_\mathfrak{p}} \quad \text{and} \quad \mathfrak{b} = \prod_{\substack{\mathfrak{p} \subseteq \mathcal{O}_K \\ \mathfrak{p} \text{ prime ideal}}} \mathfrak{p}^{\mu_\mathfrak{p}},$$

that their greatest common divisor has the factorization

$$\mathfrak{a} + \mathfrak{b} = \prod_{\substack{\mathfrak{p} \subseteq \mathcal{O}_K \\ \mathfrak{p} \text{ prime ideal}}} \mathfrak{p}^{\min(\nu_\mathfrak{p}, \mu_\mathfrak{p})}.$$

Thus, if $\mathfrak{a} + \mathfrak{b} = (1)$, we say $\mathfrak{a}$ and $\mathfrak{b}$ are *relative prime*.

If we notice that the product of ideals $\mathfrak{a} = \mathfrak{a}_1 \dots \mathfrak{a}_n$, where the $\mathfrak{a}_i$ are pair-wise relative prime, is

[8] The constructivist reader will be pleased to hear that since all ideals of $\mathcal{O}_K$ are finitely generated by Thm 1.3.13, the ring $\mathcal{O}_K$ contains only countably many prime ideals. Thus, one can fix a linear order on the set of prime ideals, such that for all ideals $\mathfrak{a} \subseteq \mathcal{O}_K$ all non-zero exponents $\nu_\mathfrak{p}$ appear in a finite initial segment of the order.

equal to the intersection

$$\mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{a}_i,$$

we have all the tools at hand to restate another important property of the integers.

THEOREM 1.3.16 (CHINESE REMAINDER THEOREM). *Let $\mathfrak{a}_1, \dots, \mathfrak{a}_n \subseteq \mathcal{O}_K$ ideals, which are pairwise relative prime, and let $\mathfrak{a} = \cap_{i=1}^{n} \mathfrak{a}_i$. Then the following isomorphism of rings holds*

$$\mathcal{O}_K/\mathfrak{a} \;\cong\; \bigoplus_{i=1}^{n} \mathcal{O}_K/\mathfrak{a}_i.$$

Proof. We consider the ring-homomorphism $\varphi : \mathcal{O}_K \to \bigoplus_{i=1}^{n} \mathcal{O}_K/\mathfrak{a}_i$ defined by

$$\alpha \mapsto (\alpha + \mathfrak{a}_i)_{i=1}^{n}.$$

Its kernel is given by $\mathfrak{a} = \cap_{i=1}^{n} \mathfrak{a}_i$. Thus, it suffices to prove that φ is surjective. For this we proceed by induction on n. If $n = 1$, then the claim is trivial. Thus, we consider the case $n = 2$. Then we can find $\beta_1 \in \mathfrak{a}_1$ and $\beta_2 \in \mathfrak{a}_2$ such that $1 = \beta_1 + \beta_2$. In other words, we find $\beta_1, \beta_2 \in \mathcal{O}_K$ such that

$$\beta_i \equiv 1 \mod \mathfrak{a}_{3-i} \quad \text{and} \quad \beta_i \equiv 0 \mod \mathfrak{a}_i$$

hold simultaneously for $i \in \{1, 2\}$. If now an arbitrary element $(x_1 + \mathfrak{a}_1, x_2 + \mathfrak{a}_2) \in \mathcal{O}_K/\mathfrak{a}_1 \times \mathcal{O}_K/\mathfrak{a}_2$ is given then

$$x := x_1\beta_2 + x_2\beta_1$$

has the property that $x \equiv x_i \mod \mathfrak{a}_i$ holds for $i \in \{1, 2\}$. Thus, we have found that φ is surjective for $n = 2$.

Let now $n \geq 2$ and note that we have the isomorphism of direct sums

$$\bigoplus_{i=1}^{n} \mathcal{O}_K/\mathfrak{a}_i \;\cong\; \mathcal{O}_K/\mathfrak{a}_n \times \bigoplus_{i=1}^{n-1} \mathcal{O}_K/\mathfrak{a}_i.$$

If we set $\mathfrak{b} := \mathfrak{a}_1 \dots \mathfrak{a}_{n-1}$ then by the induction hypothesis the factor rings $\mathcal{O}_K/\mathfrak{b}$ and $\bigoplus_{i=1}^{n-1} \mathcal{O}_K/\mathfrak{a}_i$ are isomorphic. Thus, we can deduce that

$$\bigoplus_{i=1}^{n} \mathcal{O}_K/\mathfrak{a}_i \;\cong\; \mathcal{O}_K/\mathfrak{a}_n \times \mathcal{O}_K/\mathfrak{b}$$

holds. To conclude the proof note that the ideals $\mathfrak{a}_n$ and $\mathfrak{b} := \mathfrak{a}_1 \dots \mathfrak{a}_{n-1}$ are relative prime. Now by our observation for the case $n = 2$, we find that the mapping $\tilde{\varphi} : \mathcal{O}_K \to \mathcal{O}_K/\mathfrak{a}_n \times \mathcal{O}_K/\mathfrak{b}$ defined by

$$\alpha \mapsto (\alpha + \mathfrak{a}_n, \alpha + \mathfrak{b})$$

is surjective and has kernel $\mathfrak{a}_n \cap \mathfrak{b} = \mathfrak{a}$. By the reduction steps observed above the claim holds. □

Remark. Let $\mathfrak{a}_1, \dots, \mathfrak{a}_n$ be pair-wise relative prime. Then the Chinese remainder theorem tells us, that the collection of congruences

$$x \equiv a_1 \mod \mathfrak{a}_1, \ \dots, \ x \equiv a_n \mod \mathfrak{a}_n$$

can be solved simultaneously. Indeed, in the proof of the theorem we have shown that the ring-homomorphism $\varphi : \mathcal{O}_K \to \bigoplus_{i=1}^{n} \mathcal{O}_K/\mathfrak{a}_i$ defined by

$$x \mapsto (x + \mathfrak{a}_i)_{i=1}^{n}$$

is a surjection and thus the n-tuple $(a_1 + \mathfrak{a}_1, \dots, a_n + \mathfrak{a}_n)$ is the image of some $x \in \mathcal{O}_K$. In other words, there exists an $x \in \mathcal{O}_K$ such that $x \equiv a_i \mod \mathfrak{a}_i$ for all $1 \leq i \leq n$.

In the field of rational numbers one can extend the prime decomposition of integers to a composition of positive rationals by allowing for negative powers of primes. As for ideals there exists a similar construction.

DEFINITION. A $\mathcal{O}_K$-submodule $\mathfrak{m}$ of K is called *fractional ideal* of K if there exists an algebraic integer $\alpha \in \mathcal{O}_K \setminus \{0\}$ such that $\alpha\mathfrak{m} \subseteq \mathcal{O}_K$.

Let $x := \alpha/\beta \in K$, where $\alpha, \beta \in \mathcal{O}_K$ and $\beta \neq 0$, then $x\mathcal{O}_K := \beta^{-1}(\alpha\mathcal{O}_K)$ is called the *principal fractional ideal* generated by x.

As with usual ideals every non-zero fractional ideal $\mathfrak{m}$ can be written as

$$\mathfrak{m} = \prod_{\substack{\mathfrak{p} \subseteq \mathcal{O}_K \\ \mathfrak{p} \text{ prime ideal}}} \mathfrak{p}^{\nu_\mathfrak{p}},$$

where $\nu_\mathfrak{p} \in \mathbb{Z}$ and all but finitely many exponents are zero.

To conclude this subsection we consider the principal ideals (p) generated by rational primes $p \in \mathbb{Z}$. But first let us have a look at an example. It is easy to deduce that the equality

$$(21) = (3)(7) = (1 + i2\sqrt{5})(1 - i2\sqrt{5}),$$

of principal ideals holds in $K = \mathbb{Q}[i\sqrt{5}]$ by plugging-in the definition of products of ideals. Thus, neither (3) nor (7) can be prime ideals in $\mathcal{O}_K$. We do however know that no other rational prime can divide these principal ideals. More formally we have

PROPOSITION 1.3.17. *Let $\mathfrak{p} \neq (0)$ be a prime ideal in the ring of algebraic integers of some number field K. Then there exists a unique rational prime $p \in \mathbb{Z}$ such that $\mathfrak{p}$ divides the principal ideal $(p) = p\mathcal{O}_K$.*

For a short argrument proving the proposition see the proof of Thm 3.1 in the textbook [29].

1.3.3 Geometry of numbers

In this section we want to study approximations of real numbers by rational quantities. The first main result will be Minkowski's theorem on convex bodies (1.3.18), which can be applied to prove Di-

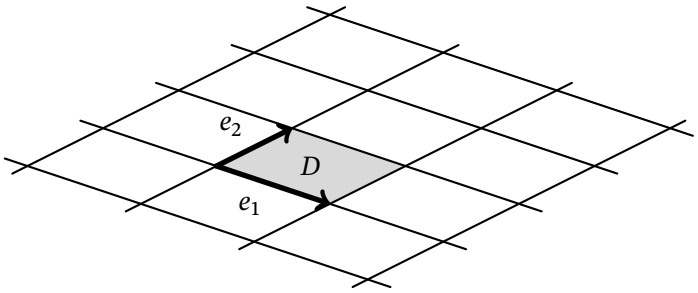


Figure 1.8: A lattice in $\mathbb{R}^2$ and its fundamental parallelepiped D

richlet's unit theorem (1.3.21). The second main result is Kronecker's approximation theorem (1.3.25), whose proof is presented as in Chap. 2 of the textbook [19].

Let $e_1, \dots, e_n \in \mathbb{R}^n$ be a collection of linearly independent vectors over $\mathbb{R}$, then the free abelian group

$$\Lambda = \mathbb{Z}e_1 + \dots + \mathbb{Z}e_n$$

is called a *lattice* and its elements are *lattice points*. The set of generators $\{e_1, \dots, e_n\}$ is called *basis* of Λ. Note that $\mathbb{Z} + \sqrt{2}\mathbb{Z}$ is not a lattice in this sense, because 1 and $\sqrt{2}$ are linearly dependent over $\mathbb{R}$.

The basis $\{e_1, \dots, e_n\}$ of a lattice Λ is not unique. For instance, a second basis is given by the elements $\{e_1 + e_2, e_2, \dots, e_n\}$. However, if $\{f_1, \dots, f_n\}$ is another basis then the $n \times n$-matrix $C := (c_{ij})_{1 \le i,j \le n}$ defined by

$$f_i = \sum_{j=1}^{n} c_{ij} e_j$$

has rational integral coefficients and is invertible. Thus, the determinant of C is either -1 or 1.

Let Vol be the measure corresponding to the usual euclidean volume[9] on $\mathbb{R}^n$. Then for a fixed lattice $\Lambda = \mathbb{Z}e_1 + \dots + \mathbb{Z}e_n$ in $\mathbb{R}^n$ the *fundamental parallelepiped*

$$D = \left\{ \sum_{i=1}^{n} \alpha_i e_i \,:\, \alpha_i \in [0,1] \right\}$$

has the volume

$$\mathrm{Vol}(D) = |\det(e_1, \dots, e_n)|.$$

Note that the fundamental parallelepiped D does depend on the choice of basis, whereas its volume $\mathrm{Vol}(D)$ is an invariant of the lattice. This is because the determinant of the matrix for change of bases has absolute value one. A lattice Λ in $\mathbb{R}^2$ and its fundamental parallelepiped are depicted in Fig. 1.8. All elements of Λ appear at intersection of the lines.

We have now all tools at hand to state our first main result. The following proof is presented as in Thm. 4.4 of the textbook [29].

THEOREM 1.3.18 (MINKOWSKI'S THEOREM ON CONVEX BODIES). *Let $\Lambda = \mathbb{Z}e_1 + \dots + \mathbb{Z}e_n$ be a*

[9] More specifically, Vol denotes the Lebesgue measure on $\mathbb{R}^n$. Since the Lebesgue measure is translation invariant, Vol is also the Haar measure with respect to the locally compact, abelian group $\langle \Lambda, + \rangle$.

lattice in the n-dimensional $\mathbb{R}$-vector space V and let D denote its fundamental parallelepiped. If $T \subseteq V$ is convex and symmetric in the origin, i.e. $\alpha \in T$ implies $-\alpha \in T$, and

$$\mathrm{Vol}(T) > 2^n \,\mathrm{Vol}(D).$$

Then T contains a non-zero lattice point $\gamma \in \Lambda \setminus \{0\}$.

Proof. We prove that there exist two distinct lattice points $\gamma_1, \gamma_2 \in \Lambda$ such that the intersection of sets

$$\left(\tfrac{1}{2}T + \gamma_1\right) \cap \left(\tfrac{1}{2}T + \gamma_2\right)$$

is non-empty. If this is the case then there exist $x_1, x_2 \in T$ such that

$$\tfrac{1}{2}x_1 + \gamma_1 = \tfrac{1}{2}x_2 + \gamma_2$$

and thus

$$0 \neq \gamma := \gamma_1 - \gamma_2 = \tfrac{1}{2}(x_2 - x_1)$$

lies in $T \cap \Lambda$, since it is the centre of the line segment between x_1 and $x_2 \in T$.

To obtain a contradiction assume that the members of the family of sets $\left(\tfrac{1}{2}T + \gamma\right)_{\gamma\in\Lambda}$ are pairwise disjoint. Then their intersections $D \cap \left(\tfrac{1}{2}T + \gamma\right)$ with the fundamental parallelepiped D are pairwise disjoint as well. It follows that

$$\mathrm{Vol}(D) \geq \sum_{\gamma\in\Lambda} \mathrm{Vol}\left(D \cap \left(\tfrac{1}{2}T + \gamma\right)\right).$$

On the other hand, since the euclidean volume is invariant under translation, we find that

$$\mathrm{Vol}\left(D \cap \left(\tfrac{1}{2}T + \gamma\right)\right) = \mathrm{Vol}\left((D - \gamma) \cap \left(\tfrac{1}{2}T\right)\right)$$

Furthermore, the sets $D - \gamma$ cover all of $\mathbb{R}^n$ and therefore all of $\frac{1}{2}T$ as well. Finally, we conclude that

$$\mathrm{Vol}(D) \geq \sum_{\gamma\in\Lambda} \mathrm{Vol}\left((D - \gamma) \cap \left(\tfrac{1}{2}T\right)\right) = \mathrm{Vol}\left(\tfrac{1}{2}T\right) = \frac{1}{2^n}\,\mathrm{Vol}(T),$$

which contradicts our assumption on the volume of T. □

Note that the approximation of $\mathrm{Vol}(T)$ cannot be improved as for instance the open square $\{(x, y) \in \mathbb{R}^2 : |x|, |y| < 1\}$ has volume 2^2 but contains no non-zero lattice point of the two-dimensional lattice $(1, 0)\mathbb{Z} + (0, 1)\mathbb{Z}$.

We will now use Minkowski's theorem to reprove an old result of Lagrange, that is of utmost importance to our task of settling Hilbert's tenth problem. The proof is taken from Remark 4.20 of Milne's lecture notes [27]. But first we need a lemma.

LEMMA 1.3.19. *Let $\Lambda \subseteq \Lambda'$ be two lattices in $\mathbb{R}^n$ and let D and D' be one of their respective fundamental parallelepipeds. Then*

$$\mathrm{Vol}(D) = \mathrm{Vol}(D')[\Lambda' : \Lambda]$$

holds, where $[\Lambda' : \Lambda] = |\Lambda'/\Lambda|$ denotes the index of Λ in Λ'.

For the proof of the proposition it will be convenient to identify the free abelian group $a_1\mathbb{Z} \times \ldots \times a_n\mathbb{Z}$ with the lattice generated by the basis $\{a_1e_1, \ldots, a_ne_n\} \subseteq \mathbb{R}^n$, where e_i denotes the i-th vector of the standard basis of $\mathbb{R}^n$.

PROPOSITION 1.3.20 (LAGRANGE'S FOUR-SQUARE THEOREM). *Every non-negative integer is the sum of four squares of integers.*

Proof. The integers 0, 1 and 2 can be written as

$$0 = 0^2 + 0^2 + 0^2 + 0^2, \quad 1 = 1^2 + 0^2 + 0^2 + 0^2, \text{ and } 2 = 1^2 + 1^2 + 0^2 + 0^2.$$

Thus, we may assume that $n > 2$. Furthermore, the set of integers representable as sum of four squares is closed under multiplication as

$$\begin{aligned}(a_1^2 + a_2^2 + a_3^2 + a_4^2)(b_1^2 + b_2^2 + b_3^2 + b_4^2) = \\ (a_1b_1 - a_2b_2 - a_3b_3 - a_4b_4)^2 + (a_1b_2 + a_2b_1 + a_3b_4 - a_4b_3)^2 + \\ (a_1b_3 - a_2b_4 + a_3b_1 + a_4b_2)^2 + (a_1b_4 + a_2b_3 - a_3b_2 + a_4b_1)^2\end{aligned}$$

holds. Hence, all that is left is to prove the claim for odd primes.

For a fixed odd prime p the squares of an integer m take exactly $(p+1)/2$ distinct values modulo p when m runs through $0, 1, \ldots, p-1$. Indeed, note that

$$m \equiv -(p-m) \mod p \quad \text{and} \quad m^2 \equiv (p-m)^2 \mod p$$

hold for all $m \in \{0, 1, \ldots, p-1\}$. Thus, we obtain $(p-1)/2$ pairs of numbers $(m, p-m)$ with the same square modulo p, plus the value $0 = 0^2$ when m runs through $0, 1, \ldots, p-1$.

By the same argument $-n^2 - 1$ runs through exactly $(p+1)/2$ distinct values modulo p for $0 \leq n \leq p-1$ as well. Hence, by the pigeonhole principle there exist integers $m, n \in \{0, 1, \ldots, p-1\}$ solving the congruence

$$m^2 + n^2 + 1 \equiv 0 \mod p.$$

For a fixed solution (m, n) of the above congruence, we consider the set Λ of all integral solutions $(a, b, c, d) \in \mathbb{Z}^4$ of the simultaneous congruence

$$c \equiv ma + nb \mod p \quad \text{and} \quad d \equiv mb - na \mod p.$$

It is not hard to see, that Λ is in fact a (free abelian) subgroup of $\mathbb{Z}^4$ of rank 4 and thus can be considered as an lattice. As (p, p, p, p) is a solution of the congruences, we find that $p\mathbb{Z}^4 \subseteq \Lambda$ is a subgroup of Λ. Considering the quotient $\Lambda/p\mathbb{Z}^4$ we note that a and b can be chosen arbitrarily modulo p, but then c and d are uniquely determined. Thus, the index $[\Lambda : p\mathbb{Z}^4]$ equals p^2. We conclude that the index $[\mathbb{Z}^4 : \Lambda]$ equals p^2 as well and by the previous lemma the volume $\mathrm{Vol}(D)$

of a fundamental parallelepiped D of Λ is $1 \cdot p^2$.

Consider the closed four-dimensional ball T of radius r around the origin. Its volume is $\pi^2 r^4/2$ and if we choose $2p > r^2 > 4\sqrt{2}p/\pi$ then

$$\mathrm{Vol}(T) > 16p^2 = 2^4 \,\mathrm{Vol}(D)$$

holds. By Minkowski's theorem there exists a non-zero lattice point $(a, b, c, d) \in (\Lambda \cap T) \setminus \{0\}$. Since (a, b, c, d) is in Λ, we know that

$$\begin{aligned} a^2 + b^2 + c^2 + d^2 &\equiv a^2 + b^2 + (ma + nb)^2 + (mb - na)^2 \\ &\equiv a^2(m^2 + n^2 + 1) + b^2(m^2 + n^2 + 1) \equiv 0 \mod p \end{aligned}$$

holds. On the other hand, since (a, b, c, d) is in T, we have that

$$a^2 + b^2 + c^2 + d^2 < 2p$$

and $p = a^2 + b^2 + c^2 + d^2$ is the desired representation. □

We now want to give a structural description of the group of units $U_K := \mathcal{O}_K^*$ of a number field K. It is easy to see that all algebraic integers $\zeta \in \mathcal{O}_K$ with finite order, say $k \in \mathbb{N}$, are roots of unity. Indeed, the property $\zeta^k = 1$ shows that ζ is a k-th root of unity. The set of all roots of unity $\zeta \in U_K$ is denoted by $\mu(K)$. If one can show, that $\mu(K)$ is finite then $\mu(K)$ is a cyclic subgroup of K^*.

By the fundamental theorem of finitely generated abelian groups, we know that every finitely generated abelian group G is isomorphic to $G_{tors} \times \mathbb{Z}^t$, where G_{tors} is the finite subgroup of elements with finite order, called the *torsion part* of G, and $t \in \mathbb{N}$ is called the *free rank* of G, denoted by $\mathrm{rk}\, G = t$. Thus, if U_K is finitely generated then its torsion part is $\mu(K)$ and all that is left to fully describe U_K is finding its free rank. This classification is the content of the following important theorem.

THEOREM 1.3.21 (DIRICHLET'S UNIT THEOREM). *Let K be a number field of degree n over the rationals $\mathbb{Q}$. If r is the number of real embeddings $\sigma : K \to \mathbb{R}$ of K then $s := (n - r)/2$ is the number of pairs of complex-conjugate embeddings $\sigma, \overline{\sigma} : K \to \mathbb{C}$. In this case the group of units U_K is isomorphic to*

$$\mu(K) \times \mathbb{Z}^{r+s-1}.$$

In other words, Dirichlet's theorem states that there exists a collection of units $u_1, \ldots, u_{r+s-1} \in U_K$, called *fundamental system of units*, such that every unit $u \in U_K$ can be written as

$$u = \zeta u_1^{m_1} \ldots u_{r+s-1}^{m_{r+s-1}}$$

where $\zeta \in \mu(K)$ is a root of unity and $m_i \in \mathbb{Z}$ is a rational integer for all $i \in \{1, \ldots, r + s - 1\}$.

A full proof of the theorem exceeds the scope of this thesis, but among others Chap. 5 of the textbook [27] and Chap. 1, §7 of the German reference [29] contain proofs based on Minkowski's theorem. The idea is to consider the mapping $\Sigma : K \to \mathbb{R}^r \times \mathbb{C}^s$ defined by

$$\Sigma(x) := (\sigma_1(x), \ldots, \sigma_r(x), \sigma_{r+1}(x), \ldots, \sigma_{r+s}(x)),$$

where $\sigma_1, \dots, \sigma_r$ are all real embeddings of K and $\sigma_{r+1}, \overline{\sigma}_{r+1}, \dots, \sigma_{r+s}, \overline{\sigma}_{r+s}$ are all non-real embeddings. Then Σ preserves sums and we obtain a group-homomorphism by taking logarithms. More formally, we consider $L : K^* \to \mathbb{R}^{r+s}$ defined by

$$L(x) := (\log|\sigma_1(x)|, \dots, \log|\sigma_r(x)|, \log|\sigma_{r+1}(x)|, \dots, \log|\sigma_{r+s}(x)|).$$

Now, since the norm $N_{K/\mathbb{Q}}(u)$ is ± 1 for every unit $u \in U_K$, we know that

$$|\sigma_1(u)|\dots|\sigma_r(u)||\sigma_{r+1}(u)|^2\dots|\sigma_{r+s}(u)|^2 = 1$$

and upon taking the logarithm we have that

$$\log|\sigma_1(u)| + \dots + \log|\sigma_r(u)| + 2\log|\sigma_{r+1}(u)| + \dots + 2|\sigma_{r+s}(u)| = 0.$$

In other words, the image $L(U_K)$ is contained in the hyperplane H defined by

$$H : x_1 + \dots + x_r + 2x_{r+1} + \dots + 2x_{r+s} = 0,$$

which is an $r+s-1$-dimensional $\mathbb{R}$-vector space. The key to proving Dirichlet's theorem is showing that $L(U_K)$ can be considered as an $r+s-1$-dimensional lattice in H.

We will now turn our attention to approximations of real numbers by the rationals and start with a result of Dirichlet. Dirichlet's direct proof makes use of the pigeonhole principle. In fact, it was he who popularized this simple combinatorial fact by giving it its German name „Schubfachprinzip". However, we base our proof on Minkowski's theorem.

THEOREM 1.3.22 (DIRICHLET'S APPROXIMATION THEOREM). *For each real number $\alpha \in \mathbb{R}$ and each integer $N > 1$ there exist integers $n, p \in \mathbb{Z}$ with $0 < n \leq N$ such that*

$$|n\alpha - p| < \frac{1}{N}$$

holds.

Proof. Consider the set

$$T := \left\{(x, y) \in \mathbb{R}^2 : -N - \tfrac{1}{2} \leq x \leq N + \tfrac{1}{2}, |\alpha x - y| \leq \frac{1}{N}\right\}.$$

If we can prove that T contains a non-zero integral tuple $(n, p) \in \mathbb{Z}^2$, we are done, as if $n < 0$ we can replace p by $-p$ as well as n by $-n$ and have found the claimed approximation. Note that n cannot be zero, as otherwise since $1/N$ is smaller than one, p must be zero as well.

As was mentioned before, we want to apply Minkowski's theorem and thus need to check that T is convex and symmetric in the origin. Symmetry is satisfied as the first condition on x is symmetric and the second condition is invariant under replacing (x, y) by $(-x, -y)$. Geometrically, T is a ribbon of width $2/N$ around the graph of $f(x) = \alpha x$ between the perpendicular lines at $\pm(N + 1/2)$. In Fig. 1.9 the set T is represented by the shaded area, the thick line represents the function f and the

dashed lines mark the area where the condition

$$-N - \tfrac{1}{2} \leq x \leq N + \tfrac{1}{2}$$

is met.[10] We need to prove that T contains a non-zero lattice point $\gamma \in \mathbb{Z}^2$. But this is now easy as by our geometrical observation T is convex and its area is equal to

$$\mathrm{Vol}(T) = \frac{2}{N}(2N+1) = 4 + \frac{2}{N} > 4$$

and Minkowski's theorem implies the existence of the claimed lattice point. □

Using the set

$$T := \left\{(x, y_1, \dots, y_k) \in \mathbb{R}^{1+k} \,:\, -N^k - \tfrac{1}{2} \leq x \leq N^k + \tfrac{1}{2}, |\alpha_i x - y_i| \leq \frac{1}{N}\right\},$$

one proves completely analogously the multidimensional version of Dirichlet's approximation theorem.

THEOREM 1.3.23 (MULTIDIMENSIONAL DIRICHLET APPROXIMATION THEOREM). *Given k real numbers $\alpha_1, \dots, \alpha_k \in \mathbb{R}$ and a fixed integer $N \geq 1$. There exist integers $p_1, \dots, p_k, n \in \mathbb{Z}$ with $0 < n \leq N^k$ such that for all $1 \leq i \leq \ell$ we have that*

$$|\alpha_i n - p_i| \leq \frac{1}{N}$$

holds.

Intuitively, Dirichlet's approximation theorem tells us that αn for $\alpha \in \mathbb{R}$ can be made arbitrarily close to an integer by varying $n \in \mathbb{N}$. The closely related approximation theorem by Leopold Kronecker tells us, that we cannot only approximate integral values, but if α is irrational then $\alpha n - p$ can be made arbitrarily close to a fixed $\beta \in \mathbb{R}$ if we vary the integers n and p.

If we identify two real numbers x, y whenever there exists an integer p with the property that $x + p = y$ then we have constructed the additive quotient group $\mathbb{R}/\mathbb{Z}$. Geometrically, this construction can be seen as rolling up the half-open unit interval $[0, 1)$ to form a unit circle (cf. Fig. 1.10). Considering the quotient topology on $\mathbb{R}/\mathbb{Z}$, Dirichlet's theorem tells us that αn can be made arbitrarily close to $0 + \mathbb{Z}$, while Kronecker's theorem states that every point of the unit circle is a cluster point of the sequence $(\alpha n)_{n \in \mathbb{N}}$ if α is irrational.

In the following I will recite the presentation of the proof of Kronecker's theorem from Chap. 2 of the textbook [19]. Note however that the material is also presented in Chap. 23 of the reference [16] and the remark following the theorem stems from this book.

THEOREM 1.3.24 (KRONECKER'S APPROXIMATION THEOREM). *For all irrational numbers $\alpha \in \mathbb{R} \setminus \mathbb{Q}$, all real numbers $\beta \in \mathbb{R}$, all integers $N \geq 1$, and all $\varepsilon > 0$ there exist integers $p, n \in \mathbb{Z}$ with $|n| \geq N$ such that*

$$|\alpha n - \beta - p| < \varepsilon$$

[10] In the example depicted N equals 3.

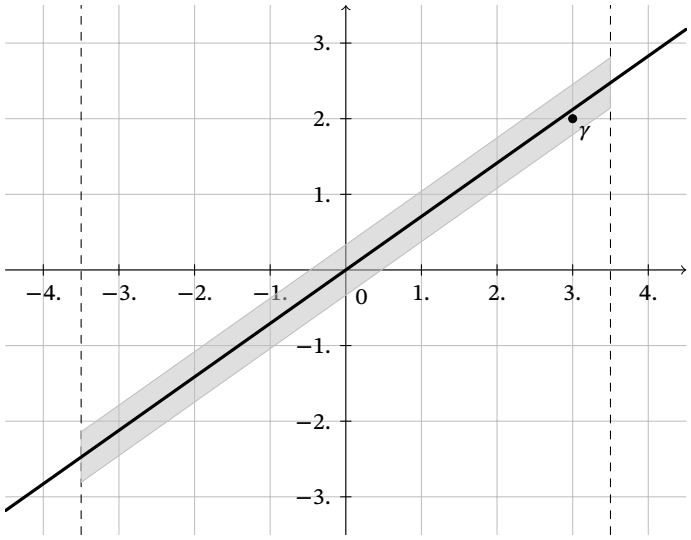


Figure 1.9: The convex set T (shaded area) contains the lattice point γ

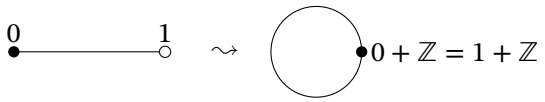


Figure 1.10: The half-open unit interval is rolled up to form a unit circle. Both can be seen as representations of the factor group $\mathbb{R}/\mathbb{Z}$

holds.

Proof. By Dirichlet's approximation theorem there exist integers $g, q \in \mathbb{Z}$ with $0 < q$ such that

$$0 < |\alpha q - g| < \varepsilon$$

holds. Indeed, for the left inequality we notice that α is irrational and the right inequality follows by setting $N > \varepsilon^{-1}$. Now we set $n := kq$ and $p := kg + c$, where the exact values of k and c will be determined in the course of the proof.

We transform the expression of interest

$$|\alpha n - \beta - p| = |k(\alpha q - g) - \beta \ - c| = |\alpha q - g| \left| k - \frac{\beta + c}{\alpha q - g} \right| \tag{1.3.1}$$

and set

$$k := \left\lfloor \frac{\beta + c}{\alpha q - g} \right\rfloor + 1,$$

where $\lfloor x \rfloor$ denotes the greatest integer smaller than x. This ensures that the last factor in (1.3.1) remains ≤ 1. Choose c to be any integer with the same sign as $\alpha q - g$ that satisfies

$$|c| \geq N|\alpha q - g| + |\beta|$$

and set k accordingly. Then

$$\begin{aligned} k = \left\lfloor \frac{\beta + c}{\alpha q - g} \right\rfloor + 1 \geq \frac{c}{\alpha q - g} - \left| \frac{\beta}{\alpha q - g} \right| \geq \\ \geq \left(N + \left| \frac{\beta}{\alpha q - g} \right| \right) - \left| \frac{\beta}{\alpha q - g} \right| = N > 0 \end{aligned}$$

and therefore $n = kq \geq k \geq N$. From (1.3.1) we can now deduce that

$$|\alpha n - \beta - p| = \underbrace{|\alpha q - g|}_{<\varepsilon} \underbrace{\left| k - \frac{\beta + c}{\alpha q - g} \right|}_{\leq 1} < \varepsilon$$

is fulfilled, which was to be shown. □

Remark. Note that the condition on α being irrational in Kronecker's theorem is necessary. Indeed, if we assume otherwise that $\alpha = a/b \in \mathbb{Q}$ then $\alpha n - \lfloor \alpha n \rfloor$ runs only through the values

$$0, \frac{1}{b}, \frac{2}{b}, ..., \frac{b-1}{b}$$

for all $n \in \mathbb{N}$. Thus, if we choose any $\beta \in [0, 1)$ that is not among these values, then

$$\left\{ \left| \frac{r}{b} - \beta \right| : 0 \leq r < b \right\}$$

has a positive maximum, say δ and the condition

$$|\alpha n - \beta - p| < \varepsilon$$

cannot be satisfied for $\varepsilon < \delta$.

As with Dirichlet's approximation theorem there is a multidimensional version of Kronecker's theorem as well. To state this theorem we need a definition.

DEFINITION. A set of real numbers $\alpha_1, \dots, \alpha_n \in \mathbb{R}$ is called *linearly independent over* $\mathbb{Z}$ if for all integers $c_1, \dots, c_n$ the fact that

$$\sum_{i=1}^{n} c_i \alpha_i$$

is an integer implies that $c_1 = c_2 = \dots = c_n = 0$.

Note that a set of real numbers $\{\alpha_1, \dots, \alpha_\ell\} \subseteq \mathbb{R}$ is linearly independent over $\mathbb{Z}$ if and only if $\{1, \alpha_1, \dots, \alpha_\ell\}$ is linearly independent over $\mathbb{Q}$ in the sense of linear algebra. Indeed, if $\{\alpha_1, \dots, \alpha_\ell\}$ is linearly independent over $\mathbb{Z}$ and there are rationals $x_0, x_1, \dots, x_\ell \in \mathbb{Q}$ such that

$$\sum_{i=1}^{\ell} x_i \alpha_i = x_0 \cdot 1$$

then upon multiplying with the least common multiple of the denominators of the non-zero x_i-s we obtain a $\mathbb{Z}$-linear combination of the α_i-s with an integral value and thus all the x_i-s must be zero.

If on the other hand, $\{1, \alpha_1, \dots, \alpha_\ell\}$ is linearly independent over $\mathbb{Q}$ then

$$\sum_{i=1}^{\ell} c_i \alpha_i = a \in \mathbb{Z}$$

for some $c_1, \dots, c_\ell \in \mathbb{Z}$ implies that all of the c_i (and a) must be zero. Thus, $\{\alpha_1, \dots, \alpha_\ell\}$ is linearly independent over $\mathbb{Z}$.

THEOREM 1.3.25 (MULTIDIMENSIONAL KRONECKER APPROXIMATION THEOREM). *Let $\alpha_1, \dots, \alpha_\ell$ be real numbers that are linearly independent over $\mathbb{Z}$. Then for all real $\beta_1, \dots, \beta_\ell \in \mathbb{R}$, all $\varepsilon > 0$, and all integers $N \geq 1$ one can find integers $n, p_1, \dots, p_\ell \in \mathbb{Z}$ with $|n| \geq N$ such that for all $i \in \{1, \dots, \ell\}$ the inequality*

$$|\alpha_i n - \beta_i - p_i| < \varepsilon$$

is satisfied.

As did Hlawka, Schoissengeier, and Taschner [19] I will present the inductive proof of Estermann [12] published in 1933.

Proof. For $\ell = 1$ we have already carried out a proof in the previous theorem, as for a single real number α to be linearly independent over $\mathbb{Z}$ is the same as being irrational. Thus let us assume that $\ell > 1$ and that the claim holds true for all collections of less than ℓ linearly independent real numbers.

We set $\delta := \varepsilon/2$ and apply the multidimensional Dirichlet approximation theorem (1.3.23) to obtain integers $q, g_1, \dots, g_\ell \in \mathbb{Z}$ with $q > 0$ such that

$$0 < |\alpha_i q - g_i| < \delta$$

holds for all $i \in \{1, \dots, \ell\}$. Again, the left inequality holds since α_i is irrational.

As in the one-dimensional case we set $n = kq$ and $p_i = kg_i + c_i$ for $1 \le i \le \ell$ and integers $k, c_1, \dots, c_\ell$ whose values will be determined later. Considering the expression of interest we can again obtain

$$|\alpha_i n - \beta_i - p_i| = |k(\alpha_i q - g_i) - \beta_i - c_i| = |\alpha_i q - g_i| \left| k - \frac{\beta_i + c_i}{\alpha_i q - g_i} \right|$$

for all $1 \le i \le \ell$. Now if

$$k := \left\lfloor \frac{\beta_\ell + c_\ell}{\alpha_\ell q - g_\ell} \right\rfloor + 1 \quad \text{and} \quad |c_\ell| \ge N|\alpha_\ell q - g_\ell| + |\beta_\ell|$$

are satisfied then one obtains analogously to the one-dimensional case that

$$|\alpha_\ell n - \beta_\ell - p_\ell| < \delta \quad \text{and} \quad |n| \ge N \tag{1.3.2}$$

hold.

Let us denote $\vartheta := k - (\beta_\ell + c_\ell)/(\alpha_\ell q - g_\ell)$. For $1 \le j < \ell$ we consider

$$\begin{aligned} \alpha_j n - \beta_j - p_j &= \alpha_j kq - \beta_j - kg_j - c_j = \\ &= \alpha_j q \left(\frac{\beta_\ell + c_\ell}{\alpha_\ell q - g_\ell} + \vartheta \right) - \left(\frac{\beta_\ell + c_\ell}{\alpha_\ell q - g_\ell} + \vartheta \right) g_j - \beta_j - c_j = \\ &= c_\ell \left(\frac{\alpha_j q - g_j}{\alpha_\ell q - g_\ell} \right) - \left(\beta_j - \frac{\beta_\ell(\alpha_j q - g_j)}{\alpha_\ell q - g_\ell} \right) - c_j + \vartheta(\alpha_j q - g_j) \end{aligned} \tag{1.3.3}$$

and define for $1 \le j < \ell$

$$\tilde{\alpha}_j := \frac{\alpha_j q - g_j}{\alpha_\ell q - g_\ell} \quad \text{and} \quad \tilde{\beta}_j := \beta_j - \frac{\beta_\ell(\alpha_j q - g_j)}{\alpha_\ell q - g_\ell}.$$

I claim that the real numbers $\tilde{\alpha}_1, \dots, \tilde{\alpha}_{\ell-1}$ are linearly independent over $\mathbb{Z}$, so that the induction hypothesis can be applied to the $\tilde{\alpha}_j$ and $\tilde{\beta}_j$. Indeed, if we have integers $f_1, \dots, f_\ell \in \mathbb{Z}$ such that

$$\sum_{j=1}^{\ell-1} f_j \tilde{\alpha}_j = -f_\ell$$

holds. We can transform this identity to the expression

$$0 = f_\ell + \sum_{j=1}^{\ell-1} f_j \tilde{\alpha}_j = f_\ell + \left(\sum_{j=1}^{\ell-1} f_j \alpha_j q - \sum_{j=1}^{\ell-1} f_j g_j \right) \frac{1}{\alpha_\ell q - g_\ell},$$

which is equivalent to

$$\sum_{j=1}^{\ell} f_j \alpha_j q = \sum_{j=1}^{\ell} f_j g_j \in \mathbb{Z}.$$

Now since q is a non-zero integer and $\alpha_1, \dots, \alpha_\ell$ are linearly independent over $\mathbb{Z}$, we find that $f_1 = \dots = f_{\ell-1} = f_\ell = 0$ and thus the claim holds true.

With these definitions for $\tilde{\alpha}_j$ and $\tilde{\beta}_j$ we can deduce from (1.3.3) that

$$|\alpha_j n - \beta_j - p_j| \leq |c_\ell \tilde{\alpha}_j - \tilde{\beta}_j - c_j| + |\alpha_j q - g_j| < |c_\ell \tilde{\alpha}_j - \tilde{\beta}_j - c_j| + \delta \tag{1.3.4}$$

holds for all $1 \leq j < \ell$. We apply the inductive assumption to obtain an estimate of the left term in the last expression. More formally, there exists an integer $\tilde{n}$ with the property

$$|\tilde{n}| \geq N|\alpha_\ell q - g_\ell| + |\beta_\ell|$$

and integers $\tilde{p}_1, \dots, \tilde{p}_{\ell-1}$, such that for all $j \in \{1, \dots, \ell - 1\}$ we have that

$$|\tilde{\alpha}_j \tilde{n} - \tilde{\beta}_j - \tilde{p}_j| < \delta.$$

Since c_ℓ needs only to satisfy

$$|c_\ell| \geq N|\alpha_\ell q - g_\ell| + |\beta_\ell|$$

we can set $c_\ell := \tilde{n}$ and $c_j := \tilde{p}_j$ $(1 \leq j < \ell)$ and therefore

$$|c_\ell \tilde{\alpha}_j - \tilde{\beta}_j - c_j| < \delta.$$

Then we find not only that $|n| \geq N$ and

$$|\alpha_\ell n - \beta_\ell - p_\ell| < \delta < \varepsilon$$

are satisfied by (1.3.2) but also that

$$|\alpha_j n - \beta_j - p_j| < 2\delta = \varepsilon$$

holds true for all $1 \leq j < \ell$ by (1.3.4). Thus, the proof is concluded. □

1.3.4 Absolute values and local fields

In this section we introduce some notions required to formulate an important principle of Helmut Hasse and Hermann Minkowski. We will only briefly discuss these topics and refer the reader to Chap. 3 of the textbook [29] or Chap. 7 of the reference [27] for a more rigour discussion.

DEFINITION. An *absolute value* on a field K is a function $|\cdot| : K \to \mathbb{R}, x \mapsto |x|$ with the properties

(i) $|x| \geq 0$ for all $x \in K$ and $|x| = 0$ if and only if $x = 0$;
(ii) $|xy| = |x||y|$ for all $x, y \in K$; and
(iii) $|x + y| \leq |x| + |y|$ for all $x, y \in K$.

If additionally the stronger condition

(iv) $|x + y| \leq \max(|x|, |y|)$

holds for all $x, y \in K$ then $|\cdot|$ is called a *non-archimedian absolute value*.

For notational convenience we introduce the function $\mathrm{ord}_{\mathfrak{p}}$ for all non-zero prime ideals $\mathfrak{p} \subseteq \mathcal{O}_K$ mapping a non-zero fractional ideal $\mathfrak{m} \subseteq K$ to the power of $\mathfrak{p}$ in its prime decomposition and $\mathrm{ord}_{\mathfrak{p}}(0) := \infty$. If $K = \mathbb{Q}$ we write ord_p instead of $\mathrm{ord}_{(p)}$ for all primes $p \in \mathbb{Z}$.

EXAMPLE 1.3.26. Let K be a number field. Then K has the following absolute values

(1) a trivial absolute value defined by $|0|_1 := 0$ and $|x|_1 := 1$ for all non-zero $x \in K \setminus \{0\}$;
(2) one absolute value for each embedding $\sigma : K \to \mathbb{C}$ by setting $|x| := |\sigma(a)|_{\mathbb{C}}$, where $|\cdot|_{\mathbb{C}}$ denotes the complex modulus; and
(3) one $\mathfrak{p}$-*adic absolute value* for each non-zero prime ideal $\mathfrak{p}$ defined by

$$|x|_{\mathfrak{p}} := \left(\frac{1}{\mathbb{N}\mathfrak{p}}\right)^{\mathrm{ord}_{\mathfrak{p}}(x\mathcal{O}_K)},$$

where $\mathbb{N}\mathfrak{p} := [\mathcal{O}_K : \mathfrak{p}]$.

LEMMA 1.3.27. *Let K be a number field and $x \in K$. Then x is an algebraic integer if and only if $|x|_{\mathfrak{p}} \leq 1$ for all prime ideals $\mathfrak{p} \subseteq \mathcal{O}_K$.*

Proof. If $x \in \mathcal{O}_K$ is an algebraic integer, then $x\mathcal{O}_K \subseteq \mathcal{O}_K$ is a principal ideal. Thus, in the factorization of $x\mathcal{O}_K$ into a product of prime ideals (cf. Thm 1.3.15) all exponents are non-negative. In other words, $\mathrm{ord}_{\mathfrak{p}}(x\mathcal{O}_K) \geq 0$ holds for all prime ideals $\mathfrak{p}$. Since $\mathbb{N}\mathfrak{p} > 1$ for every prime ideal $\mathfrak{p}$, the $\mathfrak{p}$-adic absolute value $|x|_{\mathfrak{p}}$ can at most equal 1.

If, on the other hand, $|x|_{\mathfrak{p}} > 1$ holds for some prime ideal $\mathfrak{p} \subseteq \mathcal{O}_K$, then $\mathrm{ord}_{\mathfrak{p}}(x\mathcal{O}_K)$ must be negative and thus $x\mathcal{O}_K \supsetneq \mathcal{O}_K$ is a proper fractional ideal. Hence, x cannot be an algebraic integer. □

Note that an absolute value $|\cdot|$ defines a metric on K by setting

$$d(x, y) := |x - y|.$$

Thus, we can view K as a topological space and define two absolute values to be *equivalent* if they induce the same topology on K. An equivalence class of absolute values is called a *prime* or *place* of K. The *completion* of a number field with respect to a *prime* v is the completion of K with respect to the topology induced by v. More formally, we consider first the set C_K of all Cauchy series in K with respect to the prime v and notice that C_v forms a ring with respect to pointwise addition and

multiplication. A maximal ideal M_v is given by the set of null sequences in K. Thus, we can define the completion of K with respect to v to be the quotient ring

$$\hat{K} := C_v/M_v.$$

It is easy to check that this field is indeed topologically complete. Note that one can identify $x \in K$ with the equivalence class of the constant sequence $(x, x, x, ...)$. A completion is called *non-archimedian* if it is induced by a non-archimedian absolute value. As for number fields the archimedian completions are precisely those induced by the embeddings σ of K into $\mathbb{C}$. If the embedding σ is real, one obtains $\mathbb{R}$ as an completion of K, while non-real embeddings yield $\mathbb{C}$ as a completion. The completions of number fields are examples of so called *local fields*.

We say a multivariate polynomial p is *homogeneous* if all non-zero monomials appearing in p have the same degree. Thus, $Y_1^5 + 2Y_1^3Y_2^2 - 7Y_1Y_2^4$ is homogeneous while $Y_1^4 - Y_1^2Y_2$ is not. We call a polynomial $q \in R[Y_1, ..., Y_n]$ a *quadratic form* over an integral domain R if q is homogeneous and has degree 2. If F is a field of characteristic unequal to two, one can alternatively define a quadratic form as a polynomial $q(Y_1, ..., Y_n)$ that can be written in the form

$$q(Y_1, ..., Y_n) = (Y_1, ..., Y_n)A\begin{pmatrix} Y_1 \\ \vdots \\ Y_n \end{pmatrix},$$

where $A \in M_n(F)$ is a symmetric $n \times n$-matrix over F. If A is non-singular, we call q a *regular* quadratic form. We say $x \in R$ is *represented* by q over R if there exist $y_1, \dots, y_n \in R$ such that $x = q(y_1, \dots, y_n)$. We call a quadratic form $q \in R[Y_1, \dots, Y_n]$ *universal* if it represents every element of R. As for representabilty in a number field K we have the following theorem.

THEOREM 1.3.28 (HASSE-MINKOWSKI THEOREM). *A number $x \in K$ is represented by a regular quadratic form q in a number field K if and only if x is represented by q in all completions of K.*

A proof of this theorem can be found in §66 of the textbook [30]. With regard to universal quadratic forms we have furthermore, that if the regular quadratic form q has at least four indeterminates then q is universal in all non-archimedian completions of K. A direct application of the Hasse-Minkowski theorem is the following lemma, taken from [44, Lem. 5.1.1].

LEMMA 1.3.29. *Let K be a number field and fix $x \in K$. Furthermore, let $x = x_1, \dots, x_n$ be all the conjugates of x over $\mathbb{Q}$. Then the quadratic form*

$$q(Y_1, Y_2, Y_3, Y_4) := Y_1^2 + Y_2^2 + cY_3^2 + Y_4^2$$

represents x over K if $c = c_1, \dots, c_n$ are all the conjugates of $c \in K \setminus \{0\}$ over $\mathbb{Q}$ and $c_i < 0$ whenever $x_i < 0$.

Proof. Note that q can be written as $(Y_1, Y_2, Y_3, Y_4)A(Y_1, Y_2, Y_3, Y_4)^t$, where A is a non-singular diagonal matrix. Hence, q is regular. Since q has four indeterminates it suffices to check that q represents x_i over $\mathbb{C}$ and $\mathbb{R}$. Then the Hasse-Minkowski theorem implies that q represents x over

K. But since $\mathbb{C}$ is algebraically closed, the polynomial $X^2 - x_i$ has a root y_{i1} in $\mathbb{C}$. Thus,

$$x_i = y_{i1}^2 + 0^2 + c_i\, 0^2 + 0^2$$

is the desired representation. On the other hand, in the case of $\mathbb{R}$ we distinguish two cases. If $x_i \geq 0$ then we can proceed as in the case of $\mathbb{C}$. If $x_i < 0$ then x_i/c_i is positive and thus a square in $\mathbb{R}$. Now set $y_{i3} := \sqrt{x_i/c_i}$ and notice that

$$x_i = 0^2 + 0^2 + c_i\, y_{i3}^2 + 0^2.$$

□

Furthermore, the following theorem will be useful.

THEOREM 1.3.30 (STRONG APPROXIMATION THEOREM). *Let K be a number field, let $\mathcal{M}_K$ be the set of all the absolute values of K, let $\mathcal{F}_K = \{|\cdot|_1, ..., |\cdot|_\ell\} \subseteq \mathcal{M}_K$ be a non-empty finite subset, and let $a_1, ..., a_{\ell-1} \in K$. Then for any $\varepsilon > 0$ there exists an $x \in K$ such that the following conditions are satisfied.*

(i) For $1 \leq i \leq \ell - 1$ we have that $|x - a_i|_i < \varepsilon$.
(ii) For any absolute value $|\cdot|$ not contained in $\mathcal{F}_K$ we have that $|x| \leq 1$.

For a proof of this theorem see §21 of the textbook [30].

2 Hilbert's tenth problem

2.1 Different perspectives on an old problem

2.1.1 Diophantine equations and sets

In 1900, David Hilbert held his famous lecture [18] before the *International Congress of Mathematicians* in Paris. During the talk entitled „Mathematische Probleme[1]" Hilbert posed ten mathematical problems left for the twentieth century to solve. Hilbert's list of problems was later amended to contain twenty-three problems. The tenth of these questions and its variants are the subject of this thesis. The problem states

> 10. ENTSCHEIDUNG DER LÖSBARKEIT EINER DIOPHANTISCHEN GLEICHUNG. Eine Diophantische Gleichung mit irgend welchen Unbekannten und mit ganzen rationalen Zahlencoefficienten sei vorgelegt: man soll ein Verfahren angeben, nach welchem sich mittelst einer endlichen Anzahl von Operationen entscheiden läßt, ob die Gleichung in ganzen rationalen Zahlen lösbar ist.[2] [18]

A *Diophantine equation*—in the classical sense—is of the form

$$p(\alpha_1, ..., \alpha_n) = 0,$$

where $p \in \mathbb{Z}[X_1, ..., X_n]$ is a polynomial and one only allows rational integral solutions $\alpha_1, ..., \alpha_n \in \mathbb{Z}$. Using the tools developed in Sections 1.2 and 1.3, we will exchange one or both occurrences of the rational integers by values from other rings. It took until the 1930s to formalize what Hilbert meant by a „Verfahren [mit] einer endlichen Anzahl von Operationen[3]" to the notion of *computation* that was defined in Section 1.1. In the same section we have also defined what it means to *decide a problem*, so we are left with the task of identifying Hilbert's question with a set of strings. In a first approach one could reformulate the tenth problem as

> H10. For a fixed polynomial $p \in \mathbb{Z}[X_1, X_2, ...]$ does there exist a Turing machine $\mathbb{A}_p$ that returns `1` if p has a root and `0` otherwise?

This formalization is however trivially solvable. Note that the subset of ω associated with this problem

$$\{x \in \omega : p \text{ has a root}\}$$

is either empty (if p has no roots) or all of ω (if p has a root). Turing machines with constant output `0` or `1` respectively compute the characteritic function of the problem and thus show that our first formulation of Hilbert's problem is decidable.

[1] 'mathematical problems'

[2] 10. DETERMINATION OF THE SOLVABILITY OF A DIOPHANTINE EQUATION. Given a diophantine equation with any number of unknown quantities and with rational integral numerical coefficients: To devise a process according to which it can be determined by a finite number of operations whether the equation is solvable in rational integers. [translation published in 17]

[3] 'process [with] a finite number of operations'

For this reason we must exchange the quantifiers and ask

> HIO. Does there exist a Turing machine $\mathbb{A}$ and an encoding $\ulcorner\cdot\urcorner$ such that for all polynomials $p \in \mathbb{Z}[X_1, X_2, ...]$ the output $\mathbb{A}(\ulcorner p \urcorner)$ is 1, if p has integral roots, and 0 otherwise.

We will see that if we restrict ourselves to encodings $\ulcorner\cdot\urcorner$ that allow to efficiently obtain the evaluation $\ulcorner p(\alpha)\urcorner$ from $\ulcorner p\urcorner$ and $\ulcorner\alpha\urcorner$, then the answer to the question above is negative. In fact, for all rings of algebraic integers $\mathcal{O}_K$, that we will consider, we will find a single multivariate polynomial $p_{\mathcal{K}} \in \mathcal{O}_K[X, Y_1, \dots, Y_n]$ such that for all Turing machines $\mathbb{A}$ there exists an algebraic integer $\alpha \in \mathcal{O}_K$ with the property that $\mathbb{A}$ cannot correctly decide whether the partially evaluated polynomial

$$p_{\mathcal{K}}(\alpha, Y_1, \dots, Y_n)$$

has roots in $\mathcal{O}_K$. The index $\mathcal{K}$ of the polynomial above is not chosen at random. Indeed, the polynomial $p_{\mathcal{K}}$ represents an encoded version of the halting set $\mathcal{K}$ in the sense of the following definition.

DEFINITION. Let R be a commutative ring with unity. A set $S \subseteq R^n$ is said to be *Diophantine* over R if there exists a polynomial $p \in R[X_1, ..., X_n, Y_1, ..., Y_m]$ in $n + m$ indeterminates $(m, n \geq 0)$ such that

$$(\alpha_1, ..., \alpha_n) \in S \quad \Leftrightarrow \quad \exists \beta_1, ..., \beta_m \in R : p(\alpha_1, ..., \alpha_n, \beta_1, ..., \beta_m) = 0$$

A polynomial $p \in R[X_1, ..., X_n]$ as above defines an n-ary relation $\mathcal{p}$ on R by

$$\mathcal{p}(\alpha_1, ..., \alpha_n) \quad :\Leftrightarrow \quad p(\alpha_1, ..., \alpha_n) = 0.$$

In this sense a set $S \subseteq R^i$ is Diophantine if there exists a polynomial $p \in R[X_1, ..., X_n]$ such that

$$(\alpha_1, \dots, \alpha_i) \in S \quad \Leftrightarrow \quad \exists \beta_1, \dots, \beta_{n-i} \in R : \mathcal{p}(\alpha_1, \dots, \alpha_i, \beta_1, \dots, \beta_{n-i}).$$

If the ring R is computable, it is immediate that the relation $\mathcal{p}$ is computable. Thus, we have the following lemma.

LEMMA 2.1.1. *Let R be a computable commutative ring with unity. Then every Diophantine subset of R is semi-decidable.*

Viewing n-ary relations as subsets of R^n, I will sometimes refer to Diophantine sets as *Diophantine relations*. A function $R^n \to R^m$ is called *Diophantine* if it is Diophantine viewed as an $(n + m)$-ary relation. Geometrically, Diophantine subsets are precisely the projections of roots of polynomials. Consider for instance the unit circle defined as the roots in $\mathbb{R}^2$ of the polynomial $X^2 + Y^2 - 1$. The projection onto the first coordinate can be defined in a Diophantine way by

$$\{x \in \mathbb{R} : \exists y \in \mathbb{R} \text{ such that } x^2 + y^2 - 1 = 0\}$$

and is easly seen to be the interval $[-1, 1]$. The situation is depicted in Fig. 2.1.

EXAMPLE 2.1.2. (1) Let R be an integral domain. Then every finite subset S of R is Diophantine because the roots of

$$p(X) := \prod_{s \in S} (X - s)$$

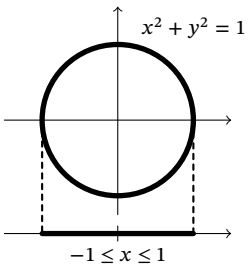


Figure 2.1: Diophantine sets are projections of roots of polynomials

are precisely the elements of S.

(2) Let R be an integral domain. Then for every polynomial $p \in R[X_1, ..., X_n]$ the associated polynomial function $p : R^n \to R$ is Diophantine. To see this we set

$$q(X_1, ..., X_n, X_{n+1}) := p(X_1, ..., X_n) - X_{n+1},$$

and notice that q has a root $(\alpha_1, ..., \alpha_n, \alpha_{n+1}) \in R$ if and only if $p(\alpha_1, ..., \alpha_n) = \alpha_{n+1}$ as claimed.

(3) Let R be a commutative ring with unity. Then divisibility in R is Diophantine. Indeed $\alpha_1 \mid \alpha_2$ in R precisely if

$$\exists \beta \in R : \alpha_1 \beta = \alpha_2.$$

(4) Let K be a number field and $\mathcal{O}_K$ its ring of algebraic integers. Then $\mathcal{O}_K \setminus \{0\}$ is Diophantine over $\mathcal{O}_K$. I extend the hint stated in [10, Prop. 1] and claim that

$$\alpha \neq 0 \quad \Leftrightarrow \quad \exists \beta, \gamma \in \mathcal{O}_K : \alpha\beta = (2\gamma - 1)(3\gamma - 1).$$

Firstly, note that the polynomial on the right hand side has the roots $1/2$ and $1/3$ in $\mathbb{Q}$. As the intersection $\mathcal{O}_K \cap \mathbb{Q}$ equals $\mathbb{Z}$ for all number fields K, one obtains that the polynomial identity can only be satisfied for $\alpha \neq 0$.

Let now $\alpha \neq 0$. We can decompose the ideal $(\alpha) = \mathfrak{x}_2\mathfrak{x}_3$ such that

$$(2) + \mathfrak{x}_2 = \mathcal{O}_K, \ (3) + \mathfrak{x}_3 = \mathcal{O}_K \text{ and } \mathfrak{x}_2 + \mathfrak{x}_3 = \mathcal{O}_K$$

hold. This is because 2 and 3 are rational primes and therefore (2) and (3) are relative prime. In other words, we find

$$\exists x_2 \in \mathfrak{x}_2, \exists y_2 \in \mathcal{O}_K : 2y_2 + x_2 = 1 \quad \text{and} \quad \exists x_3 \in \mathfrak{x}_3, \exists y_3 \in \mathcal{O}_K : 3y_3 + x_3 = 1$$

As a consequence of the Chinese remainder theorem (1.3.16) the congruences

$$\gamma \equiv y_2 \mod \mathfrak{x}_2 \quad \text{and} \quad \gamma \equiv y_3 \mod \mathfrak{x}_3$$

are simultaneously solvable. This implies that

$$2\gamma \equiv 2y_2 \equiv 1 \mod \mathfrak{x}_2 \quad \text{and} \quad 3\gamma \equiv 3y_3 \equiv 1 \mod \mathfrak{x}_3.$$

This can be rewritten as

$$2\gamma - 1 \in \mathfrak{x}_2 \quad \text{and} \quad 3\gamma - 1 \in \mathfrak{x}_3.$$

We deduce that $(2\gamma-1)(3\gamma-1)$ is contained in $\mathfrak{x}_2\mathfrak{x}_3 = (\alpha)$, or put differently, there exists a $\beta \in \mathcal{O}_K$ such that

$$\alpha\beta = (2\gamma - 1)(3\gamma - 1).$$

(5) Let R be a commutative ring with unity. The set of units U in R is Diophantine over R. This can be seen by the polynomial equation

$$x \in U \quad \Leftrightarrow \quad \exists y \in R : xy = 1.$$

In the examples above we have seen that many sets and relations are Diophantine. Before we go on proving some structural results for Diophantine sets, we turn our attention to the classical case of Diophantine subsets of $\mathbb{Z}$ and study their relations with subsets of $\mathbb{N}$.

EXAMPLE 2.1.3 (DIOPHANTINE SUBSETS OF $\mathbb{N}$). If one wants to study sets that are Diophantine over $\mathbb{N}$, one runs into the problem that $\mathbb{N}$ is not a ring. An approach that has been carried out [cf. e.g. 5] is considering sets $S \subseteq \mathbb{N}^n$ that are Diophantine over $\mathbb{Z}$ and allow only for witnesses in $\mathbb{N}$. I will show that this construction can be carried out in a Diophantine way.

First, we note that if $S_1, S_2 \subseteq \mathbb{Z}^n$ are Diophantine over $\mathbb{Z}$, then their intersection is Diophantine over $\mathbb{Z}$ as well. This is because if $p_1 \in \mathbb{Z}[X_1, \dots, X_n, Y_1, \dots, Y_{m_1}]$ represents S_1 via

$$(\alpha_1, \dots, \alpha_n) \in S_1 \quad \Leftrightarrow \quad \exists \beta_1, \dots, \beta_{m_1} : p_1(\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_{m_1}) = 0$$

and $p_2 \in \mathbb{Z}[X_1, \dots, X_n, Y_1, \dots, Y_{m_2}]$ represents S_2, we set $m := m_1 + m_2$ and consider p_1 and p_2 as polynomials in $n + m$ indeterminates, where for all $i \in \{n+1, ..., m\}$ indeterminate Y_i either appears in p_1 or p_2 but not in both. Then $(\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_m) \in \mathbb{Z}^{m+n}$ is a root of

$$q(X_1, \dots, X_n, Y_1, \dots, Y_m) := p_1(X_1, \dots, X_n, Y_1, \dots, Y_m)^2 + p_2(X_1, \dots, X_n, Y_1, \dots, Y_m)^2$$

if and only if $(\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_m)$ is a root of p_1 and p_2. Thus, we find that

$$S_1 \cap S_2 = \{\alpha_1, \dots, \alpha_n \in \mathbb{Z} : \exists \beta_1, \dots, \beta_m \in \mathbb{Z} : q(\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_m) = 0\}.$$

By Lagrange's four-square theorem (Prop. 1.3.20) we know that every non-negative integer α is the sum of four squares and as a consequence

$$x \in \mathbb{N} \quad \Leftrightarrow \quad \exists \beta_1, \beta_2, \beta_3, \beta_4 \in \mathbb{Z} : \beta_1^2 + \beta_2^2 + \beta_3^2 + \beta_4^2 = \alpha$$

is a Diophantine definition of $\mathbb{N}$ over $\mathbb{Z}$. Therefore, we can check for a given polynomial equation whether all variables take only non-negative values in a Diophantine way. More formally, we say that a subset $S \subseteq \mathbb{N}^n$ is *Diophantine over* $\mathbb{N}$ if there exists a polynomial $p \in \mathbb{Z}[X_1, ..., X_n, Y_1, ..., Y_m]$ such that

$$(\alpha_1, \dots, \alpha_n) \in S \quad \Leftrightarrow \quad \exists \beta_1, \dots, \beta_m \in \mathbb{N} : p(\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_m) = 0.$$

If this is the case, we find that S is Diophantine over $\mathbb{Z}$ as well, by conjugating the identity with the clause

$$\left(\bigwedge_{i=1}^{n} \exists \gamma_{i1}, ..., \gamma_{i4} \in \mathbb{Z} : \alpha_i = \sum_{j=1}^{4} \gamma_{ij}^2\right) \wedge \left(\bigwedge_{i=1}^{m} \exists \delta_{i1}, ..., \delta_{i4} \in \mathbb{Z} : \beta_i = \sum_{j=1}^{4} \delta_{ij}^2\right).$$

We now list some examples of sets that are Diophantine over $\mathbb{N}$.

(1) The set of composite numbers is Diophantine over $\mathbb{N}$, as $\alpha \in \mathbb{N}$ is composite if and only if

$$\exists \beta_1, \beta_2 \in \mathbb{N} : x = (\beta_1 + 2)(\beta_2 + 2).$$

Here adding 2 to β_1 and β_2 ensures, that both factors are greater than 1. Choosing

$$p(X, Y_1, Y_2) := X - (Y_1 + 2)(Y_2 + 2)$$

yields the claim. To transform this into a Diophantine definition over $\mathbb{Z}$, we must conjugate the clauses stating that α, β_1 and β_2 are non-negative. Thus, we obtain

$$\begin{aligned} \exists \beta_1, \beta_2, \gamma_1, ..., \gamma_4, \delta_{11}, ..., \delta_{14}, \delta_{21}, ..., \delta_{24} \in \mathbb{Z} : (&x = (\beta_1 + 2)(\beta_2 + 2) \wedge \\ &x = \gamma_1^2 + \gamma_2^2 + \gamma_3^2 + \gamma_4^2 \wedge \\ &\beta_1 = \delta_{11}^2 + \delta_{12}^2 + \delta_{13}^2 + \delta_{14}^2 \wedge \\ &\beta_2 = \delta_{21}^2 + \delta_{22}^2 + \delta_{23}^2 + \delta_{24}^2), \end{aligned}$$

which can be rewritten as the single Diophantine identity

$$\begin{aligned} &\exists \beta_1, \beta_2, \gamma_1, ..., \gamma_4, \delta_{11}, ..., \delta_{14}, \delta_{21}, ..., \delta_{24} \in \mathbb{Z} : \\ &\quad \Big(\big((x - (\beta_1 + 2)(\beta_2 + 2))^2 + \big(x - (\gamma_1^2 + \gamma_2^2 + \gamma_3^2 + \gamma_4^2)\big)^2\Big)^2 \\ &\quad + \big(\beta_1 - (\delta_{11}^2 + \delta_{12}^2 + \delta_{13}^2 + \delta_{14}^2)\big)^2\Big)^2 + \big(\beta_2 - (\delta_{21}^2 + \delta_{22}^2 + \delta_{23}^2 + \delta_{24}^2)\big)^2. \end{aligned}$$

(2) The usual order relation $\leq$ on $\mathbb{N}$ is Diophantine over $\mathbb{N}$. Indeed $\alpha_1 \leq \alpha_2$ in $\mathbb{N}$ if and only if

$$\exists \beta \in \mathbb{N} : \alpha_1 + \beta = \alpha_2.$$

We will now see how one can describe Diophantine sets from the view of model theory.

LEMMA 2.1.4. *Let R be a commutative ring with unity and let $\mathfrak{R}$ be its $\mathcal{L}_{ring}$-structure. Then $S \subseteq R^n$ is Diophantine if and only if there exists an atomic $\mathcal{L}_R$-formula $\phi(\mathsf{x}_1, \dots, \mathsf{x}_n, \mathsf{y}_1, \dots, \mathsf{y}_m)$ such that*

$$(\alpha_1, \dots, \alpha_n) \in S \quad \Leftrightarrow \quad \mathfrak{R} \vDash \exists \mathsf{y}_1 : \dots \exists \mathsf{y}_m : \phi(\alpha_1, \dots, \alpha_n, \mathsf{y}_1, \dots, \mathsf{y}_m)$$

holds.

Proof. By Thm 1.2.8 the formula $\phi(\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_m)$ is true in $\mathfrak{R}$ if and only if the polynomial associated with ϕ has a root at $(\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_m)$. □

Note that even more is true as a partially evaluated polynomial with coefficients in R is still a polynomial. Thus, one can decide membership in all Diophantine sets if and only if one can decide for all polynomials whether they have roots in R. As a consequence, we will identify Hilbert's tenth problem over R with the set of Gödel numbers of $\mathtt{H10}(\mathfrak{R})$ if R is a countable commutative ring with unity, and restate Hilbert's problem as

H10. Is the Diophantine theory $\mathtt{H10}(\mathfrak{R})$ decidable?

In some cases we can modify Hilbert's question even more and allow for disjunctions and conjunctions to appear in our theory.

LEMMA 2.1.5. *Let R be an integral domain, whose quotient field* $\operatorname{Quot} R$ *is not algebraically closed. Then if $S_1, S_2 \subseteq R$ are Diophantine so are*

$$S_1 \cap S_2 \quad \textit{and} \quad S_1 \cup S_2.$$

If R is computable, then there is an algorithm that derives the defining polynomial equations for union and intersection efficiently from the equations of S_1 and S_2.

In other words, conjunctions and disjunctions of existentially quantified atomic formulae can be replaced by a single existentially quantified atomic formula. Or again put differently, conjunction $\wedge$ and disjunction $\vee$ are $\mathcal{L}_R$-definable, efficiently computable predicates.

Proof. Let $p(X_1, \dots, X_n, Y_1, \dots, Y_{m_1})$ and $q(X_1, \dots, X_n, Y_1, \dots, Y_{m_2})$ give Diophantine definitions of S_1 and S_2 respectively. Then as in Example 2.1.3 we set $m = m_1 + m_2$ and interpret p, q as polynomials in $n + m$ indeterminates such that for all $i \in \{n+1, \dots, m\}$ indeterminate Y_i appears either in p or q but not in both.

Now set

$$h := pq.$$

Then h vanishes if and only if p or q vanishes. As a consequence, the n-tuple $(\alpha_1, \dots, \alpha_n) \in R^n$ is in the union of S_1 and S_2 if and only if

$$\exists \beta_1, \dots, \beta_m \in R : h(\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_m) = 0.$$

To make notation easier when proving the claim for intersections, I will assume that $n = 1$ and $m = 2$. The general cases follows analogously. Let then

$$h(T) = a_k T^k + \dots + a_1 T + a_0 \in R[T]$$

be a polynomial of degree $k > 0$ without roots in $\operatorname{Quot} R$. Then $\overline{h}(T) = T^k h(T^{-1})$ does not have roots in $\operatorname{Quot} R$ either. As if $\alpha \in \operatorname{Quot} R$ is a root of $\overline{h}$ then

$$0 = \overline{h}(\alpha) = a_k + a_{k-1}\alpha + \dots + a_1 \alpha^{k-1} + a_0 \alpha^k$$

and $\alpha = 0$ implies that $a_k = 0$. Otherwise, α^{-1} is a root of $\alpha^k h$ and therefore of h.

Now consider

$$H(\alpha, \beta_1, \beta_2) = \sum_{i=0}^{k} a_i p(\alpha, \beta_1)^i q(\alpha, \beta_2)^{k-i}.$$

I will prove for all $\alpha, \beta_1, \beta_2 \in R$ that $H(\alpha, \beta_1, \beta_2) = 0$ if and only if $p(\alpha, \beta_1)$ and $q(\alpha, \beta_2)$ vanish. Then H represents the intersection via

$$\alpha \in S_1 \cap S_2 \quad \Leftrightarrow \quad \exists \beta_1, \beta_2 \in R : H(\alpha, \beta_1, \beta_2) = 0.$$

If $H(\alpha, \beta_1, \beta_2) = 0$ but $p(\alpha, \beta_1) \neq 0$ then

$$0 = \frac{H}{p^k}(\alpha, \beta_1, \beta_2) = \frac{1}{p(\alpha, \beta_1)^k} \sum_{i=0}^{k} a_i p(\alpha, \beta_1)^i q(\alpha, \beta_2)^{k-i} = \overline{h}\left(\frac{q}{p}(\alpha, \beta_1, \beta_2)\right),$$

which is a contradiction to $\overline{h}$ not having roots. If on the other hand $H(\alpha, \beta_1, \beta_2) = 0$ but $q(\alpha, \beta_2) \neq 0$ one finds

$$0 = \frac{H}{q^k}(\alpha, \beta_1, \beta_2) = \frac{1}{q(\alpha, \beta_2)^k} \sum_{i=0}^{k} a_i p(\alpha, \beta_1)^i q(\alpha, \beta_2)^{k-i} = h\left(\frac{p}{q}(\alpha, \beta_1, \beta_2)\right).$$

The converse direction is clear as the powers of p and q sum up to k for each summand in the definition of H.

To prove the effectiveness of these methods one observes, that the defining equations contain only polynomials in p and q. Thus, Example 1.2.12.(3) implies that the polynomial equations for union and intersection of Diophantine sets can be computed from the polynomials p and q. □

Note that the algorithm presented above does not depend on the initial equations p and q but it does depend on the integral domain R. We might need different polynomials h without roots for each ring R in the case of conjunctions.

Remark. Using $h(X) = X^2 + 1$ as the polynomial without roots in $\mathbb{Z}$ for the construction described in the proof of Lem. 2.1.5, one obtains

$$H = p^2 + q^2$$

precisely as in Example 2.1.3. However, we could also have chosen $h(X) = X^2 - 2X - 2$ as a polynomial without rational roots—h has the irrational roots $1 \pm \sqrt{3}$—and obtain

$$H = p^2 - 2pq + 2q^2.$$

Using induction and the lemma above, one immediately obtains that arbitrary finite unions and intersections of Diophantine sets are Diophantine. For the special case that R is computable, one can thus deduce that Hilbert's tenth problem is essentially the same as the primitive positive diagram $D_{\exists+}(\mathfrak{R})$.

COROLLARY 2.1.6. *Let R be a computable integral domain and $\mathfrak{R}$ its $\mathcal{L}_{ring}$-structure. Then $D_{\exists+}(\mathfrak{R})$ is many-one reducible to* $\mathtt{H10}(\mathfrak{R})$.

Proof. This follows immediately from the lemma above and the properties of the Gödelization. □

One is tempted to consider Hilbert's tenth problem over the complex plane $\mathbb{C}$. By a corollary of Hilbert's Nullstellensatz we know that for every non-constant polynomial $p \in \mathbb{C}[X_1, \dots, X_n] \setminus \mathbb{C}$ there exist complex numbers $z_1, \dots, z_n \in \mathbb{C}$ such that $p(z_1, \dots, z_n) = 0$ vanishes. Thus, one might believe that Hilbert's tenth problem over $\mathbb{C}$ is decidable. There is however a technicality in the way: As $\mathbb{C}$ is uncountable, the ring of polynomials $\mathbb{C}[X_1, X_2, \dots]$ is uncountable as well—even the subset of polynomials with roots is uncountable as it contains $\{z - X_1 : z \in \mathbb{C}\}$. Hence, the analogue of Hilbert's tenth problem over $\mathbb{C}$ cannot be captured by the formalization of decision problems we gave in Section 1.1. For this reason it we consider *purely Diophantine sets*.

2.1.2 Purely Diophantine sets

DEFINITION. Let R be a commutative ring with unit. A set $S \subseteq R^n$ is said to be *purely Diophantine* over R if there exists a polynomial $p \in \mathbb{Z}[X_1, \dots, X_n, Y_1, \dots, Y_m]$ in $n+m$ indeterminates $(m, n \geq 0)$ such that

$$(\alpha_1, \dots, \alpha_n) \in S \quad \Leftrightarrow \quad \exists \beta_1, \dots, \beta_m \in R : p(\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_m) = 0$$

By demanding that the coefficients are rational integers, we immediately obtain that there can only be countably many purely Diophantine sets over a fixed ring with arbitrary cardinality. Whilst the choice of coefficients may seem random to the algebraist, it is perfectly natural from the perspective of model theory, as is shown in the following lemma.

LEMMA 2.1.7. *Let R be a commutative ring with unity and let $\mathfrak{R}$ be its $\mathcal{L}_{ring}$-structure. Then $S \subseteq R^n$ is purely Diophantine if and only if there exists an atomic $\mathcal{L}_{ring}$-formula $\phi(\mathtt{x}_1, \dots, \mathtt{x}_n, \mathtt{y}_1, \dots, \mathtt{y}_m)$ such that*

$$(\alpha_1, \dots, \alpha_n) \in S \quad \Leftrightarrow \quad \mathfrak{R} \vDash \exists \mathtt{y}_1 : \dots \exists \mathtt{y}_m : \phi(\alpha_1, \dots, \alpha_n, \mathtt{y}_1, \dots, \mathtt{y}_m)$$

holds.

Proof. The claim follows from Lem. 1.2.3 and the analogue of part (ii) of Thm 1.2.8. □

At second sight, the construction is even less surprising, as for every ring R with 1 there exists exactly one ring-homomorphism $\varphi : \mathbb{Z} \to R$ mapping $1 \in \mathbb{Z}$ to $1 \in R$. Looking back at Example 2.1.2, we note that the Diophantine sets of (3), (4), and (5) are in fact purely Diophantine, whereas finite sets (1) are in general not. As for polynomial functions $p : R^n \to R$, we obtain that they are purely Diophantine if and only if the coefficients of p are rational integers. Note however that a partially evaluated polynomial with rational integral coefficients need not be a polynomial in $\mathbb{Z}[X_1, X_2, \dots]$. Thus, one needs to be a bit more careful when dealing with purely Diophantine sets. However, the analogue of Lem. 2.1.5 holds for purely Diophantine sets.

LEMMA 2.1.8. *Let $S_1, S_2 \subseteq \mathcal{O}_K^n$ be purely Diophantine subsets of a ring of algebraic integers of some number field K. Then their union and intersection are purely Diophantine. The defining equations for union and intersection can be obtained effectively.*

Proof. I claim that there exists a polynomial $h \in \mathbb{Z}[X]$ without roots in K. Then we can use the same construction as in Lem. 2.1.5 to prove the lemma.

Such a polynomial $h \in \mathbb{Z}[X]$ must exist in every number field K, as otherwise the normal closure of K contains all algebraic integers and thus is the algebraic closure of $\overline{\mathbb{Q}}$ (in $\mathbb{C}$) by Thm 1.3.7. But the degree $[\overline{\mathbb{Q}} : K]$ is finite, implying that $[K : \mathbb{Q}]$ is infinite, which is a contradiction. □

We now want to identify the purely Diophantine sets of algebraic integers within the Diophantine subsets. For this purpose we reformulate a result of R. M. Robinson [38]. But before we state his result let us look at a simple example: In $\mathbb{Q}[\sqrt[4]{2}]$ the polynomial $p(X) := X^2 - 2$ does not give rise to a purely Diophantine representation of $\sqrt{2}$ because $-\sqrt{2}$ is a root of p as well. We can however represent $\sqrt{2}$ as follows:

$$\alpha = \sqrt{2} \quad \Leftrightarrow \quad \exists \beta \in \mathbb{Q}[\sqrt[4]{2}] : (\beta^4 = 2 \wedge \beta^2 = \alpha).$$

This is because $\mathbb{Q}[\sqrt[4]{2}] \subseteq \mathbb{R}$ is real and the square of a real number is non-negative. In general, we have the following proposition.

PROPOSITION 2.1.9. *Let K be an algebraic number field. If $x \in K$ is fixed by all automorphisms of K, then there exist polynomials $p, q \in \mathbb{Z}[X]$ and a constant $c \in \mathbb{Z}$ such that x is the only element of K satisfying*

$$\exists y \in \mathcal{O}_K : (p(y) = 0 \wedge q(y) = cx).$$

If x is an algebraic integer, then $\{x\}$ is purely Diophantine over $\mathcal{O}_K$.

Proof. By the primitive element theorem (1.3.7) there exists an algebraic integer $\delta \in \mathcal{O}_K$ such that $K = \mathbb{Q}[\delta]$. Let $\mu_{\mathbb{Q},\delta} \in \mathbb{Z}[X]$ be the minimal polynomial of δ over the rationals $\mathbb{Q}$ and let $\delta = \delta_1, \dots, \delta_k \in \mathcal{O}_K$ be the roots of $\mu_{\mathbb{Q},\delta}$ that are contained in K. Since every $z \in K$ can be written as $z = f(\delta)$, where $f(X) \in \mathbb{Q}[X]$ and the rationals are fixed by all automorphisms σ of K, we find that $\sigma(z) = f(\sigma(\delta))$ holds for all automorphisms. Thus, $\mathrm{id}_K = \sigma_1, \dots, \sigma_k$, where $\sigma_i(\delta) = \delta_i$, are all automorphisms of K.

As x is fixed by all of the σ_i, we find that

$$f(\delta) = x = \sigma_i(x) = \sigma_i(f(\delta)) = f(\sigma_i(\delta)) = f(\delta_i)$$

holds for all $1 \leq i \leq k$. Now since $\mu_{\mathbb{Q},\delta}$ defines $\{\delta_1, \dots, \delta_k\}$ in a Diophantine way, we obtain that

$$\alpha = x \quad \Leftrightarrow \quad \exists y \in \mathcal{O}_K : (\mu_{\mathbb{Q},\delta}(y) = 0 \wedge f(y) = x).$$

To finish the proof set c to be the least common multiple of all denominators of coefficients in f and multiply the right equation with c. Since $\delta_1, \dots, \delta_k \in \mathcal{O}_K$ are the only roots of $\mu_{\mathbb{Q},\delta}$, the singleton $\{x\}$ is in fact purely Diophantine over $\mathcal{O}_K$ as claimed. □

Note that the assumption of $x \in K$ being fixed by all automorphisms is necessary. Indeed, if $p(X, Y) \in \mathbb{Z}[X, Y]$ is a polynomial with rational integral coefficients such that there exists a $y \in K$ with $p(x, y) = 0$, then for every automorphism σ, we find that

$$p(\sigma(x), \sigma(y)) = \sigma(p(x, y)) = 0,$$

and thus, $\sigma(x)$ satisfies the same relation. Building on this result for singletons, Davis, Matijasevič, and J. Robinson [7] gave the following characterization of purely Diophantine sets within Diophantine sets over rings of algebraic integers.

THEOREM 2.1.10. *Let $\mathcal{O}_K$ be the ring of algebraic integers of a number field K. A set $S \subseteq \mathcal{O}_K^n$ is purely Diophantine if and only if S is Diophantine and self-conjugate, i.e. for all automorphisms $\sigma : K \to K$ and all $(\alpha_1, \dots, \alpha_n) \in S$ we have that the image $(\sigma(\alpha_1), \dots, \sigma(\alpha_n))$ is contained in S.*

Proof. We may assume that S is Diophantine, as being purely Diophantine clearly implies the former. Thus, let $p \in \mathcal{O}_K[X_1, \dots, X_n, Y_1, \dots, Y_m]$ be a polynomial witnessing that S is Diophantine i.e. we have that

$$(\alpha_1, \dots, \alpha_n) \in S \quad \Leftrightarrow \quad \exists \beta_1, \dots, \beta_m \in \mathcal{O}_K : p(\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_m) = 0.$$

To simplify notation I will assume that $n = m = 1$ and thus that $p(X, Y)$ is bivariant. The general case follows analogously.

To see the first direction, we assume that p has in fact rational integral coefficients and let α be in S. Then there exists an integer $\beta \in \mathcal{O}_K$ such that $p(\alpha, \beta) = 0$. Let now $\sigma_1, \dots, \sigma_k$ be all automorphisms of K. Since each σ_i preserves $\mathbb{Z}$ point-wise ($1 \leq i \leq k$), we know that

$$p(\sigma_i(\alpha), \sigma_i(\beta)) = \sigma_i(p(\alpha, \beta)) = 0$$

and $\sigma_i(\alpha) \in S$ as claimed.

Conversely, let S be self-conjugate and let p_i for $1 \leq i \leq k$ denote the polynomial obtained from p by replacing the coefficients of p by their images under σ_i. We define

$$q(X, Y) := \prod_{i=1}^{k} p_i(X, Y)$$

and note that the coefficients of q are preserved by all automorphisms σ_i. As a consequence of Prop. 2.1.9 we can find for all coefficients $a \in \mathcal{O}_K$ of q, polynomials $P_a, Q_a \in \mathbb{Z}[Y]$ and a constant $c_a \in \mathbb{Z}$ such that

$$\alpha = a \quad \Leftrightarrow \quad \exists \beta \in \mathcal{O}_K : (P_a(\beta) = 0 \wedge Q_a(\beta) = c_a \alpha).$$

Therefore, the relation defined by q can be rewritten in a purely Diophantine form. To see this, we assume that $J \subseteq \mathbb{N}^2$ is finite and

$$q(X, Y) = \sum_{(i,j) \in J} a_{ij} X^i Y^j.$$

Then, we have the following equivalence for all $\alpha \in \mathcal{O}_K$

$$\begin{aligned} \exists \beta \in \mathcal{O}_K : q(\alpha, \beta) = 0 \Leftrightarrow \\ \exists \beta, (\beta_{ij})_{(i,j) \in J} \in \mathcal{O}_K : \end{aligned}$$

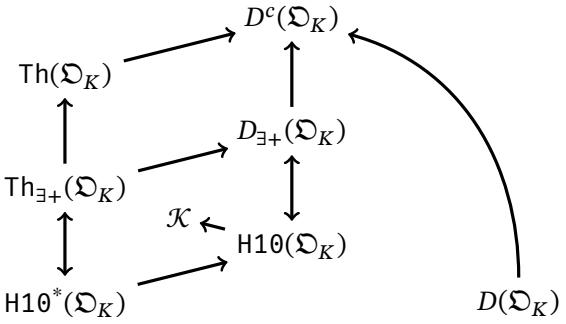


Figure 2.2: Reducibility relations holding between the theories of arbitrary rings of algebraic integers $\mathcal{O}_K$

$$\sum_{(i,j)\in J} \beta_{ij}\alpha^i\beta^j = 0 \wedge$$
$$\bigwedge_{(i,j)\in J} \exists \gamma_{ij} \in \mathcal{O}_K \,:\, (P_{a_{ij}}(\gamma_{ij}) = 0 \wedge Q_{a_{ij}}(\gamma_{ij}) = \beta_{ij}).$$

All that is left to prove is that q and p represent S i.e. that

$$\exists \beta \in \mathcal{O}_K \,:\, p(\alpha,\beta) = 0 \quad \Leftrightarrow \quad \exists \beta \in \mathcal{O}_K \,:\, q(\alpha,\beta) = 0$$

holds for all algebraic integers $\alpha \in \mathcal{O}_K$. To see this, first assume that $p(\alpha,\beta) = 0$ holds. Then since the identity is an automorphism of K, we find that one factor of

$$q(\alpha,\beta) := \prod_{i=1}^{k} p_i(\alpha,\beta)$$

is zero, and thus that $q(\alpha,\beta) = 0$. If on the other hand, $q(\alpha,\beta) = 0$ then one of the factors of q must be zero. Say $p_i(\alpha,\beta) = 0$ and let σ_j be the inverse of σ_i. Then we find that

$$0 = \sigma_j(p_i(\alpha,\beta)) = p(\sigma_j(\alpha),\sigma_j(\beta))$$

and therefore $\sigma_j(\alpha) \in S$. Now since S is self-conjugate by assumption, we can deduce that $\alpha = \sigma_i(\sigma_j(\alpha))$ is contained in S as claimed. □

The diagram in Fig. 2.2 summarizes all the reducibility relations between the theories of rings of algebraic integers that we have proven so far. By the transitivity of many-one reducibility all that is left to prove is many-one reducibility of the halting set $\mathcal{K}$ to the purely Diophantine theory $\mathtt{H10}^*(\mathfrak{O}_K)$. Then the diagram collapses as depicted in Fig. 2.2.

2.1.3 Related problems

The beauty of the model theoretic approach to Hilbert's tenth problem is that it directly gives rise to various generalizations. To conclude this section I will list some results on variants of the problem.

In 1936 Rosser [39] proved—extending a result of Gödel [15]—that the full first order theory

$\mathtt{Th}(\mathfrak{N})$ of the natural numbers is undecidable.[4] As a consequence, the full first order theory of $\mathbb{Z}$ is undecidable, as one can translate a sentence in $\mathbb{N}$ to an equivalent sentence in $\mathbb{Z}$ via the construction described in Example 2.1.3. Considering the full first order theory of $\mathcal{O}_K$, J. Robinson [37] proved as early as 1959 that $\mathtt{Th}(\mathfrak{O}_K)$ is undecidable. In 1970 Matijasevič [26] showed—building on the work of Davis, Putnam, and J. Robinson—the undecidability of Hilbert's tenth problem over $\mathbb{Z}$. More specifically, he provided the last piece of the proof of the Davis-Putnam-Robinson-Matijasevič theorem (DPRM).

THEOREM 2.1.11 (DPRM-THEOREM). *A subset of the natural numbers is semi-decidable if and only if it is Diophantine over* $\mathbb{N}$.

This result is remarkably similar to the key theorem (7) of Gödel's proof [15] of his celebrated first incompleteness theorem. Quite in his spirit [cf. 15, Thm. 9] we can deduce

COROLLARY 2.1.12. *The halting set* $\mathcal{K}$ *is many-one reducible to* $\mathtt{H10}(\mathfrak{Z})$. *Thus, Hilbert's tenth problem over* $\mathbb{Z}$ *is undecidable.*

Proof. Throughout this proof I will identify $\mathbb{Z}$ with the domain of one of its computable representations. Then $\mathbb{N} \subseteq \mathbb{Z}$ is decidable. Indeed, for a given integer $n \in \mathbb{Z}$ we know that

$$n \in \mathbb{N} \quad \Leftrightarrow \quad \exists x_1, x_2, x_3, x_4 \in \mathbb{Z} : n = x_1^2 + x_2^2 + x_3^2 + x_4^2$$

and

$$n \notin \mathbb{N} \quad \Leftrightarrow \quad \exists x_1, x_2, x_3, x_4 \in \mathbb{Z} : n = -\left(x_1^2 + x_2^2 + x_3^2 + x_4^2 + 1\right)$$

hold by Prop. 1.3.20 and $\mathbb{N}$ is decidable by Prop. 1.1.9. As a consequence, we have found a computable representation of the $\mathcal{L}_{ring}$-structure of the non-negative integers and by Example 1.2.15 there exists a computable bijection $f : \omega \to \mathbb{N}$ with an computable inverse.

Now consider $f(\mathcal{K}) \subseteq \mathbb{Z}$. Then the inverse mapping f^{-1} witnesses that $f(\mathcal{K})$ is many-one reducible to $\mathcal{K}$. Thus, $f(\mathcal{K})$ is semi-decidable and by the DPRM-theorem $f(\mathcal{K})$ is Diophantine over $\mathbb{N}$ and therefore Diophantine over $\mathbb{Z}$ as well. Hence, there exists a polynomial $p_{\mathcal{K}} \in \mathbb{Z}[X, Y_1, ..., Y_m]$ with the property that

$$\alpha \in f(\mathcal{K}) \quad \Leftrightarrow \quad \exists \beta_1, \dots, \beta_m \in \mathbb{Z} : p_{\mathcal{K}}(\alpha, \beta_1, \dots, \beta_m) = 0.$$

Finally, we find for all $x \in \omega$ that the $\mathcal{L}_{\mathbb{Z}}$-sentence

$$\exists \mathtt{y}_1 : \dots \exists \mathtt{y}_m : p_{\mathcal{K}}(f(x), \mathtt{y}_1, \dots, \mathtt{y}_m) \doteq 0 \tag{2.1.1}$$

is contained in $\mathtt{H10}(\mathfrak{Z})$ precisely if $x \in \mathcal{K}$. Thus, the function mapping $x \in \omega$ to the Gödelization of (2.1.1) witnesses that $\mathcal{K}$ is many-one reducible to $\mathtt{H10}(\mathfrak{Z})$.

Now Prop. 1.1.13 implies that $\mathtt{H10}(\mathfrak{Z})$ is undecidable, as $\mathcal{K}$ is undecidable. □

[4] At this point I should mention that I assume throughout this thesis that the Peano arithmetic is consistent. See e.g. Chap. 8 of the textbook [4] for a more rigorous discussion of Gödel's results.

In 1986, Rumely [40] published his surprising result that HIO is solvable over $\mathcal{O}$, the ring of all algebraic integers. Van den Dries [11] extended this result to the full first order theory of $\mathcal{O}$ in 1988.

Probably the most prominent open problem in this area is the case of $\mathbb{Q}$. A positive answer to HIO over $\mathbb{Q}$ would imply that there is a universal algorithm deciding whether a variety over $\mathbb{Q}$ has a rational point. By giving a first order definition of $\mathbb{Z}$ over $\mathbb{Q}$, J. Robinson [36] could derive the undecidability of the full first order theory of $\mathbb{Q}$ from the undecidability of the theory of $\mathbb{Z}$ in 1949. But her definition involves universal quantifiers and cannot be used for inferring to HIO. Park [31] strengthend the results of J. Robinson [36, 37] by providing a universal first order definition of $\mathcal{O}_K$ over an arbitrary number field K in 2013. Again moving to larger rings proves to be easier. Tarski [47] showed in 1931 using the method of *quantifier elimination* that the full $\mathcal{L}_{ring}$-theory of the real numbers is decidable. For complex numbers the tools for proving the analogous result were already known in the nineteenth century.

The surveys [22, 33] offer a more extensive overview of problems related to undecidability in number theory.

2.2 Some structural results

Before tackling Hilbert's tenth problem over selected rings of algebraic integers, I list some structural results and methods used within the subsequent proofs. For further structural results see the study [43].

LEMMA 2.2.1. *Let $R_1 \subseteq R_2$ be integral domains such that the quotient field of R_2 is not algebraically closed. If $S \subseteq R_1^m$ is Diophantine over R_1 and R_1 has a Diophantine definition over R_2, then S is Diophantine over R_2. If R_2 is computable, then the defining equation of S over R_2 can be obtained efficiently from the equation over R_1.*

Proof. Let $f(X, Y_1, ..., Y_n)$ give rise to a Diophantine definition of R_1 over R_2 and let $S \subseteq R_1^m$ be Diophantine over R_1. Then there exists some polynomial

$$p \in R_1[X_1, ..., X_m, Y_1, ..., Y_\ell]$$

witnessing that S is Diophantine. To make notation clearer, I assume $\ell = m = n = 1$. The general case follows completely analogously. Then

$$S = \{\alpha \in R_2 : \exists \beta, \gamma_1, \gamma_2 \in R_2 \text{ with } p(\alpha, \beta) = 0 \wedge f(\alpha, \gamma_1) = 0 \wedge f(\beta, \gamma_2) = 0\}$$

is a Diophantine definition of S over R_2. □

Shlapentokh [43] notes that the previous lemma and its corollary are 'the only tool[s] successfully used to show the undecidability of HIO for various subrings of the number fields'. They explain the usefulness of Diophantine definitions.

COROLLARY 2.2.2. *Let $R \supseteq \mathbb{Z}$ be a computable integral domain, whose quotient field is not algebraically closed. If $\mathbb{Z}$ has a Diophantine definition over R then the Diophantine theory* $\mathtt{H10}(\mathfrak{R})$ *of the ring-structure $\mathfrak{R}$ of R is undecidable.*

Proof. Since the non-negative integers are Diophantine over $\mathbb{Z}$ and $\mathbb{Z}$ is Diophantine over R, we know by the lemma above that $\mathbb{N}$ is Diophantine over R and thus $\mathbb{N} \subseteq R$ is semi-decidable. However, the complement $\mathbb{Z} \setminus \mathbb{N}$ is Diophantine over $\mathbb{Z}$ as well, and thus $\mathbb{N} \subseteq R$ is decidable.

As in the proof of Cor. 2.1.12, we can embed the halting set $\mathcal{K} \subseteq \omega$ by a computable bijection $f : \omega \to \mathbb{N} \subseteq R$. Again, $f(\mathcal{K})$ is semi-decidable and thus Diophantine over the rational integers $\mathbb{Z}$. By the lemma $f(\mathcal{K})$ is Diophantine over R. Thus, there exists a polynomial $p_{\mathcal{K}} \in R[X, Y_1, \dots, Y_m]$ such that

$$x \in \mathcal{K} \quad \Leftrightarrow \quad \exists y_1, \dots, y_m \in R : p_{\mathcal{K}}(f(x), y_1, \dots, y_m) = 0, \tag{2.2.1}$$

and as before the computable function mapping $x \in \omega$ to the Gödelization of the equation above witnesses many-one reducibility of $\mathcal{K}$ to $\mathtt{H10}(\mathfrak{R})$. □

Note that this corollary applies to $\mathcal{O}_K$ for each algebraic number field K since the quotient field of $\mathcal{O}_K$ is (isomorphic to) K. In fact, in the case of algebraic integers one can prove that if $\mathbb{Z}$ is Diophantine over $\mathcal{O}_K$, then the purely Diophantine theory of $\mathcal{O}_K$ is equally hard to decide as the Diophantine theory and the halting set.

COROLLARY 2.2.3. *Let K be a number field such that the rational integers $\mathbb{Z}$ are Diophantine over its ring of algebraic integers $\mathcal{O}_K$. Then the halting set $\mathcal{K}$ is many-one reducible to the purely Diophantine theory $\mathtt{H10}^*(\mathfrak{O}_K)$ of $\mathcal{O}_K$.*

Proof. As in the proof of Cor. 2.2.2 one finds a computable bijection $f : \omega \to \mathbb{N} \subseteq \mathcal{O}_K$ and considers $f(\mathcal{K})$. Since $\mathbb{Z}$ is fixed point-wise by all automorphisms of K, in particular $f(\mathcal{K})$ is fixed point-wise, and by Thm 2.1.10 the set $f(\mathcal{K})$ is in fact purely Diophantine.

This means that the polynomial $p_{\mathcal{K}}$ in (2.2.1) can be chosen to have rational integral coefficients. Now since $f(\mathcal{K})$ is a subset of $\mathbb{N}$, we deduce that the partially evaluated polynomial

$$p_{\mathcal{K}}(f(x), Y_1, \dots, Y_m)$$

still has rational integral coefficents. It follows that the Gödelization of (2.2.1) is contained in the theory $\mathtt{H10}^*(\mathfrak{O}_K)$ if and only if $x \in \mathcal{K}$, which concludes the proof. □

One can even strengthen the result of the corollary to obtain the full analogue of the DPRM-theorem (2.1.11) for rings of algebraic integers. This was shown by Davis, Matijasevič, and J. Robinson [7, §11].

THEOREM 2.2.4. *Let K be an algebraic number field and $\mathcal{O}_K$ its ring of algebraic integers. Then every semi-decidable subset of $\mathcal{O}_K$ is Diophantine if and only if the rational integers $\mathbb{Z}$ are Diophantine over $\mathcal{O}_K$.*

Proof. As the $\mathcal{L}_{\mathcal{O}_K}$-structure of $\mathcal{O}_K$ is computable, the interpretations of the constants $-1, 0, 1$ and addition are computable. As a consequence, the surjective function $f : \omega \to \mathbb{Z} \subseteq \mathcal{O}_K$ defined by

$$f(\ulcorner n \urcorner) = \begin{cases} 0 \overbrace{+ 1 \dots + 1}^{k\text{-times}} & \text{if } n = 2k \\ 0 \underbrace{+ (-1) \dots + (-1)}_{k\text{-times}} & \text{if } n = 2k + 1 \end{cases}$$

is computable and $\mathbb{Z}$ is semi-decidable. Thus, it suffices to prove that if $\mathbb{Z}$ is Diophantine over $\mathcal{O}_K$, then every semi-decidable set is Diophantine over $\mathcal{O}_K$.

Let $A \subseteq \mathcal{O}_K^k$ be semi-decidable and let $\{\xi_1, ..., \xi_n\}$ be an integral basis for $\mathcal{O}_K$ over $\mathbb{Z}$. We define the set of all coefficients of elements in A by

$$S := \left\{(a_{11}, ..., a_{1n}, ..., a_{k1}, ..., a_{kn}) \in \mathbb{Z}^{kn} \,:\, \left(\sum_{i=1}^{n} a_{ij}\xi_i\right)_{1\leq j\leq k} \in A\right\}.$$

As A is semi-decidable so is S. Note that this is exactly how we efficiently represent finitely generated free $\mathbb{Z}$-algebras and thus $\mathcal{O}_K$ in Example 1.2.12.(4). By the DPRM-theorem (2.1.11) the set S is Diophantine over $\mathbb{Z}$, i.e. there exists a polynomial p with coefficients in $\mathbb{Z}$ such that

$$\begin{aligned}&(a_{11}, ..., a_{1n}, ..., a_{k1}, ..., a_{kn}) \in R \Leftrightarrow\\ &\quad \exists \beta_1, \dots, \beta_m \in \mathbb{Z} \,:\, p(a_{11}, ..., a_{1n}, ..., a_{k1}, ..., a_{kn}, \beta_1, \dots, \beta_m) = 0.\end{aligned}$$

It immediately follows that

$$\begin{aligned}&(\alpha_1, \dots, \alpha_k) \in A \Leftrightarrow\\ &\quad \exists a_{11}, ..., a_{1n}, ..., a_{k1}, ..., a_{kn},\ \beta_1, \dots, \beta_m \in \mathbb{Z} :\\ &\quad \begin{cases} p(a_{11}, ..., a_{1n}, ..., a_{k1}, ..., a_{kn}, \beta_1, \dots, \beta_m) = 0\\ \alpha_1 = a_{11}\xi_1 + ... + a_{1n}\xi_n\\ \vdots\\ \alpha_k = a_{k1}\xi_1 + ... + a_{kn}\xi_n \end{cases}.\end{aligned}$$

By assumption there exists a Diophantine definition of $\mathbb{Z}$ over $\mathcal{O}_K$. So by the procedure described in the proof of Cor. 2.2.2, one can translate the conditions above into a Diophantine definition of A over $\mathcal{O}_K$. □

Given the tools and structural results that we have just introduced, all that is left to prove the undecidability of Hilbert's tenth problem over a fixed ring of algebraic integers $\mathcal{O}_K$, is showing that $\mathbb{Z}$ has a Diophantine definition over $\mathcal{O}_K$. This task will fill the remainder of this thesis. But before moving on to the case of specific number fields, I will present an important tool in proving that a field extension L/K has a Diophantine definition of $\mathcal{O}_K$ over $\mathcal{O}_L$. This so called *strong vertical method* was formalized by Denef and Lipshitz and successfully applied over various number fields [e.g. 8–10, 32, 42]. I do however present a version of this result that can be obtained from Lem. 1 of [10] and Lem. 8 of [8] and is similar to Lem. 7.1.3 of [44].

THEOREM 2.2.5. *Let L/K be an extension of number fields and $n = [L : \mathbb{Q}]$. If $x, y \in \mathcal{O}_L$, $y \neq 0$, and $\alpha \in \mathcal{O}_K$ satisfy*

$$|\sigma_i(x)| < \frac{1}{2}|N_{L/\mathbb{Q}}(y)|^{\frac{1}{n}} \text{ for all } 1 \leq i \leq n, \tag{2.2.2}$$

$$|\sigma_i(\alpha)| < \frac{1}{2}|N_{L/\mathbb{Q}}(y)|^{\frac{1}{n}} \text{ for all } 1 \leq i \leq n, \text{ and} \tag{2.2.3}$$

$$x \equiv \alpha \mod (y) \text{ in } \mathcal{O}_L, \tag{2.2.4}$$

where $\sigma_1, \dots, \sigma_n$ *denote the embeddings of* L *into the complex pane* $\mathbb{C}$. *Then*

$$x = \alpha \in \mathcal{O}_K.$$

Proof. By (2.2.4) we know that there exists an integer $\beta \in \mathcal{O}_L$ such that $x - \alpha = \beta y$. As a consequence, either $x = \alpha$ or

$$|N_{L/\mathbb{Q}}(x - \alpha)| = |N_{L/\mathbb{Q}}(\beta y)| \geq |N_{L/\mathbb{Q}}(y)|$$

holds. However, (2.2.2) and (2.2.3) imply that

$$|N_{L/\mathbb{Q}}(x - \alpha)| = \prod_{i=1}^{n} |\sigma_i(x - \alpha)| \leq \prod_{i=1}^{n} 2 \max(|\sigma_i(x)|, |\sigma_i(\alpha)|) < |N_{L/\mathbb{Q}}(y)|.$$

□

Unlike Shlapentokh's formulation, if $y \in \mathcal{O}_K$ then the conditions on the embeddings are easily seen to be Diophantine [cf. 8, Lem. 8].

LEMMA 2.2.6. *Let* K *be a number field of degree* n *over* $\mathbb{Q}$ *and let* $\sigma_1, \dots, \sigma_n$ *be its embeddings into the complex pane. Let* $\alpha, \beta \in \mathcal{O}_K$ *be algebraic integers with* $\beta \neq 0$ *such that*

$$2^{n+1} \prod_{i=0}^{n-1} (\alpha + i)^n \mid \beta.$$

Then $|\sigma_i(\alpha)| < 1/2 |N_{K/\mathbb{Q}}(\beta)|^{1/n}$ *for all* $1 \leq i \leq n$.

Proof. Fix some $j \in \{0, 1, ..., n-1\}$ and notice that $2^{n+1}(\alpha + j)^n$ divides β. From this it follows that

$$|N_{K/\mathbb{Q}}(2^{n+1}(\alpha + j)^n)| \leq |N_{K/\mathbb{Q}}(\beta)|,$$

or put differently

$$1 \leq |N_{K/\mathbb{Q}}(\alpha + j)| \leq |N_{K/\mathbb{Q}}(2^{-n-1}\beta)|^{\frac{1}{n}}.$$

Set $c := |N_{K/\mathbb{Q}}(2^{-n-1}\beta)|^{1/n}$ then

$$|N_{K/\mathbb{Q}}(\alpha + j)| = \prod_{i=1}^{n} |\sigma_i(\alpha) + j| \leq c.$$

I claim that this implies that $|\sigma_i(a)| < 2^n c = 1/2 |N_{K/\mathbb{Q}}(\beta)|^{1/n}$.

Indeed, this follows from a more general property of complex numbers. Namely, if $a_1, \dots, a_n \in \mathbb{C}$

are fixed complex numbers with the property that

$$\prod_{i=1}^{n} |a_i + j| \leq C$$

for a fixed constant $C \geq 1$ and all $0 \leq j \leq n-1$ then $|a_i| < 2^n C$ for all $1 \leq i \leq n$.

Note that if $0 \leq j_1, j_2 \leq n-1$ have the property that $|a_i + j_k| < \frac{1}{2}$ then

$$|j_1 - j_2| \leq |a_i + j_1| + |a_i + j_2| < \frac{1}{2} + \frac{1}{2} = 1$$

and thus $j_1 = j_2$.

We will argue by induction on n and notice that the claim is trivial for $n = 1$. Thus, we may assume that $n > 1$ and that the claim is proven for all smaller collections of complex numbers. We will distinguish two cases.

Firstly, let us assume that

$$\forall j \in \{0, ..., n-1\} : \exists i_j \in \{1, ..., n\} : |a_{i_j} + j| < \frac{1}{2}.$$

Since we allow only n values for both j and i_j and we know by the observation that two different values of j must have two different witnesses i_j, we find that there must exist a bijective function $f : \{0, ..., n-1\} \to \{1, ..., n\}$ with the property that

$$|a_{f(j)} + j| < \frac{1}{2}.$$

Then for all indices $j' \neq j$ we must have

$$|a_{f(j)} + j'| \geq \frac{1}{2}.$$

Set $i_0 := f(n-1)$ then we know for all $0 \leq j \leq n-2$ that $|a_{i_0} + j| \geq 1/2$ and therefore that

$$C \geq \prod_{i=1}^{n} |a_i + j| \geq \frac{1}{2} \prod_{\substack{i=1 \\ i \neq i_0}}^{n} |a_i + j|.$$

Thus, $a_1, ..., a_{i_0-1}, a_{i_0+1}, ..., a_n$ satisfy the assumption of the induction hypothesis (w.r.t. $C' := 2C$) and hence

$$|a_i| < 2^{n-1} 2C.$$

To reach a contradiction assume that $|a_{i_0}| \geq 2^n C$. But then

$$\frac{1}{2} > |a_{i_0} + n - 1| \geq |a_{i_0}| - |n-1| \geq 2^n C - n + 1 \geq 2^n - n + 1 \geq 2$$

holds, thus, concluding the first case.

As for the second case, let us assume that

$$\exists j_0 \in \{0, ..., n-1\} : \forall i \in \{1, ..., n\} : |a_i + j_0| \geq \frac{1}{2}.$$

Then we have for all $1 \leq k \leq n$ that

$$C \geq \prod_{i=1}^{n} |a_i + j_0| \geq \frac{1}{2^{n-1}} |a_k + j_0|.$$

From this it is immediate that

$$|a_k + j_0| \leq C 2^{n-1}.$$

Now a simple application of the triangular inequality yields

$$|a_k| = |a_k + j_0 - j_0| \leq |a_k + j_0| + |j_0| \leq 2^{n-1} C + n - 1 < 2^{n-1} C + 2^{n-1} C = 2^n C.$$

□

If σ_i is a real embedding, the following lemma [cf. 8, Lem. 9] could have been used as well.

LEMMA 2.2.7. *Let K be a number field and $\sigma : K \to \mathbb{R}$ be a real embedding. Then the relation $\sigma(\alpha) \geq 0$ is Diophantine over $\mathcal{O}_K$.*

Proof. I claim that there exists an algebraic integer $c \in \mathcal{O}_K$ such that $\sigma(c) > 0$ and $\tau(c) < 0$ for all other real embeddings $\tau \neq \sigma$. Indeed let $\sigma = \sigma_1, \dots, \sigma_{r_K} : K \to \mathbb{R}$ be the real embeddings and $\sigma_{r_K+1}, \overline{\sigma_{r_K+1}}, ..., \sigma_{r_K+s_K}, \overline{\sigma_{r_K+s_K}} : K \to \mathbb{C}$ be the complex embeddings of K. Then the mapping $\mathcal{O}_K \to \mathbb{R}^n$ (with $n = r_K + 2s_K = [K : \mathbb{Q}]$) defined by

$$x \mapsto (\sigma_1(x), ..., \sigma_{r_K}(x), \mathfrak{R}\sigma_{r_K+1}(x), \mathfrak{I}\sigma_{r_K+1}(x), ..., \mathfrak{R}\sigma_{r_K+s_K}(x), \mathfrak{I}\sigma_{r_K+s_K}(x))$$

maps $\mathcal{O}_K$ to a lattice Λ of rank n in $\mathbb{R}^n$ [see 29, Chap. I, §5]. The claimed conditions on the sign of $\sigma(c)$ and $\tau(c)$ respectively correspond directly to the sign of the first r_K coordinates with respect to the standard basis of $\mathbb{R}^n$. They can clearly be satisfied as all of $\mathbb{R}^n$ can be covered by translating the fundamental parallelepiped of Λ allong the lattice points of Λ.

Let $\alpha \in \mathcal{O}_K$ be such that $\sigma(\alpha) \geq 0$. Then byLem. 1.3.29 there exist $z_1, z_2, z_3, z_4 \in K$ such that

$$x = z_1^2 + z_2^2 + c z_3^2 + z_4^2$$

Since K is the fraction field of $\mathcal{O}_K$, there exists an algebraic integer y_0 such that $y_0 z_i$ is an algebraic integer for $1 \leq i \leq 4$. We conclude that

$$\exists y_0, y_1, y_2, y_3, y_4 \in \mathcal{O}_K : \left(y_0 \neq 0 \wedge y_0^2 x = y_1^2 + y_2^2 + c y_3^2 + y_4^2\right)$$

is a Diophantine representation of a set containing x. To finish the proof note that if x satisfies the

representation above then

$$\sigma(x) = \sigma\left(\frac{y_1}{y_0}\right)^2 + \sigma\left(\frac{y_2}{y_0}\right)^2 + c\sigma\left(\frac{y_3}{y_0}\right)^2 + \sigma\left(\frac{y_4}{y_0}\right)^2 \geq 0.$$

□

Note that we can exchange the bound 0 to any value in the image $\sigma(K) \subseteq \mathbb{R}$. Indeed, for a given bound $\sigma(a/b)$, where $a, b \in \mathcal{O}_K$ (cf. Thm 1.3.6), this can be achieved by the relation

$$\exists \beta \in \mathcal{O}_K \,:\, (\sigma(\beta) \geq 0) \wedge \left(\beta = \alpha - \frac{a}{b}\right)$$

which is equivalent to the Diophantine relation

$$\exists \beta \in \mathcal{O}_K \,:\, (\sigma(\beta) \geq 0) \wedge (b\beta = b\alpha - a).$$

Similarly, one can obtain upper bounds by replacing x by $-x$.

2.3 Hilbert's tenth problem over totally real number fields and number fields with one pair of non-real embeddings

I will closely follow the papers of Denef [8] and Pheidas [32], whose structure in turn heavily depends on the article 'Hilbert's tenth problem is unsolvable' by Davis [5]. This way, one can prove the undecidability of Hilbert's tenth problem over rings of algebraic integers in totally real number fields and number fields with one pair of non-real embeddings and at least one real embedding in one go. This approach is also present in Sections 6.3 and 7.2 of the study [44] by Shlapentokh. The same author has proven the second result independently of Pheidas in her thesis [42].

2.3.1 Finitely many easy lemmas

We start by defining two sequences, that satisfy Pell's equation stated below.

$$x^2 - dy^2 = 1 \tag{2.3.1}$$

Using modified versions of the techniques presented by Matijasevič [26], it will be shown that the index m can be obtained in a Diophantine way from $\mathrm{y}_m(a)$ for certain subsequences of the sequences defined below.

DEFINITION. Let K be an algebraic number field, $\mathcal{O}_K$ its ring of algebraic integers and fix $a \in \mathcal{O}_K$. One defines $\delta(a) := \sqrt{a^2 - 1}$ and $\varepsilon(a) := a + \delta(a)$, where we demand that $-\pi/2 < \arg \delta(a) \leq \pi/2$. If $\delta(a) \notin K$ one defines $\mathrm{x}_m(a), \mathrm{y}_m(a) \in \mathcal{O}_K$ for $m \in \mathbb{N}$ by

$$\mathrm{x}_m(a) + \delta(a)\mathrm{y}_m(a) = (\varepsilon(a))^m. \tag{2.3.2}$$

This definition includes the case $K = \mathbb{Q}$ with $\mathcal{O}_K = \mathbb{Z}$ of [5]. However, I am using the slightly modified notation of [8, 32]. Under the assumptions of the definition, $\delta(a)$ is a root of the monic quadratic polynomial

$$X^2 - a^2 + 1 \in \mathcal{O}_K[X].$$

Therefore, the extension $K[\delta(a)]/K$ is quadratic and $\delta(a) \in \mathcal{O}_{K[\delta(a)]}$ in an algebraic integer. The sequences $\mathrm{x}_m(a)$ and $\mathrm{y}_m(a)$ are well defined for each $m \in \mathbb{N}$ as they correspond to the coefficients of $(\varepsilon(a))^m$ in $K[\delta(a)]/K$ with respect to the basis $\{1, \delta(a)\}$. If the reference is clear, I will omit the dependency on a writing $\delta, \varepsilon, \mathrm{x}_m$ and y_m instead. In the following the number field $K[\delta(a)]$ will be denoted by L.

Remark. As L/K with $L = K[\delta]$ has degree two, there is exactly one pair of field automorphisms on L preserving K point-wise, namely $\sigma_1^K(\alpha+\delta\beta) = \alpha+\delta\beta$ and $\sigma_2^K(\alpha+\delta\beta) = \alpha-\delta\beta$ for $\alpha, \beta \in \mathcal{O}_K$. The latter will be denoted by $(\eta)^* = \sigma_2^K(\eta)$ to emphasize the analogy of complex conjugation.

EXAMPLE 2.3.1. Consider the number field $K := \mathbb{Q}[\sqrt{2}]$. It is not hard to check that $\left\{1, \sqrt{2}\right\}$ is an integral basis for $\mathcal{O}_K$. We may choose $a = 2$ as the integer in the definition of the sequences. Indeed, we find $\delta = \sqrt{a^2 - 1} = \sqrt{3}$ and if $\sqrt{3}$ were contained in K then it would be an algebraic integer in $\mathcal{O}_K$. Thus, there exist $m, n \in \mathbb{Z}$ such that

$$\sqrt{3} = m + n\sqrt{2}.$$

Now since neither $\sqrt{3}$ nor $\sqrt{3/2}$ are rational integers, we may assume that both m and n are non-zero. But then

$$3 = m^2 + 2mn\sqrt{2} + 2n^2$$

which is equivalent to

$$\sqrt{2} = \frac{3 - m^2 - 2n^2}{2mn} \in \mathbb{Q}.$$

Note that $\varepsilon = a + \delta = 2 + \sqrt{3}$ then by definition of the sequences we have for all $m \in \mathbb{N}$ that

$$\begin{aligned} \mathrm{x}_m + \delta\mathrm{y}_m = \varepsilon^m = \left(2 + \sqrt{3}\right)^m &= \sum_{j=0}^{m} \binom{m}{j} 2^{m-j}\sqrt{3^j} \\ &= \sum_{\substack{j=0 \\ j \text{ even}}}^{m} \binom{m}{j} 2^{m-j} 3^{\frac{j}{2}} + \sqrt{3} \sum_{\substack{j=0 \\ j \text{ odd}}}^{m} \binom{m}{j} 2^{m-j} 3^{\frac{j-1}{2}}. \end{aligned}$$

Thus, we have found that

$$\mathrm{x}_m = \sum_{\substack{j=0 \\ j \text{ even}}}^{m} \binom{m}{j} 2^{m-j} 3^{\frac{j}{2}}$$

and

$$y_m = \sum_{\substack{j=0 \\ j \text{ odd}}}^{m} \binom{m}{j} 2^{m-j} 3^{\frac{j-1}{2}}.$$

Let me now collect some properties of these sequences. The proofs are generalized versions of the ones given in Davis' paper [5].

LEMMA 2.3.2. *Let K be an algebraic number field and $a \in \mathcal{O}_K$ such that $\delta(a) \notin K$. Then*

(i) ε is a unit in $\mathcal{O}_L$, its inverse is given by $\varepsilon^{-1} = a - \delta = (\varepsilon)^*$, and

(ii) x_m, y_m satisfy Pell's equation (2.3.1) for all $m \in \mathbb{N}$, using $d = \delta(a)^2$ as parameter.

Proof. (i) We have $\varepsilon\,(a - \delta) = (a + \delta)(a - \delta) = a^2 - \delta^2 = 1$ as desired.

(ii) One uses induction on m. If $m = 0$, the pair $x_0 = 1$ and $y_0 = 0$ yields a trivial solution to equation (2.3.1). Let the claim be proven for all pairs x_n, y_n with $n \leq m$. Then rewriting the definition of x_{m+1}, y_{m+1} one obtains

$$x_{m+1} + \delta y_{m+1} = \varepsilon^{m+1} = (x_m + \delta y_m)\varepsilon.$$

Applying the automorphism $(\cdot)^*$ implies

$$(x_{m+1} + \delta y_{m+1})^* = x_{m+1} - \delta y_{m+1} = (x_m - \delta y_m)\varepsilon^{-1}$$

and multiplication of both equations yields

$$x_{m+1}^2 - d y_{m+1}^2 = (x_{m+1} + \delta y_{m+1})(x_{m+1} - \delta y_{m+1}) = 1,$$

as claimed.

□

The defining equation

$$x_m + \delta y_m = \varepsilon^m = (x_1 + \delta y_1)^m$$

can be seen as an analogue of the trigonometric identity

$$\cos m + i \sin m = e^{im} = (\cos 1 + i \sin 1)^m,$$

where x_m plays the role of $\cos m$, y_m the one of $\sin m$, and i is replaced by δ. In this view Pell's equation (2.3.1) is the analogue of the Pythagorean identity

$$\cos(m)^2 + \sin(m)^2 = 1.$$

The next lemma proves the identities corresponding to $\cos m = \mathfrak{Re}^{im}$, $\sin m = \mathfrak{Im}^{im}$, and the addition formulas.

LEMMA 2.3.3. *Let K be an algebraic number field and $a \in \mathcal{O}_K$ such that $\delta = \delta(a) \notin K$. Then for all $m, k \in \mathbb{N}$ one has*

(i) $\mathrm{x}_m = (\varepsilon^m + \varepsilon^{-m})/2$ *and* $\mathrm{y}_m = (\varepsilon^m - \varepsilon^{-m})/(2\delta)$*, as well as,*
(ii) $\mathrm{x}_{m\pm k} = \mathrm{x}_m\mathrm{x}_k \pm \delta^2\mathrm{y}_m\mathrm{y}_k$*, and* $\mathrm{y}_{m\pm k} = \mathrm{x}_k\mathrm{y}_m \pm \mathrm{x}_m\mathrm{y}_k$.

Proof. (i) In Lem. 2.3.2.(i) we have seen that $\varepsilon^{-1} = (\varepsilon)^*$ and therefore $\varepsilon^{-m} = \left((\varepsilon)^*\right)^m$. Observe that for arbitrary $\alpha, \beta \in \mathcal{O}_K$ we have

$$\alpha + \beta\delta + (\alpha + \delta\beta)^* = 2\alpha \quad \text{and} \quad \alpha + \beta\delta - (\alpha + \delta\beta)^* = 2\delta\beta.$$

Now, setting $\alpha + \delta\beta = \varepsilon^m$ yields the claim.
(ii) By the defining equation for x_{m+k} and y_{m+k} we have

$$\begin{aligned}\mathrm{x}_{m+k} + \delta\mathrm{y}_{m+k} = \varepsilon^{m+k} &= (\mathrm{x}_m + \delta\mathrm{y}_m)(\mathrm{x}_k + \delta\mathrm{y}_k) = \\ &= (\mathrm{x}_m\mathrm{x}_k + \delta^2\mathrm{y}_m\mathrm{y}_k) + \delta(\mathrm{x}_m\mathrm{y}_k + \mathrm{x}_k\mathrm{y}_m)\end{aligned}$$

and thus

$$\begin{aligned}\mathrm{x}_{m+k} &= \mathrm{x}_m\mathrm{x}_k + \delta^2\mathrm{y}_m\mathrm{y}_k, \\ \mathrm{y}_{m+k} &= \mathrm{x}_m\mathrm{y}_k + \mathrm{x}_k\mathrm{y}_m.\end{aligned}$$

The identities for x_{m-k} and y_{m-k} follow analogously.

□

Setting $k = 1$ in the lemma above, one obtains $\mathrm{x}_{m\pm1} = a\mathrm{x}_m \pm \delta^2\mathrm{y}_m$ and $\mathrm{y}_{m\pm1} = a\mathrm{y}_m \pm \mathrm{x}_m$. A further immediate consequence of this lemma is the subsequent one, which brings divisibility into play.

LEMMA 2.3.4. *Let K be a number field and $a \in \mathcal{O}_K$ such that $\delta = \delta(a) \notin K$. Then for all $m, k \in \mathbb{N}$, $k \neq 0$ we have that*

(i) y_m *divides* y_{mk} *in* $\mathcal{O}_K$*,*
(ii) $\mathrm{y}_{mk} \equiv k\mathrm{x}_m^{k-1}\mathrm{y}_m \mod (\mathrm{y}_m^3)$ *in* $\mathcal{O}_K$*, as well as*
(iii) the principal ideals (x_m) *and* (y_m) *are relative prime in* $\mathcal{O}_K$ *for all* $m \in \mathbb{N}$

Proof. (i) I argue by induction on k. The claim is trivial if $k = 1$ and Lem. 2.3.3.(ii) implies that

$$\mathrm{y}_{m(k+1)} = \mathrm{x}_m\mathrm{y}_{mk} + xmk\mathrm{y}_m.$$

If the claim is proven for all factors up to k, one finds that $\mathrm{y}_m \mid \mathrm{y}_{mk}$ and $\mathrm{y}_m \mid \mathrm{y}_m$ trivially. As a consequence, $\mathrm{y}_m \mid \mathrm{y}_{m(k+1)}$.
(ii) Again the defining equation yields

$$\mathrm{x}_{mk} + \delta\mathrm{y}_{mk} = \varepsilon^{mk} = (\mathrm{x}_m + \delta\mathrm{y}_m)^k = \sum_{j=0}^{k} \binom{k}{j} \mathrm{x}_m^{k-j}\mathrm{y}_m^j\delta^j$$

and

$$\mathrm{y}_{mk} = \sum_{\substack{j=0 \\ j \text{ odd}}}^{k} \binom{k}{j} \mathrm{x}_m^{k-j} \mathrm{y}_m^j \delta^{j-1}.$$

In the equation above all terms for $j > 1$ are divisible by y_m^3 and thus vanish modulo (y_m^3). The only term remaining is $k\mathrm{x}_m^{k-1}\mathrm{y}_m$ as claimed.

(iii) Since $(\mathrm{x}_m, \mathrm{y}_m)$ is a solution to bells equation, we know that

$$1 = \mathrm{x}_m^2 - (a^2 - 1)\mathrm{y}_m^2.$$

is contained in the sum of ideals $(\mathrm{x}_m) + (\mathrm{y}_m)$ and thus the ideals are relative prime as claimed.

□

The next lemma even though being easy to prove provides a valuable tool in studying the sequences x_m and y_m. It derives a recursive definition and lets one prove properties of the sequences, by proving them for $m \in \{0, 1\}$ and inferring the properties for $m + 1$ from m and $m - 1$.

LEMMA 2.3.5. *Let K be a number field and $a \in \mathcal{O}_K$ such that $\delta = \delta(a) \notin K$. For $m > 1$ the following recursive conditions hold in $\mathcal{O}_K$.*

$$\begin{aligned} \mathrm{x}_{m+1} &= 2a\mathrm{x}_m - \mathrm{x}_{m-1}, & \mathrm{x}_1 &= a, \mathrm{x}_0 = 1 \\ \mathrm{y}_{m+1} &= 2a\mathrm{y}_m - \mathrm{y}_{m-1}, & \mathrm{y}_1 &= 1, \mathrm{y}_0 = 0 \end{aligned}$$

Proof. The initial conditions follow from $\varepsilon = a + \delta$ and $\varepsilon^0 = 1$. To prove the the difference equations one uses Lem. 2.3.3.(ii) and obtains

$$\begin{aligned} \mathrm{x}_{m+1} &= a\mathrm{x}_m + \delta^2\mathrm{y}_m, & \mathrm{y}_{m+1} &= a\mathrm{y}_m + \mathrm{x}_m, \\ \mathrm{x}_{m-1} &= a\mathrm{x}_m - \delta^2\mathrm{y}_m, & \mathrm{y}_{m-1} &= a\mathrm{y}_m - \mathrm{x}_m. \end{aligned}$$

Summation yields $\mathrm{x}_{m+1} + \mathrm{x}_{m-1} = 2a\mathrm{x}_m$ and $\mathrm{y}_{m+1} + \mathrm{y}_{m-1} = 2a\mathrm{y}_m$. □

One applies the previous lemma to prove some congruence conditions.

LEMMA 2.3.6. *Let K be a number field and $a, b, c \in \mathcal{O}_K$ such that $\delta(a), \delta(b) \notin K$. Then for all $m \in \mathbb{N}$ the following congruences hold in $\mathcal{O}_K$.*

(i) $\mathrm{y}_m(a) \equiv m \mod (a - 1)$
(ii) If $a \equiv b \mod (c)$, *then* $\mathrm{x}_m(a) \equiv \mathrm{x}_m(b) \mod (c)$ *and* $\mathrm{y}_m(a) \equiv \mathrm{y}_m(b) \mod (c)$.

Proof. Both congruences become equalities if $m = 0$. As for $m = 1$, the first congruence is again an equality as $\mathrm{y}_1(a) = 1$ independently of a. The second claim is trivial since $x_1(\eta) = \eta$ and $\mathrm{y}_1(\eta) = 1$ for $\eta \in \{a, b\}$. At this point one proceeds inductively and assumes the claims to be proven for all indices lower than $m + 1$.

(i) Note that $a \equiv 1 \mod (a-1)$ and thus by Lem. 2.3.5

$$y_{m+1} = 2ay_m - y_{m-1} \equiv 2m - (m-1) = m+1 \mod (a-1)$$

as claimed.

(ii) Using Lem. 2.3.5 again, we see that for fixed m the coefficients $x_m(\eta)$ and $y_m(\eta)$ can be expressed as some fixed polynomial in η. For the congruence this means

$$x_{m+1}(a) = 2ax_m(a) - x_{m-1}(a) \equiv 2bx_m(b) - x_{m-1}(b) = x_{m+1}(b) \mod (c)$$

and for y_{m+1} completely analogously.

□

LEMMA 2.3.7. *Let K be a number field and $a \in \mathcal{O}_K$ such that $\delta = \delta(a) \notin K$. Then for $m, k \in \mathbb{N}$ such that $m \pm k \geq 0$ the following congruence holds in $\mathcal{O}_K$.*

$$x_{2m\pm k} \equiv -x_k \mod (x_m)$$

Proof. By applying the addition formulas of Lem. 2.3.3.(ii) twice and using that x_m and y_m solve Pell's equation (2.3.1) one obtains

$$\begin{aligned} x_{2m\pm k} &= x_m x_{m\pm k} + \delta^2 y_m y_{m\pm k} \equiv \delta^2 y_m (y_m x_k \pm x_m y_k) \\ &\equiv \delta^2 y_m^2 x_k = (x_m^2 - 1)x_k \equiv -x_k \mod (x_m). \end{aligned}$$

□

At this point for the first time in this section I state a result that is no direct generalization of a result of Davis [5] and present proofs given in [8] or [44]. Note however that the results are nevertheless true for the case $K = \mathbb{Q}$ and $\mathcal{O}_K = \mathbb{Z}$.

LEMMA 2.3.8. *Let K be a number field and $a \in \mathcal{O}_K$ such that $\delta = \delta(a) \notin K$. Then for all non-negative integers $k, m \in \mathbb{N}$ the following congruence holds in $\mathcal{O}_K$.*

$$x_{2km} \equiv (-1)^k \mod (x_m)$$

Proof. If $k = 0$ the congruence becomes and identity and if $k = 1$ the claim follows directly from the lemma above. Assuming the claim to be proven for all integers lower than k, we find—by applying Lem. 2.3.3.(ii) twice—that

$$\begin{aligned} x_{2km} &= x_{2(k-1)m} x_{2m} + \delta^2 y_{2(k-1)m} y_{2m} \equiv (-1)^k + \delta^2 y_{2(k-1)m} y_{2m} \\ &= (-1)^k + \delta^2 y_{2(k-1)m}\, 2x_m y_m \equiv (-1)^k \mod (x_m) \end{aligned}$$

□

LEMMA 2.3.9. *Let K be a number field and $a \in \mathcal{O}_K$ such that $\delta = \delta(a) \notin K$. Then for all $\eta \in \mathcal{O}_K \setminus \{0\}$ there exists an $m \in \mathbb{N}$ such that $\eta \mid y_m$ in $\mathcal{O}_K$.*

Proof. I claim that the factor ring $\mathcal{O}_L/(2\delta\eta)$, where $(2\delta\eta)$ denotes the principal ideal generated by $2\delta\eta$ in $\mathcal{O}_L = \mathcal{O}_{K[\delta]}$, is finite.

To show this let $\alpha \in (2\delta\eta) \setminus \{0\}$ and let $a_0 \in \mathbb{Z}$ be the constant term of its minimal polynomial $\mu_{\mathbb{Q},\alpha}(X) := \alpha^m + ... + a_1\alpha + a_0 \in \mathbb{Z}[X]$. Since α is non-zero and $\mu_{\mathbb{Q},\alpha}$ is irreducible, a_0 is non-zero as well. Furthermore, note that $a_0 = -\alpha^m - ... - a_1\alpha \in (\alpha)$ and thus we have the inclusion of $\mathcal{O}_L$-ideals

$$(0) \subsetneq (a_0) \subseteq (\alpha) \subseteq (2\delta\eta).$$

If we can show that $\mathcal{O}_L/(a_0)$ is finite, then the $\mathcal{O}_L/(a_0)$-ideal $(2\delta\eta)/(a_0)$ is finite as well. Observing

$$\mathcal{O}_L/(2\delta\eta) \cong (\mathcal{O}_L/(a_0)) \,/\, ((2\delta\eta)/(a_0))$$

will prove the claim. Let $\zeta_1, ..., \zeta_\ell \in \mathcal{O}_L$ with $\ell := [L : \mathbb{Q}]$ be an integral basis of $\mathcal{O}_L$ over $\mathbb{Q}$. Then every $\beta \in \mathcal{O}_L$ can be written as $\beta = k_1\zeta_1 + ...k_\ell\zeta_\ell$ for some $k_1, ..., k_\ell \in \mathbb{Z}$. But every k_i must belong to one of at most $|a_0|$ many congruence classes modulo $a_0\mathbb{Z} \subseteq a_0\mathcal{O}_L = (a_0)$. Thus, k_i must belong to one of at most $|a_0|$ cosets of $\mathcal{O}_L/(a_0)$. Since $k_1, ..., k_\ell$ determine every $\beta \in \mathcal{O}_L$ uniquely, the factor ring $\mathcal{O}_L/(a_0)$ can have at most cardinality $|a_0|^\ell$.

Let m be the order of the group of units in the finite ring $\mathcal{O}_L/(2\delta\eta)$. Then $\varepsilon^{\pm m} \equiv 1 \mod (2\delta\eta)$. Hence, $2\delta\eta \mid \varepsilon^m - \varepsilon^{-m}$ in $\mathcal{O}_L$ and therefore

$$\eta \,\Big|\, \frac{\varepsilon^m - \varepsilon^{-m}}{2\delta}$$

in $\mathcal{O}_L$, where the right hand side equals y_m by Lem. 2.3.3.(i). Thus, there exists $\zeta \in \mathcal{O}_L$ such that $\eta\zeta = \mathrm{y}_m$. Now since η is non-zero, it is invertible in K. Hence, $\zeta = \mathrm{y}_m\eta^{-1}$ is contained in K. In fact, since $\mathcal{O}_K$ is integrally closed, we even find that ζ is contained in $\mathcal{O}_K$ and η divides y_m in $\mathcal{O}_K$ as claimed. □

LEMMA 2.3.10. *Let K be a number field and $a \in \mathcal{O}_K$ such that $\delta = \delta(a) \notin K$. Then the set*

$$G := \{\alpha + \delta\beta : (\alpha, \beta) \in \mathcal{O}_K^2 \text{ is a solution to (2.3.1) with parameter } d = \delta^2\}$$

is a subgroup of the kernel of the norm map $N_{L/K} : U_L \to U_K$, where U_K and U_L denote the groups of units in $\mathcal{O}_K$ and $\mathcal{O}_L$ respectively.

Proof. First of all, note that, if $\alpha + \delta\beta \in G$, so is $(\alpha + \delta\beta)^* = \alpha - \delta\beta \in G$ because

$$\alpha^2 - d(-\beta)^2 = \alpha^2 - d\beta^2 = 1.$$

Now let $\alpha + \delta\beta$ be an arbitrary element of G, then

$$N_{L/K}(\alpha + \delta\beta) = (\alpha + \delta\beta)(\alpha + \delta\beta)^* = \alpha^2 - d\beta^2 = 1.$$

This implies that $\alpha + \delta\beta \in \ker N_{L/K}$ but also that $\alpha + \delta\beta$ is a unit, as $\alpha - \delta\beta$ is its inverse. The product of two arbitrary elements $\alpha_1 + \delta\beta_1, \alpha_2 + \delta\beta_2 \in G$ is

$$(\alpha_1 + \delta\beta_1)(\alpha_2 + \delta\beta_2) = (\alpha_1\alpha_2 + \delta^2\beta_1\beta_2) + \delta(\alpha_1\beta_2 + \alpha_2\beta_1).$$

We apply the automorphism $(\cdot)^*$ and multiply to obtain

$$(\alpha_1\alpha_2 + \delta^2\beta_1\beta_2)^2 - \delta^2(\alpha_1\beta_2 + \alpha_2\beta_1)^2 = (\alpha_1 + \delta\beta_1)(\alpha_2 + \delta\beta_2)\left((\alpha_1 + \delta\beta_1)(\alpha_2 + \delta\beta_2)\right)^* = \\ = (\alpha_1 + \delta\beta_1)(\alpha_1 + \delta\beta_1)^*(\alpha_2 + \delta\beta_2)(\alpha_2 + \delta\beta_2)^* = 1.$$

As a consequence, G is closed under multiplication and the claim is proven. □

LEMMA 2.3.11. *Let L and K be number fields as defined above. The image $N_{L/K}(U_L) \leq U_K$ has finite index in U_K.*

Proof. I claim that $N_{L/K}(U_L)$ contains α^2 for every $\alpha \in U_K$. This is because the restriction $\sigma_i^K|_{\mathcal{O}_K}$ is just the identity on $\mathcal{O}_K$ for $i \in \{1, 2\}$ and therefore, $N_{L/K}(\alpha) = \alpha^2$ for all $\alpha \in U_K \subseteq U_L$.

Let now $k := \operatorname{rk} U_K$ and identify $U_K = \mu(K) \times \mathbb{Z}^k$, where $\mu(K)$ is the finite cyclic group of roots of unity in K (cf. Thm 1.3.21). Consider the following k elements

$$([0], 1, 0, ..., 0),\ ([0], 0, 1, 0, ..., 0),\ ...,\ ([0], 0, ..., 0, 1)$$

contained in U_K. By the claim their 'squares' are contained in $N_{L/K}(U_L)$ i.e.

$$([0], 2, 0, ..., 0),\ ([0], 0, 2, 0, ..., 0),\ ...,\ ([0], 0, ..., 0, 2) \in N_{L/K}(U_L).$$

As a consequence, the direct product

$$G := \{[0]\} \times \underbrace{2\mathbb{Z} \times ... \times 2\mathbb{Z}}_{k\text{-times}}$$

is a subgroup of $N_{L/K}(U_L)$ and therefore

$$[U_K : N_{L/K}(U_L)] \leq [U_K : G] < \infty.$$

□

As for the free ranks of $U_K, U_L, N_{L/K}(U_L)$ and G the lemma above implies that $\operatorname{rk} N_{L/K}(U_L) = \operatorname{rk} U_K$ and therefore, as an immediate consequence of the first isomorphism theorem [see 23, II §1, p. 89] the following inequality holds

$$\operatorname{rk} G \leq \operatorname{rk} \ker N_{L/K} = \operatorname{rk} U_L - \operatorname{rk} U_K. \tag{2.3.3}$$

Before proving the main result of this section (Cor. 2.3.28) I sketch how Davis [5] establishes the DPRM-theorem.

THEOREM 2.1.11 (DPRM-THEOREM). *A subset of the natural numbers is semi-decidable if and only if it is Diophantine over $\mathbb{N}$.*

First he proves using the sequences above that the exponential function is Diophantine over $\mathbb{N}$ [5, Thm 3.3]. Then he is able to extend the language of Diophantine predicates by *bounded existential*

and *bounded universal quantifiers*, i.e. by

$$\begin{aligned}(\exists y)_{\leq x}\phi(x,y) &\quad\Leftrightarrow\quad \exists y\ (y \leq x \wedge \phi(x,y)),\\ (\forall y)_{\leq x}\phi(x,y) &\quad\Leftrightarrow\quad \forall y\ (y > x \vee \phi(x,y))\end{aligned}$$

where ϕ is a positive existential formula [5, Thm 5.1]. The first one is easily seen to be Diophantine as the order relation on $\mathbb{N}$ is Diophantine. Proving the second claim takes the rest of the section. Now using this result together with the sequence number theorem [5, Thm 1.3] Davis proofs that a function is Diophantine over $\mathbb{N}$ if and only if it is computable [5, Thm 6.1].

This already implies the DPRM-theorm as Davis has introduced Diophantine pairing functions in [5, Thm 1.1] and therefore all ranges of Diophantine—and therefore all computable functions—are Diophantine over $\mathbb{N}$. But the ranges of computable functions are exactly the semi-decidable subsets of ω by Prop. 1.1.8, thus proving the claim of the theorem.

2.3.2 Diophantine definition of $\mathbb{Z}$ over K

For the remainder of this section let $K \neq \mathbb{Q}$ be a totally real number field or a number field with exactly one pair of non-real embeddings of degree $n := [K : \mathbb{Q}] \geq 3$ over the rationals $\mathbb{Q}$. For any number field K we set r_K to be the number of real embeddings of K and s_K to be the number of pairs of complex-conjugate embeddings of K. Then the conditions on the number fields we are considering in this section can be restated as $r_K = n > 1$, or $r_K = n - 2 > 0$ and $s_K = 1$ respectively. As before we set $L = K[\delta(a)]$, where $\delta(a) \notin \mathcal{O}_K$ is a root of $X^2 - a^2 + 1$ and $-\pi/2 < \arg\delta(a) \leq \pi/2$.

Furthermore, let us assume that $\sigma_1 = \mathrm{id}_K, \sigma_2, ..., \sigma_n : K \to \mathbb{C}$ are all embeddings of K into the complex pane $\mathbb{C}$. If $s_K = 1$ we demand without loss of generality that $K, \sigma_2(K) \not\subset \mathbb{R}$ and that $\sigma_2(\alpha) = \overline{\sigma_1(\alpha)}$ for all $\alpha \in K$. In other words, (σ_1, σ_2) is the pair of complex embeddings and all other morphisms embed K into the reals $\mathbb{R}$.

LEMMA 2.3.12. *Let $K \neq \mathbb{Q}$ be a number field of degree n over $\mathbb{Q}$. If $a \in \mathcal{O}_K$ satisfies*

$$\begin{cases} r_K = n > 1 \\ a > 2^{2(n+1)} \\ 0 < \sigma_i(a) < \frac{1}{2} \quad \textit{for } 1 < i \leq n \end{cases} \quad \textit{or} \quad \begin{cases} r_K = n - 2 > 0 \\ |\sigma_i(a)| > 2^{2(n+1)} \quad \textit{for } i \in \{1,2\} \\ 0 < \sigma_i(a) < \frac{1}{2} \quad \textit{for } 2 < i \leq n \end{cases}, \tag{2.3.4}$$

then $\delta(a) = \sqrt{a^2 - 1}$ is not contained in K.

Proof. By assumption we have $0 < \sigma_n(a) < 1/2$ and therefore $\sigma_n(a)^2 - 1 < 0$ cannot be a square in the real number field $\sigma_n(K) \subseteq \mathbb{R}$. As K is isomorphic to $\sigma_n(K)$, the algebraic integer $\delta(a) = \sqrt{a^2 - 1}$ cannot be contained in K. □

LEMMA 2.3.13. *Let $K \neq \mathbb{Q}$ be a number field of degree n over $\mathbb{Q}$ and $s_K \in \{0, 1\}$ the number of pairs of non-real embeddings $\sigma : K \to \mathbb{C}$. Then there exists an algebraic integer $a \in \mathcal{O}_K$ that satisfies* (2.3.4).

Proof. We will apply the strong approximation theorem (1.3.30) to prove the existence of such an algebraic integer a. To this end, we consider the set of absolute values $\mathcal{F}_K := \{|\cdot|_1, |\cdot|_{s_K+1}, ..., |\cdot|_n\}$, where $|\cdot|_i$ denotes the absolute value defined by

$$|x|_i := |\sigma_i(x)|_{\mathbb{C}}.$$

By the strong approximation theorem there exists $b \in K$ such that

$$\left|\sigma_i(b) - \frac{1}{2^5}\right| = \left|\sigma_i\left(b - \frac{1}{2^5}\right)\right| < \frac{1}{2^6} \qquad \text{for } s_K + 1 < i \leq n \text{ and} \tag{2.3.5}$$

$$|b|_{\mathfrak{p}} \leq 1 \qquad \text{for every prime ideal } \mathfrak{p} \tag{2.3.6}$$

holds. Note that (2.3.6) implies that $b \in \mathcal{O}_K$ is an algebraic integer by Lem. 1.3.27. Form (2.3.5) we firstly conclude, that b is non-zero as

$$\left|\sigma_n(0) - \frac{1}{2^5}\right| = \frac{1}{2^5} > \frac{1}{2^6}.$$

Secondly, we find that for all $s_K + 1 < i \leq n$ we have

$$|\sigma_i(b)| = \left|\sigma_i(b) - \frac{1}{2^5} + \frac{1}{2^5}\right| \leq \left|\sigma_i(b) - \frac{1}{2^5}\right| + \frac{1}{2^5} < \frac{1}{2^6} + \frac{1}{2^5} < \frac{1}{2^4}.$$

Now since b is non-zero, we know that

$$1 \leq |N_{K/\mathbb{Q}}(b)| = \prod_{i=1}^{s_K+1} |\sigma_i(a)| \prod_{i=s_K+2}^{n} |\sigma_i(a)| < |\sigma_1(b)|^{s_K+1} 2^{-4(n-s_K+2)}.$$

We conclude that

$$2^{4(n+1)} \leq 2^{4(n-s_K+2)} < |\sigma_1(b)|^{s_K+1} < |\sigma_1(b)|^2.$$

Setting $a := b$ finishes the proof for the case $r_K = n - 2$. If all embeddings are real, we set $a := |b|_{\mathbb{R}}$. □

EXAMPLE 2.3.14. Consider again the case of $K := \mathbb{Q}[\sqrt{2}]$. Since both embeddings of K into $\mathbb{C}$ are uniquely determined by $\sigma(\sqrt{2}) = \pm\sqrt{2}$ it suffices to find two integers $k, \ell \in \mathbb{Z}$ such that $|k + \ell\sqrt{2}| > 2^{2\cdot 2+2} = 64$ and $|k - \ell\sqrt{2}| < 1/2$. Then we can set $a := k + \ell\sqrt{2}$ and the a fulfils (2.3.4). Such a pair of integers is given by $a = 34 + 24\sqrt{2}$. In this case

$$\delta = \sqrt{4\left(12\sqrt{2} + 17\right)^2 - 1}.$$

Remark. As the expansion L/K is quadratic by Lem. 2.3.12, every σ_i can be extended to exactly two

embeddings σ_{i1} and σ_{i2} of L into the complex plane $\mathbb{C}$ by 'composing' with σ_1^K or σ_2^K. This yields

$$\begin{aligned}\sigma_{i1}(\alpha+\delta\beta) &= \sigma_i(\alpha)+\sqrt{\sigma_i(a)^2-1}\,\sigma_i(\beta) \quad \text{and}\\ \sigma_{i2}(\alpha+\delta\beta) &= \sigma_i(\alpha)-\sqrt{\sigma_i(a)^2-1}\,\sigma_i(\beta)\end{aligned} \tag{2.3.7}$$

for all $\alpha, \beta \in \mathcal{O}_K$ and all $1 \leq i \leq n$.

I will identify the field L with its embedding $\sigma_{11}(L)$ and write x instead of $\sigma_{11}(x)$ for its elements.

LEMMA 2.3.15. *Let $K \neq \mathbb{Q}$ be a number field of degree n over $\mathbb{Q}$ and let $a \in \mathcal{O}_K$ be such that* (2.3.4) *is satisfied. Then*

(i) if $r_K = n$, only σ_{11} and σ_{12} embed L into the reals, and
(ii) if $r_K = n-2$, the field L is totally complex.

Proof. (i) If K is totally real and $i > 1$, then $0 < \sigma_i(a) < 1/2$ and therefore the radicands in (2.3.7) are both negative. As a consequence, $(\sigma_{i1}, \sigma_{i2})$ is a pair of non-real embeddings.

On the other hand, if $i = 1$ then $a > 2^{2(n+1)} > 1$ and the radicands are both positive. We deduce that σ_{11} and σ_{12} are both real embeddings and L is a subfield of the reals by our identification.

(ii) As σ_1 and σ_2 are already non-real embeddings and σ_i^K preserve $\sigma_j(K)$ point-wise ($1 \leq i, j \leq 2$), $\sigma_{11}, \sigma_{12}, \sigma_{21}$ and σ_{22} are non-real as well. For the remaining embeddings one argues completely analogously to (i).

□

LEMMA 2.3.16. *Let $K \neq \mathbb{Q}$ be a number field of degree n over $\mathbb{Q}$ and let $a \in \mathcal{O}_K$ be such that* (2.3.4) *is satisfied. If s_K is the number of pairs of non-real embeddings of K, then*

(i) $\sigma_{i1}(\varepsilon)^{-1} = \sigma_{i2}(\varepsilon)$ for all $1 \leq i \leq n$,
(ii) $\sigma_{i1}(\varepsilon)$ and $\sigma_{i2}(\varepsilon)$ are complex conjugates for $s_K + 1 < i \leq n$, and
(iii) $|\sigma_{i1}(\varepsilon)| = |\sigma_{i2}(\varepsilon)| = 1$ for $s_K + 1 < i \leq n$.

Proof. In Lem. 2.3.2.(i) we have seen, that the claim holds true for $i = 1$. We extend this method to obtain the results for the other cases. For all $1 \leq i \leq n$ we have

$$\begin{aligned}\sigma_{i1}(\varepsilon)\sigma_{i2}(\varepsilon) &= (\sigma_i(a)+\sigma_{i1}(\delta))(\sigma_i(a)-\sigma_{i1}(\delta)) = \\ &= \sigma_i(a)^2 - \sigma_{i1}(\delta)^2 = \sigma_i(a)^2 - \sigma_i(a)^2 + 1 = 1.\end{aligned}$$

For all $s_K + 1 < i \leq n$ we have defined $\sigma_i : K \to \mathbb{C}$ to be a real embedding. Thus $\sigma_i(a)$ is a real number and as $0 < \sigma_i(a) < 1/2$, we find that $\sigma_{i1}(\delta)$ is purely imaginary. Hence, we deduce that $\sigma_{i1}(\varepsilon)$ and $\sigma_{i2}(\varepsilon)$ are complex conjugates. But then the complex moduli of these algebraic integers must coincide, leaving no other option than $|\sigma_{i1}(\varepsilon)| = |\sigma_{i2}(\varepsilon)| = 1$. □

Before we can start proving some approximations for the complex moduli of ε, δ and a, we need to fix some notations.

DEFINITION. Let $K \neq \mathbb{Q}$ be a number field of degree n over $\mathbb{Q}$ and let $a \in \mathcal{O}_K$ be such that (2.3.4) is satisfied. For $1 \leq i \leq n$ we set

(i) $a_i := \sigma_i(a)$,
(ii) $\varepsilon_i := \sigma_{i1}(\varepsilon)$ if $|\sigma_{i1}(\varepsilon)| \geq 1$ and $\varepsilon_i := \sigma_{i2}(\varepsilon)$ otherwise, and
(iii) $\delta_i := \sigma_{i1}(\delta)$.

Remark. (1) In the definition above we could have equivalently defined $\varepsilon_i := \sigma_{i1}(\varepsilon)$ for $s_K + 1 < i \leq n$, as by Lem. 2.3.16.(iii) the complex modulus of $\sigma_{i1}(\varepsilon)$ is 1.
(2) Note that by (2.3.7) we have $\sigma_{i2}(\delta) = -\delta_i$ and therefore $|\delta_i| = |\sigma_{i2}(\delta)|$ for all $1 \leq i \leq n$.

We will use the following result by Kronecker.

LEMMA 2.3.17. *If a non-zero algebraic integer η and all its conjugates have complex modulus not exceeding* 1*, then η is a root of unity.*

Proof. Let $M := \mathbb{Q}[\eta]$ and $n := [M : \mathbb{Q}]$. Since $1, \eta, \eta^2, \eta^3, \ldots$ is a sequence contained in M, all minimal polynomials $\mu_{\mathbb{Q},\eta^k}$ have at most degree n. As all of the conjugates of η lie within the closed unit disk, so do all the complex conjugates of η^k (for $k \in \mathbb{N}$). This implies that all the coefficients of the minimal polynomials $\mu_{\mathbb{Q},\eta^k}$ lie between $\pm \max\left\{\binom{n}{j} : 0 \leq j \leq n\right\}$. We deduce that the sequence $1, \eta, \eta^2, \eta^3, \ldots$ can at most have finitely many distinct terms and η is a root of unity. □

LEMMA 2.3.18. *Suppose $K \neq \mathbb{Q}$ is a number field of degree n over $\mathbb{Q}$ and let $a \in \mathcal{O}_K$ be such that* (2.3.4) *is satisfied. Then the following inequalities hold.*

(i) $|a_i|/2 < |\delta_i| < |a_i| + 1$ *for* $1 \leq i \leq s_K + 1$.
(ii) $1/2 < |\delta_i| < 1$ *for* $s_K + 1 < i \leq n$.
(iii) If $\eta \in \ker N_{L/K}$ *then* $|\sigma_{ij}(\eta)| = 1$ *for* $s_K + 1 < i \leq n$ *and* $j \in \{1, 2\}$. *Furthermore,* $|\eta| = 1$ *if and only if η is a root of unity.*
(iv) $|a| - \sqrt{|a^2 - 1|} < 1$.
(v) $|a| < |\varepsilon_1| < 2|a| + 1$.
(vi) ε is not a root of unity.

Proof. (i) By assumption we have $|a_i| > 2^{2(n+1)}$ and therefore

$$\begin{aligned}\frac{|a_i|^2}{4} = |a_i|^2 - \frac{3|a_i|^2}{4} \leq |a_i|^2 - \frac{3}{4}2^{4(n+1)} < |a_i|^2 - 1 \\ \leq |\delta_i|^2 = |a_i^2 - 1| \leq |a_i|^2 + 1 < (|a_i| + 1)^2\end{aligned}$$

(ii) Again by our assumption $|a_i| < 1/2$. Thus, we find

$$\frac{1}{4} < \frac{3}{4} < 1 - a_i^2 = |\delta_i|^2 < 1.$$

(iii) As in Lem. 2.3.16 one uses that $\overline{\sigma_{i1}(\delta)} = \sigma_{i2}(\delta)$ for all $s_K + 1 < i \leq n$ and finds for $\eta = \alpha + \delta\,\beta \in \ker N_{L/K}$ that

$$\begin{aligned}\sigma_{i1}(\eta) &= \sigma_i(\alpha) + \sigma_{i1}(\delta)\sigma_i(\beta) \text{ and} \\ \sigma_{i2}(\eta) &= \sigma_i(\alpha) + \sigma_{i2}(\delta)\sigma_i(\beta) = \sigma_i(\alpha) - \sigma_{i1}(\delta)\sigma_i(\beta)\end{aligned}$$

are complex conjugates. Now one can deduce,

$$1 = N_{L/K}(\eta) = \sigma_{i1}(\eta)\sigma_{i2}(\eta) = |\sigma_{ij}(\eta)|^2$$

for both $j = 1$ and 2.

To prove the second part of the claim, we notice that all roots of unity have complex modulus 1, so one direction is trivial. Let now $\eta = \alpha + \delta\beta \in \ker N_{L/K}$ and additionally $|\eta| = 1$, we differentiate two cases. If K is totally real, then all embeddings of the algebraic integer η have complex modulus 1. Therefore, η is a root of unity.

If on the other hand, $s_K = 1$, then note firstly, that the complex conjugate $\overline{\delta}$ is a root of the polynomial

$$X^2 - \overline{a}^2 + 1 = X^2 - \sigma_2(a)^2 + 1.$$

As a consequence, $\sigma_{2j}(\delta) = (-1)^{1+j}\overline{\delta}$ for $j \in \{1, 2\}$. We deduce that

$$\overline{\sigma_{11}(\eta)} = \overline{\eta} = \overline{\alpha + \delta\beta} = \sigma_2(\alpha) + \sigma_{21}(\delta)\sigma_2(\beta) = \sigma_{21}(\eta)$$

and

$$\overline{\sigma_{12}(\eta)} = \overline{\alpha - \delta\beta} = \sigma_2(\alpha) - \sigma_{21}(\delta)\sigma_2(\beta) = \sigma_{21}(\eta) = \sigma_2(\alpha) + \sigma_{22}(\delta)\sigma_2(\beta) = \sigma_{22}(\eta).$$

This implies that $|\sigma_{21}(\eta)| = |\eta| = 1$ and $|\sigma_{22}(\eta)| = |\sigma_{12}(\eta)|$. Finally, note that $N_{L/\mathbb{Q}} = N_{K/\mathbb{Q}} \circ N_{L/K}$ and therefore

$$1 = |N_{K/\mathbb{Q}}(1)| = |N_{K/\mathbb{Q}} \circ N_{L/K}(\eta)| = \left| \prod_{\substack{1 \le i \le n \\ 1 \le j \le 2}} \sigma_{ij}(\eta) \right| = |\sigma_{12}(\eta)||\sigma_{22}(\eta)| = |\sigma_{12}(\eta)|^2.$$

(iv) The inequality

$$|a| - \sqrt{|a^2 - 1|} < 1$$

is equivalent to $|a|^2 - 2|a| + 1 < |a^2 - 1|$. But this inequality can easily seen to be satisfied, as

$$|a|^2 + 1 < |a|^2 + 2|a| - 1 \le |a^2 - 1| + 2|a|$$

and the claim is proven.

(v) Consider the inequality

$$|\varepsilon_1|^2 = |a + \delta_1|^2 = |a^2 + 2a\delta_1 + \delta_1^2| \ge |2a^2 + 2a\delta_1| - 1 = 2|a||\varepsilon_1| - 1$$

which can be rewritten as

$$0 \le |\varepsilon_1|^2 - 2|a||\varepsilon_1| + 1 = \left(|\varepsilon_1| - |a| - \sqrt{|a|^2 - 1}\right)\left(|\varepsilon_1| - |a| + \sqrt{|a|^2 - 1}\right)$$

Thus, either both factors are non-positive real numbers or both are non-negative. In the first case

$$0 < |\varepsilon_1| \leq |a| - \sqrt{|a|^2 - 1} \overset{\text{by (iv)}}{<} 1,$$

which is impossible. Hence, both factors are non-negative and

$$|\varepsilon_1| > |a| + \sqrt{|a|^2 - 1} > |a|,$$

proving the first estimate. The second inequality follows from $|\varepsilon_1| = |a + \delta_1| < 2|a| + 1$ by (i).

(vi) Note that by (v), $|\varepsilon_1| > |a| > 2^{2(n+1)} > 1$ and therefore the complex modulus of ε cannot be equal to 1. The claim follows from (iii).

□

As a next step, we want to show that we have essentially found all solutions of Pell's equation (2.3.1). For this we need some lemmas.

Recall the group $G \leq \ker N_{L/K}$ defined in Lem. 2.3.10. We have seen in Lem. 2.3.11 and the subsequent inequality (2.3.3) that the free rank of G can be bound from above by $\operatorname{rk} U_L - \operatorname{rk} U_K$. I claim that this difference of ranks is equal to 1 in both cases of algebraic number fields we are considering.

If $K \neq \mathbb{Q}$ is totally real, then by Dirichlet's unit theorem (1.3.21) we find that $\operatorname{rk} U_K = n - 1$ and by Lem. 2.3.15 that $\operatorname{rk} U_L = n$. If on the other hand, K satisfies $r = n - 2 > 0$ then $\operatorname{rk} U_K = n - 2$ and by Lem. 2.3.15 we have $\operatorname{rk} U_L = n - 1$.

Note that ε is contained in G and by the previous lemma, ε is not a root of unity. As a consequence, the group $\langle\varepsilon\rangle \leq G$ has free rank at least equal to 1. We deduce that

$$\operatorname{rk}\langle\varepsilon\rangle = \operatorname{rk} G = 1.$$

Thus, there exists a unit $\varepsilon_0 \in G$ such that for all $\eta \in G$ there exists a root of unity $\zeta \in \mathcal{O}_L$ and an integer k, such that $\eta = \zeta\varepsilon_0^k$. However, even more is true, as one can set $\varepsilon = \varepsilon_0$, but before we can prove this, we need a lemma.

LEMMA 2.3.19. *Let $K \neq \mathbb{Q}$ be a number field and let $a \in U_L$ satisfy (2.3.4). Furthermore, let ε_0 be a generator of the torsion free part of G. Then $2\delta \mid (\varepsilon_0 - \varepsilon_0^{-1})$ and*

(i) if K is totally real, then

$$|N_{L/\mathbb{Q}}(2\delta)| > a^2 \quad \text{and} \quad |N_{L/\mathbb{Q}}(\varepsilon_0 - \varepsilon_0^{-1})| < 2^{2n}|\varepsilon_0|^2;$$

(ii) if $[K : \mathbb{Q}] \geq 3$ and K has exactly one pair of non-real embeddings, then

$$|N_{L/\mathbb{Q}}(2\delta)| > a^4 \quad \text{and} \quad |N_{L/\mathbb{Q}}(\varepsilon_0 - \varepsilon_0^{-1})| < 2^{2n}|\varepsilon_0|^4.$$

Proof. Let $\varepsilon_0 = \alpha + \delta\beta$ for some $\alpha, \beta \in \mathcal{O}_K$, then $\varepsilon_0^{-1} = \alpha - \delta\beta$ (cf. Lem. 2.3.10) and

$$\varepsilon_0 - \varepsilon_0^{-1} = 2\delta\,\beta,$$

proving that $2\delta \mid (\varepsilon_0 - \varepsilon_0^{-1})$.

We assert without loss of generality that $\varepsilon = \zeta\varepsilon_0^k$, where $|\varepsilon_0| \geq 1$. Then for all $1 \leq i \leq n$ and all $1 \leq j \leq 2$, we have

$$|\sigma_{ij}(\varepsilon)| = |\sigma_{ij}(\zeta\varepsilon_0^k)| = |\sigma_{ij}(\varepsilon_0)|^k,$$

and thus, $|\varepsilon_1| = |\varepsilon_0|^k \geq |\varepsilon_0| \geq 1$. Furthermore, by Lem. 2.3.18.(iii) the following inequality holds

$$|\sigma_{i1}(\varepsilon_0) - \sigma_{i1}(\varepsilon_0^{-1})||\sigma_{i2}(\varepsilon_0) - \sigma_{i2}(\varepsilon_0^{-1})| \leq 4 \tag{2.3.8}$$

for all $s_K + 1 < i \leq n$.

(i) If $K \neq \mathbb{Q}$ is totally real, then by Lem. 2.3.18.(i) and (ii) we find that

$$|N_{L/\mathbb{Q}}(2\delta)| = 2^{2n}\prod_{i=1}^{n}|\delta_i|^2 > \frac{2^{2n}}{2^{2n-2}}\frac{|a|^2}{4} = a^2.$$

To see the second inequality, we use (2.3.8) to find

$$\begin{aligned}|N_{L/\mathbb{Q}}(\varepsilon_0 - \varepsilon_0^{-1})| &= \prod_{\substack{1\leq i\leq n\\ 1\leq j\leq 2}}|\sigma_{ij}(\varepsilon_0) - \sigma_{ij}(\varepsilon_0^{-1})| \\ &\leq 2^{2n-2}|\varepsilon_0 - \varepsilon_0^{-1}|^2 \leq 2^{2n-2}(|\varepsilon_0| + 1)^2 < 2^{2n}|\varepsilon_0|^2\end{aligned}$$

as claimed.

(ii) Completely analogously using the fact, that

$$\begin{aligned}&|\sigma_{11}(\varepsilon_0) - \sigma_{11}(\varepsilon_0^{-1})||\sigma_{12}(\varepsilon_0) - \sigma_{12}(\varepsilon_0^{-1})||\sigma_{21}(\varepsilon_0) - \sigma_{21}(\varepsilon_0^{-1})||\sigma_{22}(\varepsilon_0) - \sigma_{22}(\varepsilon_0^{-1})| \\ &\quad = |\sigma_{11}(\varepsilon_0) - \sigma_{11}(\varepsilon_0^{-1})|^2|\overline{\sigma_{21}(\varepsilon_0) - \sigma_{21}(\varepsilon_0^{-1})}|^2 = |\sigma_{11}(\varepsilon_0) - \sigma_{11}(\varepsilon_0^{-1})|^4.\end{aligned}$$

□

PROPOSITION 2.3.20. *Let $K \neq \mathbb{Q}$ be a number field and let $a \in \mathcal{O}_K$ satisfy* (2.3.4)*. Then for every $\eta \in G$ there exists an integer k and a root of unity $\zeta \in L$ such that $\eta = \zeta\varepsilon^k$.*

Proof. By the discussion above all that is left to prove is that in the equation

$$\varepsilon_1 = \zeta\varepsilon_0^k$$

with $|\varepsilon_0| \geq 1$ the integer k is 1. Then

$$\varepsilon_0 = \zeta^{-1}\varepsilon_1 = \zeta^{-1}\varepsilon^{\pm 1}$$

and the proposition is proven.

Assume to the contrary, that $k \geq 2$, then $|\varepsilon_1| \geq |\varepsilon_0|^2 \geq 1$. By the lemma above $2\delta \mid (\varepsilon_0 - \varepsilon_0^{-1})$ and therefore

$$|N_{L/\mathbb{Q}}(2\delta)| \leq |N_{L/\mathbb{Q}}(\varepsilon_0 - \varepsilon_0^{-1})|.$$

The previous lemma implies now that $1 < |a|^{2m_0} < 2^{2n}|\varepsilon_0|^{2m_0}$, where $m_0 = s_K + 1 \in \{1, 2\}$ is chosen accordingly. Applying Lem. 2.3.18.(v) yields

$$|a|^{2m_0} < 2^{2n}|\varepsilon_0|^{2m_0} \leq 2^{2n}|\varepsilon_1|^{m_0} < 2^{2n+m_0}(|a|+1)^{m_0} < 2^{2n+1+m_0}|a|^{m_0}.$$

If m_0 is one then the inequality above reads $|a|^2 < 2^{2n+2}|a|$, which is a contradiction to (2.3.4). If on the other hand $m_0 = 2$ holds then we obtain $|a|^4 < 2^{2n+3}|a|^2$. But this can be transformed upon dividing by $|a|^2$ and taking square roots to $|a| < 2^{n+3/2}$, which is again a contradiction to (2.3.4). □

Recall the sequences $(\mathrm{x}_m)_{m\in\mathbb{N}}$ and $(\mathrm{y}_m)_{m\in\mathbb{N}}$ defined in (2.3.2). If K is totally real we can conclude from the proposition above that all solutions of Pell's equation with the parameter $d = a^2 - 1$ are of the form

$$(\pm\mathrm{x}_m(a), \pm\mathrm{y}_m(a))$$

for some integer $m \in \mathbb{N}$. This is because $L = K[\sqrt{d}]$ has two real embeddings ($\sigma_{1,1}$ and $\sigma_{1,2}$) and the only real roots of unity are ± 1. If K has one pair of non-real embeddings and at least one real embedding. This argument can no longer be used as L is totally complex in this case. One can however impose a Diophantine condition on the solutions of Pell's equation to force them to be of this shape [cf. 32, Lem. 3].

COROLLARY 2.3.21. *Let K be a number field of positive degree n over $\mathbb{Q}$ and let $a \in \mathcal{O}_K$ satisfy (2.3.4). Then there exists a constant $\nu \in \mathbb{N} \setminus \{0\}$ with the property, that if $x' + \delta y' \in G$ and*

$$(x' + \delta y')^\nu = x + \delta y \tag{2.3.9}$$

for two algebraic integers $x, y \in \mathcal{O}_K$ then there exists an index $m \in \mathbb{N}$ such that

$$(x, y) = (\pm\mathrm{x}_m, \pm\mathrm{y}_m).$$

In particular, (x, y) is a solution to Pell's equation.

Proof. Set $\nu := |\mu(K)|$ which is finite by Dirichlet's unit theorem (1.3.21). By the proposition there exists a root of unity $\zeta \in L$ and an integer $m_1 \in \mathbb{N}$ such that $\zeta\varepsilon^{m_1} = x' + \delta y'$. We conclude that

$$x + \delta y = (x' + \delta y')^\nu = (\zeta\varepsilon^{m_1})^\nu = \zeta^\nu \varepsilon^{m_1\nu} = \varepsilon^{m_1\nu}$$

and therefore that $(x, y) = (\pm\mathrm{x}_{m_1\nu}, \pm\mathrm{y}_{m_1\nu})$. The claim follows from Lem. 2.3.2.(ii). □

Note that (2.3.9) is not a Diophantine relation over $\mathcal{O}_K$ as δ is not contained in K. We can however use the binomial theorem to rewrite the identity as

$$x + \delta y = (x' + \delta y')^\nu = \sum_{i=0}^{\nu} \binom{\nu}{i} x'^{\nu-i}\delta^i y'^i$$

and by equating coefficients of δ we get the two Diophantine definitions

$$x = \sum_{\substack{i=1 \\ i \text{ even}}}^{\nu} \binom{\nu}{i} x'^{\nu-i} (a^2-1)^{\frac{i}{2}} y'^{i}$$

and

$$y = \sum_{\substack{i=1 \\ i \text{ odd}}}^{\nu} \binom{\nu}{i} x'^{\nu-i} (a^2-1)^{\frac{i-1}{2}} y'^{i}$$

As a next step we derive further properties of the sequences $(\mathrm{x}_m)_{m\in\mathbb{N}}$ and $(\mathrm{y}_m)_{m\in\mathbb{N}}$.

LEMMA 2.3.22. *Let $K \neq \mathbb{Q}$ be a number field and let $a \in \mathcal{O}_K$ satisfy* (2.3.4). *Then the following inequality holds*

$$m < |\sigma_i(\mathrm{x}_m)|$$

for all non-negative integers $m \in \mathbb{N}$ and all $1 \leq i \leq s_K + 1$.

Proof. By Lem. 2.3.18.(v) we know that $|\varepsilon_1| > |a| > 1$ and since $\varepsilon_1 = \varepsilon^{\pm 1}$, Lem. 2.3.3.(i) implies

$$|x_m| = \frac{|\varepsilon_1^m + \varepsilon_1^{-m}|}{2} > \frac{|a|^m - 1}{2} > \frac{2^{2(n+1)m} - 1}{2} > m$$

If $s_K = 1$, then $\sigma_2(\mathrm{x}_m)$ is the complex conjugate of $\sigma_1(\mathrm{x}_m) = \mathrm{x}_m$. As a consequence, their moduli must coincide. □

LEMMA 2.3.23. *Let $K \neq \mathbb{Q}$ be a number field and let $a \in \mathcal{O}_K$ satisfy* (2.3.4). *There exists a constant $C > 0$ depending on K and a such that for all $k \in \mathbb{N} \setminus \{0\}$ there exist $m, h \in \mathbb{N}$ with $k \mid m$ and $k \mid h$, and*

$$|\sigma_i(\mathrm{x}_m)| > \frac{1}{2},$$
$$|\sigma_i(\mathrm{y}_h)| > C$$

for $s_K + 1 < i \leq n$.

Proof. Fix any positive integer k. By Lem. 2.3.16.(iii) we know that $|\varepsilon_j| = 1$ for $s_K + 1 < j \leq n$. It follows that there exist arguments $\vartheta_{s_K+2}, \ldots, \vartheta_n \in \mathbb{R}$ such that

$$\varepsilon_j = e^{i\pi\vartheta_j}.$$

Let $A = \{\vartheta_{j_1}, \ldots, \vartheta_{j_s}\}$ be a maximal $\mathbb{Z}$-linear independent subset of $\{\vartheta_{s_K+2}, \ldots, \vartheta_n\}$. Since ε is not a root of unity by Lem. 2.3.18.(vi), none of the ϑ_j can be rational. Indeed, if $\vartheta_j = p/q$ then $\varepsilon_j^{2q} = e^{i\pi 2p} = 1$ and ε_j is a root of unity. Hence, A contains at least one element.

Let $J_0 := \{j_1, \dots, j_s\}$ be the set of indices of elements in A, then the construction implies that for all $s_K + 1 < r \leq n$ there exist integers $b_r, b_{rj} \in \mathbb{Z}$ with $b_r \neq 0$ such that

$$b_r \vartheta_r = \sum_{j \in J_0} b_{rj} \vartheta_j.$$

For otherwise, $1, \vartheta_{j_1}, \dots, \vartheta_{j_s}, \vartheta_r$ would be $\mathbb{Q}$-linear independent, contradicting the maximality of A. In other words, we have that

$$\varepsilon_r^{b_r} = \prod_{j \in J_0} \varepsilon_j^{b_{rj}}.$$

We set $b := \prod_{r=s_K+2}^{n} b_r \neq 0$ and find for all $s_K + 1 < r \leq n$ integers $c_{rj} \in \mathbb{Z}$ with

$$\varepsilon_r^{b} = \prod_{j \in J_0} \varepsilon_j^{c_{rj}}.$$

We exponent this expression by a multiple $\ell \in k\mathbb{Z}$ of k, whose value will be fixed later, and rewrite it to obtain

$$\begin{aligned} \sigma_r(\mathrm{x}_{\ell b}) + \sigma_{r1}(\delta)\sigma_r(\mathrm{y}_{\ell b}) = \varepsilon_r^{\ell b} = \prod_{j \in J_0} \varepsilon_j^{\ell c_{rj}} = e^{i\pi \sum_{j \in J_0} \ell c_{rj} \vartheta_j} \\ = \cos\left(\pi \sum_{j \in J_0} \ell c_{rj} \vartheta_j\right) + i \sin\left(\pi \sum_{j \in J_0} \ell c_{rj} \vartheta_j\right). \end{aligned} \tag{2.3.10}$$

By continuity of $|\cos(\pi\vartheta)|$ in ϑ, we can find a constant $\lambda > 0$ such that $1 - |\cos(\pi\vartheta)| < 1/2$ whenever $|\vartheta| < \lambda$. Or put differently, $|\cos(\pi\vartheta)| > 1/2$.

Let $c_0 = \max_{r,j}(|c_{rj}|)$. Setting $\alpha_j := k\vartheta_j$, $\beta_j = 0$, and $N = 1$ we obtain by Kronecker's theorem (1.3.25) integers $\tilde{\ell}, \tilde{\ell}_j$ with $\tilde{\ell} > 0$ such that

$$|\tilde{\ell} k \vartheta_j - \tilde{\ell}_j| < \frac{\lambda}{2c_0 n}$$

holds for all $j \in J_0$ simultaneously. But then

$$|2\tilde{\ell} k \vartheta_j - 2\tilde{\ell}_j| < \frac{\lambda}{c_0 n}$$

holds as well and we set $\ell := 2\tilde{\ell}k$ and $\ell_j := 2\tilde{\ell}_j$. This does not only implies that

$$\left| \sum_{j \in J_0} \ell c_{rj} \vartheta_j - \sum_{j \in J_0} \ell_j c_{rj} \right| < \lambda$$

but also by the choice of the ℓ_j that $\sum_{j \in J_0} \ell_j c_{rj} \in \mathbb{Z}$ is divisible by 2 for all $s_K + 1 < r \leq n$. From

(2.3.10) we conclude that

$$|\sigma_r(\mathrm{x}_{\ell b})| = \left|\cos\left(\pi \sum_{j\in J_0} \ell c_{rj}\vartheta_j\right)\right| = \left|\cos\left(\pi \sum_{j\in J_0} \ell c_{rj}\vartheta_j - \pi \sum_{j\in J_0} \ell_j c_{rj}\right)\right| > \frac{1}{2}.$$

Setting $m := \ell b$ proves the first claim as ℓ is divisible by k.

To prove the claimed bound for y_h let $C_r := \sum_{j\in J_0} c_{rj}$ for all $s_K + 1 < r \leq n$ and fix a constant $C_0 \in \mathbb{N}$ such that $C_0 > \max_r(|C_r|)$ and in the prime factorization of C_0 appear at least as many twos as in all the prime factorizations of the C_r. In other words,

$$\operatorname{ord}_2 C_0 \geq \operatorname{ord}_2 C_t, \quad \text{for all } s_K + 1 < t \leq n.$$

As $|\sin(\pi\vartheta)|$ is uniformly continuous on the compact interval $[-1, 1]$ we can find for all positive $\lambda_1 > 0$ a real number $0 < \lambda_2 < 1/4$ such that $||\sin(\pi\vartheta)| - |\sin(\pi\varphi)|| < \lambda_1$ whenever $|\vartheta - \varphi| < \lambda_2$ and $\vartheta, \varphi \in [-1, 1]$ are satisfied. We apply Kronecker's theorem again with the parameters $\alpha_j := k\vartheta_j$, $\beta_j := 1/(4C_0)$, and $N := 1$ to obtain integers $\tilde{\ell}, \tilde{\ell}_j$ with $\tilde{\ell} > 0$ and the property that

$$\left|\tilde{\ell}k\vartheta_j - \tilde{\ell}_j - \frac{1}{4C_0}\right| < \frac{\lambda_2}{2C_0 n}$$

holds for all $j \in J_0$ simultaneously. We again multiply by 2 to obtain

$$\left|2\tilde{\ell}k\vartheta_j - 2\tilde{\ell}_j - \frac{1}{2C_0}\right| < \frac{\lambda_2}{C_0 n}$$

and set $\ell := 2\tilde{\ell}k$ and $\ell_j := 2\tilde{\ell}_j$ for all $s_K + 1 < r \leq n$. Hence, we can deduce that

$$\left|\sum_{j\in J_0} (\ell c_{rj}\vartheta_j - \ell_j c_{rj}) - \frac{C_r}{2C_0}\right| = \left|\sum_{j\in J_0} \left(\ell c_{rj}\vartheta_j - \ell_j c_{rj} - \frac{c_{rj}}{2C_0}\right)\right| < \lambda_2$$

and again that $\sum_{j\in J_0} \ell_j c_{rj}$ is divisible by 2 for all $s_K + 1 < r \leq n$. Set now

$$\lambda_1 := \frac{\left|\sin\left(\frac{\pi C_r}{2C_0}\right)\right|}{2}$$

then we can use (2.3.10) to obtain

$$\begin{aligned}
\left||\sigma_{r1}(\delta)\sigma_r(y_{\ell b})| - \left|\sin\left(\pi\frac{C_r}{2C_0}\right)\right|\right| &= \left|\left|\sin\left(\pi \sum_{j\in J_0} \ell c_{rj}\vartheta_j\right)\right| - \left|\sin\left(\pi\frac{C_r}{2C_0}\right)\right|\right| \\
&= \left|\left|\sin\left(\pi \sum_{j\in J_0} \ell c_{rj}\vartheta_j - \pi \sum_{j\in J_0} \ell_j c_{rj}\right)\right| - \left|\sin\left(\pi\frac{C_r}{2C_0}\right)\right|\right| \\
&< \lambda_1 = \frac{1}{2}\left|\sin\left(\pi\frac{C_r}{2C_0}\right)\right|
\end{aligned}$$

for all $s_K + 1 < r \leq n$. Thus, we can conclude that $|\sigma_{r1}(\delta)\sigma_r(y_{\ell b})| > \lambda_1$.

Note that $\sin(\pi C_r/(2C_0)) \neq 0$ as $C_r/(2C_0)$ cannot be an integer by the choice of C_0. Now set

$$C := \min_r \frac{\left|\sin\left(\pi \frac{C_r}{2C_0}\right)\right|}{2|\sigma_{r1}(\delta)|}$$

then C satisfies the claim. □

LEMMA 2.3.24. *Let K be a number field of degree $n > 0$ over $\mathbb{Q}$ and let $a \in \mathcal{O}_K$ satisfy* (2.3.4). *If y_{eh} satisfies Lem. 2.3.23 for an arbitrary but fixed positive integer $k \in \mathbb{N} \setminus \{0\}$ dividing h, where $e \in \mathbb{N}$ is an integer such that*

$$|\varepsilon_1|^e > \frac{2^{s_K+1}|\delta_1|^{s_K+1}}{C^{n-s_K-1}} \tag{2.3.11}$$

holds for the constant C of the same lemma, then

(i) $\mathrm{y}_{eh} \mid \mathrm{y}_{e\ell}$ *in* $\mathcal{O}_K$ *implies* $h \mid \ell$ *in* $\mathbb{Z}$ *and*
(ii) $\mathrm{y}_{eh}^2 \mid \mathrm{y}_{e\ell}$ *in* $\mathcal{O}_K$ *implies* $h\mathrm{y}_{eh} \mid \ell$ *in* $\mathcal{O}_K$.

Proof. Note that such an integer e must exist as $|\varepsilon_1| > 1$ by Lem. 2.3.18.(v). Let now $r \in \mathbb{N}$ be such that $0 < r < h$. As before let $L := K[\delta]$. Considering the field norm $N_{L/\mathbb{Q}}$ of y_{eq} we use Lem. 2.3.3.(i) to obtain

$$\begin{aligned}
|N_{L/\mathbb{Q}}(\mathrm{y}_{er})| &= \prod_{i=1}^{n}\prod_{j=1}^{2}\left|\sigma_{ij}\left(\frac{\varepsilon^{er}-\varepsilon^{-er}}{2\delta}\right)\right| \\
&\leq \prod_{i=1}^{s_K+1}\frac{|\varepsilon_i^{er}-\varepsilon_i^{-er}||\varepsilon_i^{-er}-\varepsilon_i^{er}|}{4|\delta_i|^2}\prod_{i=s_K+2}^{n}\frac{1}{|\delta_i|^2} \\
&\leq \frac{4^{s_K+1}|\varepsilon_1|^{2er(s_K+1)}}{4^{s_K+1}|N_{K/\mathbb{Q}}(a^2-1)|} < |\varepsilon_1|^{2er(s_K+1)},
\end{aligned}$$

where the approximations follow completely analogously as in the proof of Prop. 2.3.20. As y_{er} is in $\mathcal{O}_K$ we deduce that

$$|N_{K/\mathbb{Q}}(\mathrm{y}_{er})| < |\varepsilon_1|^{er(s_K+1)}.$$

On the other hand, by our assumption on $|\sigma_i(\mathrm{y}_{eh})|$ we know that

$$\begin{aligned}
|N_{K/\mathbb{Q}}(\mathrm{y}_{eh})| &= \prod_{i=1}^{n}|\sigma_i(\mathrm{y}_{eh})| \geq C^{n-s_K-1}\prod_{i=1}^{s_K+1}|\sigma_i(\mathrm{y}_{eh})| \\
&= C^{n-s_K-1}\prod_{i=1}^{s_K+1}\frac{|\varepsilon_i^{eh}-\varepsilon_i^{-eh}|}{2|\delta_i|} \geq C^{n-s_K-1}\left(\frac{|\varepsilon_1|^{eh}-1}{2|\delta_1|}\right)^{s_K+1} \\
&> C^{n-s_K-1}\frac{|\varepsilon_1|^{eh(s_K+1)}}{2^{s_K+1}|\delta_1|^{s_K+1}},
\end{aligned}$$

where the second inequality follows from $|\varepsilon_1^{-1}| \leq 1$. Using our assumption on e, it follows that

$$|N_{K/\mathbb{Q}}(\mathrm{y}_{eh})| > |N_{K/\mathbb{Q}}(\mathrm{y}_{er})|. \tag{2.3.12}$$

Let $\mathrm{y}_{eh} \mid \mathrm{y}_{e\ell}$ and set $\ell = th + r$ for $t, r \in \mathbb{N}$ with $0 \leq r < h$. Assume to reach a contradiction that $r > 0$, then

$$\mathrm{y}_{e\ell} = \mathrm{y}_{eth+er} \overset{\text{Lem. 2.3.3.(ii)}}{=} \mathrm{y}_{eth}\mathrm{x}_{er} + \mathrm{x}_{eth}\mathrm{y}_{er}.$$

By Lem. 2.3.4.(i) we know that $\mathrm{y}_{eh} \mid \mathrm{y}_{eth}$ and consequently $\mathrm{y}_{eh} \mid \mathrm{x}_{eth}\mathrm{y}_{er}$ in $\mathcal{O}_K$. But by part (iii) of the same lemma the principal ideals (x_{eth}) and (y_{eth}) are relative prime in $\mathcal{O}_K$. Now Lem. 2.3.4.(i) implies that (x_{eth}) and (y_{eh}) are relative prime as well. And therefore $y_{eh} \mid y_{er}$, contradicting (2.3.12). Consequently, $r = 0$ and $h \mid \ell$ in $\mathbb{Z}$.

To see the second divisibility condition we assume $\mathrm{y}_{eh}^2 \mid \mathrm{y}_{e\ell}$ in $\mathcal{O}_K$. Then by the first part of the lemma, we know that there exists an integer t such that $\ell = th$. Using the binomial formula we obtain

$$\begin{aligned}\mathrm{x}_{eth} + \delta\mathrm{y}_{eth} = (\varepsilon^{eh})^t = (\mathrm{x}_{eh} + \delta\mathrm{y}_{eh})^t = \\ = \sum_{\substack{0\leq i\leq t\\ 2 \text{ even}}} \binom{t}{i} \mathrm{x}_{eh}^{t-i}\delta^i\mathrm{y}_{eh}^i + \delta \sum_{\substack{0\leq i\leq t\\ 2 \text{ odd}}} \binom{t}{i} \mathrm{x}_{eh}^{t-i}\delta^{i-1}\mathrm{y}_{eh}^i\end{aligned}$$

and, since (x_{eh}) and (y_{eh}) are relative prime, we can conclude that

$$0 \equiv \mathrm{y}_{eth} \equiv t\mathrm{x}_{eh}^{t-1}\mathrm{y}_{eh} \equiv t\mathrm{y}_{eh} \mod (\mathrm{y}_{eh}^2).$$

It follows that $\mathrm{y}_{eh} \mid t$ and therefore $h\mathrm{y}_{eh} \mid \ell$ (both in $\mathcal{O}_K$). □

As a next step we prove a similar result for x_m.

LEMMA 2.3.25. *Let K be a number field of degree $n > 0$ over $\mathbb{Q}$ and let $a \in \mathcal{O}_K$ satisfy (2.3.4). If x_m satisfies*

$$|\sigma_i(\mathrm{x}_m)| > \frac{1}{2}$$

for $s_K + 1 < i \leq n$ then for all integers $\ell, j \in \mathbb{Z}$ and some sign $\varsigma \in \{-1, 1\}$ we have that $\mathrm{x}_\ell \equiv \mathrm{x}_j\varsigma \mod (\mathrm{x}_m)$ in $\mathcal{O}_K$ implies $\ell \equiv \pm j \mod m$ in $\mathbb{Z}$.

Proof. Set $\ell = 2m\ell_1 + r_1$ as well as $j = 2mj_1 + r_2$ with $-m < r_1, r_2 \leq m$. Without loss of generality we may assume that $0 \leq r_1, r_2 \leq m$ holds, since we have

$$\mathrm{x}_\ell = \mathrm{x}_{2m\ell_1 \pm r_1} \equiv -\mathrm{x}_{r_1} \mod (\mathrm{x}_m) \quad \text{and} \quad \mathrm{x}_j = \mathrm{x}_{2mj_1 \pm r_2} \equiv -\mathrm{x}_{r_2} \mod (\mathrm{x}_m)$$

by Lem. 2.3.7. Thus, we can deduce that $\mathrm{x}_{r_1} \equiv \mathrm{x}_{r_2}\varsigma \mod (\mathrm{x}_m)$. We will prove that $\mathrm{x}_{r_1} = \mathrm{x}_{r_2}\varsigma$ and will deduce $r_1 = r_2\varsigma$. Assume otherwise that $r_1 \neq r_2$ and $\mathrm{x}_{r_1} \neq \mathrm{x}_{r_2}\varsigma$ then from the congruence it follows that

$$|N_{K/\mathbb{Q}}(\mathrm{x}_m)| \leq |N_{K/\mathbb{Q}}(\mathrm{x}_{r_1} - \mathrm{x}_{r_2}\varsigma)|. \tag{2.3.13}$$

To reach a contradiction we assume without loss of generality that $r_1 \leq r_2$ and apply Lem. 2.3.3.(i)

to express $\mathrm{x}_m, \mathrm{x}_{r_1}$ and x_{r_2} as the 'real part' of a power of ε. Now as in the proof of Lem. 2.3.24, we have that

$$\begin{aligned} |N_{K/\mathbb{Q}}(\mathrm{x}_m)| &= \prod_{i=1}^{s_K+1} |\sigma_i(\mathrm{x}_m)| \prod_{i=s_K+2}^{n} |\sigma_i(\mathrm{x}_m)| \geq \frac{1}{2^{n-s_K-1}} |\sigma_1(\mathrm{x}_m)|^{s_K+1} \\ &= \frac{1}{2^{n-s_K-1}} \left| \frac{\varepsilon_1^m + \varepsilon_1^{-m}}{2} \right|^{s_K+1} \geq \frac{(|\varepsilon_1|^m - 1)^{s_K+1}}{2^n} \end{aligned} \tag{2.3.14}$$

Again the last inequality follows from the triangular inequality and the fact that $|\varepsilon_1^{-1}| \leq 1$. To estimate the norm of $\mathrm{x}_{r_1} - \mathrm{x}_{r_2}\zeta$ we note that by Lem. 2.3.16 we know for all $s_K + 1 < i \leq n$ that

$$|\sigma_i(\mathrm{x}_{r_1}) - \sigma_i(\mathrm{x}_{r_2}\zeta)| \leq \frac{|\varepsilon_i^{r_1} - \varepsilon_i^{-r_1}| + |\zeta||\varepsilon_i^{r_2} - \varepsilon_i^{-r_2}|}{2} \leq \frac{|\varepsilon_i|^{r_1} + |\varepsilon_i|^{-r_1} + |\varepsilon_i|^{r_2} + |\varepsilon_i|^{-r_2}}{2} = 2.$$

Thus, we can conclude that

$$\begin{aligned} |N_{K/\mathbb{Q}}(\mathrm{x}_{r_1} - \mathrm{x}_{r_2}\zeta)| &= \prod_{i=1}^{n} |\sigma_i(\mathrm{x}_{r_1}) - \sigma_i(\mathrm{x}_{r_2}\zeta)| \leq 2^{n-s_K-1} |\sigma_i(\mathrm{x}_{r_1}) - \sigma_i(\mathrm{x}_{r_2}\zeta)|^{s_K+1} \\ &\leq 2^{n-s_K-1} \left(\frac{|\varepsilon_1|^{r_1} + |\varepsilon_1|^{-r_1} + |\varepsilon_1|^{r_2} + |\varepsilon_1|^{-r_2}}{2} \right)^{s_K+1} \\ &\leq 2^{n-s_K-1} (|\varepsilon_1|^{r_2} + 1)^{s_K+1}. \end{aligned} \tag{2.3.15}$$

We know by Lem. 2.3.18.(v) that $|\varepsilon_1| > 2$. So $|\varepsilon_1|^{r_2} + 1 < 2|\varepsilon_1|^{r_2}$ and we have that

$$|\varepsilon_1|^m - 1 > \tfrac{1}{2}|\varepsilon_1|^m.$$

Now notice that $s_K \leq 1$ and thus we can deduce from (2.3.14) and (2.3.15) that

$$|N_{K/\mathbb{Q}}(\mathrm{x}_m)| \geq \frac{|\varepsilon_1|^{m(s_K+1)}}{2^{n+s_K+1}} \geq \frac{|\varepsilon_1|^{m(s_K+1)}}{2^{n+2}} \tag{2.3.16}$$

and

$$|N_{K/\mathbb{Q}}(\mathrm{x}_{r_1} - \mathrm{x}_{r_2}\zeta)| \leq 2^n |\varepsilon_1|^{r_2(s_K+1)}. \tag{2.3.17}$$

We will now distinguish two cases. Either $r_2 < m$ then we have that

$$2^{2n+2} < |a| < |\varepsilon_1| \leq |\varepsilon_1|^{s_K+1} \leq |\varepsilon_1|^{(m-r_2)(s_K+1)},$$

which together with the inequalities in (2.3.16) and (2.3.17) implies

$$|N_{K/\mathbb{Q}}(\mathrm{x}_m)| > |N_{K/\mathbb{Q}}(\mathrm{x}_{r_1} - \mathrm{x}_{r_2}\zeta)|.$$

Thus, we have reached a contradiction with (2.3.13) and we must assume that $r_2 = m$ holds. But this

implies that x_m actually divides x_{r_1}, yielding

$$|N_{K/\mathbb{Q}}(\mathrm{x}_m)| \leq |N_{K/\mathbb{Q}}(\mathrm{x}_{r_1})|.$$

As for the norm of x_{r_1} we find that

$$\begin{aligned}
|N_{K/\mathbb{Q}}(\mathrm{x}_{r_1})| &= |\sigma_1(\mathrm{x}_{r_1})|^{s_K+1} \prod_{i=s_K+2}^{n} |\sigma_i(\mathrm{x}_{r_1})| \\
&\leq |\sigma_1(\mathrm{x}_{r_1})|^{s_K+1} \prod_{i=s_K+2}^{n} \frac{|\varepsilon_i|^{r_1} + |\varepsilon_i|^{-r_1}}{2} \\
&\leq \left(\frac{|\varepsilon_1|^{r_1} + |\varepsilon_1|^{-r_1}}{2}\right)^{s_K+1} \leq \\
&\leq \left(\frac{|\varepsilon_1|^{r_1} + 1}{2}\right)^{s_K+1} \leq |\varepsilon_1|^{r_1(s_K+1)}
\end{aligned}$$

holds. Remember that we are assuming that $r_1 \neq r_2$ and we have already shown $r_2 = m$. Thus, we can conclude that $2^{n+2} < |\varepsilon_1|^{m-r_1}$. But then the inequality above implies together with (2.3.16) that

$$|N_{K/\mathbb{Q}}(\mathrm{x}_m)| > |N_{K/\mathbb{Q}}(\mathrm{x}_{r_1})|,$$

which is again an contradiction.

As a consequence, our assumption that both $r_1 \neq r_2$ and $\mathrm{x}_{r_1} \neq \mathrm{x}_{r_2}\varsigma$ are true cannot hold. So the only thing left to check is that $\mathrm{x}_{r_1} = \mathrm{x}_{r_2}\varsigma$ implies $r_1 = \pm r_2$, which yields the desired congruence of rational integers. We know that $\mathrm{x}_{r_1} = \mathrm{x}_{r_2}\varsigma$ implies $\varepsilon^{r_1} + \varepsilon^{-r_1} = (\varepsilon^{r_2} + \varepsilon^{-r_2})\varsigma$. If $\varsigma = 1$ we find that this is equivalent to

$$0 = \varepsilon^{r_1}(\varepsilon^{r_1} + \varepsilon^{-r_1} - \varepsilon^{r_2} - \varepsilon^{-r_2}) = \varepsilon^{2r_1} + 1 - \varepsilon^{r_1+r_2} - \varepsilon^{r_1-r_2} = (\varepsilon^{r_1+r_2} - 1)(\varepsilon^{r_1-r_2} - 1).$$

Hence, $r_1 = \pm r_2$ as claimed. If on the other hand, $\varsigma = -1$ holds we find

$$0 = -\varepsilon^{r_2}(\varepsilon^{r_1} + \varepsilon^{-r_1} - \varepsilon^{r_2} - \varepsilon^{-r_2}) = -\varepsilon^{r_2+r_1} - \varepsilon^{r_2-r_1} + \varepsilon^{2r_2} + 1 = (\varepsilon^{r_2+r_1} - 1)(\varepsilon^{r_2-r_1} - 1),$$

yielding $r_1 = \pm r_2$. □

LEMMA 2.3.26. *Let K be a number field of degree n over $\mathbb{Q}$ and let $a \in \mathcal{O}_K$ satisfy (2.3.4). Then for all positive $m \in \mathbb{N} \setminus \{0\}$ and all constants $C_1, C_2 > 0$ there exists an algebraic integer b such that*

(i) $b \equiv 1 \mod (\mathrm{y}_m(a))$,
(ii) $b \equiv a \mod (\mathrm{x}_m(a))$, *and*
(iii) b *satisfies* $|\sigma_i(b)| > C_1$ *for all* $1 \leq i \leq s_K + 1$ *and* $|\sigma_i(b)| < C_2$ *for all* $s_K + 1 < i \leq n$. *In particular, we may whish that* b *satisfies the approximations of the embeddings of* a *in* (2.3.4).

Proof. Set

$$b := \left(\mathrm{x}_m(a)^2 + \mathrm{y}_m(a)^2(a^2 - 1)\right)^{2s} \left(\mathrm{x}_m(a)^4 + a\left(1 - \mathrm{x}_m(a)^2\right)^2\right)$$

for some positive integer s, whose value will be determined later. Note that since $\mathrm{x}_m(a)$ and $\mathrm{y}_m(a)$ solve Pell's equation, we have

$$\mathrm{x}_m(a)^2 - (a^2-1)\mathrm{y}_m(a)^2 = 1,$$

which implies that $(a^2-1)\mathrm{y}_m(a)^2 \equiv -1 \mod (\mathrm{x}_m(a))$. Thus, condition (ii) is satisfied. As for condition (i), we note that by the same argument $\mathrm{x}_m(a)^2 \equiv 1 \mod (\mathrm{y}_m(a))$ holds.

To prove the last claim note that for all positive m, we have

$$|\sigma_i(\mathrm{x}_m(a))| = \left|\frac{\varepsilon_i(a)^m + \varepsilon_i(a)^{-m}}{2}\right| \leq \frac{|\varepsilon_i(a)|^m + |\varepsilon_i(a)|^{-m}}{2} = 1$$

for all $s_K + 1 < i \leq n$. The only way equality can be reached in the inequality above is if $|\varepsilon_i(a)^m + \varepsilon_i(a)^{-m}| = |\varepsilon_i(a)|^m + |\varepsilon_i(a)|^{-m}$. But this can only happen, if their arguments coincide, which implies that both $\varepsilon_i(a)^m$ and $\varepsilon_i(a)^{-m}$ are real numbers with complex modulus 1. Hence, $\varepsilon_i(a)^{2m} = 1$ and $\varepsilon(a)$ would be a $2m$-th root of unity, contradicting Lem. 2.3.18.(vi). We conclude that the approximation of the modulus $|\sigma_i(\mathrm{x}_m(a))| < 1$ holds for all $s_K + 1 < i \leq n$. But since

$$|N_{K/\mathbb{Q}}(\mathrm{x}_m(a))| = |\sigma_1(\mathrm{x}_m(a))|^{s_K+1} \prod_{i=s_K+2}^{n} |\sigma_i(\mathrm{x}_m(a))|$$

is a positive integer we must also have $|\sigma_1(\mathrm{x}_m(a))| > 1$.

As for the embeddings of b we have

$$\sigma_i(b) = \left(\sigma_i(\mathrm{x}_m(a))^2 + \sigma_i(\mathrm{y}_m(a))^2(a_i^2-1)\right)^{2s}\left(\sigma_i(\mathrm{x}_m(a))^4 + a_i\left(1 - \sigma_i(\mathrm{x}_m(a))^2\right)^2\right)$$

where $|a_i| > 1$ for all $1 \leq i \leq s_K + 1$ and $|a_i| < 1$ for all $s_K + 1 < i \leq n$ by (2.3.4). Let us first consider the case for $1 \leq i \leq s_K + 1$. Then

$$|\sigma_i(\mathrm{x}_m(a))^2 + \sigma_i(\mathrm{y}_m(a))^2(a_i^2-1)| = |2\sigma_i(\mathrm{x}_m(a))^2 - 1| \geq 2|\sigma_i(\mathrm{x}_m(a))|^2 - 1 > 1$$

holds and thus $|\sigma_i(b)|$ is strictly increasing in s. On the other hand, if $s_K + 1 < i \leq n$ we note that $\sigma_i(\mathrm{x}_m)$ is a real number as $\sigma_i : K \to \mathbb{R}$ is a real embedding and conclude that both

$$\sigma_i(\mathrm{x}_m(a))^2 - \sigma_i(\mathrm{y}_m(a))^2(1-a_i^2) < \sigma_i(\mathrm{x}_m(a))^2 < 1$$

as well as

$$\sigma_i(\mathrm{x}_m(a))^2 - \sigma_i(\mathrm{y}_m(a))^2(1-a_i^2) = 2\sigma_i(\mathrm{x}_m(a))^2 - 1 > -1$$

hold. As a consequence, the modulus $|\sigma_i(b)|$ is strictly decreasing in s. Hence, we can arrange for $|\sigma_i(b)| > C_1$ and $|\sigma_j(b)| < C_2$ to hold $(1 \leq i \leq s_K + 1 < j \leq n)$, as claimed. □

Finally, we have all the tools at hand to present a Diophantine representation of $\mathbb{Z}$ over $\mathcal{O}_K$.

THEOREM 2.3.27. *Let K be a number field of degree $n > 0$ over $\mathbb{Q}$ and let $a \in \mathcal{O}_K$ satisfy* (2.3.4).

Let $\sigma_1, \dots, \sigma_n$ be all embeddings of K into $\mathbb{C}$, where we demand that σ_i is a non-real embedding if and only if $i \leq 2s_K$. Furthermore, let C be the bound defined in Lem. 2.3.23, e defined as in (2.3.11)*, and $\nu := |\mu(K)|$. Then the set S defined by the following relations is Diophantine over $\mathcal{O}_K$ and satisfies $\nu\mathbb{N} \subseteq S \subseteq \mathbb{Z}$.*

$$\begin{aligned}
\xi \in S \quad \Leftrightarrow \quad & \exists x, y, w, z, u, v, s, t, x', y', w', z', u', v', s', t', b \in \mathcal{O}_K : \\
& \begin{cases} x'^2 - (a^2-1)y'^2 = 1 \\ w'^2 - (a^2-1)z'^2 = 1 \\ u'^2 - (a^2-1)v'^2 = 1 \\ s'^2 - (b^2-1)t'^2 = 1 \end{cases} && (2.3.18) \\
& \begin{cases} x + \delta y = (x' + \delta(a)y')^{\nu} \\ u + \delta v = (u' + \delta(a)v')^{\nu} \\ s + \delta y = (s' + \delta(b)t')^{\nu} \end{cases} && (2.3.19) \\
& w + \delta z = (w' + \delta(a)z')^{\nu e} && (2.3.20) \\
& 0 < \sigma_i(b) < 2^{-18} \quad \textit{for all } s_K + 1 < i \leq n && (2.3.21) \\
& |\sigma_i(z)| \geq C, \quad |\sigma_i(u)| \geq \tfrac{1}{2} \quad \textit{for all } s_K + 1 < i \leq n && (2.3.22) \\
& v \neq 0 && (2.3.23) \\
& z^2 \mid v && (2.3.24) \\
& b \equiv 1 \mod (z), \quad b \equiv a \mod (u) && (2.3.25) \\
& s \equiv x \mod (u) && (2.3.26) \\
& t \equiv \xi \mod (z) && (2.3.27) \\
& 2^{n+1} \prod_{i=0}^{n-1} (\xi + i)^n (x + i)^n \mid z && (2.3.28)
\end{aligned}$$

Proof. Note that the set S defined by the relations above is indeed Diophantine since

- (2.3.19) as well as (2.3.20) can be rewritten in a Diophantine form (over $\mathcal{O}_K$) as was demonstrated below the proof of Cor. 2.3.21;
- (2.3.21) as well as (2.3.22) can be rewritten in a Diophantine form by Lem. 2.2.7; and
- (2.3.23) is Diophantine by Example 2.1.2.(4).

Finally, the conjunction of all of these Diophantine relations is Diophantine by Lem. 2.1.5.

First suppose that the relations above have a common solution ξ. We need to show that ξ is a rational integer. To see this I first claim that b satisfies (2.3.4). Indeed, the part for the embeddings $\sigma_i(b)$ with $s_K + 1 < i \leq n$ are guaranteed by (2.3.21). For the embeddings $\sigma_i(b)$ with $1 \leq i \leq s_K + 1$ we note that since b is an algebraic integer, its norm $N_{K/\mathbb{Q}}(b)$ must have an absolute value of at least

one. Thus, we have

$$1 \leq |N_{K/\mathbb{Q}}(b)| = |\sigma_1(b)|^{s_K+1} \prod_{i=s_K+2}^{n} |\sigma_i(b)| \leq |\sigma_1(b)|^{s_K+1} 2^{-18(n-s_K-1)},$$

which implies

$$|\sigma_1(b)| \geq 2^{18\frac{n-s_K-1}{s_K+1}}.$$

Now if $s_K = 0$, then $n \geq 2$ and since $18(n-1) > 2(n+1)$ the claim holds. If on the other hand $s_K = 1$, then we have demanded that $n \geq 3$ holds and again since $9(n-2) > 2(n+1)$ the claim holds true.

Now (2.3.18), (2.3.19), and (2.3.20) imply by Cor. 2.3.21 that there exist integers $k, h, m, j \in N$ such that

$$\begin{aligned} x &= \pm \mathrm{x}_k(a), & y &= \pm \mathrm{y}_k(a), \\ w &= \pm \mathrm{x}_{eh}(a), & z &= \pm \mathrm{y}_{eh}(a), \\ u &= \pm \mathrm{x}_m(a), & v &= \pm \mathrm{y}_m(a), \\ s &= \pm \mathrm{x}_j(b), \text{ and} & t &= \pm \mathrm{y}_j(b). \end{aligned}$$

We can thus rewrite conditions (2.3.22) to (2.3.27) to obtain

$$|\sigma_i(\mathrm{y}_{eh}(a))| \geq C, \quad |\sigma_i(\mathrm{x}_m(a))| \geq \tfrac{1}{2} \quad \text{for all } s_K + 1 < i \leq n, \tag{2.3.29}$$

$$\mathrm{y}_m(a) \neq 0, \tag{2.3.30}$$

$$\mathrm{y}_{eh}^2 \mid \mathrm{y}_m(a), \tag{2.3.31}$$

$$b \equiv 1 \mod (\mathrm{y}_{eh}(a)), \quad b \equiv a \mod (\mathrm{x}_m(a)), \tag{2.3.32}$$

$$\mathrm{x}_j(b) \equiv \pm \mathrm{x}_k(a) \mod (\mathrm{x}_m(a)), \text{ and} \tag{2.3.33}$$

$$\pm \mathrm{y}_j(b) \equiv \xi \mod (\mathrm{y}_{eh}(a)). \tag{2.3.34}$$

Now from Lem. 2.3.6.(i) we can conclude that

$$\mathrm{y}_j(b) \equiv j \mod (b-1).$$

By (2.3.32) this implies that

$$\mathrm{y}_j(b) \equiv j \mod (\mathrm{y}_{eh}(a))$$

holds. Now from condition (2.3.34) we can deduce that the congruence

$$j \equiv \pm \xi \mod (\mathrm{y}_{eh}(a)) \tag{2.3.35}$$

must be satisfied. Furthermore, from (2.3.32) and Lem. 2.3.6.(ii) we can infer that

$$\mathrm{x}_j(b) \equiv \mathrm{x}_j(a) \mod \mathrm{x}_m(a)$$

holds, implying together with (2.3.33)

$$\mathrm{x}_j(a) \equiv \pm \mathrm{x}_k(a) \mod (\mathrm{x}_m(a)).$$

Now we can use Lem. 2.3.25, whose assumption on x_m is satisfied by (2.3.29), to deduce that

$$k \equiv \pm j \mod m. \tag{2.3.36}$$

Again (2.3.29) allows us to apply Lem. 2.3.24 so that we can infer

$$\mathrm{y}_{eh}(a) \mid m \text{ in } \mathcal{O}_K$$

from Eq. (2.3.31). We use this relation and find from (2.3.36) that

$$k \equiv \pm j \mod (\mathrm{y}_{eh}(a))$$

must hold. We can now infer from (2.3.35) that

$$k \equiv \pm \xi \mod (\mathrm{y}_{eh}(a))$$

holds. From (2.3.28) it follows by Lem. 2.2.6 that

$$|\sigma_i(\xi)| < \tfrac{1}{2}|N_{K/\mathbb{Q}}(\mathrm{y}_{eh}(a))|^{\frac{1}{n}}$$

for all $1 \leq i \leq n$. Analogously, one can deduce from the same condition that

$$|\sigma_i(k)| = k \leq |\sigma_i(\mathrm{x}_k(a))| < \tfrac{1}{2}|N_{K/\mathbb{Q}}(\mathrm{y}_{eh}(a))|^{\frac{1}{n}}$$

holds, where the first inequality follows from Lem. 2.3.22. Thus, all the conditions of the strong vertical method (Thm 2.2.5) are satisfied for k and ξ and we find

$$\xi = \pm k \in \mathbb{Z}$$

as claimed.

To show the other direction let $\xi = \ell\nu \in \nu\mathbb{N}$ be given. We set $k := \xi, x := \mathrm{x}_k(a), x' := \mathrm{x}_\ell(a), y := \mathrm{x}_k(a)$ and $y' := \mathrm{x}_\ell(a)$, then the parts of (2.3.18) and (2.3.19) involving x, x', y and y' can be satisfied. By Lem. 2.3.9 we can find an index $h' \in \mathbb{N}$ such that

$$2^{n+1} \prod_{i=0}^{n-1} (\xi + i)^n (x + i)^n \mid \mathrm{y}_{h'}(a).$$

By Lem. 2.3.4.(i) we can set $h := \nu h'$ and $z := \mathrm{y}_{eh}(a)$ then (2.3.28) is satisfied. Now Lem. 2.3.24 implies that $|\sigma_i(z)| = |\sigma_i(\mathrm{y}_{eh}(a))| \geq C$ for $s_K + 1 < i \leq n$. Set $w := \mathrm{x}_{eh}(a)$ then the parts of (2.3.18), (2.3.20), and (2.3.22) involving z, z', w and w' can be satisfied, by setting $z' := \mathrm{y}_{h'}(a)$ as well as $w' := \mathrm{x}_{h'}(a)$. To obtain algebraic integers u, u', v and v' satisfying the respective parts

of (2.3.22), (2.3.23), and (2.3.24) we appeal to Lem. 2.3.9 to find an index $m' \in \mathbb{N}$ such that $\mathrm{y}_{eh}(a)^2$ divides $\mathrm{y}_{m'}(a)$. Now apply Lem. 2.3.23 to find an index $m \in \mathbb{N}$ that is divisible by $\nu m'$, such that $|\sigma_i(\mathrm{x}_m(a)| > 1/2$ for all $s_K + 1 < i \leq n$. By Lem. 2.3.4.(i) we have that $\mathrm{y}_{eh}(a)^2$ divides $\mathrm{y}_m(a)$. Thus, we can set $u := \mathrm{x}_m(a)$ and $v := \mathrm{y}_m(a)$ (and u', v' accordingly). By Lem. 2.3.26 we can find an algebraic integer $b \in \mathcal{O}_K$ satisfying (2.3.21), (2.3.25), and (2.3.4). Finally, set $s := \mathrm{x}_k(b), t := \mathrm{y}_k(b)$, and s', t' accordingly. From (2.3.25) and Lem. 2.3.6.(ii) it follows that (2.3.26) holds. Condition (2.3.27) follws completely analogously as in the first part. □

COROLLARY 2.3.28. *Let K be a totally real number field or a number field with exactly one pair of non-real embeddings and at least one real embedding. Then $\mathbb{Z}$ is Diophantine over $\mathcal{O}_K$.*

Proof. By the theorem there exists a Diophantine set $S \subseteq \mathcal{O}_K$ with the property $\nu\mathbb{N} \subseteq S \subseteq \mathbb{Z}$, where $\nu := |\mu(K)|$. Thus, $\mathbb{Z}$ can be defined in a Diophantine way as follows

$$\begin{aligned} \alpha \in \mathbb{Z} \Leftrightarrow \exists \beta_1, \beta_2, \beta_3 \in \mathcal{O}_K : \\ \alpha = \beta_1\beta_2 + \beta_3 \\ \beta_1 \in S \\ \beta_2 \in \{-1, 1\}) \wedge (\beta_3 \in \{0, 1, ..., \nu - 1\}) = 0. \end{aligned}$$

□

We have just seen that the rational integers are Diophantine over rings of algebraic integers $\mathcal{O}_K$ if the number field $K \neq \mathbb{Q}$ is totally real, or $[K : \mathbb{Q}] \geq 3$ and there is exactly one pair of complex embeddings. From our observations in Cor. 2.2.2 Hilbert's tenth problem over these rings is not decidable. The restriction on the degree in the second case can be omitted, since Denef [9] showed in 1975 that $\mathbb{Z}$ is Diophantine over rings of algebraic integers in quadratic number fields. This result was further strengthened by Denef and Lipshitz [10]. They proved that $\mathbb{Z}$ is Diophantine over $\mathcal{O}_K$ if K/M is a quadratic extension of a totally real number field M. Shapiro and Shlapentokh [41] used these results to deduce that all cyclotomic fields posses a Diophantine definition of $\mathbb{Z}$ over their rings of algebraic integers. More generally, they deduced this result for all fields K, for which $K/\mathbb{Q}$ is normal and the Galois group of the extension is abelian.

All these results make the conjecture of Denef and Lipshitz [10], that such a Diophantine definition of $\mathbb{Z}$ over $\mathcal{O}_K$ exists for all number fields K, very plausible. This is especially true since promising techniques using elliptic curves have been developed, for instance by Poonen [34].

Notice however that a Diophantine definition of $\mathbb{Z}$ might not be necessary for the Diophantine theory $\mathtt{H10}(\mathfrak{O}_K)$ to be undecidable. Indeed, there might exist rings of algebraic integers whose Diophantine theory forms a kind of set that Post [35] calls 'creative'. Then $\mathtt{H10}(\mathfrak{O}_K)$ would be undecidable as well, but the halting set is not many-one reducible to this Diophantine theory. As a consequence of Thm 2.2.4, such a ring of integers cannot posses a Diophantine definition of $\mathbb{Z}$.

A Collected *Haskell* implementations

A.1 Simulating Turing machines

I have published a simulator of Turing machines implemented in *Haskell* at `https://github.com/tim6her/h10-turing-machines`. To obtain a copy of the source code and build it using *GHC* and *cabal* run

```
git clone https://github.com/tim6her/h10-turing-machines.git
cd h10-turing-machines
cabal setup && cabal build && cabal install
```

To run the example codes for Turing machines enter the folder 'listings' and start `ghci`. The following listing shows how to run the Turing machine deciding the tally encoding of non-negative integers. It might be necessary to turn on Unicode printing in your *GHC* installation.

```
>>> import Automaton.TuringMachine
>>> :l tally
>>> let d = toTransition tally "error" -- mark the errornous state
>>> let turing = TuringMachine "start" '_' "halt" d
>>> "§1111" >>> turing -- Tally encoding of 4
Just "§1"
>>> "§1011" >>> turing -- Not tally encoded
Just "§0"
```

A full documentation of the Turing machine simulator is available on the *GitHub* repository.

A.2 Polynomials

The following listings show a *Haskell* implementationf the monoid of monomials and the algebra of polynomials in countably many indeterminates. Note that the axioms of monoids and algebras respectively are only heuristically verified but not formally proven.

Listing A.1: A Haskell *implementation of monomials in countably many indeterminates*

```
{-# LANGUAGE RebindableSyntax #-}
module Monomial
( Monomial
, (<*>)
, idt
, mfromList
, clean
) where
```

```
import NumericPrelude
import Data.Map (Map, delete, empty, foldrWithKey, fromList, member, insert,
                 insertWith, (!))
import Algebra.Monoid as Monoid

import Test.Tasty
import Test.Tasty.HUnit
import Test.Tasty.QuickCheck as QC


-- | Monomials are mappings from ZZ to NN with finite support
newtype Monomial = Monomial (Map Integer Integer) deriving (Eq, Ord)

instance Monoid.C Monomial where
  idt = Monomial empty
  (<*>) = mmul

instance Show Monomial where
  show (Monomial m)
    | m == empty = "1"
    | otherwise =  foldrWithKey
                     (\x e sh -> "X" ++ show x ++ "^" ++ show e ++ " " ++ sh)
                      "" m

-- | Creates monomials from list of tuples
--
-- Left entry is index of indeterminate, right index is power of the
-- indeterminate
--
-- === Example
-- >>> mfromList [(1, 2), (0, 3), (4, 7)]
-- X0^3 X1^2 X4^7
mfromList :: [(Integer, Integer)] -> Monomial
mfromList l = clean $ Monomial $ fromList l

-- | Multiplies two monomials
--
-- === Example
-- >>> mmul (mfromList [(1, 2), (2, 4)]) (mfromList [(2, 1), (3, 2)])
-- X1^2 X2^5 X3^2
mmul :: Monomial -> Monomial -> Monomial
mmul xx@(Monomial m1) yy@(Monomial m2)
  | m1 == empty = yy
  | m2 == empty = xx
  | otherwise = clean $ Monomial $ foldrWithKey
```

```
                  (\x e m -> if x `member` m
                             then insertWith (+) x e m
                             else insert x e m)
                  m2 m1

clean :: Monomial -> Monomial
clean (Monomial m)
  | m == empty = (Monomial m)
  | otherwise = Monomial $ foldrWithKey
                  (\x e m -> if e <= 0
                             then delete x m
                             else m)
                  m m

-- * Testing

main :: IO ()
main = defaultMain tests

tests :: TestTree
tests = testGroup "Tests" [properties, unitTests]

properties :: TestTree
properties = testGroup "Properties" [qcProps]

qcProps = testGroup "Axioms of monoids"
  [ QC.testProperty "left multiplication by identity" $
    \x -> (let m = mfromList (x :: [(Integer, Integer)])
           in idt <*> m == m)
  , QC.testProperty "right multiplication by identity" $
    \x -> (let m = mfromList (x :: [(Integer, Integer)])
           in m <*> idt == m)
  , QC.testProperty "associativity" $
    \x y z -> (let m1 = mfromList (x :: [(Integer, Integer)])
                   m2 = mfromList (y :: [(Integer, Integer)])
                   m3 = mfromList (z :: [(Integer, Integer)])
               in (m1 <*> m2) <*> m3 == m1 <*> (m2 <*> m3))
  , QC.testProperty "commutativity" $
    \x y -> (let m1 = mfromList (x :: [(Integer, Integer)])
                 m2 = mfromList (y :: [(Integer, Integer)])
             in m1 <*> m2 == m2 <*> m1)
  ]

unitTests = testGroup "Unit tests"
  [ testCase "show X0^3 X1^2 X4^7" $
      show (mfromList [(1, 2), (0, 3), (4, 7)]) @?= "X0^3 X1^2 X4^7 "
```

```
  , testCase "sample multiplication" $
      show (mmul (mfromList [(1, 2), (2, 4)]) (mfromList [(2, 1), (3, 2)])) @?=
      "X1^2 X2^5 X3^2 "
  , testCase "test clean" $
      mfromList [(1, 0), (2, 0), (3, 1)] @?= mfromList [(3, 1)]
  ]
```

Listing A.2: A Haskell *implementation of polynomials in countable many indeterminates*

```
{-# LANGUAGE RebindableSyntax #-}
{-# LANGUAGE FlexibleInstances #-}
{-# LANGUAGE MultiParamTypeClasses #-}
import NumericPrelude

import qualified Monomial

import qualified Data.Map as Map
import Algebra.Monoid as Monoid
import Algebra.Ring as Ring
import Algebra.Module as Module
import Algebra.Additive as Additive

import Test.Tasty
import Test.Tasty.HUnit
import Test.Tasty.QuickCheck as QC

-- | Polynomials over a ring R are finitely supported functions
-- from the set of monomials to R
newtype Polynomial a = Polynomial (Map.Map Monomial.Monomial a)

-- | Polynomials form an additive (abelian) group
instance (Ring.C a, Eq a) => Additive.C (Polynomial a) where
  zero = Polynomial Map.empty
  (+) = padd
  negate (Polynomial m) = Polynomial $ Map.map negate m

-- | Polynomials from an R-module
instance (Ring.C a, Eq a) => Module.C a (Polynomial a) where
  (*>) 0 _ = zero
  (*>) a (Polynomial m) = Polynomial $ Map.map (a*) m

-- | Polynomials form a ring with unit
instance (Ring.C a, Eq a) => Ring.C (Polynomial a) where
  one = pfromList [(1, [])]
  (*) p@(Polynomial m1) q
    | p == zero = zero
    | q == zero = zero
```

```
    | p == one = q
    | q == one = p
    | otherwise = Map.foldrWithKey
                    (\mono coeff poly -> (coeff *> mono `mmul` q) + poly)
                    0 m1

-- | Two polynomials are equal if their difference is zero
instance (Ring.C a, Eq a) => Eq (Polynomial a) where
  (==) p q = let (Polynomial m) = p - q in m == Map.empty

instance (Show a, Eq a) => Show (Polynomial a) where
  show (Polynomial p)
    | p == Map.empty = "0"
    | otherwise = Map.foldrWithKey
                    (\m a sh -> show a ++ " " ++ show m ++ "+ " ++ sh)
                    "" p

-- | Adds two polynomials over the same ring
--
-- If a coefficient of a monoid equals 0 the monoid is dropped out of the map
padd :: (Ring.C a, Eq a) => Polynomial a -> Polynomial a -> Polynomial a
padd p@(Polynomial m1) q@(Polynomial m2)
  | m1 == Map.empty = q
  | m2 == Map.empty = p
  | otherwise = clean $ Polynomial $ Map.foldrWithKey
                  (\mono coeff poly -> if mono `Map.member` poly
                            then Map.insertWith (+) mono coeff poly
                            else Map.insert mono coeff poly)
                  m2 m1

mmul :: (Ring.C a, Eq a) => Monomial.Monomial -> Polynomial a -> Polynomial a
mmul mono poly@(Polynomial mp)
  | mono == Monomial.idt = Polynomial mp
  | poly == zero = zero
  | otherwise = Polynomial $ Map.mapKeys (mono Monomial.<*>) mp


-- | Generate polynomials from lists
pfromList :: (Ring.C a, Eq a) => [(a, [(Integer, Integer)])] -> Polynomial a
pfromList [] = zero
pfromList ((a, m):l) = deepClean . clean  $ (Polynomial $ Map.singleton
                         (Monomial.mfromList m) a) + pfromList l

-- | Comfort function for creating polynomials
--
-- === Example
```

```
-- >>> 2 *> ((x 1 + x 2) * (x 1 - x 2)) == 2 *> x 1 ^ 2 - 2 *> x 2 ^ 2
-- True
x :: (Ring.C a, Eq a) => Integer -> Polynomial a
x i = pfromList [(1, [(i, 1)])]

-- | Remove monoids with coefficient zero from support
clean :: (Ring.C a, Eq a) => Polynomial a -> Polynomial a
clean (Polynomial m) = Polynomial $ Map.foldrWithKey
                        (\mono coeff poly -> if coeff == 0
                                             then Map.delete mono poly
                                             else poly)
                         m m

-- | Remove variables with power zero from monomials
--
-- This function runs in O(n log(n)) so use it sparsely
deepClean :: (Ring.C a, Eq a) => Polynomial a -> Polynomial a
deepClean (Polynomial m) = Polynomial $ Map.mapKeys Monomial.clean m

-- * Testing

main :: IO ()
main = defaultMain tests

tests :: TestTree
tests = testGroup "Tests" [properties, unitTests]

properties :: TestTree
properties = testGroup "Properties" [qcAddProps, qcModProps,
               localOption (QuickCheckTests 5) qcRingProps,
               qcAlgebraProps]

qcAddProps = testGroup "Group axioms for addition"
  [ QC.testProperty "addition is commutative" $
    \x y -> (let p = pfromList (x :: [(Int, [(Integer, Integer)])])
                 q = pfromList (y :: [(Int, [(Integer, Integer)])])
             in p + q == q + p)
  , QC.testProperty "addition is associative" $
    \x y z -> (let p1 = pfromList (x :: [(Int, [(Integer, Integer)])])
                   p2 = pfromList (y :: [(Int, [(Integer, Integer)])])
                   p3 = pfromList (z :: [(Int, [(Integer, Integer)])])
             in (p1 + p2) + p3 == p1 + (p2 + p3))
  , QC.testProperty "addition by zero" $
    \x -> (let p = pfromList (x :: [(Int, [(Integer, Integer)])])
             in p + zero == p)
  , QC.testProperty "addition with inverse" $
```

```
    \x -> (let p = pfromList (x :: [(Int, [(Integer, Integer)])])
           in p - p == zero)
  ]

qcModProps = testGroup "Module axioms"
  [ QC.testProperty "first distributive law" $
    \a x y -> (let p = pfromList (x :: [(Int, [(Integer, Integer)])])
                   q = pfromList (y :: [(Int, [(Integer, Integer)])])
           in (a :: Int) *> (p + q) == a *> q + a *> p)
  , QC.testProperty "second distributive law" $
    \a b x -> (let p = pfromList (x :: [(Int, [(Integer, Integer)])])
           in (a + b :: Int) *> p == a *> p + b *> p)
  , QC.testProperty "multiplications commute" $
    \a b x -> (let p = pfromList (x :: [(Int, [(Integer, Integer)])])
           in (a * b :: Int) *> p == a *> (b *> p))
  , QC.testProperty "multiplication by one" $
    \x -> (let p = pfromList (x :: [(Int, [(Integer, Integer)])])
           in (one :: Int) *> p == p)
  ]

qcRingProps = testGroup "Ring axioms"
  [ QC.testProperty "multiplication is associative" $
    \x y z -> (let p1 = pfromList (x :: [(Int, [(Integer, Integer)])])
                   p2 = pfromList (y :: [(Int, [(Integer, Integer)])])
                   p3 = pfromList (z :: [(Int, [(Integer, Integer)])])
           in (p1 * p2) * p3 == p1 * (p2 * p3))
  , QC.testProperty "left multiplication by one" $
    \x -> (let p = pfromList (x :: [(Int, [(Integer, Integer)])])
           in one * p == p)
  , QC.testProperty "right multiplication by one" $
    \x -> (let p = pfromList (x :: [(Int, [(Integer, Integer)])])
           in p * one == p)
  , QC.testProperty "distributive law" $
    \x y z -> (let p1 = pfromList (x :: [(Int, [(Integer, Integer)])])
                   p2 = pfromList (y :: [(Int, [(Integer, Integer)])])
                   p3 = pfromList (z :: [(Int, [(Integer, Integer)])])
               in p1 * (p2 + p3) == p1 * p2 + p1 * p3)
  ]

qcAlgebraProps = testGroup "Algebra axioms"
  [ QC.testProperty "multiplications commute" $
    \x y a -> (let p1 = pfromList (x :: [(Int, [(Integer, Integer)])])
                   p2 = pfromList (y :: [(Int, [(Integer, Integer)])])
           in (a :: Int) *> (p1 * p2) == (a *> p1) * p2)
  ]
```

```
unitTests = testGroup "Unit tests"
  [ testCase "sample polynomial" $
      show (pfromList [(1, [(1, 2), (3, 4)]), (-4, [(1, 4), (2, 3)])]
               :: Polynomial Int) @?= "1 X1^2 X3^4 + -4 X1^4 X2^3 + "
  , testCase "test equality" $
      pfromList [(0, [(1, 1)])] @?= (zero :: Polynomial Int)
  ]
```

B Summaries

B.1 Zusammenfassung

Hilberts zehntes Problem fragt, ob ein Algorithmus existiert, der zu gegebenen multivariaten Polynom mit ganzzahligen Koeffizienten entscheiden kann, ob dieses ganzzahlige Nullstellen besitzt. Obwohl das Problem breits im Jahr 1900 von Hilbert [18] formuliert wurde, dauerte es bis 1970, bis Matijasevič [26] beweisen konnte, dass es keinen solchen Algorithmus geben kann. Das Problem lässt sich direkt auf andere kommutative Ringe R mit 1 übertragen, indem Koeffizienten aus $\mathbb{Z}$ oder R und Nullstellen aus R gewählt werden. In dieser Masterarbeit werden wir uns vor allem mit dem Fall von Ringen ganzalgebraischer Zahlen beschäftigen. Wie eng Hilberts zehntes Problem mit anderen Entscheidungsproblemen verwandt ist, kommt allerdings erst dann zu Tage, wenn wir Hilberts Problem als die Frage der Entscheidbarkeit einer Theorie auffassen. Wir werden zum Beispiel erkennen, dass Matijasevic' DPRM-Theorem (2.1.11) sehr ähnlich zu Gödels Haupttheorem in seinem Beweis [15] des ersten Unvollständigkeitssatzes ist.

Um Hilberts Problem in dieser Allgemeinheit verstehen zu können, werden im ersten Abschnitt Grundlagen der Berechenbarkeitstheorie und der Modelltheorie vorgestellt. Dabei werden wir auf das Halteproblem stoßen, dessen Unentscheidbarkeit die Schlüsselzutat für alle unsere Beweise der Unentscheidbarkeit sein wird. Weiters werden wir die für uns relevanten Begriffe und Resultate der algebraischen Zahlentheorie sowie der Geometrie der Zahlen wiederholen und teilweise beweisen.

Nach diesen einführenden Kapiteln werden wir im zweiten Teil der Arbeit Hilberts zehntes Problem formalisieren und eine ausführlichere Betrachtung verwandter Probleme und der historischen Entwicklung dieser anstellen. Um das Problem schließlich negativ für ausgewählte Ringe zu entscheiden, werden wir diophantische Mengen über kommutativen Ringen mit 1 einführen und einige wichtige strukturelle Eigenschaften diophantischer Mengen beweisen. Das Hauptresultat dieser Arbeit ist, dass über einem Ring ganzalgebraischer Zahlen $\mathcal{O}_K$, über dem die ganzen Zahlen $\mathbb{Z}$ eine diophantische Menge bilden, unabhängig davon, ob Koeffizienten aus $\mathbb{Z}$ oder $\mathcal{O}_K$ gewählt werden, das zehnte hilbertsche Problem unentscheidbar ist.

Im letzten Abschnitt der Arbeit werden die Resultate von Denef [8], Pheidas [32] und Shlapentokh [42] präsentiert. Diese konnten im Fall von total-reellen algebraischen Zahlkörpern $K \neq \mathbb{Q}$ und algebraischen Zahlkörpern K mit mindestens einer reellen und genau einem Paar komplexer Einbettungen zeigen, dass $\mathbb{Z}$ über $\mathcal{O}_K$ eine diophantische Menge ist. Damit ist Hilberts zehntes Problem über $\mathcal{O}_K$ in diesen Fällen unentscheidbar. Für allgemeine Zahlkörper steht noch nicht fest, ob Hilberts Problem entscheidbar ist. Die Vermutung von Denef und Lipshitz [10], dass für alle Zahlkörper K Hilberts zehntes Problem über $\mathcal{O}_K$ unentscheidbar ist, ist noch unbewiesen.

B.2 Summary

Hilbert's tenth problem asks, whether there exists an algorithm that can decide for a given multivariate polynomial p with integral coefficients, if p has integral roots. Even though the problem was already posed in 1900 by Hilbert [18], it took until 1970 til Matijasevič [26] could prove that such an algorithm cannot exist. The problem can be translated directly to other commutative rings R with 1 by letting the coefficients range over $\mathbb{Z}$ or R and consider roots in R. In this thesis we put special interest on the case of R being a ring of algebraic integers. How closely Hilbert's tenth problem is related to other decision problems, will however only become apparent when we consider the problem as a question of decidability of a theory. For instance, we will see that Matijasevič' DPRM-theorem (2.1.11) is very similar to Gödel's central theorem in his proof [15] of the first incompleteness theorem.

To understand Hilbert's problem in this general setting, we introduce the basics of computability theory and model theory in the first part of this thesis. During these introductory sections we will present the halting problem. The undecidability of this fundamental problem will be the key ingredient in every proof of undecidability we will encounter. Furthermore, we will remind the reader of the relevant results of algebraic number theory and geometry of numbers.

In a second step we will formalize Hilbert's tenth problem and will extensively study related problems and their historical developments. In order to eventually answer the problem to the negative for selected rings, we will define Diophantine sets over commutative rings with 1 and prove some of their important structural properties. The main result of this thesis is, that Hilbert's tenth problem is unsolvable over a ring of algebraic integers $\mathcal{O}_K$ if $\mathbb{Z}$ is Diophantine over $\mathcal{O}_K$. This statement remains true whether we allow the polynomials to have coefficients in $\mathbb{Z}$ or $\mathcal{O}_K$.

In the final section of this thesis we will present the results of Denef [8], Pheidas [32], and Shlapentokh [42]. They where able to prove in the case of totally real number fields $K \neq \mathbb{Q}$ and number fields of degree at least 3 over $\mathbb{Q}$ with exactly one pair of non-real embeddings, that $\mathbb{Z}$ is Diophantine over $\mathcal{O}_K$. As a consequence, Hilbert's tenth problem is undecidable over $\mathcal{O}_K$. For general number fields it is not known whether Hilbert's tenth problem is decidable over their ring of algebraic integers. The conjecture by Denef and Lipshitz [10], that Hilbert's tenth problem is undecidable over $\mathcal{O}_K$ for all algebraic number fields K, is still unproven.

List of Figures

Bibliography

[1] Stanley Burris and Hanamantagoud P. Sankappanavar. *A course in universal algebra*. Vol. 78. Graduate Texts in Mathematics. Springer-Verlag, New York-Berlin, 1981, pp. xvi+276. ISBN: 0-387-90578-2.

[2] Alonzo Church. 'A note on the Entscheidungsproblem'. In: *The Journal of Symbolic Logic* 1.1 (1936), pp. 40–41. ISSN: 00224812. URL: http://www.jstor.org/stable/2269326.

[3] Alonzo Church. 'An unsolvable problem of elementary number theory'. In: *Amer. J. Math.* 58.2 (1936), pp. 345–363. ISSN: 0002-9327. DOI: 10.2307/2371045.

[4] S. Barry Cooper. *Computability theory*. Chapman & Hall/CRC, Boca Raton, FL, 2004, pp. x+409. ISBN: 1-58488-237-9.

[5] Martin Davis. 'Hilbert's tenth problem is unsolvable'. In: *The American Mathematical Monthly* 80.3 (Mar. 1973), pp. 233–269. ISSN: 00029890, 19300972. DOI: 10.2307/2318447. URL: http://www.jstor.org/stable/2318447.

[6] Martin Davis. 'Why there is no such discipline as hypercomputation'. In: *Appl. Math. Comput.* 178.1 (2006), pp. 4–7. ISSN: 0096-3003. DOI: 10.1016/j.amc.2005.09.066. URL: https://doi.org/10.1016/j.amc.2005.09.066.

[7] Martin Davis, Yuri V. Matijasevič, and Julia Robinson. 'Hilbert's tenth problem: Diophantine equations: positive aspects of a negative solution'. In: *Mathematical developments arising from Hilbert problems (Proc. Sympos. Pure Math., Vol. XXVIII, Northern Illinois Univ., De Kalb, Ill., 1974)*. Amer. Math. Soc., Providence, R. I., 1976, pp. 323–378.

[8] Jan Denef. 'Diophantine sets over algebraic integer rings. II'. In: *Trans. Amer. Math. Soc.* 257.1 (1980), pp. 227–236. ISSN: 0002-9947. DOI: 10.2307/1998133.

[9] Jan Denef. 'Hilbert's tenth problem for quadratic rings'. In: *Proc. Amer. Math. Soc.* 48.1 (Mar. 1975), pp. 214–220. ISSN: 0002-9939. DOI: 10.2307/2040720.

[10] Jan Denef and Leonard Lipshitz. 'Diophantine sets over some rings of algebraic integers'. In: *J. London Math. Soc. (2)* 18.3 (1978), pp. 385–391. ISSN: 0024-6107. DOI: 10.1112/jlms/s2-18.3.385.

[11] Lou van den Dries. 'Elimination theory for the ring of algebraic integers'. In: *J. Reine Angew. Math.* 388 (1988), pp. 189–205. ISSN: 0075-4102. DOI: 10.1515/crll.1988.388.189. URL: https://doi.org/10.1515/crll.1988.388.189.

[12] Theodor Estermann. 'A proof of Kronecker's theorem by induction'. In: *J. London Math. Soc.* 8.1 (1933), pp. 18–20. DOI: 10.1112/jlms/s1-8.1.18.

[13] Kurt Gödel. *Collected works. Vol. I*. Publications 1929–1936, Edited and with a preface by Solomon Feferman. The Clarendon Press, Oxford University Press, New York, 1986, pp. xvi+474. ISBN: 0-19-503964-5.

[14] Kurt Gödel. *On undecidable propositions of formal mathematical systems*. Lecture notes by Stephen C. Kleene and J. Barkely Rosser, Princeton University. Reprinted in [13]. 1934.

[15] Kurt Gödel. 'Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I'. German. In: *Monatsh. Math. Phys.* 38.1 (1931), pp. 173–198. ISSN: 1812-8076. DOI: 10.1007/BF01700692. URL: https://doi.org/10.1007/BF01700692.

[16] Godfrey Harold Hardy and Edward Maitland Wright. *An introduction to the theory of numbers*. English. Oxford: Clarendon Press, 1975.

[17] David Hilbert. 'Mathematical problems'. In: *Bull. Amer. Math. Soc. (N.S.)* 37.4 (2000). Reprinted from Bull. Amer. Math. Soc. 8 (1902), 437–479, pp. 407–436. ISSN: 0273-0979. DOI: 10.1090/S0273-0979-00-00881-8.

[18] David Hilbert. 'Mathematische Probleme. Vortrag, gehalten auf dem internationalen Mathematiker-Kongreß zu Paris 1900'. German. In: *Nachrichten von der Königl. Gesellschaft der Wissenschaften zu Göttingen.* (1900), pp. 253–279.

[19] Edmund Hlawka, Johannes Schoissengeier, and Rudolf Taschner. *Geometric and analytic number theory*. Universitext. Translated from the 1986 German edition by Charles Thomas. Springer-Verlag, Berlin, 1991, pp. x+238. ISBN: 3-540-52016-3. DOI: 10.1007/978-3-642-75306-0.

[20] Bakhadyr Khoussainov and Arkadii Slinko. 'Computable rings, groups and their isomorphisms'. In: *Nonassociative algebra and its applications (São Paulo, 1998)*. Vol. 211. Lecture Notes in Pure and Appl. Math. Dekker, New York, 2000, pp. 397–416.

[21] Stephen C. Kleene. 'λ-definability and recursiveness'. In: *Duke Math. J.* 2.2 (1936), pp. 340–353. ISSN: 0012-7094. DOI: 10.1215/S0012-7094-36-00227-2. URL: https://doi.org/10.1215/S0012-7094-36-00227-2.

[22] Jochen Koenigsmann. 'Undecidability in number theory'. In: *Model Theory in Algebra, Analysis and Arithmetic: Cetraro, Italy 2012, Editors: H. Dugald Macpherson, Carlo Toffalori*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, pp. 159–195. ISBN: 978-3-642-54936-6. DOI: 10.1007/978-3-642-54936-6_5.

[23] Serge Lang. *Algebra*. third. Vol. 211. Graduate Texts in Mathematics. Springer-Verlag, New York, 2002, pp. xvi+914. ISBN: 0-387-95385-X. DOI: 10.1007/978-1-4613-0041-0. URL: https://doi.org/10.1007/978-1-4613-0041-0.

[24] Anatoli I. Mal'cev. 'Constructive algebras. I'. Russian. In: *Uspehi Mat. Nauk* 16.3 (99) (1961), pp. 3–60. ISSN: 0042-1316.

[25] David Marker. *Model Theory : An Introduction*. Graduate texts in mathematics ; 217. New York, NY: Springer New York, Aug. 21, 2002. 356 pp. ISBN: 9780387987606. URL: https://www.ebook.de/de/product/3665990/david_marker_model_theory_an_introduction.html.

[26] Yuri V. Matijasevič. 'The Diophantineness of enumerable sets'. In: *Doklady Akademii Nauk SSSR* 191 (1970). Russian, pp. 279–282. ISSN: 0002-3264.

[27] James S. Milne. *Algebraic Number Theory (v3.07)*. Online. 2017. URL: www.jmilne.org/math/.

[28] Moritz Müller. *Introduction to theoretical computer science*. lecture notes published online. Apr. 18, 2016. URL: http://www.logic.univie.ac.at/~muellem3/TCS.pdf (visited on 12/30/2017).

[29] Jürgen Neukirch. *Algebraische Zahlentheorie*. German. Berlin, Heidelberg: Springer-Verlag Berlin Heidelberg, 2006. ISBN: 978-3-540-37547-0.

[30] Onorato T. O'Meara. *Introduction to quadratic forms*. repr. of the 1973 ed. Classics in mathematics. Berlin [i.a.]: Springer, 2000. 360 pp. ISBN: 35406-6564-1. URL: http://ubdata.univie.ac.at/AC05622932.

[31] Jennifer Park. 'A universal first-order formula defining the ring of integers in a number field'. In: *Math. Res. Lett.* 20.5 (2013), pp. 961–980. ISSN: 1073-2780. DOI: 10.4310/MRL.2013.v20.n5.a12.

[32] Thanases Pheidas. 'Hilbert's tenth problem for a class of rings of algebraic integers'. In: *Proc. Amer. Math. Soc.* 104.2 (1988), pp. 611–620. ISSN: 0002-9939. DOI: 10.2307/2047021. URL: https://doi.org/10.2307/2047021.

[33] Bjorn Poonen. 'Undecidability in number theory'. In: *Notices of the American Mathematical Society* 55.3 (Mar. 2008), pp. 344–350. ISSN: 0002-9920. URL: http://www.ams.org/notices/200803/tx080300344p.pdf.

[34] Bjorn Poonen. 'Using elliptic curves of rank one towards the undecidability of Hilbert's tenth problem over rings of algebraic integers'. In: *Algorithmic number theory (Sydney, 2002)*. Vol. 2369. Lecture Notes in Comput. Sci. Springer, Berlin, 2002, pp. 33–42. DOI: 10.1007/3-540-45455-1_4.

[35] Emil L. Post. 'Recursively enumerable sets of positive integers and their decision problems'. In: *Bull. Amer. Math. Soc.* 50 (1944), pp. 284–316. ISSN: 0002-9904. DOI: 10.1090/S0002-9904-1944-08111-1. URL: https://doi.org/10.1090/S0002-9904-1944-08111-1.

[36] Julia Robinson. 'Definability and decision problems in arithmetic'. In: *The Journal of Symbolic Logic* 14.2 (June 1949), pp. 98–114. ISSN: 00224812. DOI: 10.2307/2266510.

[37] Julia Robinson. 'The undecidability of algebraic rings and fields'. In: *Proc. Amer. Math. Soc.* 10.6 (June 1959), pp. 950–957. ISSN: 0002-9939. DOI: 10.2307/2033628. URL: https://doi.org/10.2307/2033628.

[38] Raphael M. Robinson. 'Arithmetical definability of field elements'. In: *J. Symbolic Logic* 16.02 (June 1951), pp. 125–126. ISSN: 0022-4812. DOI: 10.2307/2266685.

[39] Barkley Rosser. 'Extensions of some theorems of Gödel and Church'. In: *Journal of Symbolic Logic* 1.3 (1936), pp. 87–91. DOI: 10.2307/2269028.

[40] Robert S. Rumely. 'Arithmetic over the ring of all algebraic integers'. In: *J. Reine Angew. Math.* 368 (1986), pp. 127–133. ISSN: 0075-4102. DOI: 10.1515/crll.1986.368.127. URL: https://doi.org/10.1515/crll.1986.368.127.

[41] Harold N. Shapiro and Alexandra Shlapentokh. 'Diophantine relationships between algebraic number fields'. In: *Comm. Pure Appl. Math.* 42.8 (Dec. 1989), pp. 1113–1122. ISSN: 0010-3640. DOI: 10.1002/cpa.3160420805. URL: https://doi.org/10.1002/cpa.3160420805.

[42] Alexandra Shlapentokh. 'Extension of Hilbert's tenth problem to some algebraic number fields'. In: *Comm. Pure Appl. Math.* 42.7 (1989), pp. 939–962. ISSN: 0010-3640. DOI: 10.1002/cpa.3160420703.

[43] Alexandra Shlapentokh. 'Hilbert's tenth problem over number fields, a survey'. In: *Hilbert's tenth problem: relations with arithmetic and algebraic geometry (Ghent, 1999)*. Vol. 270. Contemp. Math. Amer. Math. Soc., Providence, RI, 2000, pp. 107–137. URL: https://doi.org/10.1090/conm/270/04370.

[44] Alexandra Shlapentokh. *Hilbert's tenth problem; diophantine classes and extensions to global fields*. 1. publ. New mathematical monographs ; 7. Cambridge: Cambridge Univ. Press, 2007. 320 pp. ISBN: 0-521-83360-4. URL: http://www.ebook.de/de/product/6433593/alexandra_shlapentokh_hilbert_s_tenth_problem_diophantine_classes_and_extensions_to_global_fields.html.

[45] Richard A. Shore. *Computable structures: presentations matter*. Online. URL: http://math.cornell.edu/~shore/papers/pdf/proc4t.pdf (visited on 04/02/2018).

[46] Viggo Stoltenberg-Hansen and John V. Tucker. 'Chapter 12 - computable rings and fields'. In: *Handbook of Computability Theory*. Ed. by Edward R. Griffor. Vol. 140. Studies in Logic and the Foundations of Mathematics. Elsevier, 1999, pp. 363–447. DOI: 10.1016/S0049-237X(99)80028-7. URL: http://www.sciencedirect.com/science/article/pii/S0049237X99800287.

[47] Alfred Tarski. 'Sur les ensembles définissables de nombres réels'. French. In: *Fundamenta Mathematicae* 17.1 (1931), pp. 210–239. URL: http://eudml.org/doc/212515.

[48] Alan M. Turing. 'On computable numbers, with an application to the Entscheidungsproblem'. In: *Proc. London Math. Soc. (2)* 42.3 (1936), pp. 230–265. ISSN: 0024-6115. DOI: 10.1112/plms/s2-42.1.230. URL: https://doi.org/10.1112/plms/s2-42.1.230.